



Безопасность платформы Apple

Май 2022 г.



Содержание

Безопасность платформы Apple	5
Обзор безопасности платформы Apple	5
Аппаратные функции безопасности и биометрические системы	8
Обзор аппаратных функций безопасности	8
Безопасность систем на кристалле Apple	10
Secure Enclave	11
Face ID и Touch ID	21
Аппаратное отключение микрофона	31
Экспресс-карты с резервным питанием	32
Безопасность системы	33
Обзор безопасности системы	33
Безопасная загрузка	34
Безопасность подписанного системного тома в iOS, iPadOS и macOS	63
Безопасное обновление программного обеспечения	65
Целостность операционной системы	67
Дополнительные функции безопасности системы в macOS	70
Безопасность системы watchOS	83
Генератор случайных чисел	88
Устройство Apple Security Research Device	89
Шифрование и защита данных	91
Обзор шифрования и защиты данных	91
Код-пароли и пароли	92
Защита данных	95
FileVault	112
Меры, принимаемые Apple для защиты персональных данных пользователей	116
Цифровая подпись и шифрование	120

Безопасность приложений	122
Обзор безопасности приложений	122
Безопасность приложений в iOS и iPadOS	124
Безопасность приложений в macOS	131
Функции безопасности в приложении «Заметки»	137
Функции безопасности в приложении «Быстрые команды»	139
Безопасность служб	140
Обзор безопасности служб	140
Apple ID и управляемый Apple ID	140
iCloud	143
Управление код-паролями и паролями	155
Apple Pay	167
Использование Apple Wallet	183
iMessage	196
Безопасность Apple Messages for Business	200
Безопасность FaceTime	201
Локатор	202
Непрерывность	206
Безопасность сети	210
Обзор безопасности сети	210
Безопасность TLS	210
Безопасность протокола IPv6	213
Безопасность виртуальной частной сети (VPN)	214
Безопасность Wi-Fi	215
Безопасность Bluetooth	219
Безопасность сверхширокополосной технологии в iOS	221
Единый вход	221
Безопасность AirDrop	223
Безопасность предоставления доступа к паролям Wi-Fi на iPhone и iPad	225
Безопасность брандмауэра в macOS	225
Безопасность комплекта разработчика	226
Обзор безопасности комплекта разработчика	226
Безопасность HomeKit	226
Безопасность SiriKit для iOS, iPadOS и watchOS	233
Безопасность DriverKit для macOS	234
Безопасность ReplayKit в iOS и iPadOS	234
Безопасность ARKit в iOS и iPadOS	236

Безопасное управление устройствами	237
Обзор безопасного управления устройствами	237
Безопасность модели создания пары для iPhone и iPad	238
Управление мобильными устройствами	239
Безопасность Apple Configurator	248
Безопасность Экранного времени	249
Глоссарий	252
История правок документа	258
История правок документа	258
Авторские права	265

Безопасность платформы Apple

Обзор безопасности платформы Apple

Apple продумывает вопросы безопасности на уровне ядра своих платформ. Опираясь на опыт создания самой передовой мобильной операционной системы в мире, компания Apple разработала архитектуры безопасности, которые отвечают уникальным требованиям мобильных устройств, часов, настольных компьютеров и домашних аксессуаров.

Каждое устройство Apple представляет собой систему, состоящую из *программного обеспечения, оборудования и служб*. Слаженная работа всех компонентов обеспечивает высокую безопасность и прозрачность использования, а также конфиденциальность личных данных. Например, в основе критически важных функций безопасности лежат разработанные Apple аппаратные средства. А программные средства защиты призваны обеспечить безопасность операционной системы и приложений сторонних разработчиков. Наконец, службы обеспечивают работу механизма безопасного и своевременного обновления программного обеспечения, вносят вклад в безопасность экосистемы приложений, а также делают работу в интернете и совершение платежей проще и безопаснее. В результате устройства Apple защищают не только само устройство и данные на нем, но и всю экосистему, включая действия пользователя на устройстве, использование сетей и основных интернет-служб.

При разработке своих продуктов мы заботимся не только об их простоте, интуитивности и функциональности, но и о безопасности. Основные функции безопасности, например аппаратное шифрование устройств, невозможно отключить по ошибке. Другие функции, такие как Face ID и Touch ID, облегчают использование устройства благодаря тому, что обеспечивать его защиту становится проще и удобнее. А поскольку многие из этих функций включены по умолчанию, пользователям и ИТ-отделам не нужно выполнять сложную настройку.

В данных материалах представлены сведения о реализации технологий и функций обеспечения безопасности в платформах Apple. Они также помогут организациям объединить технологии и функции безопасности платформы Apple со своими внутренними политиками и процедурами для удовлетворения своих особых потребностей в области безопасности.

Материалы состоят из следующих тематических разделов:

- **Аппаратные функции безопасности и биометрические системы.** Чип и аппаратное обеспечение, которые служат основой системы безопасности устройств Apple, включая чип Apple, Secure Enclave, криптографические модули, Face ID и Touch ID.
- **Безопасность системы.** Интегрированные аппаратные и программные функции, которые обеспечивают безопасную загрузку, обновление и текущую работу операционных систем Apple.
- **Шифрование и защита данных.** Архитектурные решения, которые защищают данные пользователя в случае потери или кражи устройства, а также в случае, если данные пытается использовать или изменить посторонний человек или неразрешенный процесс.
- **Безопасность приложений.** Программное обеспечение и службы, которые защищают экосистему приложений и обеспечивают возможность безопасной работы приложений без нарушения целостности платформы.
- **Безопасность служб.** Службы Apple для идентификации пользователей, управления паролями, оплаты покупок, связи и поиска пропавших устройств.
- **Безопасность сети.** Стандартные отраслевые сетевые протоколы, которые обеспечивают надежную аутентификацию и шифрование данных во время передачи.
- **Безопасность комплекта разработчика.** «Комплекты» программных сред для безопасного и конфиденциального управления домом и медданными, а также для предоставления доступа к функциям устройств и служб Apple приложениям сторонних разработчиков.
- **Безопасное управление устройствами.** Средства, которые позволяют управлять устройствами Apple, помогают предотвратить несанкционированное использование устройств и выполнить удаленное стирание в случае потери или кражи устройства.

Безопасность платформы Apple: введение

Компания Apple делает все возможное для защиты клиентов, предлагая передовые технологии обеспечения конфиденциальности и безопасности для защиты персональной информации, а также комплексные методы для защиты корпоративных данных в корпоративной среде. Компания Apple внедрила программу Apple Security Bounty для поощрения исследователей, которые занимаются поиском уязвимостей ее систем. Подробнее о программе и категориях вознаграждения см. на <https://developer.apple.com/security-bounty/>.

У нас есть специальная команда по безопасности, которая отвечает за поддержку всех продуктов Apple. Эта команда проводит аудит безопасности и тестирование продуктов, как находящихся в стадии разработки, так и выпущенных. Команда Apple предоставляет необходимые инструменты, проводит обучение и активно отслеживает новые угрозы и сообщения о новых проблемах безопасности. Компания Apple является членом [форума FIRST](#), который объединяет группы по безопасности и реагированию на инциденты.

Apple продолжает расширять границы возможного в области безопасности и конфиденциальности. Apple использует систему на кристалле собственной разработки во всей линейке продуктов — от часов Apple Watch до iPhone, iPad, чипа безопасности T2 и чипа Apple в Mac. Эта система обеспечивает не только высокую вычислительную мощность, но и передовые функции безопасности. Например, чип Apple лежит в основе безопасной загрузки, Face ID, Touch ID и технологии защиты данных. Кроме того, функции безопасности устройств, обеспечиваемые чипом Apple, включая защиту целостности ядра, коды аутентификации указателя и быстрые ограничения разрешений, помогают предупредить основные типы кибератак. Следовательно, если злоумышленнику все же удастся запустить код, все упомянутые ранее функции значительно снизят ущерб от атаки.

Чтобы максимально эффективно использовать обширные функции безопасности, встроенные в наши платформы, компаниям рекомендуется проанализировать свои политики в области ИТ и безопасности и убедиться, что они задействуют все возможности многоуровневой системы безопасности, предлагаемые этими платформами.

Информацию о том, как сообщить о проблемах в Apple и подписаться на уведомления о безопасности, Вы найдете на странице [Обращение в Apple по поводу проблем с безопасностью или конфиденциальностью](#).

По убеждению Apple, конфиденциальность — одно из основных прав человека, поэтому Apple предлагает множество настроек и инструментов, с помощью которых пользователи могут решить, как и когда приложения могут использовать информацию, а также какая информация может быть передана. Дополнительные сведения о подходе компании Apple к конфиденциальности, о настройках конфиденциальности на устройствах Apple, а также о политике конфиденциальности Apple можно найти по адресу <https://www.apple.com/ru/privacy>.

Примечание. Если не указано иное, этот документ относится к следующим версиям операционных систем: iOS 15.4, iPadOS 15.4, macOS 12.3, tvOS 15.4 и watchOS 8.5.

Аппаратные функции безопасности и биометрические системы

Обзор аппаратных функций безопасности

Для безопасной работы программного обеспечения требуется оборудование со встроенными функциями безопасности. Вот почему на устройствах Apple — с iOS, iPadOS, macOS, tvOS и watchOS — функции безопасности встроены в процессор. К этим функциям относится центральный процессор, обеспечивающий работу функций безопасности системы, а также дополнительный выделенный чип, который отвечает только за функции, связанные с безопасностью. Аппаратные средства безопасности следуют принципу поддержки ограниченного набора функций, которые определяются по отдельности, чтобы минимизировать атакуемую область. Такие компоненты включают загрузочное ПЗУ, которое задает аппаратный корень доверия для безопасной загрузки, выделенные модули AES для эффективного и безопасного шифрования и дешифрования, а также Secure Enclave. *Secure Enclave* — это система на кристалле (SoC), которой оснащены все устройства iPhone, iPad, Apple Watch, Apple TV и HomePod последних поколений, а также все компьютеры Mac с чипом Apple и компьютеры Mac с чипом безопасности Apple T2. Secure Enclave построен по тому же принципу, что и вся система на кристалле: он содержит собственное дискретное загрузочное ПЗУ и собственный дискретный модуль AES. Secure Enclave также закладывает основу для безопасного создания и хранения ключей, необходимых для шифрования хранящихся на устройстве данных, и защищает и оценивает биометрические данные для Face ID и Touch ID.

Шифрование хранилища должно выполняться быстро и эффективно. При этом не должны раскрываться те данные (или *данные ключей*), которые используются для построения отношений в криптографической системе с ключами. Аппаратный модуль AES решает эту задачу, выполняя быстрое шифрование и дешифрование *по мере записи или чтения файлов*. Необходимые данные ключей передаются по специальному каналу из Secure Enclave в модуль AES, не раскрывая эту информацию процессору приложений (или центральному процессору) или всей операционной системе. Это помогает функции защиты данных и технологии FileVault компании Apple защитить файлы пользователей, не раскрывая долговременные ключи шифрования.

Компания Apple разработала безопасную загрузку, чтобы защитить программное обеспечение самых низких уровней от взлома и чтобы при запуске загружалось только доверенное программное обеспечение операционной системы, разработанное Apple. В основе безопасной загрузки лежит постоянный код загрузочного ПЗУ, который закладывается в процессе изготовления систем на кристалле Apple и называется *аппаратным корнем доверия*. На компьютерах Mac с чипом T2 цепочка доверия безопасной загрузки macOS начинается с чипа T2. (Чип T2 и Secure Enclave также выполняют собственную безопасную загрузку, используя собственное загрузочное ПЗУ, что представляет собой точный аналог безопасной загрузки чипа серии A и семейства чипов M1.)

Secure Enclave также обрабатывает данные распознавания лиц и отпечатков пальцев, полученные от сенсоров Face ID и Touch ID на устройствах Apple. Таким образом обеспечивается безопасная аутентификация с сохранением конфиденциальности биометрических данных. Пользователи также могут использовать более длинные и сложные пароли и код-пароли для повышения безопасности, при этом во многих ситуациях продолжая использовать быструю аутентификацию для доступа к функциям и совершения покупок.

Безопасность систем на кристалле Apple

Чип, разработанный Apple, создает общую архитектуру для всех продуктов Apple, и теперь он заложен в основу компьютеров Mac, а также iPhone, iPad, Apple TV и Apple Watch. Уже более десяти лет команда разработчиков чипов Apple мирового класса занимается созданием и совершенствованием систем на кристалле Apple. Результатом этой работы стала масштабируемая архитектура для любых устройств, которая занимает ведущие в отрасли позиции в области обеспечения безопасности. Эта общая основа для функций системы безопасности стала возможной благодаря тому, что компания стала производить собственные чипы для своего программного обеспечения.

Чип Apple разработан и изготовлен специально для реализации следующих возможностей системы безопасности:

Функция	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	Семейство M1
Защита целостности ядра	✓	✓	✓	✓	✓	✓
Быстрые ограничения разрешений		✓	✓	✓	✓	✓
Защита целостности системного сопроцессора			✓	✓	✓	✓
Коды аутентификации указателя			✓	✓	✓	✓
Уровень защиты страниц		✓	✓	✓	✓	См. примечание ниже.

Примечание. Уровень защиты страниц (PPL) требует, чтобы платформа исполняла только подписанный и надежный код. Эта модель безопасности не применяется в macOS.

Чип Apple также изготовлен специально для реализации следующих возможностей по защите данных.

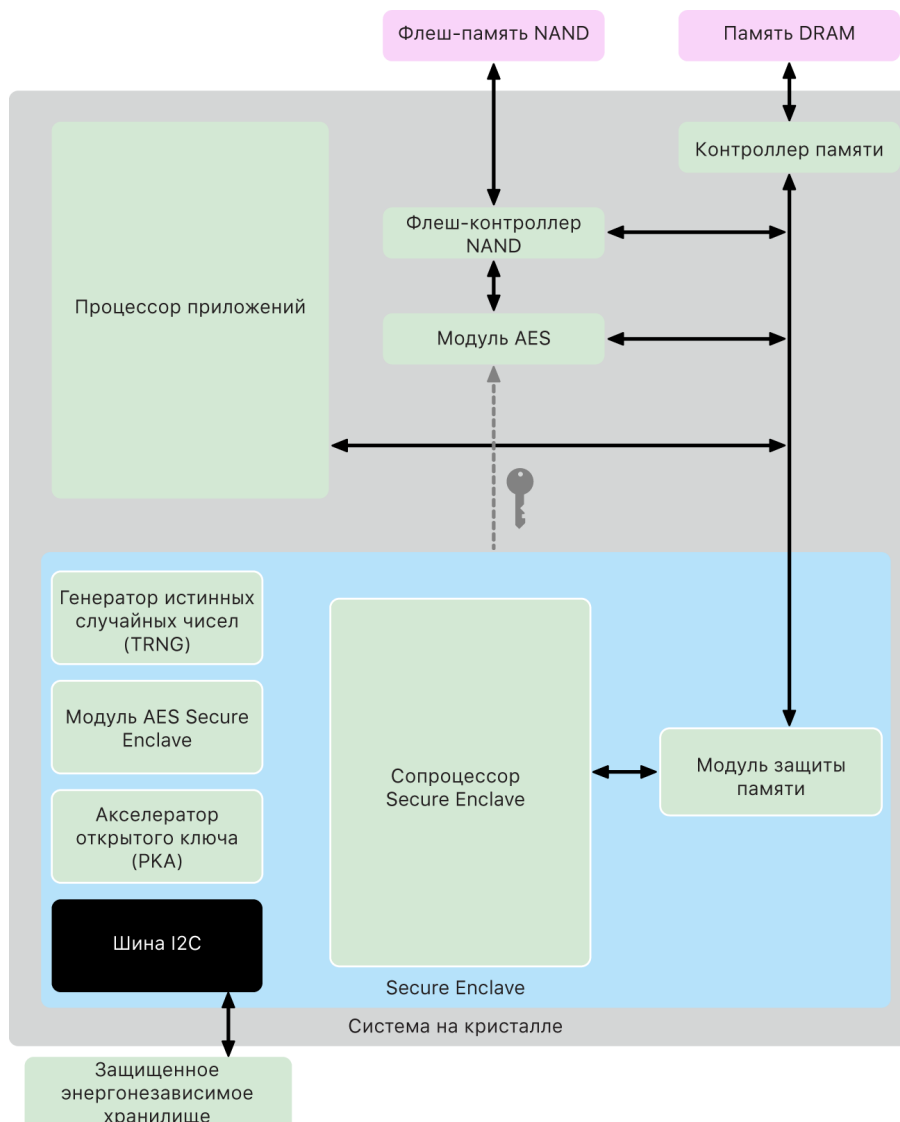
Функция	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, семейство M1
Технология защиты запечатыванием ключей (SKP)	✓	✓	✓	✓	✓
recoveryOS — данные всех классов защиты защищены	✓	✓	✓	✓	✓
Режимы обновления прошивки устройства, диагностики и обновления — защищены данные класса A, B и C			✓	✓	✓

Secure Enclave

Secure Enclave представляет собой выделенную защищенную подсистему новейших версий iPhone, iPad, iPod touch, Mac, Apple TV, Apple Watch и HomePod.

Обзор

Secure Enclave — это выделенная защищенная подсистема, встроенная в системы на кристалле Apple. Подсистема Secure Enclave изолирована от основного процессора для обеспечения дополнительного уровня защиты и предназначена для защиты конфиденциальных данных пользователя даже в случае взлома ядра процессора приложений. Эта подсистема построена по тому же принципу, что и вся система на кристалле: загрузочное ПЗУ задает аппаратный корень доверия, модуль AES отвечает за эффективные и безопасные криптографические операции, а память защищена. Несмотря на то, что Secure Enclave не имеет собственного хранилища, Secure Enclave использует механизм безопасного хранения информации в подключенном хранилище отдельно от флеш-памяти NAND, используемой процессором приложений и операционной системой.



Secure Enclave представляет собой аппаратный компонент большинства версий iPhone, iPad, Mac, Apple TV, Apple Watch и HomePod, а именно:

- iPhone 5s или новее;
- iPad Air или новее;
- компьютеры MacBook Pro с Touch Bar (2016 г. и 2017 г.) и чипом Apple T1;
- компьютеры Mac с процессором Intel и чипом безопасности Apple T2;
- Компьютеры Mac с чипом Apple;
- Apple TV HD или новее;
- Apple Watch Series 1 или новее;
- HomePod и HomePod mini.

Сопроцессор Secure Enclave

Сопроцессор Secure Enclave обеспечивает основную вычислительную мощность для Secure Enclave. В целях надежной изоляции сопроцессор Secure Enclave используется исключительно системой Secure Enclave. Это позволяет предотвратить атаки со сторонними каналами с применением вредоносного программного обеспечения, которое использует то же ядро выполнения, что и атакуемое целевое программное обеспечение.

Сопроцессор Secure Enclave использует версию микроядра L4, доработанную компанией Apple. Оно позволяет ему эффективно работать на более низкой тактовой частоте, что позволяет защитить его от атак, направленных на изменение тактовой частоты и питания процессора. Начиная с A11 и S4 сопроцессор Secure Enclave включает модуль защиты памяти и зашифрованную память с функциями антиповтора, безопасную загрузку, отдельный генератор случайных чисел и собственный модуль AES.

Модуль защиты памяти

Secure Enclave работает в выделенной области памяти DRAM устройства. Защищенная память Secure Enclave изолирована от процессора приложений с помощью нескольких уровней защиты.

При запуске устройства загрузочное ПЗУ Secure Enclave генерирует случайный кратковременный ключ защиты памяти для модуля защиты памяти. Каждый раз, когда Secure Enclave выполняет запись в свою выделенную область памяти, модуль защиты памяти шифрует соответствующий блок памяти с помощью шифрования AES в режиме Mac XEX (xor-encrypt-xor), а также вычисляет тег аутентификации кода аутентификации сообщения на основе шифра (CMAC) для памяти. Модуль защиты памяти хранит тег аутентификации вместе с зашифрованной памятью. Когда Secure Enclave выполняет чтение из памяти, модуль защиты памяти проверяет тег аутентификации. В случае совпадения тега модуль защиты памяти расшифровывает блок памяти. Если тег не совпадает, модуль защиты памяти сообщает сопроцессору Secure Enclave об ошибке. После ошибки аутентификации памяти система Secure Enclave останавливает прием запросов до перезагрузки системы.

Начиная с систем на кристалле с процессорами Apple A11 и S4, модуль защиты памяти обеспечивает защиту памяти Secure Enclave с помощью механизма антиповтора. Для того чтобы препятствовать повторной отправке критически важных данных безопасности, модуль защиты памяти хранит уникальное одноразовое число, называемое значением *nonce*, для блока памяти вместе с тегом аутентификации. Значение *nonce* используется в качестве дополнительной поправки для тега аутентификации CMAC. Значения *nonce* для всех блоков памяти защищены с помощью дерева целостности, корень которого находится в выделенной памяти SRAM в Secure Enclave. При выполнении операций записи модуль защиты памяти *обновляет* значение *nonce* и каждый уровень дерева целостности до уровня памяти SRAM. При выполнении операций чтения модуль защиты памяти *проверяет* значение *nonce* и каждый уровень дерева целостности до уровня памяти SRAM. Несоответствия значений *nonce* обрабатываются так же, как несоответствия тега аутентификации.

В системах на кристалле Apple A14, A15, семейства M1 или новее модуль защиты памяти поддерживает два динамических ключа защиты памяти. Первый используется для данных, к которым имеет доступ только Secure Enclave, а второй используется для данных, к которым также имеет доступ защищенный нейронный модуль.

Модуль защиты памяти является встроенным и прозрачным для Secure Enclave. Secure Enclave выполняет операции чтения из памяти и записи в память так, как если бы это была обычная незашифрованная память DRAM, тогда как внешнему наблюдателю вне Secure Enclave доступна только зашифрованная и аутентифицированная версия памяти. За счет этого обеспечивается надежная защита памяти без ущерба производительности или сложности программного обеспечения.

Загрузочное ПЗУ Secure Enclave

В состав Secure Enclave входит специальное загрузочное ПЗУ Secure Enclave. Аналогично загрузочному ПЗУ процессора приложений, загрузочное ПЗУ Secure Enclave представляет собой постоянный код, который задает аппаратный корень доверия для Secure Enclave.

При запуске системы загрузчик iBoot назначает Secure Enclave выделенную область памяти. Перед использованием памяти загрузочное ПЗУ Secure Enclave инициализирует модуль защиты памяти для обеспечения криптографической защиты защищенной области памяти Secure Enclave.

Затем процессор приложений отправляет в загрузочное ПЗУ Secure Enclave образ *sepOS*. После копирования образа *sepOS* в защищенную память Secure Enclave загрузочное ПЗУ Secure Enclave проверяет криптографический хэш и подпись образа для подтверждения того, что указанное программное обеспечение *sepOS* разрешено запускать на этом устройстве. Если образ *sepOS* имеет соответствующую подпись для запуска на устройстве, загрузочное ПЗУ Secure Enclave передает управление программному обеспечению *sepOS*. Загрузочное ПЗУ Secure Enclave разработано таким образом, чтобы предотвратить дальнейшее использование Secure Enclave до следующего сброса чипа, если подпись недействительна.

В системах на кристалле Apple A10 и новее загрузочное ПЗУ Secure Enclave блокирует хэш *sepOS* в предназначенном для этого реестре. Акселератор открытого ключа использует этот хэш для ключей привязки к операционной системе.

Монитор загрузки Secure Enclave

В системах на кристалле Apple A13 и новее в Secure Enclave имеется Монитор загрузки, предназначенный для сохранения высокого уровня целостности хэша загруженного программного обеспечения `sepOS`.

При запуске системы конфигурация защиты целостности системного сопроцессора (SCIP) Secure Enclave помогает предотвратить запуск сопроцессором Secure Enclave любого кода, который отличается от имеющегося в загрузочном ПЗУ Secure Enclave. Монитор загрузки помогает предотвратить прямое изменение сопроцессором Secure Enclave конфигурации SCIP. Чтобы сделать загруженное программное обеспечение `sepOS` исполняемым, загрузочное ПЗУ Secure Enclave отправляет Монитору загрузки запрос с указанием адреса и размера загруженного программного обеспечения `sepOS`. После получения запроса Монитор загрузки сбрасывает сопроцессор Secure Enclave, хэширует загруженное программное обеспечение `sepOS`, обновляет настройки SCIP, чтобы разрешить выполнение загруженного программного обеспечения `sepOS`, а затем запускает выполнение в новом загруженном коде. По мере загрузки системы этот же процесс применяется к новому исполняемому коду. Каждый раз Монитор загрузки обновляет выполняющийся хэш процесса загрузки. Монитор загрузки также включает в выполняющийся хэш критически важные параметры безопасности.

По завершении загрузки Монитор загрузки финализирует выполняющийся хэш и отправляет его в акселератор открытого ключа, который будет использовать этот хэш для ключей привязки к операционной системе. Этот процесс разработан для того, чтобы привязку ключей к операционной системе не удалось обойти даже в случае наличия уязвимости в загрузочном ПЗУ Secure Enclave.

Генератор истинных случайных чисел

Генератор истинных случайных чисел (TRNG) используется для генерирования защищенных случайных данных. Secure Enclave использует TRNG каждый раз, когда требуется сгенерировать случайный криптографический ключ, начальный бит случайного ключа или другой энтропийно закодированный элемент. В основе TRNG лежат несколько кольцевых генераторов, сигнал которых обрабатывается генератором CTR_DRBG (алгоритм на основе блочных шифров в режиме счетчика).

Корневые криптографические ключи

Secure Enclave содержит корневой криптографический ключ уникального идентификатора (UID). UID является уникальным для каждого отдельного устройства и не связан с каким-либо другим идентификатором на устройстве.

Случайно сгенерированные UID вшиваются в систему на кристалле во время производства. Начиная с систем на кристалле A9, UID генерируется с помощью TRNG Secure Enclave во время производства и записывается на плавких перемычках с помощью программного процесса, исполняемого полностью в Secure Enclave. Этот процесс делает UID невидимым за пределами устройства во время производства, поэтому доступ к нему и хранению в нем не будут иметь ни Apple, ни ее поставщики.

serOS использует UID для защиты секретов устройства. UID обеспечивает возможность криптографической привязки данных к конкретному устройству. Например, UID входит в иерархию ключей, используемых для защиты файловой системы, поэтому при физическом перемещении памяти SSD из одного устройства в другое файлы становятся недоступны. В число других защищенных секретных данных конкретных устройств входят данные Face ID или Touch ID. На Mac этот уровень шифрования используется только для полностью внутреннего хранилища, связанного с модулем AES. Например, внешние устройства хранения, подключенные через USB, и хранилища на основе PCIe для Mac Pro 2019 г. не зашифровываются этим способом.

В Secure Enclave также имеется идентификатор группы устройств (GID), который является общим для всех устройств, где используется определенная система на кристалле (например, на всех устройствах с процессором Apple A15 используется одинаковый GID).

Идентификаторы UID и GID недоступны через Joint Test Action Group (JTAG) и другие интерфейсы отладки.

Модуль AES Secure Enclave

Модуль AES Secure Enclave представляет собой аппаратный блок, который выполняет симметричное шифрование на основе шифра AES. Модуль AES исключает утечку информации посредством анализа тактовой частоты и статического анализа питания (SPA). В системах на кристалле A9 и новее модуль AES также содержит компоненты противодействия динамическому анализу питания (DPA).

Модуль AES поддерживает аппаратные и программные ключи. Аппаратные ключи получают из идентификаторов UID или GID Secure Enclave. Эти ключи остаются в модуле AES и не видны даже программному обеспечению serOS. Несмотря на то, что программное обеспечение может запросить операции шифрования и дешифрования с использованием аппаратных ключей, оно не может извлечь сами ключи.

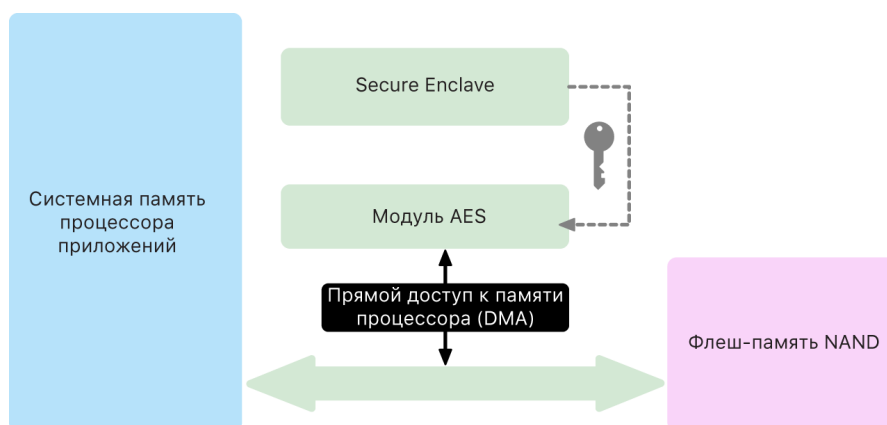
В системах на кристалле Apple A10 и новее модуль AES содержит блокируемые начальные биты, которые изменяют ключи, полученные из идентификаторов UID или GID. Таким образом обеспечивается условный доступ к данным в зависимости от режима работы устройства. Например, блокируемые начальные биты используются для того, чтобы закрыть доступ к данным, защищенным паролем, при загрузке в режиме обновления прошивки устройства (DFU). Подробнее см. в разделе [Код-пароли и пароли](#).

Модуль AES

В каждом устройстве Apple с сопроцессором Secure Enclave имеется специализированный криптографический модуль AES256 («модуль AES»), который встроен непосредственно в канал прямого доступа к памяти (DMA) между энергонезависимой флеш-памятью NAND и основной системной памятью для повышения эффективности шифрования файлов. На устройствах с процессором A9 или более новым процессором серии A подсистема флеш-памяти находится на изолированной шине, которая получает доступ к памяти с пользовательскими данными только через криптографический модуль DMA.

Во время загрузки `sepOS` с помощью TRNG генерирует случайный кратковременный ключ для упаковки ключа. Secure Enclave передает этот ключ в модуль AES по выделенным проводным каналам. Эта мера направлена на то, чтобы предотвратить доступ к нему любого программного обеспечения вне Secure Enclave. Затем `sepOS` может использовать этот динамический ключ для упаковки, чтобы упаковать ключи файлов для использования драйвером файловой системы процессора приложений. Когда драйвер файловой системы выполняет чтение файла или запись в него, он отправляет упакованный ключ в модуль AES, который, в свою очередь, распаковывает его. Модуль AES никогда не раскрывает дешифрованный ключ программному обеспечению.

Примечание. Модуль AES отделен от Secure Enclave и модуля AES подсистемы Secure Enclave, но его работа тесно связана с Secure Enclave, как показано далее.



Акселератор открытого ключа

Акселератор открытого ключа (PKA) — это аппаратный блок, который выполняет асимметричные криптографические операции. PKA поддерживает алгоритмы подписи и шифрования RSA и ECC (криптография на основе эллиптических кривых). PKA противостоит утечкам информации из-за атак на основе анализа тактовой частоты и атак по сторонним каналам, таких как SPA и DPA.

PKA поддерживает программные и аппаратные ключи. Аппаратные ключи получаются из идентификаторов UID или GID Secure Enclave. Эти ключи остаются в PKA и не видны даже программному обеспечению `sepOS`.

Начиная с систем на кристалле с процессорами Apple A13, математическая правильность реализации шифрования PKA является доказанной благодаря применению методов формальной проверки.

В системах на кристалле Apple A10 и новее PKA поддерживает ключи привязки к операционной системе. Эта технология называется [защитой запечатыванием ключей \(SKP\)](#). Такие ключи генерируются на основе сочетания UID устройства и хэша программного обеспечения `sepOS`, которое выполняется на устройстве. В системах на кристалле Apple A13 и новее этот хэш предоставляется загрузочным ПЗУ Secure Enclave или Монитором загрузки Secure Enclave. Ключи привязки к операционной системе также используются для проверки версии `sepOS` при отправке запросов к определенным службам Apple и для повышения уровня защиты данных, защищенных код-паролем, помогая предотвратить доступ к данным ключей, если в систему внесены критически важные изменения без авторизации пользователя.

Защищенное энергонезависимое хранилище

Secure Enclave оснащается выделенным безопасным энергонезависимым устройством хранения. Для подключения защищенного энергонезависимого хранилища к Secure Enclave используется выделенная шина I2C, поэтому доступ к хранилищу имеет только Secure Enclave. Корни всех ключей шифрования данных пользователей энтропийно закодированы и хранятся в энергонезависимом хранилище Secure Enclave.

На устройствах с системами на кристалле A12, S4 и новее для хранения энтропийно закодированных элементов сопроцессор Secure Enclave объединяется в пару с компонентом защищенного хранилища. Сам компонент защищенного хранилища содержит неизменяемый код ПЗУ, аппаратный генератор случайных чисел, уникальные криптографические ключи устройств, криптографические модули и функцию обнаружения физического вмешательства. Для взаимодействия друг с другом Secure Enclave и компонент защищенного хранилища используют зашифрованный и аутентифицированный протокол, предоставляющий эксклюзивный доступ к энтропийно закодированным элементам.

Устройства, которые выпущены впервые осенью 2020 года или позже, оснащены компонентом защищенного хранилища второго поколения. В компонент защищенного хранилища второго поколения добавлены защищенные хранилища счетчиков. В каждом защищенном хранилище счетчиков хранятся 128-битное случайное значение («соль»), 128-битное проверочное значение код-пароля, 8-битный счетчик и 8-битное значение максимального количества попыток. Для доступа к защищенным хранилищам счетчиков используется зашифрованный и аутентифицированный протокол.

Защищенные хранилища счетчиков содержат энтропийно закодированное значение, необходимое для разблокирования пользовательских данных, защищенных код-паролем. Для доступа к этим пользовательским данным требуется объединенный в пару сопроцессор Secure Enclave, который получает правильное энтропийно закодированное значение на основе код-пароля пользователя и UID Secure Enclave. Код-пароль пользователя нельзя узнать путем многократных попыток разблокирования, совершаемых из любого источника, отличного от сопроцессора Secure Enclave, который объединен в пару. Если превышено количество попыток ввода код-пароля (например, 10 попыток на iPhone), компонент защищенного хранилища безвозвратно стирает данные, защищенные код-паролем.

Для создания защищенного хранилища счетчика сопроцессор Secure Enclave отправляет компоненту защищенного хранилища энтропийно закодированное значение код-пароля и значение максимального количества попыток. Компонент защищенного хранилища генерирует случайное значение («соль»), используя собственный генератор случайных чисел. Затем он получает проверочное значение код-пароля и энтропийно закодированное значение защищенного хранилища из предоставленного энтропийно закодированного значения код-пароля, уникального криптографического ключа компонента защищенного хранилища и случайного значения («соль»). Компонент защищенного хранилища инициализирует защищенное хранилище счетчика с количеством «0», предоставленным значением максимального количества попыток, полученным проверочным значением код-пароля и случайным значением («соль»). Затем компонент защищенного хранилища возвращает в Secure Enclave сгенерированное энтропийно закодированное значение защищенного хранилища.

Для того чтобы позднее извлечь энтропийно закодированное значение защищенного хранилища из защищенного хранилища счетчика, Secure Enclave отправляет компоненту защищенного хранилища энтропийно закодированное значение код-пароля. Сначала компонент защищенного хранилища увеличивает значение счетчика для защищенного хранилища. Если увеличенное значение счетчика превышает значение максимального количества попыток, компонент защищенного хранилища полностью стирает защищенное хранилище счетчика. Если максимальное количество попыток не достигнуто, компонент защищенного хранилища пытается получить проверочное значение код-пароля и энтропийно закодированное значение защищенного хранилища с помощью того же алгоритма, который использовался для создания защищенного хранилища счетчика. Если полученное проверочное значение код-пароля совпадает с сохраненным проверочным значением код-пароля, компонент защищенного хранилища возвращает энтропийно закодированное значение защищенного хранилища в Secure Enclave и сбрасывает счетчик до 0.

Корни ключей, которые используются для доступа к защищенным паролем данным, энтропийно закодированы и хранятся в защищенных хранилищах счетчиков. Подробнее см. в разделе [Обзор защиты данных](#).

Защищенное энергонезависимое хранилище используется для всех служб антиповтора в Secure Enclave. Службы антиповтора в Secure Enclave используются для аннуляции данных в случае событий, которые отмечают границы антиповтора, включая следующие ситуации (но не ограничиваясь ими):

- изменение код-пароля;
- включение или выключение Face ID или Touch ID;
- добавление или удаление лица для Face ID или отпечатка пальца для Touch ID;
- сброс Face ID или Touch ID;
- добавление или удаление карты Apple Pay;
- стирание всего контента и настроек.

В архитектурах без компонента защищенного хранилища для предоставления безопасного хранилища сопроцессору Secure Enclave используется EEPROM (электрически стираемая программируемая постоянная память). Аналогично компонентам защищенного хранилища память EEPROM подключается к Secure Enclave и доступна только из него, однако она не содержит выделенных аппаратных функций безопасности, не гарантирует эксклюзивный доступ к энтропийно закодированным элементам (за исключением характеристик физического подключения) и не предоставляет функций защищенного хранилища счетчика.

Защищенный нейронный модуль

На устройствах с Face ID защищенный нейронный модуль преобразует двумерные изображения и карты глубины в математические представления лица пользователя.

В системах на кристалле с процессорами Apple с A11 по A13 защищенный нейронный модуль встроен в Secure Enclave. Для обеспечения высокой производительности защищенный нейронный модуль использует прямой доступ к памяти (DMA). Модуль управления памятью ввода-вывода (IOMMU) в элементе управления ядром serOS ограничивает возможность прямого доступа только разрешенными областями памяти.

Начиная с чипов A14 и семейства M1 защищенная система Neural Engine реализуется как безопасный режим в системе Neural Engine процессора приложений. Выделенный аппаратный контроллер безопасности переключается между задачами процессора приложений и Secure Enclave, сбрасывая состояние нейронного модуля при каждой транзакции для защиты данных Face ID. Выделенный модуль выполняет шифрование памяти, аутентификацию и управление доступом. В то же время он использует отдельный криптографический ключ и диапазон памяти для ограничения возможностей доступа защищенного нейронного модуля только разрешенными областями памяти.

Мониторы питания и тактовой частоты

Все электронные компоненты разработаны для работы в ограниченном диапазоне напряжения и частоты электрического тока. Выход за пределы рабочего диапазона может привести к сбоям в работе электронных компонентов и последующему обходу средств обеспечения безопасности. Secure Enclave оснащается микросхемами для контроля напряжения. Эти микросхемы помогают сохранять характеристики электропитания в пределах рабочего диапазона. Рабочий диапазон таких микросхем намного больше, чем у остальных компонентов Secure Enclave. При обнаружении запрещенного режима работы тактовые генераторы Secure Enclave автоматически останавливаются и не перезапускаются до следующего сброса системы на кристалле.

Обзор функций Secure Enclave

Примечание. Устройства с чипами A12, A13, S4 и S5, впервые выпущенные осенью 2020 года, оснащаются компонентом защищенного хранилища второго поколения, тогда как более ранние устройства на основе этих систем на кристалле оснащены компонентом защищенного хранилища первого поколения.

Система на кристалле	Модуль защиты памяти	Защищенное хранилище	Модуль AES	PKA
A8	Шифрование и аутентификация	EEPROM	Да	Нет
A9	Шифрование и аутентификация	EEPROM	Защита DPA	Да
A10	Шифрование и аутентификация	EEPROM	Защита DPA и блокируемые начальные биты	Ключи привязки к операционной системе

Система на кристалле	Модуль защиты памяти	Защищенное хранилище	Модуль AES	PKA
A11	Шифрование, аутентификация и механизм антиповтора	EEPROM	Защита DPA и блокируемые начальные биты	Ключи привязки к операционной системе
A12 (устройства Apple, выпущенные до осени 2020 г.)	Шифрование, аутентификация и механизм антиповтора	Компонент защищенного хранилища 1-го поколения	Защита DPA и блокируемые начальные биты	Ключи привязки к операционной системе
A12 (устройства Apple, выпущенные после осени 2020 г.)	Шифрование, аутентификация и механизм антиповтора	Компонент защищенного хранилища 2-го поколения	Защита DPA и блокируемые начальные биты	Ключи привязки к операционной системе
A13 (устройства Apple, выпущенные до осени 2020 г.)	Шифрование, аутентификация и механизм антиповтора	Компонент защищенного хранилища 1-го поколения	Защита DPA и блокируемые начальные биты	Ключи привязки к операционной системе и монитор загрузки
A13 (устройства Apple, выпущенные после осени 2020 г.)	Шифрование, аутентификация и механизм антиповтора	Компонент защищенного хранилища 2-го поколения	Защита DPA и блокируемые начальные биты	Ключи привязки к операционной системе и монитор загрузки
A14, A15	Шифрование, аутентификация и механизм антиповтора	Компонент защищенного хранилища 2-го поколения	Защита DPA и блокируемые начальные биты	Ключи привязки к операционной системе и монитор загрузки
S3	Шифрование и аутентификация	EEPROM	Защита DPA и блокируемые начальные биты	Да
S4	Шифрование, аутентификация и механизм антиповтора	Компонент защищенного хранилища 1-го поколения	Защита DPA и блокируемые начальные биты	Ключи привязки к операционной системе
S5 (устройства Apple, выпущенные до осени 2020 г.)	Шифрование, аутентификация и механизм антиповтора	Компонент защищенного хранилища 1-го поколения	Защита DPA и блокируемые начальные биты	Ключи привязки к операционной системе
S5 (устройства Apple, выпущенные после осени 2020 г.)	Шифрование, аутентификация и механизм антиповтора	Компонент защищенного хранилища 2-го поколения	Защита DPA и блокируемые начальные биты	Ключи привязки к операционной системе
S6, S7	Шифрование, аутентификация и механизм антиповтора	Компонент защищенного хранилища 2-го поколения	Защита DPA и блокируемые начальные биты	Ключи привязки к операционной системе
T2	Шифрование и аутентификация	EEPROM	Защита DPA и блокируемые начальные биты	Ключи привязки к операционной системе
Семейство M1	Шифрование, аутентификация и механизм антиповтора	Компонент защищенного хранилища 2-го поколения	Защита DPA и блокируемые начальные биты	Ключи привязки к операционной системе и монитор загрузки

Face ID и Touch ID

Безопасность Face ID и Touch ID

Код-пароли и пароли критически важны для безопасности устройств Apple. В то же время удобный доступ немаловажен для тех, кто обращается к своим устройствам более ста раз в день. Биометрическая аутентификация поддерживает безопасность надежного код-пароля и даже повышает ее уровень, так как не требует ручного ввода, и вместе с тем позволяет быстро разблокировать устройство по отпечатку пальца или просто взглядом. Face ID и Touch ID не заменяют пароль или код-пароль, но в большинстве случаев пользоваться ими проще и удобнее.

Архитектура биометрической безопасности Apple основана на строгом разделении ответственности между биометрическим сенсором и Secure Enclave, а также на безопасном соединении между ними. Сенсор фиксирует биометрическое изображение и безопасно передает его в Secure Enclave. При регистрации Secure Enclave обрабатывает, шифрует и сохраняет данные соответствующих шаблонов Face ID и Touch ID. При сопоставлении Secure Enclave сравнивает входные данные, получаемые от биометрического сенсора, с сохраненными шаблонами, чтобы определить, следует ли разблокировать устройство или ответить, что совпадение найдено (для Apple Pay, приложений и других вариантов использования Face ID и Touch ID). Архитектура поддерживает устройства, которые включают как сенсор, так и Secure Enclave (например, iPhone, iPad и многие системы Mac), а также возможность физически выделить сенсор как периферийное устройство, которое затем безопасно объединяется в пару с Secure Enclave на Mac с чипом Apple.

Безопасность Face ID

Пользователю достаточно взглянуть на свое устройство, и Face ID выполнит безопасную разблокировку устройства Apple. Интуитивно понятная безопасная аутентификация выполняется с помощью камеры TrueDepth, которая точно распознает геометрию лица, задействуя передовые технологии. Face ID задействует нейросети для распознавания внимания пользователя, сопоставления лица и предотвращения несанкционированного доступа. Это дает возможность разблокировать телефон взглядом, даже при использовании устройств в маске, если они поддерживают такую возможность. Face ID автоматически адаптируется к изменениям внешности пользователя и тщательно сохраняет конфиденциальность и безопасность биометрических данных.

Функция Face ID создана для того, чтобы устройство активировалось только в том случае, если на него направлен взгляд пользователя. Она также служит для надежной аутентификации с низкой долей ошибок и предотвращения электронных и физических способов несанкционированного доступа.

Камера TrueDepth автоматически выполняет поиск лица пользователя, когда пользователь выводит из режима сна устройство Apple с Face ID, поднимая его или касаясь экрана, либо когда на устройстве запрашивается идентификация пользователя для отображения входящего уведомления, либо когда аутентификация с помощью Face ID запрашивается приложением с поддержкой этой функции. Когда лицо обнаружено, Face ID подтверждает внимание пользователя и его намерение разблокировать устройство, распознавая открытые глаза и взгляд, направленный на устройство. Для поддержки Универсального доступа проверка внимания Face ID выключается при активации VoiceOver, а при необходимости эту функцию можно выключить самостоятельно. При использовании Face ID в маске всегда требуется распознавание внимания.

Когда камера TrueDepth подтверждает присутствие лица и внимание пользователя, она проецирует и считывает тысячи инфракрасных точек для составления карты глубины лица, а также создает двумерное инфракрасное изображение. На основе этих данных создается последовательность двумерных изображений и карт глубины, которые защищаются цифровой подписью и отправляются в Secure Enclave. Для предотвращения электронных и физических способов мошенничества камера TrueDepth располагает последовательность двумерных изображений и снимков карт глубины в случайном порядке, а также проецирует случайную схему, уникальную для данного устройства. Один из элементов защищенного нейронного модуля, безопасность которого обеспечивается Secure Enclave, создает математическое представление этих данных и сравнивает его с данными зарегистрированного лица. Эти данные являются математическим представлением лица пользователя, сфотографированного под различными углами.

Безопасность Touch ID

Touch ID — это система считывания отпечатка пальца, которая ускоряет и упрощает процесс безопасного доступа к устройствам Apple с поддержкой этой функции. Эта технология считывает отпечатки пальцев под любым углом. При каждом использовании датчик выявляет дополнительные перекрывающиеся узловые точки, расширяя базу данных об отпечатках пальцев пользователя.

Устройства Apple с сенсором Touch ID можно разблокировать с помощью отпечатка пальца. Touch ID не избавляет от необходимости в код-пароле устройства или пароле пользователя, который по-прежнему требуется вводить после загрузки, перезагрузки устройства или выхода из системы (на Mac). В некоторых приложениях Touch ID может использоваться вместо код-пароля устройства или пароля пользователя, например, для разблокировки защищенных паролем заметок в приложении «Заметки», для разблокировки веб-сайтов, защищенных при помощи связи ключей, а также вместо паролей в поддерживаемых приложениях. Однако в некоторых случаях обязательным является использование код-пароля устройства или пароля пользователя. Например, это необходимо для изменения существующего код-пароля устройства или пароля пользователя, а также для удаления зарегистрированных отпечатков пальцев или сохранения новых отпечатков.

Когда датчик отпечатков пальцев распознает прикосновение пальца, он сканирует палец с помощью усовершенствованной матрицы и отправляет изображение в Secure Enclave. Канал, используемый для защиты этого соединения, зависит от того, встроен ли сенсор Touch ID в устройство с Secure Enclave или расположен в отдельном периферийном устройстве.

В процессе векторизации сканированного отпечатка пальца для анализа это растровое изображение временно сохраняется в зашифрованном участке памяти Secure Enclave, а затем удаляется. Анализ выполняется путем сопоставления дуговых папиллярных узоров, при котором изучаются только некоторые фрагменты, что не позволяет восстановить фактический отпечаток пальца пользователя. При регистрации полученная карта узлов сохраняется в зашифрованной форме, которую может прочитать только Secure Enclave, причем она доступна только в виде шаблона для сравнения при дальнейших сопоставлениях и не содержит какой-либо информации, на основе которой можно установить личность. Эти данные никогда не покидают устройства. Они не отправляются в Apple и не включаются в резервные копии устройства.

Встроенная защита канала Touch ID

Встроенный сенсор Touch ID обменивается данными с Secure Enclave по шине последовательного периферийного интерфейса. Процессор не может прочитать эти данные, а просто перенаправляет их сопроцессору Secure Enclave. Для шифрования и аутентификации этих данных используется ключ сеанса, который согласовывается с помощью общего ключа, назначаемого при производстве каждому сенсору Touch ID и соответствующему ему Secure Enclave. Общий ключ каждого сенсора Touch ID является надежным, случайно сгенерированным и уникальным. При обмене ключом сеанса используется алгоритм защиты ключа AES: обе стороны предоставляют случайный ключ, который задает ключ сеанса и использует транспортное шифрование, благодаря чему обеспечивается аутентификация и конфиденциальность (с помощью AES-CCM).

Magic Keyboard с Touch ID

Клавиатура Magic Keyboard с Touch ID (и клавиатура Magic Keyboard с Touch ID и цифровой панелью) — это внешняя клавиатура с сенсором Touch ID, которая подключается к Mac с чипом Apple. Клавиатура Magic Keyboard с Touch ID служит биометрическим считывателем. Она не хранит биометрические шаблоны, не выполняет биометрическое сопоставление и не обеспечивает соблюдение политик безопасности (например, не требует ввести пароль, если разблокировка не выполнялась в течение 48 часов). Перед использованием сенсор Touch ID на клавиатуре Magic Keyboard с Touch ID необходимо безопасно объединить в пару с Secure Enclave на Mac. После этого Secure Enclave сможет выполнять регистрацию и сопоставление, а также обеспечивать соблюдение политик безопасности так же, как и для встроенного сенсора Touch ID. Если компьютер Mac поставляется с клавиатурой Magic Keyboard с сенсором Touch ID, Apple выполняет создание пары на заводе-изготовителе. При необходимости пользователь также может выполнить создание пары. Клавиатуру Magic Keyboard с Touch ID можно безопасно объединить в пару только с одним компьютером Mac за раз, но компьютер Mac может поддерживать защищенные пары с пятью различными клавиатурами Magic Keyboard с Touch ID.

Клавиатура Magic Keyboard с Touch ID и встроенные сенсоры Touch ID совместимы. Если отпечаток пальца, который был зарегистрирован на встроенном в Mac сенсоре Touch ID, считывается клавиатурой Magic Keyboard с Touch ID, то Secure Enclave на компьютере Mac успешно обрабатывает совпадение, и наоборот.

Для поддержки защищенного создания пары и, следовательно, связи между Secure Enclave компьютера Mac и клавиатурой Magic Keyboard с Touch ID клавиатура оснащена аппаратным блоком акселератора открытого ключа (PKA) для обеспечения сертификации и аппаратными ключами для выполнения необходимых криптографических процессов.

Защищенное создание пары

Прежде чем использовать Touch ID на клавиатуре Magic Keyboard с Touch ID, необходимо безопасно объединить ее в пару с Mac. Для того чтобы создать пару, Secure Enclave компьютера Mac и блок PKA клавиатуры Magic Keyboard с Touch ID обмениваются открытыми ключами с корнем в доверенном сертификате Apple. Они используют аппаратные сертификационные ключи и временный ключ ECDH для безопасного подтверждения идентификации. На Mac эти данные защищает Secure Enclave; на клавиатуре Magic Keyboard с Touch ID эти данные защищает блок PKA. После защищенного создания пары все данные Touch ID, передаваемые между Mac и клавиатурой Magic Keyboard с Touch ID, шифруются с помощью AES-GCM, используя 256-битные ключи и динамические ключи ECDH, которые задействуют кривую NIST P-256 на основе сохраненных идентификаторов. (Обычные нажатия клавиш передаются с применением средств защиты Bluetooth так же, как и у любой другой клавиатуры Bluetooth.)

Безопасное подтверждение намерения создать пару

Перед первым использованием Touch ID для совершения некоторых действий, в том числе перед регистрацией нового отпечатка пальца, пользователь должен подтвердить свое намерение использовать клавиатуру Magic Keyboard с Touch ID с компьютером Mac. Для этого требуется выполнить физическое действие. Намерение пользователя подтверждается, если пользователь дважды нажимает кнопку питания компьютера Mac при появлении запроса в пользовательском интерфейсе или если были успешно сопоставлены отпечатки пальцев, ранее зарегистрированные на Mac. Подробнее см. в разделе [Безопасное подтверждение намерения и подключения к Secure Enclave](#).

Транзакции Apple Pay можно авторизовать с помощью сопоставления Touch ID или ввода пароля пользователя macOS и двойного нажатия на кнопку Touch ID на Magic Keyboard с Touch ID. Последним способом пользователь может подтвердить намерение даже без сопоставления Touch ID.

Защита канала клавиатуры Magic Keyboard с Touch ID

Для того чтобы помочь обеспечить безопасность канала связи между сенсором Touch ID на клавиатуре Magic Keyboard с Touch ID и сопроцессором Secure Enclave объединенного в пару компьютера Mac, требуется следующее:

- Защищенное создание пары между блоком PKA клавиатуры Magic Keyboard с Touch ID и сопроцессором Secure Enclave, как описано выше.
- Безопасный канал между клавиатурой Magic Keyboard с сенсором Touch ID и ее блоком PKA.

Безопасный канал между клавиатурой Magic Keyboard с сенсором Touch ID и ее блоком PKA налаживается на заводе-изготовителе с использованием уникального ключа, общего для клавиатуры и блока. (Этот метод также используется для создания безопасного канала между сопроцессором Secure Enclave компьютера Mac и встроенным в компьютер сенсором (это относится к компьютерам Mac со встроенным Touch ID).)

Face ID, Touch ID, код-пароли и пароли

Чтобы использовать Face ID или Touch ID, необходимо настроить устройство таким образом, чтобы для его разблокировки требовался код-пароль или пароль. Если Face ID или Touch ID находит соответствие, устройство разблокируется, не запрашивая код-пароль или пароль устройства. Это повышает рациональность использования более длинного и сложного код-пароля или пароля, поскольку его не нужно будет вводить слишком часто. Face ID и Touch ID не заменяют код-пароль или пароль пользователя, но обеспечивают легкий доступ к устройству в разумных границах и временных рамках. Это важно, поскольку надежный код-пароль или пароль служит основанием для криптографической защиты данных пользователя на устройстве iPhone, iPad, Mac или Apple Watch.

Ситуации, когда необходим ввод код-пароля или пароля

В любое время вместо Face ID или Touch ID пользователи могут ввести код-пароль или пароль; однако иногда воспользоваться биометрической аутентификацией невозможно. Ввод пароля или код-пароля необходим в следующих случаях, требующих особых мер безопасности:

- обновление программного обеспечения;
- стирание содержимого и настроек устройства;
- просмотр или изменение настроек код-пароля;
- установка профилей конфигурации;
- разблокирование панели «Защита и безопасность» в Системных настройках на Mac;
- разблокирование панели «Пользователи и группы» в Системных настройках на Mac (если включена функция FileVault).

Код-пароль или пароль также требуется, если устройство находится в одном из следующих состояний:

- устройство только что включено или перезагружено;
- пользователь вышел из учетной записи Mac (или еще не вошел в нее);
- пользователь не выполнял разблокировку устройства на протяжении более 48 часов;
- пользователь не вводил пароль или код-пароль для разблокировки устройства на протяжении более чем 156 часов (шести с половиной дней) и не выполнял биометрическую аутентификацию для разблокировки устройства в течение более чем 4 часов;
- устройство получило команду удаленной блокировки;
- пользователь отменил выключение устройства или работу функции «Экстренный вызов — SOS» путем нажатия и удержания одновременно одной из кнопок громкости и кнопки «Сон/Пробуждение» в течение двух секунд, а затем нажатия кнопки «Отменить»;
- выполнено пять неудачных попыток сопоставления биометрических данных (однако для удобства пользователя устройство может предложить ввести код-пароль или пароль вместо использования биометрических данных и после меньшего числа неудачных попыток).

Когда на iPhone включена функция Face ID в маске, ею можно воспользоваться в течение 6,5 ч после одного из следующих действий пользователя:

- успешной попытки сопоставления Face ID (в маске или без нее);
- успешной проверки код-пароля, введенного на устройстве;
- разблокировки устройства с помощью часов Apple Watch.

После любого из этих действий период работы функции продлевается на следующие 6,5 ч.

Когда на iPhone или iPad включена функция Face ID или Touch ID, устройство немедленно блокируется при нажатии кнопки «Сон/Пробуждение» и блокируется каждый раз при переходе в режим сна. Для Face ID и Touch ID требуется успешное сопоставление (либо ввод код-пароля) при каждом выходе из режима сна.

Вероятность того, что случайный человек разблокирует iPhone или iPad, составляет меньше чем 1 к 1 000 000 при использовании Face ID, в том числе если включена функция Face ID в маске. В случае моделей iPhone, iPad, Mac с Touch ID и моделей, объединенных в пару с клавиатурой Magic Keyboard, вероятность составляет меньше чем 1 к 50 000. Вероятность возрастает, если зарегистрировано несколько отпечатков пальцев (до уровня 1 к 10 000 при пяти отпечатках) или изображений (до уровня 1 к 500 000 при двух изображениях). Для дополнительной защиты функции Face ID и Touch ID разрешают выполнить только 5 безуспешных попыток сопоставления, после чего для доступа к устройству или учетной записи пользователя потребуется ввести код-пароль или пароль. В случае с Face ID вероятность ошибочного сопоставления выше, если:

- у пользователя есть близнец или похожий на пользователя родственник, например брат или сестра;
- функцией пользуются дети до 13 лет (потому что отличительные черты лица еще формируются).

В этих случаях вероятность еще больше повышается, когда используется Face ID в маске. Тем, кто беспокоится о таком ошибочном сопоставлении, Apple рекомендует использовать для аутентификации код-пароль.

Безопасность сопоставления лица

Сопоставление лица выполняется внутри Secure Enclave с использованием нейросетей, специально обученных для этой задачи. Компания Apple разработала нейросети для сопоставления лиц на основе более миллиарда изображений, включая инфракрасные (ИК) изображения и карты глубины, собранные в ходе исследований, которые проводились с информированного согласия участников. Затем, работая с добровольцами со всего мира, компания Apple собрала репрезентативную группу людей на основе пола, возраста, этнического происхождения и других факторов. При необходимости охват исследований расширялся, чтобы обеспечить высокую степень точности для любых пользователей. Функция Face ID распознает пользователей в головных уборах, шарфах, с контактными линзами, в обычных очках и многих видах солнцезащитных очков. Face ID также поддерживает разблокировку в маске на устройствах iPhone, начиная с iPhone 12 и iOS 15.4 или новее. Кроме того, она работает в помещении, на открытом воздухе и даже в полной темноте. Дополнительная нейросеть, обученная для распознавания и предотвращения мошенничества, защищает от попыток разблокировать устройство при помощи фотографий или масок. Данные Face ID, в том числе математические представления лица пользователя, зашифрованы и доступны только модулю Secure Enclave. Эти данные никогда не покидают устройства. Они не отправляются в Apple и не включаются в резервные копии устройства. При обычном использовании устройства следующие данные Face ID сохраняются в зашифрованном виде только для использования Secure Enclave:

- математические представления лица пользователя, рассчитанные при регистрации;
- математические представления лица пользователя, рассчитанные во время некоторых попыток разблокировки, если Face ID считает их полезными для повышения точности сопоставления в будущем.

Фотографии лица, сделанные в ходе обычного использования устройства, не сохраняются; они немедленно удаляются после расчета математического представления в целях регистрации или сравнения с зарегистрированными данными Face ID.

Повышение эффективности сопоставления Face ID

Чтобы повысить эффективность сопоставления и следить за естественными изменениями внешнего вида пользователя, Face ID периодически дополняет сохраненные математические представления. После успешного сопоставления Face ID может использовать заново рассчитанное математическое представление (если его качество достаточно высоко) в течение ограниченного числа дополнительных сопоставлений, после чего эти данные удаляются. Однако если Face ID не распознает пользователя, но качество сопоставления выше определенного порога, а сразу после неудачного сопоставления пользователь вводит код-пароль, Face ID делает новый снимок и дополняет зарегистрированные данные Face ID заново рассчитанным математическим представлением. Эти новые данные Face ID удаляются по мере устаревания и после ограниченного числа сопоставлений. Они также удаляются при сбросе Face ID. Благодаря этим механизмам дополнения Face ID продолжает работать с минимумом ошибок даже при значительных изменениях лица, то есть если пользователь отрастит или сбреет бороду или же нанесет макияж.

Использование Face ID и Touch ID

Разблокирование устройства или учетной записи пользователя

Если функция Face ID или Touch ID выключена, то, когда блокируется устройство или учетная запись, ключи высшего класса защиты данных, хранящиеся в Secure Enclave, удаляются. Доступ к файлам и элементам связки ключей этого класса отсутствует, пока пользователь не разблокирует устройство или учетную запись, введя код-пароль или пароль.

Когда функция Face ID или Touch ID включена, ключи не удаляются при блокировке устройства или учетной записи; вместо этого они защищаются ключом, выделенным для подсистемы Face ID или Touch ID в Secure Enclave. Если пользователь пытается разблокировать устройство или учетную запись и устройство распознает успешное сопоставление, оно предоставляет ключ для доступа к ключам защиты данных, и устройство или учетная запись разблокируется. Эта процедура обеспечивает дополнительную защиту, поскольку для разблокировки устройства требуется взаимодействие подсистемы защиты данных с подсистемой Face ID или Touch ID.

При перезапуске устройства ключи, необходимые Face ID или Touch ID для разблокировки устройства или учетной записи, утрачиваются. Secure Enclave удаляет эти ключи, как только требуется ввести код-пароль или пароль.

Защита покупок с помощью Apple Pay

Face ID или Touch ID также можно использовать с Apple Pay, чтобы легко и безопасно совершать покупки в магазинах, приложениях и интернете.

- *Использование Face ID в магазинах.* Чтобы авторизовать платеж в магазине посредством Face ID, пользователь сначала должен подтвердить свое намерение произвести оплату, дважды нажав боковую кнопку. Двойное нажатие служит подтверждением оплаты. Это физическое действие напрямую передается в Secure Enclave, и его невозможно симитировать с помощью вредоносного процесса. Затем пользователь проходит аутентификацию посредством Face ID, а только потом подносит устройство к терминалу бесконтактной оплаты. Если после аутентификации посредством Face ID пользователь решает выбрать другое платежное средство для Apple Pay, он должен заново пройти аутентификацию, но без повторного двойного нажатия боковой кнопки.
- *Использование Face ID в приложениях и в интернете.* Для платежей в приложениях и в интернете пользователь подтверждает свое намерение произвести платеж, дважды нажимая боковую кнопку, а затем проходя аутентификацию посредством Face ID, чтобы подтвердить платеж. Если транзакция Apple Pay не завершается в течение 60 секунд после двойного нажатия боковой кнопки, пользователь должен заново подтвердить свое намерение произвести платеж, снова нажав боковую кнопку два раза.
- *Использование Touch ID.* В случае Touch ID пользователь подтверждает платеж, приложив палец к сенсору Touch ID. Оплата совершается после успешного сопоставления отпечатка пользователя.

Использование API, предоставленных системой

Приложения сторонних разработчиков могут использовать API, предоставленные системой, чтобы запрашивать у пользователя аутентификацию посредством Face ID или Touch ID либо ввод код-пароля или пароля. А приложения, поддерживающие Touch ID, автоматически поддерживают Face ID без каких-либо изменений.

При использовании Face ID или Touch ID приложение получает информацию только о том, успешно ли выполнена аутентификация; оно не имеет доступа к Face ID, Touch ID или данным, которые связаны с зарегистрированным пользователем.

Защита элементов связки ключей

Face ID или Touch ID также можно использовать для защиты объектов связки ключей: в этом случае Secure Enclave разблокирует объекты связки ключей только при успешном сопоставлении или вводе код-пароля устройства или пароля учетной записи. С помощью API разработчики приложений могут проверять, что пользователь установил код-пароль или пароль, прежде чем требовать Face ID или Touch ID либо ввод код-пароля или пароля для разблокировки объектов связки ключей. Разработчикам приложений доступны следующие возможности.

- Запрещать применение пароля приложения или код-пароля устройства для выполнения операций, использующих API аутентификации. Они могут запрашивать подтверждение регистрации пользователя, разрешая использование Face ID или Touch ID в качестве второго фактора аутентификации в приложениях, требующих особых мер безопасности.
- Генерировать и использовать ключи криптографии на основе эллиптических кривых (ECC) внутри Secure Enclave, которые могут быть защищены посредством Face ID или Touch ID. Операции с этими ключами всегда производятся внутри Secure Enclave после того, как Secure Enclave авторизует их использование.

Совершение и авторизация покупок

Пользователи также могут настроить Face ID или Touch ID, чтобы подтверждать покупки в iTunes Store, App Store, Apple Books и других сервисах без ввода пароля своего Apple ID. При совершении покупок Secure Enclave проверяет факт биометрической аутентификации, а затем выдает ключи ECC, которые использовались для подписи запроса магазина.

Безопасное подтверждение намерения и подключения к Secure Enclave

Безопасное подтверждение намерения — это способ подтверждения намерения пользователя без какого-либо взаимодействия с операционной системой или процессором приложений. Подключение — физический канал связи между физической кнопкой и Secure Enclave. Этот канал есть в следующих устройствах:

- iPhone X или новее
- Apple Watch Series 1 или новее
- iPad Pro (все модели)
- iPad Air (2020 г.)
- Компьютеры Mac с чипом Apple

С помощью этого канала пользователи могут подтвердить свое намерение совершить действие, что не может подделать даже программное обеспечение, запущенное с правами уровня корня или ядра.

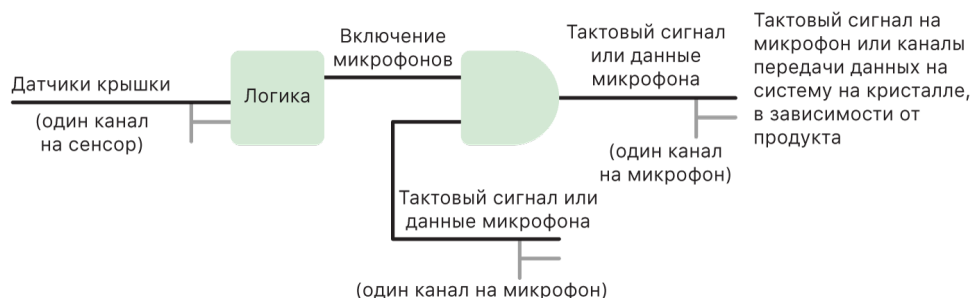
Эта функция используется для подтверждения намерения пользователя при совершении транзакций Apple Pay и при завершении объединения клавиатуры Magic Keyboard с Touch ID в пару с компьютером Mac с чипом Apple. Двойное нажатие на соответствующую кнопку (в случае Face ID) или на датчик отпечатка пальца (в случае Touch ID) по запросу пользовательского интерфейса служит подтверждением намерения пользователя. Подробнее см. в разделе [Защита покупок с помощью Apple Pay](#). Аналогичный механизм, основанный на Secure Enclave и прошивке T2, поддерживается на моделях MacBook с чипом безопасности Apple T2 и без Touch Bar.

Аппаратное отключение микрофона

Во всех ноутбуках Mac с чипом Apple и ноутбуках Mac с процессором Intel и чипом безопасности Apple T2 имеется функция аппаратного отключения, которая выключает микрофон при закрытии крышки. На всех 13-дюймовых ноутбуках MacBook Pro и MacBook Air с чипом T2, а также на всех ноутбуках MacBook с чипом T2 от 2019 г. и новее и ноутбуках Mac с чипом Apple это отключение реализовано исключительно на аппаратном уровне. Аппаратное отключение было разработано для того, чтобы программное обеспечение — даже с правами уровня корня или ядра в macOS, а также программное обеспечение на чипе T2 или иная прошивка — не могло использовать микрофон, если крышка закрыта. (Аппаратное отключение камеры не выполняется, поскольку при закрытой крышке все ее поле обзора и так полностью перекрыто.)

Модели iPad 2020 г. и новее также поддерживают аппаратное отключение микрофона. Если на iPad надет чехол MFi (в том числе из тех, что продает Apple), а верхняя крышка закрыта, микрофон отключается на аппаратном уровне. Эта мера направлена на то, чтобы предотвратить аудиопередачу данных с микрофона программному обеспечению, в том числе с правами уровня корня или ядра в iPadOS или прошивки любого другого устройства.

Методы защиты, указанные в этом разделе, реализованы напрямую с помощью аппаратной логики в соответствии со следующей принципиальной схемой:



В каждом продукте, который оснащен аппаратной блокировкой микрофона, один или несколько датчиков крышки обнаруживают физическое закрытие крышки или корпуса по физическим характеристикам взаимодействия (например, датчик эффекта Холла или датчик угла наклона шарнирного соединения). Для датчиков, требующих калибровки, параметры задаются при производстве устройства, а процесс калибровки предусматривает необратимую аппаратную блокировку любых последующих изменений важных параметров датчика. Такие датчики выдают прямой аппаратный сигнал, который проходит через простой набор аппаратных логических операций, который невозможно перепрограммировать. Эта логика обеспечивает устранение ложных срабатываний, гистерезис и/или задержку до 500 мс перед отключением микрофона. В зависимости от продукта этот сигнал реализуется либо путем отключения каналов передачи данных между микрофоном и системой на кристалле (SoC), либо путем отключения одного из каналов ввода микрофона, которые обеспечивают его активность, например, линии передачи тактовых сигналов или аналогичного применяемого элемента управления.

Экспресс-карты с резервным питанием

Если iOS не запускается из-за того, что iPhone требуется зарядка, возможно, в аккумуляторе еще осталось достаточно энергии для поддержки транзакций экспресс-карт. Поддерживаемые устройства iPhone автоматически поддерживают эту функцию для следующих карт:

- платежные или транспортные карты типа Express Transit;
- студенческие билеты с включенным экспресс-режимом;
- ключи от автомобиля с включенным экспресс-режимом;
- ключи от дома с включенным экспресс-режимом;
- карточки от гостиничных номеров или корпоративные карты-пропуска с включенным экспресс-режимом.

При нажатии на боковую кнопку (или кнопку «Домой» на iPhone SE 2-го поколения) отображается значок низкого уровня заряда, а также сообщение о возможности использования экспресс-карт. Контроллер NFC выполняет транзакции экспресс-карт на тех же условиях, которые действуют при запущенной iOS, однако при проведении таких транзакций выдаются только тактильные уведомления (визуальные уведомления отсутствуют). На iPhone SE 2-го поколения отображение выполненных транзакций на экране может занять несколько секунд. Эта функция недоступна, если выполнено стандартное выключение устройства по инициативе пользователя.

Безопасность системы

Обзор безопасности системы

Механизм обеспечения безопасности системы, который основывается на уникальных возможностях устройств Apple, отвечает за контроль доступа к ресурсам системы на устройствах Apple без ущерба для удобства пользователей. Механизм обеспечения безопасности системы объединяет в себе процесс загрузки, обновление программного обеспечения и защиту вычислительных ресурсов системы, таких как процессор, память, диск, программное обеспечение и сохраненные данные.

Самые новые версии операционных систем Apple являются самыми безопасными. Важным компонентом безопасности Apple является *безопасная загрузка*, которая защищает систему от заражения вредоносным программным обеспечением во время загрузки. В основе безопасной загрузки лежит аппаратное обеспечение, с которого начинается цепочка доверия, объединяющая все модули программного обеспечения. Каждый шаг направлен на то, чтобы звено убеждалось в том, что следующее звено функционирует должным образом, прежде чем передать ему управление. Эта модель безопасности поддерживает не только стандартную загрузку устройств Apple, но и различные режимы восстановления и своевременного обновления на устройствах Apple. Такие подкомпоненты, как чип T2 и сопроцессор Secure Enclave, также выполняют собственную безопасную загрузку. Это помогает гарантировать, что они загружают только заведомо безопасный код Apple. Система обновления разработана для предотвращения атак через понижение версии, так что злоумышленник не может установить на устройстве предыдущую версию операционной системы (которую он умеет взламывать) для кражи пользовательских данных.

Устройства Apple также оснащены средствами защиты на этапах загрузки и выполнения, которые обеспечивают их целостность в процессе текущей работы. Чипы Apple в iPhone, iPad, Apple Watch, Apple TV, HomePod и компьютерах Mac с чипом Apple формируют общую архитектуру для защиты целостности операционной системы. Кроме того, в macOS имеется расширенный настраиваемый набор функций защиты для поддержки своей отличающейся вычислительной модели, а также возможностей, поддерживаемых на всех аппаратных платформах Mac.

Безопасная загрузка

Процесс загрузки для устройств iOS и iPadOS

На каждом этапе загрузки используются компоненты, которые подписаны Apple с использованием криптографических методов для гарантии целостности и того, чтобы загрузка продолжалась только после проверки цепочки доверия. Среди этих компонентов — загрузчики системы, ядро, расширения ядра и прошивка для немодулированной передачи по сотовой сети. Эта безопасная последовательность загрузки предназначена для того, чтобы убедиться, что в низкоуровневое программное обеспечение не были внесены изменения.

Сразу после включения устройства iOS или iPadOS процессор приложений исполняет код загрузочного ПЗУ, которое доступно только для чтения. Этот постоянный код, называемый *аппаратным корнем доверия*, закладывается в процессе изготовления чипа и считается безоговорочно надежным. Код загрузочного ПЗУ содержит открытый ключ корневого центра сертификации (ЦС) Apple. Перед выполнением загрузки устройство использует этот ключ, чтобы проверить, подписан ли загрузчик системы iBoot компанией Apple. Этот этап является первым звеном цепочки доверия, каждое звено в которой проверяет, подписано ли следующее звено компанией Apple. Когда iBoot завершает свои задачи, он проверяет и запускает ядро iOS или iPadOS. На устройствах с A9 или более старым процессором серии A добавляется еще один этап: загрузочное ПЗУ загружает и проверяет низкоуровневый загрузчик, который в свою очередь загружает и проверяет iBoot.

В случае неудачи при проверке следующих этапов дальнейшие действия системы зависят от оборудования.

- *Boot ROM не может загрузить LLB (на более старых устройствах):* режим обновления прошивки устройства (DFU).
- *Низкоуровневый загрузчик или iBoot:* режим восстановления.

В любом из этих случаев необходимо подключить устройство к Finder (в macOS 10.15 и новее) или iTunes (в macOS 10.14 и более ранних версиях) через USB и восстановить заводские настройки.

Для ограничения доступа к пользовательским данным в разных режимах сопроцессор Secure Enclave использует реестр процесса загрузки (BPR), который обновляется перед переходом в следующие режимы:

- *Режим обновления прошивки устройства (DFU).* Устанавливается загрузочным ПЗУ на устройствах с системой на кристалле Apple A12 или новее.
- *Режим восстановления.* Устанавливается iBoot на устройствах с системой на кристалле Apple A10, S2 или новее.

На устройствах с поддержкой сотовой связи подсистема немодулированной передачи по сотовой сети запускает дополнительный процесс безопасной загрузки с использованием подписанного программного обеспечения и ключей, проверенных процессором немодулированной передачи.

Secure Enclave также выполняет безопасную загрузку, которая проверяет, что специализированное программное обеспечение (sepOS) проверено и подписано компанией Apple.

Реализация iBoot, безопасная для памяти

В iOS 14 и iPadOS 14 корпорация Apple изменила пакет инструментов для компилятора C, который использовался для создания загрузчика iBoot, чтобы усилить безопасность. Измененный пакет инструментов реализует код, который направлен на то, чтобы избежать проблем с безопасностью памяти и типов, которые обычно возникают в программах, написанных на языке C. Например, это помогает предотвратить большинство уязвимостей следующих классов:

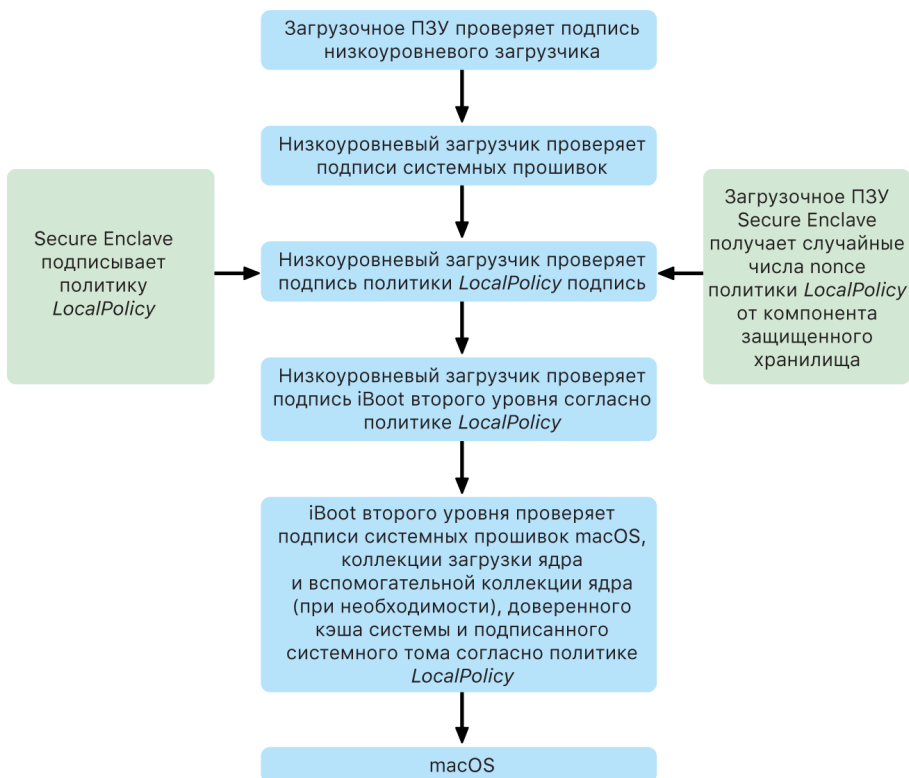
- Предотвращение переполнения памяти путем проверки того, что все указатели содержат сведения о привязках, что проверяется при доступе к памяти.
- Предотвращение использования уязвимостей кучи путем отделения данных кучи от ее метаданных и точного определения условий возникновения ошибки, например двойного высвобождения.
- Предотвращение путаницы с типами за счет обеспечения того, что все указатели содержат сведения о типе среды выполнения, которые проверяются во время выполнения операций приведения указателя.
- Предотвращение путаницы с типами, вызванной ошибками использования после высвобождения, путем отделения всех операций динамического выделения памяти по статическому типу.

Данная технология доступна на устройствах iPhone с системой на кристалле Apple A13 Bionic и новее, а также на устройствах iPad с системой на кристалле A14 Bionic.

Компьютеры Mac с чипом Apple

Процесс загрузки компьютера Mac с чипом Apple

При включении компьютера Mac с чипом Apple он выполняет процесс загрузки, который очень похож на процесс загрузки iPhone и iPad.



Чип исполняет код из загрузочного ПЗУ, что является первым звеном цепочки доверия. Процесс безопасной загрузки macOS на компьютере Mac с чипом Apple проверяет не только сам код операционной системы, но и политики безопасности и даже расширения ядра (поддерживается, но не рекомендуется), настроенные авторизованными пользователями.

После запуска низкоуровневого загрузчика он проверяет подписи и загружает парную системную прошивку для ядер внутри системы на кристалле, таких как контроллеры хранилища, дисплея, управления системой и контроллер Thunderbolt. Низкоуровневый загрузчик также отвечает за загрузку политики *LocalPolicy*, которая представляет собой файл с подписью сопроцессора Secure Enclave. В ней содержится описание конфигурации, выбранной пользователем для загрузки системы, и политик безопасности среды выполнения. Структура данных политики *LocalPolicy* имеет такой же формат, как и у всех других объектов загрузки, однако файл политики подписан локально личным ключом, который доступен только в Secure Enclave определенного компьютера, а не центральным сервером Apple (как обновления программного обеспечения).

Для того чтобы предотвратить повторное выполнение предыдущих политик LocalPolicy, низкоуровневому загрузчику следует найти значение nonce в компоненте защищенного хранилища с Secure Enclave. Для этого используется загрузочное ПЗУ Secure Enclave. Затем выполняется проверка того, совпадает ли значение nonce в политике LocalPolicy со значением nonce в компоненте защищенного хранилища. Эта мера направлена на то, чтобы предупредить повторное применение к системе старой политики LocalPolicy, которая, возможно, была ранее настроена на обеспечение более низкого уровня защиты, после повышения уровня безопасности системы. В результате безопасная загрузка на компьютере Mac с чипом Apple помогает защитить не только от возврата к предыдущим версиям операционной системы, но и от понижения уровня политики безопасности.

В политике LocalPolicy фиксируется уровень настройки безопасности операционной системы: высший уровень безопасности, сниженный уровень безопасности и низкий уровень безопасности.

- *Высший уровень безопасности.* В этом режиме система работает так же, как и iOS и iPadOS; допускается загрузка только программного обеспечения, которое было заведомо наиболее актуальным на момент установки.
- *Сниженный уровень безопасности.* Низкоуровневому загрузчику предписывается доверять «глобальным» подписям, которые поставляются в комплекте с операционной системой. Благодаря этому на компьютере можно использовать более ранние версии macOS. Поскольку в старых версиях macOS неизбежно имеются неустраненные уязвимости, данный уровень безопасности называется *сниженным*. Кроме того, этот уровень политики необходим для поддержки загрузки расширений ядра.
- *Низкий уровень безопасности.* Если выбран этот уровень безопасности, система работает так же, как и в режиме сниженного уровня безопасности в отношении использования глобальных подписей для iBoot и не только, однако в этом режиме iBoot предписывается принимать некоторые объекты загрузки, подписанные Secure Enclave с помощью того же ключа, который использовался для подписания политики LocalPolicy. Этот уровень политики поддерживает создание, подписание и загрузку пользователями собственных ядер XNU.

Если политика LocalPolicy указывает низкоуровневому загрузчику, что операционная система запущена в режиме высшего уровня безопасности, низкоуровневый загрузчик проверяет персональную подпись для iBoot. Если операционная система запущена в режиме сниженного или низкого уровня безопасности, проверяется глобальная подпись. В случае возникновения любых ошибок при проверке система загружает recoveryOS для предоставления вариантов исправления ошибок.

После того как низкоуровневый загрузчик передает управление загрузчику iBoot, последний загружает парную прошивку macOS, например: прошивку для защищенной системы Neural Engine, всегда включенного процессора и другие прошивки. Загрузчик iBoot также проверяет информацию о политике LocalPolicy, переданную ему низкоуровневым загрузчиком. Если во время загрузки политика LocalPolicy указывает на то, что необходима вспомогательная коллекция ядра (AuxKC), iBoot выполняет поиск AuxKC в файловой системе, проверяет, была ли она подписана Secure Enclave с использованием того же ключа, что и для политики LocalPolicy, а затем проверяет, совпадает ли ее хэш с тем, который хранится в политике LocalPolicy. После проверки AuxKC загрузчик iBoot помещает ее в память вместе с загрузочной коллекцией ядра, прежде чем заблокировать всю область памяти, в которой находятся загрузочная коллекция ядра и AuxKC, с помощью защиты целостности системного сопроцессора (SCIP). Если в политике указано, что необходима коллекция AuxKC, однако она не найдена, система продолжает загрузку macOS без нее. iBoot также отвечает за проверку корневого хэша подписанного системного тома (SSV), чтобы убедиться в полной целостности файловой системы, которую будет подключать ядро.

Режимы загрузки компьютера Mac с чипом Apple

Режимы загрузки компьютера Mac с чипом Apple описаны далее.

Режим	Сочетание клавиш	Описание
macOS	Когда компьютер выключен, нажмите и отпустите кнопку питания.	<ol style="list-style-type: none">1. Загрузочное ПЗУ передает управление низкоуровневому загрузчику.2. Низкоуровневый загрузчик загружает парную системную прошивку и политику LocalPolicy для выбранной macOS.3. Низкоуровневый загрузчик фиксирует в реестре хода загрузки сведения о том, что он загружает macOS, а затем передает управление загрузчику iBoot.4. iBoot загружает парную прошивку операционной системы, статический доверенный кэш, дерево устройств и загрузочную коллекцию ядра.5. Если это разрешено политикой LocalPolicy, iBoot загружает вспомогательную коллекцию ядра (AuxKC) со сторонними расширениями ядра.6. Если это не отключено политикой Local Policy, iBoot проверяет корневой хэш подписи подписанного системного тома (SSV).

Режим	Сочетание клавиш	Описание
Парная среда recoveryOS	Когда компьютер выключен, нажмите и не отпускайте кнопку питания.	<ol style="list-style-type: none"> 1. Загрузочное ПЗУ передает управление низкоуровневому загрузчику. 2. Низкоуровневый загрузчик загружает парную системную прошивку и политику LocalPolicy для среды recoveryOS. 3. Низкоуровневый загрузчик фиксирует в реестре хода загрузки сведения о том, что он загружает парную recoveryOS, а затем передает управление загрузчику iBoot для парной recoveryOS. 4. iBoot загружает парную прошивку macOS, доверенный кэш, дерево устройств и загрузочную коллекцию ядра. 5. Если загрузка парной среды recoveryOS не удалась, предпринимается попытка загрузить резервную среду recoveryOS. <p><i>Примечание.</i> Политика LocalPolicy парной среды recoveryOS не допускает снижения уровня безопасности.</p>
Резервная среда recoveryOS	Когда компьютер выключен, дважды нажмите и не отпускайте кнопку питания.	<ol style="list-style-type: none"> 1. Загрузочное ПЗУ передает управление низкоуровневому загрузчику. 2. Низкоуровневый загрузчик загружает парную системную прошивку и политику LocalPolicy для среды recoveryOS. 3. Низкоуровневый загрузчик фиксирует в реестре хода загрузки сведения о том, что он загружает парную среду recoveryOS, а затем передает управление загрузчику iBoot для среды recoveryOS. 4. iBoot загружает парную прошивку macOS, доверенный кэш, дерево устройств и загрузочную коллекцию ядра. <p><i>Примечание.</i> Политика LocalPolicy парной среды recoveryOS не допускает снижения уровня безопасности.</p>
Безопасный режим	Загрузите среду recoveryOS, как описано ранее, а затем удерживайте клавишу Shift при выборе загрузочного тома.	<ol style="list-style-type: none"> 1. Выполняется загрузка среды recoveryOS, как указано выше. 2. Нажатие и удерживание клавиши Shift при выборе тома приводит к тому, что приложение BootPicker разрешает загрузку macOS в обычном режиме; кроме того, задается переменная nvram, которая сообщает загрузчику iBoot, что не следует загружать AukKC при следующей загрузке. 3. Система перезагружается и загружается с использованием целевого тома, однако iBoot не загружает AukKC.

Ограничения для парных сред recoveryOS

В macOS 12.0.1 или новее каждая новая устанавливаемая система macOS также устанавливает парную версию recoveryOS в соответствующей группе томов APFS. Этот принцип знаком пользователям компьютеров Mac с процессором Intel, но на компьютере Mac с чипом Apple он работает как дополнительное средство обеспечения безопасности и совместимости. Поскольку теперь у каждой устанавливаемой системы macOS есть своя парная среда recoveryOS, только из этой парной среды recoveryOS можно снизить уровень безопасности. Это помогает защитить установленные системы macOS более новых версий от взлома, выполняемого из более ранней версии macOS, и наоборот.

Ограничения в отношении пар работают следующим образом.

- У каждой установленной системы macOS 11 есть парная среда recoveryOS. Если по умолчанию выбрана загрузка установленной системы macOS 11, то recoveryOS можно загрузить, удерживая клавишу питания, когда компьютер Mac с чипом Apple загружается. В recoveryOS можно снизить уровень безопасности любой установленной системы macOS 11, но не каждой установленной системы macOS 12.0.1.
- Если по умолчанию выбрана загрузка установленной системы macOS 12.0.1 или новее, то соответствующую ей парную среду recoveryOS можно загрузить, удерживая клавишу питания, когда загружается компьютер Mac. Из парной среды recoveryOS можно снизить уровень безопасности в установленной системе macOS, соответствующей этой парной среде, но не в любой другой установленной системе macOS.

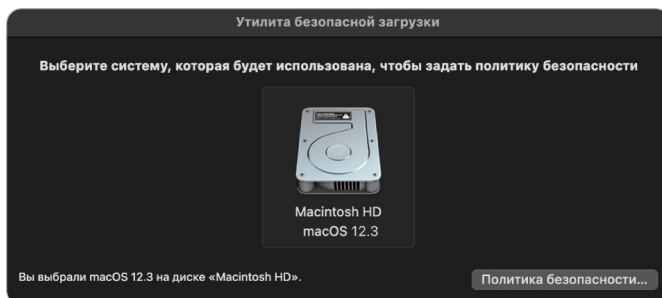
Чтобы загрузить парную среду recoveryOS, соответствующую какой-либо установленной системе macOS, выберите эту установленную систему по умолчанию. Для этого откройте раздел «Загрузочный диск» Системных настроек или запустите любую recoveryOS и удерживайте клавишу Option при выборе тома.

Примечание. В резервной среде recoveryOS нельзя снизить уровень безопасности в какой-либо установленной системе macOS.

Управление политикой безопасности Загрузочного диска на компьютере Mac с чипом Apple

Обзор

В отличие от политик безопасности на компьютере Mac с процессором Intel политики безопасности на компьютере Mac с чипом Apple относятся к конкретной установленной операционной системе. Это означает, что на одном компьютере Mac может быть установлено несколько экземпляров macOS с разными версиями и политиками безопасности. Поэтому в Утилиту безопасной загрузки был добавлен инструмент выбора операционной системы.

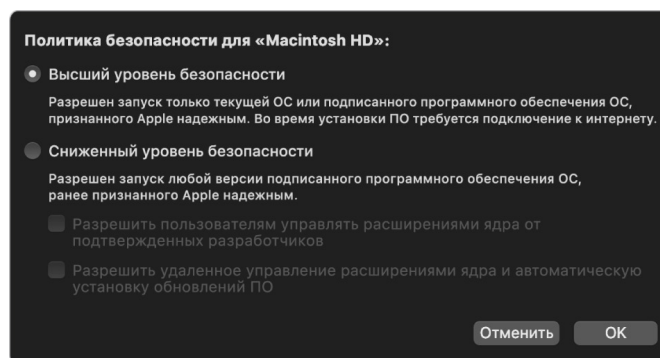


На компьютере Mac с чипом Apple утилита системной безопасности показывает общее состояние настроенной пользователем безопасности macOS, например загрузку расширения ядра или конфигурацию защиты целостности системы (SIP). Если изменение настроек безопасности приводит к значительному снижению уровня защиты или существенно упрощает вмешательство в систему, для внесения такого изменения пользователю потребуется войти в среду recoveryOS путем удерживания кнопки питания (благодаря этому вредоносное программное обеспечение не может передать сигнал; это может сделать только человек с физическим доступом). Поэтому компьютер Mac с чипом Apple также не требует (и не поддерживает) пароль прошивки, так как все критически важные изменения уже регулируются авторизацией пользователя. Подробнее о SIP см. в разделе [Защита целостности системы](#).

Высший уровень безопасности или сниженный уровень безопасности можно задать с помощью Утилиты безопасной загрузки в среде recoveryOS. Режим низкого уровня безопасности может быть вызван только из командной строки для пользователей, которые решили существенно снизить уровень защиты своего Mac и принимают сопряженные с этим риски.

Политика «Высший уровень безопасности»

Высший уровень безопасности выбран по умолчанию и работает так же, как и в iOS и iPadOS. При загрузке и подготовке к установке такого программного обеспечения операционная система macOS вместо использования глобальной подписи, прилагаемой к программному обеспечению, обращается к тому же серверу подписания Apple, который используется для iOS и iPadOS, и запрашивает новую «персонализированную» подпись. Подпись называется персонализированной, если запрос на подписание содержит уникальный идентификатор чипа ECID — в данном случае уникальный идентификатор процессора Apple. В этом случае подпись, возвращаемая сервером подписания, является уникальной и может использоваться только этим конкретным процессором Apple. При использовании высшего уровня безопасности загрузочное ПЗУ и низкоуровневый загрузчик помогают убедиться в том, что подпись не просто предоставлена Apple, а предназначена для этого конкретного Mac, то есть что эта версия macOS привязана к этому Mac.

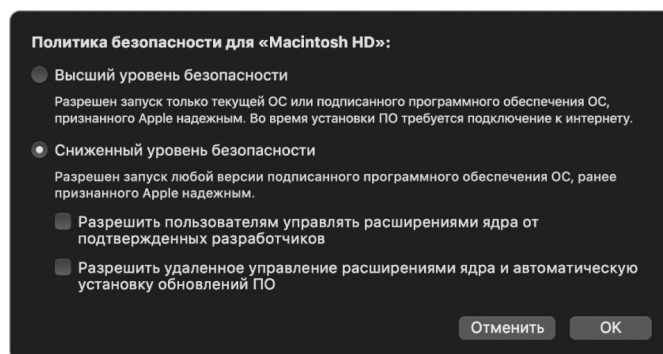


Использование интернет-сервера подписания также обеспечивает лучшую защиту от атак методом отката, чем обычные подходы, в которых используются глобальные подписи. В системе на основе глобальных подписей новая эпоха безопасности может наступить несколько раз, но система, на которой никогда не была установлена последняя версия прошивки, этого не знает. Например, компьютер, который считает, что находится в эпохе безопасности 1, принимает программное обеспечение из эпохи безопасности 2, хотя на самом деле уже наступила эпоха безопасности 5. С системой интернет-подписания чипа Apple сервер подписания может отклонять запросы создания подписей от программного обеспечения, которое не соответствует последней эпохе безопасности.

Кроме того, если злоумышленник обнаружит уязвимость после смены эпохи безопасности, он не сможет просто взять уязвимое программное обеспечение из системы А, принадлежащей предыдущей эпохе, и с его помощью атаковать систему В. Тот факт, что уязвимое программное обеспечение из более ранней эпохи было персонализировано для системы А, помогает предупредить его передачу и, следовательно, его использование для атаки системы В. Совместное применение всех этих механизмов дает более твердую гарантию того, что злоумышленники не смогут преднамеренно поместить уязвимое программное обеспечение на компьютер, чтобы обойти средства защиты, предоставляемые новейшим программным обеспечением. Однако обладатель имени и пароля администратора Mac всегда может выбрать политику безопасности, которая наилучшим образом подходит для его ситуации.

Политика «Сниженный уровень безопасности»

Сниженный уровень безопасности аналогичен среднему уровню безопасности на компьютере Mac с процессором Intel и чипом T2, при этом поставщик (в данном случае Apple) генерирует цифровую подпись для кода, чтобы подтвердить, что этот код получен от поставщика. Эта мера помогает предотвратить добавление неподписанного кода злоумышленниками. Apple называет эту подпись «глобальной», поскольку ее можно использовать на любом компьютере Mac в течение любого периода времени, если в данный момент на компьютере Mac установлена политика «Сниженный уровень безопасности». Сниженный уровень безопасности сам по себе не обеспечивает защиту от атак методом отката, однако несанкционированное изменение операционной системы может привести к тому, что пользовательские данные станут недоступными. Подробнее см. в разделе [Расширения ядра на компьютере Mac с чипом Apple](#).

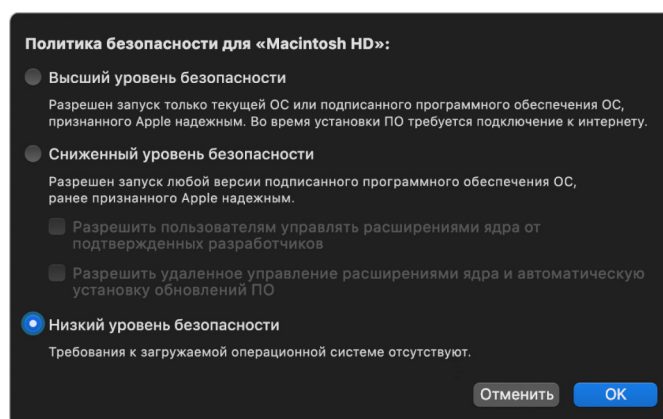


Помимо возможности запуска более ранних версий macOS, сниженный уровень безопасности требуется для выполнения других действий, таких как установка сторонних расширений ядра, в результате чего система пользователя подвергается риску. Расширения ядра имеют те же разрешения, что и само ядро, поэтому любые уязвимости в них могут привести к возникновению прямой угрозы для всей операционной системы. Именно поэтому разработчикам настоятельно рекомендуется переходить на расширения системы, прежде чем поддержка расширений ядра будет удалена из macOS для будущих компьютеров Mac с чипом Apple. Даже если возможность добавления сторонних расширений ядра включена, отдельные расширения невозможно загружать в ядро по запросу. Вместо этого расширения ядра объединяются во вспомогательную коллекцию ядра (AuxKC), хэш которой хранится в политике LocalPolicy, и поэтому затем требуется перезагрузка. Подробнее о создании AuxKC см. в разделе [Расширения ядра в macOS](#).

Политика «Низкий уровень безопасности»

Низкий уровень безопасности предназначен для тех, кто принимает риск значительного снижения уровня защиты своего Mac. Данный режим отличается от политики «Функции безопасности отключены» на компьютере Mac с процессором Intel и чипом T2. В режиме низкого уровня безопасности по-прежнему выполняется проверка подписи и выполняется вся безопасная последовательность загрузки, однако переход в режим низкого режима безопасности сигнализирует загрузчику iBoot о том, что ему следует принять объекты загрузки с локальной подписью Secure Enclave, такие как сгенерированная пользователем загрузочная коллекция ядра, созданная на основе настраиваемого ядра XNU. Таким образом в режиме низкой безопасности на уровне архитектуры обеспечивается возможность запуска произвольного ядра «полностью ненадежной операционной системы». После загрузки настраиваемой загрузочной коллекции ядра или ненадежной операционной системы некоторые ключи дешифрования становятся недоступными. Эта мера направлена на то, чтобы исключить возможность доступа ненадежной операционной системы к данным надежных операционных систем.

Важно! Apple не предоставляет настраиваемые ядра XNU и не обеспечивает поддержку их использования.



Политика «Низкий уровень безопасности» также отличается от политики «Функции безопасности отключены» на компьютере Mac с процессором Intel и чипом T2 тем, что она необходима для ослабления ряда функций безопасности, которые в прошлом управлялись независимо. Особенно важно, что для отключения защиты целостности системы (SIP) на компьютере Mac с чипом Apple пользователь должен подтвердить, что намеренно задает для системы политику «Низкий уровень безопасности». Это необходимо, поскольку отключение SIP всегда облегчает взлом ядра системы. В частности, отключение SIP на компьютере Mac с чипом Apple приводит к отключению применения подписи расширения ядра во время создания AuthKCS, в результате чего в память ядра можно загрузить произвольное расширение ядра. На компьютере Mac с чипом Apple защита SIP была усилена путем перемещения хранилища политик из энергонезависимой памяти в политику LocalPolicy. Теперь для отключения SIP требуется аутентификация, выполненная пользователем, у которого есть доступ к ключу подписания политики LocalPolicy, из среды recoveryOS, перейти в которую можно путем длительного нажатия кнопки питания. Это значительно усложняет отключение SIP для злоумышленников, использующих только программное обеспечение, а также и при наличии физического доступа к компьютеру.

Невозможно выбрать режим низкого уровня безопасности из Утилиты безопасной загрузки. Для снижения уровня безопасности пользователи должны использовать инструменты командной строки из Терминала в `recoveryOS`, например `csrutil` (для отключения SIP). Когда пользователь снижает уровень безопасности, этот факт отражается в Утилите безопасной загрузки, так что пользователь может легко установить более защищенный режим.

Примечание. Компьютер Mac с чипом Apple не требует и не поддерживает определенные политики загрузки с носителя, поскольку с технической точки зрения все загрузки выполняются локально. Если пользователь хочет выполнить загрузку с внешнего носителя, необходимо сначала персонализировать версию операционной системы, используя аутентифицированную перезагрузку из `recoveryOS`. При перезагрузке на внутреннем диске создается файл `LocalPolicy`, который используется для выполнения надежной загрузки из операционной системы, хранящейся на внешнем носителе. Это означает, что конфигурация загрузки с внешнего носителя всегда явным образом включается для конкретной операционной системы и уже требует авторизации пользователя, поэтому дополнительная безопасная конфигурация не нужна.

Создание ключа подписания политики `LocalPolicy` и управление им

Создание

При первой установке macOS на заводе-изготовителе или при стирании и последующей установке с использованием кабельного подключения компьютер Mac запускает код с диска оперативной памяти временного восстановления, чтобы задать заводские настройки. Во время этого процесса среда восстановления создает новую пару из открытого и личного ключей, которые находятся в Secure Enclave. Этот личный ключ называется *ключом удостоверения владельца (OIK)*. Если ключ OIK уже существует, он уничтожается в ходе этого процесса. Среда восстановления также инициализирует ключ, используемый для блокировки активации, то есть *ключ удостоверения пользователя (UIK)*. В рамках этого процесса, который выполняется только на компьютере Mac с чипом Apple, когда сертификация ключа UIK запрашивается для блокировки активации, включаются запрошенные ограничения, которые будут введены во время проверки политики `LocalPolicy`. Если устройство не может получить ключ UIK, сертифицированный для блокировки активации (например потому, что устройство на данный момент связано с учетной записью «Найти Mac» и объявлено пропавшим), тогда это устройство не сможет продолжить создавать политику `LocalPolicy`. Если устройству выдан *сертификат удостоверения пользователя (ucrt)*, этот сертификат содержит ограничения, накладываемые сервером на политику, а также ограничения политики, запрошенные пользователем в расширении X.509 версии 3.

В случае успешного извлечения блокировки активации или сертификата `ucrt` информация об этом сохраняется в базе данных на стороне сервера, а также передается обратно на устройство. После того как устройство получило сертификат `ucrt`, запрос открытого ключа, который соответствует ключу ОИК, передается на сервер центра основной аттестации (ВАА). Центр ВАА проверяет сертификацию ключа ОИК с использованием открытого ключа из сертификата `ucrt`, который хранится в базе данных, доступ к которой открыт для центра ВАА. Если центру ВАА удастся проверить сертификацию, он сертифицирует открытый ключ, возвращая сертификат удостоверения владельца (ОИС), подписанный центром ВАА и содержащий ограничения, сохраненные в сертификате `ucrt`. Сертификат ОИС передается обратно в Secure Enclave. С этого момента, когда Secure Enclave подписывает новую политику LocalPolicy, Secure Enclave вносит сертификат ОИС в манифест Image4. Низкоуровневый загрузчик располагает встроенным доверенным корневым сертификатом центра ВАА, поэтому загрузчик считает сертификат ОИС доверенным, что ведет к тому, что подпись LocalPolicy в целом признается доверенной.

Ограничения RemotePolicy

Все файлы манифеста Image4, а не только политики LocalPolicy, содержат ограничения в отношении оценки манифеста Image4. Эти ограничения закодированы с помощью специальных идентификаторов объектов (OID) в некорневом сертификате. Библиотека проверки манифеста Image4 выполняет поиск идентификатора OID со специальным ограничением сертификата во время проверки подписи, а затем автоматически оценивает указанные в нем ограничения. Ограничения имеют следующую форму:

- параметр X должен существовать;
- параметр X должен отсутствовать;
- параметр X должен иметь определенное значение.

Так, например, ограничения сертификата для «персонализированных» подписей будут содержать условие «Параметр ECID должен существовать», а для «глобальных» подписей ограничения будут содержать условие «Параметр ECID должен отсутствовать». Эти ограничения направлены на то, чтобы все файлы Image4, подписанные с помощью указанного ключа, соответствовали определенным требованиям во избежание создания ошибочно подписанного манифеста Image4.

В контексте политик LocalPolicy эти ограничения сертификата Image4 рассматриваются как относящиеся к политике RemotePolicy. Политики LocalPolicy у сред загрузки иного типа могут иметь другую политику RemotePolicy. Политика RemotePolicy используется для ограничения политики LocalPolicy среды recoveryOS, чтобы при загрузке recoveryOS она загружалась так, как если бы применялась политика «Высший уровень безопасности». Это повышает доверие к целостности recoveryOS как среды загрузки, в которой допускается изменение политики. Политика RemotePolicy ограничивает возможность хранения в политике LocalPolicy идентификатора ECID компьютера Mac, на котором была создана политика LocalPolicy, а также возможность хранения определенного хэша случайного значения nonce удаленной политики (rpnh) в компоненте защищенного хранилища на этом компьютере Mac. rpnh, а значит и политика RemotePolicy, изменяется только при выполнении действий, связанных с функциями «Найти Mac» и «Блокировка активации». К таким действиям относятся: регистрация, отмена регистрации, удаленная блокировка и удаленное стирание. Ограничения политики RemotePolicy определяются и указываются во время сертификации ключа удостоверения пользователя (UIK), а также вносятся в выпущенный сертификат удостоверения пользователя (ucrt). Некоторые ограничения политики RemotePolicy, такие как ECID, ChipID и BoardID, определяются сервером. Таким образом можно предупредить подписание файлов LocalPolicy на одном устройстве для другого. Устройство может задать другие ограничения политики RemotePolicy, что поможет не допустить понижения уровня безопасности политики LocalPolicy без локальной аутентификации и одновременно удаленной аутентификации. Локальная аутентификация требуется для доступа к текущему ключу OIK, а удаленная аутентификация необходима для учетной записи, в которой выполнена блокировка активации устройства.

Содержимое файла LocalPolicy для компьютера Mac с чипом Apple

LocalPolicy — это файл Image4, подписанный Secure Enclave. Image4 представляет собой формат структуры данных в кодировке ASN.1 (абстрактная синтаксическая нотация версии 1) DER, который используется для описания информации об объектах безопасной последовательности загрузки на платформах Apple. В модели безопасной загрузки на основе Image4 запрос политик выполняется во время установки программного обеспечения с помощью запроса на подписание к центральному серверу подписания Apple. Если политика была приемлемой, сервер подписания возвращает подписанный файл Image4, который содержит набор последовательностей четырехзначных кодов (4CC). Во время загрузки эти подписанные файлы Image4 и 4CC оцениваются программным обеспечением, таким как загрузочное ПЗУ или низкоуровневый загрузчик.

Передача права владения между операционными системами

Правом владения называется право доступа к ключу удостоверения владельца (ОИК). Право владения необходимо, чтобы разрешить пользователям заново подписывать политику LocalPolicy после внесения изменений в политику или программное обеспечение. Ключ ОИК защищен иерархией ключей, как описано в разделе [Технология защиты запечатыванием ключей \(SKP\)](#), и ключом ОИК, защищенным тем же ключом шифрования ключа (КЕК), что и ключ шифрования тома (ВЕК). Это означает, что обычно защита обеспечивается паролем пользователя и измерениями операционной системы и политики. Для всех операционных систем компьютера Mac существует один ключ ОИК. Следовательно, во время установки второй операционной системы требуется, чтобы пользователи первой операционной системы явным образом передали право владения пользователям второй операционной системы. Однако пользователи второй операционной системы еще не существуют на момент запуска установщика из первой операционной системы. Пользователи операционных систем обычно не создаются, пока не выполнена загрузка операционной системы и пока не запущен Ассистент настройки. Поэтому для установки второй операционной системы на компьютере Mac с чипом Apple требуется выполнить два следующих действия:

- создать политику LocalPolicy для второй операционной системы;
- создать учетную запись пользователя для передачи права владения.

При запуске Ассистента установки и подготовке к установке дополнительного пустого тома отображается запрос о том, требуется ли скопировать учетную запись пользователя с текущего тома, чтобы сделать ее учетной записью первого пользователя второго тома. Если пользователь одобряет запрос, то создание учетной записи пользователя в действительности представляет собой ключ шифрования ключей (КЕК), полученный из пароля выбранного пользователя и аппаратных ключей. Полученный ключ КЕК затем используется для шифрования ключа ОИК, так как он передается второй операционной системе. Затем из Ассистента установки во второй операционной системе появляется запрос пароля пользователя, с помощью которого новая операционная система получает доступ к ключу ОИК в Secure Enclave. Если было решено не копировать учетную запись пользователя, создание учетной записи пользователя выполняется по описанной схеме, но вместо пароля пользователя используется пустой пароль. Этот второй вариант существует для определенных сценариев системного администрирования. Однако пользователям, которым необходимо выполнить установку на несколько томов и передать право владения наиболее надежным способом, следует всегда выбирать копирование учетной записи пользователя первой операционной системы во вторую.

Политика LocalPolicy на компьютере Mac с чипом Apple

На компьютере Mac с чипом Apple управление локальной политикой безопасности было делегировано приложению, запускаемому в Secure Enclave. Такое программное обеспечение может использовать учетные данные пользователя и режим загрузки основного ЦП, чтобы определить, кто может изменять политику безопасности и из какой среды загрузки. Это мешает вредоносному программному обеспечению использовать элементы управления политики безопасности во вред пользователю путем исключения возможности получить дополнительные права.

Свойства манифеста политики LocalPolicy

В файле LocalPolicy содержится ряд кодов 4CC уровня архитектуры, которые имеются почти во всех файлах Image4, таких как BORD (обозначает плату или идентификатор модели), CHIP (обозначает определенный чип Apple) или универсальный идентификатор чипа (ECID). Однако приведенные ниже коды 4CC касаются исключительно политик безопасности, которые может настраивать пользователь.

Примечание. Apple использует термин *одна парная подлинная среда recoveryOS (1TR)* для обозначения загрузки парной среды recoveryOS путем физического нажатия и удерживания кнопки питания. Она отличается от загрузки обычной среды recoveryOS, которая выполняется с помощью энергонезависимой памяти, вызывается двойным нажатием и удерживанием или может произойти при возникновении ошибок загрузки. Необходимость физического нажатия определенным способом позволяет гарантировать, что среда загрузки будет недоступна для проникшего в macOS злоумышленника, который использует только программное обеспечение.

Хэш случайного значения nonce политики LocalPolicy (lprnh)

- *Тип:* OctetString (48)
- *Изменяемые среды:* 1TR, recoveryOS, macOS
- *Описание:* lprnh используется для защиты от повтора политики LocalPolicy. Это хэш SHA384 случайного значения nonce политики LocalPolicy (LPN), который хранится в компоненте защищенного хранилища и доступ к которому осуществляется через загрузочное ПЗУ Secure Enclave или через Secure Enclave. Необработанное значение nonce никогда не доступно процессору приложений, а только sepOS. Злоумышленнику, пытающемуся убедить низкоуровневый загрузчик в том, что предоставленная им прошлая политика LocalPolicy является корректной, потребовалось бы поместить значение в компонент защищенного хранилища, который хэширует его в то же значение lprnh, содержащееся в политике LocalPolicy, которую злоумышленник пытается использовать повторно. Обычно в системе существует только одно корректное число LPN (за исключением обновлений программного обеспечения, когда одновременно корректными являются два значения, чтобы обеспечить возможность возврата к старому программному обеспечению в случае сбоя обновления). При изменении любой политики LocalPolicy любой операционной системы все политики подписываются заново с помощью нового значения lprnh, соответствующего новому числу LPN, которое хранится в компоненте защищенного хранилища. Это изменение происходит при изменении пользователем настроек безопасности или создании новых операционных систем с новой политикой LocalPolicy для каждой из них.

Хэш случайного значения nonce удаленной политики (rprnh)

- *Тип:* OctetString (48)
- *Изменяемые среды:* 1TR, recoveryOS, macOS
- *Описание:* rprnh аналогично lprnh, однако оно обновляется только при обновлении удаленной политики, например при изменении состояния регистрации в Локаторе. Это изменение происходит при изменении пользователем состояния своего Mac в Локаторе.

Хэш случайного значения nonce среды recoveryOS (ronh)

- *Тип:* OctetString (48)
- *Изменяемые среды:* 1TR, recoveryOS, macOS
- *Описание:* Хэш ronh аналогичен lрnh, но он есть только в политике LocalPolicy для системной среды recoveryOS. Он обновляется вместе с системной средой recoveryOS, в том числе при обновлении программного обеспечения. Здесь используется случайное значение nonce, которое отделено от lрnh и грnh, поэтому, когда Локатор выключает устройство, существующие операционные системы можно выключить (путем удаления их LPN и RPN из компонента защищенного хранилища), одновременно оставив возможность загрузки системной среды recoveryOS. Таким образом можно повторно активировать операционные системы, когда владелец системы подтверждает получение прав контроля системы путем ввода своего пароля iCloud, используемого для доступа к учетной записи Локатора. Это изменение происходит, когда пользователь обновляет системную среду recoveryOS или создает новые операционные системы.

Хэш манифеста Image4 следующего этапа (nsih)

- *Тип:* OctetString (48)
- *Изменяемые среды:* 1TR, recoveryOS, macOS
- *Описание:* В поле *nsih* находится хэш SHA384 структуры данных манифеста Image4, которая описывает загруженную macOS. В манифесте Image4 macOS содержатся измерения для всех объектов загрузки, таких как iBoot, статический доверенный хэш, дерево устройств, загрузочная коллекция ядра и корневой хэш подписанного системного тома (SSV). Когда низкоуровневому загрузчику предписывается загрузить определенную macOS, предполагается, что он проверит, совпадает ли хэш прикрепленного к iBoot манифеста Image4 macOS с тем, который был зафиксирован в поле *nsih* политики LocalPolicy. Таким образом *nsih* фиксирует намерение пользователя, касающееся операционной системы, для которой создана политика LocalPolicy. Пользователи меняют значение *nsih* неявным образом во время обновления программного обеспечения.

Хэш политики вспомогательной коллекции ядра (AuxKC) (auxr)

- *Тип:* OctetString (48)
- *Изменяемые среды:* macOS
- *Описание:* *auxr* — это хэш SHA384 политики списка авторизованных пользователем расширений ядра (UAKL). Он используется во время создания AuxKC, способствуя тому, чтобы в AuxKC были включены только расширения ядра, авторизованные пользователем. Для настройки этого поля необходимо свойство smb2. Пользователи изменяют значение *auxr* неявным образом при изменении UAKL путем утверждения расширения ядра в диалоговом окне раздела «Системные настройки» > «Защита и безопасность».

Хэш манифеста Image4 вспомогательной коллекции ядра (AuxKC) (auxi)

- *Тип:* OctetString (48)
- *Изменяемые среды:* macOS
- *Описание:* После того как система подтвердит, что хэш UAKL соответствует тому, что указано в поле auxr политики LocalPolicy, она запрашивает подпись AuxKC у приложения процессора Secure Enclave, которое отвечает за подписание политики LocalPolicy. Затем хэш SHA384 подписи манифеста Image4 AuxKC помещается в политику LocalPolicy во избежание возможной путаницы и совпадения с подписанными ранее AuxKC в операционной системе во время ее загрузки. Если загрузчик iBoot находит поле auxi в политике LocalPolicy, он пытается загрузить AuxKC из хранилища и проверить его подпись. Он также проверяет соответствие хэша манифеста Image4, вложенного в AuxKC, значению в поле auxi. Если по какой-либо причине системе не удастся загрузить AuxKC, она продолжает загрузку без этого объекта загрузки и (как следствие) без загрузки сторонних расширений ядра. Поле auxr является обязательным для настройки поля auxi в политике LocalPolicy. Пользователи изменяют значение auxi неявным образом при изменении UAKL путем утверждения расширения ядра в диалоговом окне раздела «Системные настройки» > «Защита и безопасность».

Хэш ответа вспомогательной коллекции ядра (AuxKC) (auxr)

- *Тип:* OctetString (48)
- *Изменяемые среды:* macOS
- *Описание:* auxr — это хэш SHA384 ответа AuxKC, в котором указывается точный набор расширений ядра, которые были включены в AuxKC. Ответ AuxKC может быть поднабором UAKL, поскольку расширения ядра могут быть исключены из AuxKC, даже будучи авторизованными пользователем, если известно, что их можно использовать для атак на систему. Кроме того, некоторые расширения ядра, которые можно использовать для взлома границы между пользователем и ядром, могут привести к ограничению функционала, что выражается, например, в невозможности использовать Apple Pay или воспроизвести контент 4K/HDR. Пользователям, которым требуются такие функциональные возможности, необходимо выбрать включение AuxKC с более широким набором ограничений. Поле auxr является обязательным для настройки поля auxr в LocalPolicy. Пользователи изменяют значение auxr неявным образом при создании новой коллекции AuxKC в панели «Защита и безопасность» Системных настроек.

Хэш манифеста Image4 CustomOS (coih)

- *Тип:* OctetString (48)
- *Изменяемые среды:* 1TR
- *Описание:* coih представляет собой хэш SHA384 манифеста Image4 CustomOS. Полезная нагрузка для этого манифеста используется iBoot (вместо ядра XNU) для передачи управления. Пользователи неявно изменяют значение coih, когда используют инструмент командной строки `kmutil configure-boot` в 1TR.

UUID группы томов APFS (vuid)

- *Тип:* OctetString (16)
- *Изменяемые среды:* 1TR, recoveryOS, macOS
- *Описание:* vuid указывает на группу томов, которую ядру следует использовать в качестве корневого тома. Это поле в основном носит информативный характер, и оно не используется для ограничений безопасности. Этот vuid неявно задается пользователем при создании новой установки операционной системы.

UUID группы ключа шифрования ключа (КЕК) (kuid)

- *Тип:* OctetString (16)
- *Изменяемые среды:* 1TR, recoveryOS, macOS
- *Описание:* kuid указывает на том, который был загружен. Ключ шифрования ключей обычно используется для защиты данных. В политиках LocalPolicy он используется для защиты ключа подписания политики LocalPolicy. kuid неявно задается пользователем при создании новой установки операционной системы.

Измерение политики надежной загрузки парной среды recoveryOS (prot)

- *Тип:* OctetString (48)
- *Изменяемые среды:* 1TR, recoveryOS, macOS
- *Описание:* Измерение политики надежной загрузки (TBPM) парной среды recoveryOS — это особое итерационное вычисление хэша SHA384 на основе манифеста Image4 политики LocalPolicy без случайных значений попсе. Это вычисление выполняется для предоставления согласованного измерения с течением времени (поскольку случайные значения попсе, как и lprh, часто обновляются). Поле prot, которое содержится только в политике LocalPolicy macOS, обеспечивает создание пары для указания политики LocalPolicy recoveryOS, которая соответствует политике LocalPolicy macOS.

Наличие подписанной Secure Enclave локальной политики recoveryOS (hr1p)

- *Тип:* Логическое значение
- *Изменяемые среды:* 1TR, recoveryOS, macOS
- *Описание:* hr1p указывает, является ли значение prot (описанное ранее) измерением подписанной Secure Enclave локальной политики recoveryOS или нет. Если нет, тогда политика LocalPolicy recoveryOS подписана сервером интернет-подписания Apple, который подписывает такие объекты, как файлы Image4 macOS.

Версия локальной операционной системы (значение love)

- *Тип:* Логическое значение
- *Изменяемые среды:* 1TR, recoveryOS, macOS
- *Описание:* Значение love обозначает версию операционной системы, для которой создана политика LocalPolicy. Эта версия получена из манифеста следующего этапа во время создания политики LocalPolicy. Она используется, чтобы вводить ограничения для парных сред recoveryOS.

Безопасная мультизагрузка (smb0)

- *Тип:* Логическое значение
- *Изменяемые среды:* 1TR, recoveryOS
- *Описание:* Если свойство smb0 задано и является истинным, низкоуровневый загрузчик разрешает глобальную подпись следующего этапа манифеста Image4 вместо требования персональной подписи. Пользователи могут изменить это поле с помощью Утилиты безопасной загрузки или с помощью bputil для перехода на сниженный уровень безопасности.

Безопасная мультизагрузка (smb1)

- *Тип:* Логическое значение
- *Изменяемые среды:* 1TR
- *Описание:* Если свойство smb1 задано и является истинным, загрузчик iBoot разрешает подпись Secure Enclave для объектов загрузки, таких как настраиваемая коллекция ядра, с использованием того же ключа, что и для LocalPolicy. Наличие свойства smb0 является обязательным для наличия свойства smb1. Пользователи могут изменить это поле с помощью инструментов командной строки, таких как csrutil или bputil, для выбора режима низкого уровня безопасности.

Безопасная мультизагрузка (smb2)

- *Тип:* Логическое значение
- *Изменяемые среды:* 1TR
- *Описание:* Если свойство smb2 задано и является истинным, загрузчик iBoot разрешает подпись Secure Enclave для вспомогательной коллекции ядра с использованием того же ключа, что и для LocalPolicy. Наличие свойства smb0 является обязательным для наличия свойства smb2. Пользователи могут изменить это поле с помощью Утилиты безопасной загрузки или с помощью bputil для выбора режима сниженной безопасности и включения сторонних расширений ядра.

Безопасная мультизагрузка (smb3)

- *Тип:* Логическое значение
- *Изменяемые среды:* 1TR
- *Описание:* Если свойство smb3 задано и является истинным, пользователь устройства дал разрешение на контроль операционной системы через систему управления мобильными устройствами (MDM). Наличие этого поля предписывает приложению процессора Secure Enclave, управляющему политикой LocalPolicy, принять проверку подлинности MDM вместо требования локальной аутентификации пользователя. Пользователи могут изменить это поле с помощью Утилиты безопасной загрузки или утилиты bputil для включения управления сторонними расширениями ядра и обновлениями программного обеспечения. (В macOS 11.2 и новее MDM также позволяет инициировать обновление до новейшей версии macOS, если используется высший уровень безопасности.)

Безопасная мультизагрузка (smb4)

- *Тип:* Логическое значение
- *Изменяемые среды:* macOS
- *Описание:* Если имеется истинное значение smb4, устройство разрешает доступ к своей операционной системе через MDM с помощью Apple School Manager, Apple Business Manager или Apple Business Essentials. Наличие этого поля предписывает политике LocalPolicy, управляющей программой Secure Enclave, принять проверку подлинности MDM вместо требования локальной аутентификации пользователя. Это поле изменяется с помощью MDM, если в любой из трех служб обнаружен серийный номер устройства.

Защита целостности системы (sip0)

- *Тип:* 64-битное целое число без знака
- *Изменяемые среды:* 1TR
- *Описание:* sip0 содержит биты существующей политики защиты целостности системы (SIP), которые ранее хранились в энергонезависимой памяти. В него добавляются биты новой политики SIP (вместо использования полей политики LocalPolicy, как указано ниже), если они используются только в macOS, а не низкоуровневым загрузчиком. Пользователи могут изменить это поле с помощью утилиты csrutil из 1TR, чтобы отключить SIP и выбрать режим низкого уровня безопасности.

Защита целостности системы (sip1)

- *Тип:* Логическое значение
- *Изменяемые среды:* 1TR
- *Описание:* Если свойство sip1 задано и является истинным, загрузчик iBoot разрешает сбои при проверке корневого хэша подписанного системного тома (SSV). Пользователи могут изменить это поле с помощью csrutil или bputil из 1TR.

Защита целостности системы (sip2)

- *Тип:* Логическое значение
- *Изменяемые среды:* 1TR
- *Описание:* Если свойство sip2 задано и является истинным, загрузчик iBoot не блокирует аппаратный регистр *настраиваемой текстовой области только для чтения (CTRR)*, а аппаратный регистр помечает память ядра как не доступную для записи. Пользователи могут изменить это поле с помощью csrutil или bputil из 1TR.

Защита целостности системы (sip3)

- *Тип:* Логическое значение
- *Изменяемые среды:* 1TR
- *Описание:* Если свойство sip3 задано и является истинным, загрузчик iBoot не применяет свой встроенный список разрешений для переменной boot-args в энергонезависимой памяти, что в противном случае привело бы к фильтрации параметров, переданных ядру. Пользователи могут изменить это поле с помощью csrutil или bputil из 1TR.

Сертификаты и RemotePolicy

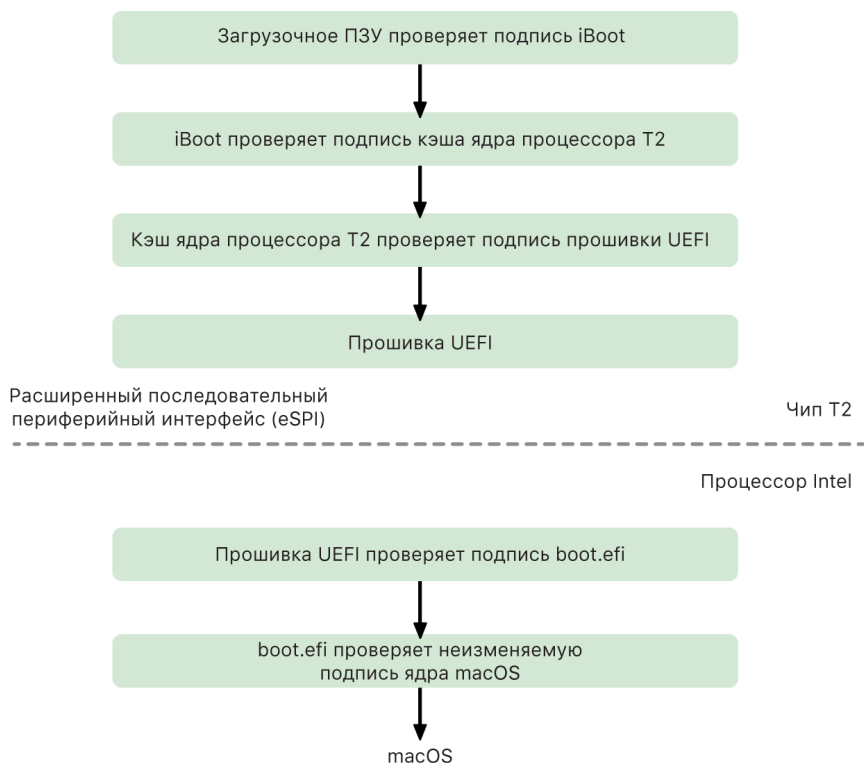
Как описано в разделе [Создание ключа подписания политики LocalPolicy и управление им](#), манифест Image4 политики LocalPolicy Image4 также содержит сертификат удостоверения владельца (OIC) и встроенную политику RemotePolicy.

Компьютеры Mac с процессором Intel

Процесс загрузки компьютера Mac с процессором Intel

Компьютеры Mac с процессором Intel и чипом безопасности Apple T2

При включении компьютера Mac с процессором Intel и чипом безопасности Apple T2 чип выполняет безопасную загрузку из своего загрузочного ПЗУ так же, как на iPhone, iPad и компьютере Mac с чипом Apple. Этот этап, на котором проверяется загрузчик iBoot, представляет собой первое звено цепочки доверия. iBoot проверяет ядро и код расширения ядра на чипе T2, который затем проверяет прошивку Intel UEFI. Прошивка UEFI и связанная подпись изначально доступны только чипу T2.



После проверки образ прошивки UEFI переносится в раздел памяти чипа T2. Доступ к памяти предоставляется процессору Intel через расширенный последовательный периферийный интерфейс (eSPI). При первой загрузке процессора Intel он извлекает прошивку UEFI через eSPI из проверенной на целостность копии прошивки, расположенной в памяти чипа T2.

Оценка цепочки доверия продолжается в процессоре Intel: прошивка UEFI оценивает подпись файла boot.efi, который является загрузчиком macOS. Подписи безопасной загрузки macOS в процессоре Intel хранятся в том же формате Image4, который используется для безопасной загрузки iOS, iPadOS и чипа T2, а для анализа файлов Image4 используется тот же защищенный код, который используется в текущей реализации безопасной загрузки iOS и iPadOS. Boot.efi в свою очередь проверяет подпись нового файла, называемого неизменяемым ядром. Если включена безопасная загрузка, файл неизменяемого ядра представляет собой полный набор расширений ядра Apple, необходимых для загрузки macOS. Действие политики безопасной загрузки завершается при переходе к неизменяемому ядру, после чего в действие вступают политики безопасности macOS (такие как защита целостности системы и подписанные расширения ядра).

Если во время этого процесса происходят какие-либо ошибки или сбои, Mac переходит в режим восстановления, режим восстановления чипа безопасности Apple T2 или режим обновления прошивки устройства (DFU) чипа безопасности Apple T2.

Microsoft Windows на компьютере Mac с процессором Intel без чипа T2

По умолчанию компьютер Mac с процессором Intel, который поддерживает безопасную загрузку, доверяет только контенту, подписанному Apple. Однако для повышения безопасности установок Boot Camp компания Apple также поддерживает безопасную загрузку для Windows. Прошивка унифицированного расширяемого интерфейса (UEFI) включает копию сертификата Microsoft Windows Production CA 2011, используемого для аутентификации загрузчиков Microsoft.

Примечание. В настоящее время Microsoft Corporation UEFI CA 2011 не считается доверенным и не позволяет подтверждать код, подписанный партнерами Microsoft. Этот сертификат UEFI CA обычно используется для проверки подлинности загрузчиков для других операционных систем, таких как различные версии Linux.

Поддержка безопасной загрузки Windows не включена по умолчанию; она включается с помощью Ассистента Boot Camp (BCA). Когда пользователь запускает BCA, происходит перенастройка macOS на доверие коду, подписанному непосредственно Microsoft, во время загрузки. Затем во время безопасной загрузки для macOS выполняется оценка доверия к коду, подписанному первой стороной. Если в результате оценки получен отрицательный ответ, прошивка UEFI пытается оценить доверие к объекту в соответствии с форматом безопасной загрузки UEFI. Если оценка доверия пройдена успешно, Mac продолжает процедуру и загружает Windows. Если нет, Mac переходит в среду recoveryOS и сообщает пользователю о том, что оценка доверия не пройдена.

Компьютеры Mac с процессором Intel без чипа T2

Компьютер Mac с процессором Intel без чипа T2 не поддерживает безопасную загрузку. Следовательно, прошивка унифицированного расширяемого интерфейса (UEFI) без проверки скачивает загрузчик macOS (boot.efi) из файловой системы, а затем загрузчик без проверки скачивает ядро (prelinkedkernel) из файловой системы. Чтобы защитить целостность последовательности загрузки, пользователи должны включить все перечисленные ниже механизмы безопасности.

- *Защита целостности системы (SIP)*. Эта функция включена по умолчанию и защищает загрузчик и ядро от вредоносных операций записи изнутри запущенной macOS.
- *FileVault*. Эту функцию может включить либо пользователь, либо администратор системы управления мобильными устройствами (MDM). Это не позволит злоумышленнику, у которого есть физический доступ к компьютеру, использовать режим внешнего диска для замены загрузчика.
- *Пароль прошивки*. Эту функцию может включить либо пользователь, либо администратор MDM. Эта мера направлена на то, чтобы не позволить злоумышленнику, у которого есть физический доступ к компьютеру, запустить другие режимы загрузки, такие как recoveryOS, однопользовательский режим или режим внешнего диска, из которых можно заменить загрузчик. Это мера также помогает предупредить загрузку с другого носителя, чтобы злоумышленник не мог запустить код для замены загрузчика.



Режимы загрузки компьютеров Mac с процессором Intel и чипом безопасности Apple T2

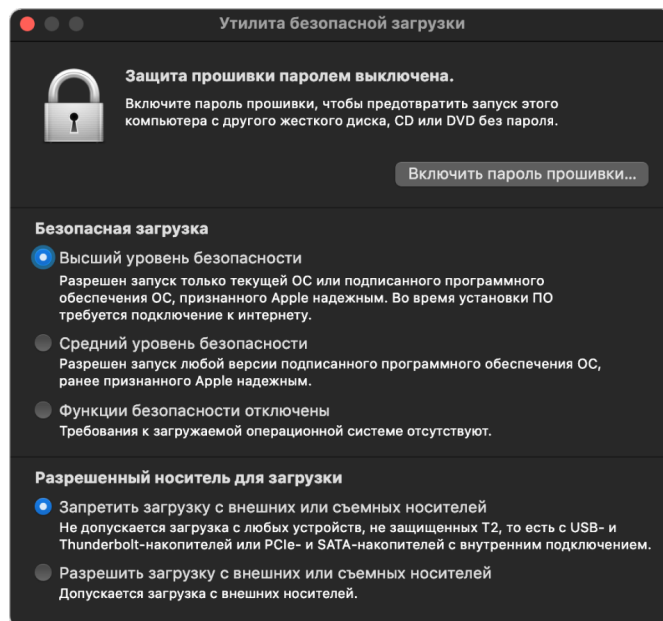
Во время загрузки компьютера Mac с процессором Intel и чипом безопасности Apple T2 компьютер можно перевести в один из режимов загрузки, нажав сочетание клавиш, распознаваемое прошивкой UEFI или загрузчиком. Некоторые режимы загрузки, например однопользовательский режим, не работают, пока в Утилите безопасной загрузки не изменена политика безопасности, то есть пока не установлен параметр «Функции безопасности отключены».

Режим	Сочетание клавиш	Описание
Загрузка macOS	Нет	Прошивка UEFI передает управление загрузчику macOS (приложению UEFI), которое передает управление ядру macOS. Если выполняется стандартная загрузка компьютера Mac с включенной функцией FileVault, загрузчик macOS отображает интерфейс входа в систему, где нужно ввести пароль, чтобы расшифровать хранилище.
Менеджер загрузки	Option (⌥)	Прошивка UEFI запускает встроенное приложение UEFI, которое отображает интерфейс выбора загрузочного устройства.
Режим внешнего диска (TDM)	T	Прошивка UEFI запускает встроенное приложение UEFI, которое предоставляет доступ к внутреннему устройству хранения в режиме неформатированного блочного устройства хранения через FireWire, Thunderbolt, USB или любое их сочетание (в зависимости от модели Mac).
Однопользовательский режим	Command (⌘)-S	Ядро macOS передает флаг <code>-s</code> в векторе аргументов <code>launchd</code> , затем <code>launchd</code> создает однопользовательскую оболочку в tty приложения «Консоль». <i>Примечание.</i> Если пользователь выходит из оболочки, macOS продолжает загрузку и отображает окно входа.
recoveryOS	Command (⌘)-R	Прошивка UEFI загружает минимальную версию macOS из файла подписанного образа диска (.dmg) на внутреннем устройстве хранения.
recoveryOS из интернета	Option (⌥)-Command (⌘)-R	Подписанный образ диска загружается из интернета по протоколу HTTP.
Диагностика	D	Прошивка UEFI загружает минимальную диагностическую среду UEFI из файла подписанного образа диска на внутреннем устройстве хранения.
Диагностика через интернет	Option (⌥)-D	Подписанный образ диска загружается из интернета по протоколу HTTP.
Загрузка Windows	Нет	Если операционная система Windows была установлена с помощью Boot Camp, прошивка UEFI передает управление загрузчику Windows, который передает управление ядру Windows.

Утилита безопасной загрузки на компьютере Mac с чипом безопасности Apple T2

Обзор

На компьютере Mac с процессором Intel и чипом безопасности Apple T2 Утилита безопасной загрузки управляет рядом параметров политики безопасности. Для доступа к утилите необходимо выполнить загрузку в режиме recoveryOS и выбрать Утилиту безопасной загрузки в меню «Утилиты». Утилита защищает поддерживаемые параметры безопасности, усложняя манипуляции с ними со стороны злоумышленника.



Для внесения критически важных изменений в политику безопасности требуется аутентификация — даже в режиме восстановления. При первом открытии Утилиты безопасной загрузки она запрашивает у пользователя пароль администратора для основной установки macOS, которая связана с текущей загруженной версией recoveryOS. Если администратора не существует, сначала необходимо его создать, и только затем можно будет изменить политику. Для изменения политики чипу T2 требуется, чтобы на компьютере Mac была загружена среда recoveryOS и чтобы была пройдена аутентификация с использованием учетных данных, которые защищены Secure Enclave. Для изменения политики безопасности необходимо соблюдение двух неявных требований. recoveryOS:

- Должна быть загружена с устройства хранения, напрямую подключенного к чипу T2, поскольку разделы на других устройствах не имеют учетных данных, которые защищены Secure Enclave и привязаны к внутреннему устройству хранения.
- Должна находиться на томе APFS, поскольку поддерживается хранение только учетных данных аутентификации в режиме восстановления, отправленных в Secure Enclave на предзагрузочном томе APFS на диске. Тома в формате HFS+ не могут использовать безопасную загрузку.

Эта политика отображается только в Утилите безопасной загрузки на компьютерах Mac с процессором Intel и чипом T2. В большинстве случаев изменять политику безопасной загрузки не требуется, однако окончательное решение по настройке своих устройств остается за пользователями. Они могут выключить функцию безопасной загрузки на своем Mac в зависимости от своих потребностей или снять часть ограничений, действующих в отношении данной функции.

Изменения политики безопасной загрузки, внесенные в этом приложении, применяются только к оценке цепочки доверия, проверяемой процессором Intel. Параметр безопасной загрузки чипа T2 отключить невозможно.

Для политики безопасной загрузки можно установить один из трех вариантов: «Высший уровень безопасности», «Средний уровень безопасности» и «Функции безопасности отключены». Если выбран вариант «Функции безопасности отключены», процессор Intel не выполняет оценку безопасной загрузки, и пользователь может загружать все, что он хочет.

Политика загрузки «Высший уровень безопасности»

Высший уровень безопасности — это политика загрузки по умолчанию, которая во многом похожа на механизм работы iOS и iPadOS или на высший уровень безопасности на компьютере Mac с чипом Apple. При загрузке и подготовке к установке такого программного обеспечения оно «персонализируется» с помощью подписи, чей запрос на подписание содержит универсальный идентификатор чипа (ECID), то есть идентификатор чипа T2 в данном случае. В этом случае подпись, возвращаемая сервером подписания, является уникальной и может использоваться только этим конкретным чипом T2. Прошивка унифицированного расширяемого интерфейса (UEFI) проверяет, что при использовании высшего уровня безопасности подпись не просто предоставлена Apple, а предназначена для этого конкретного Mac, то есть что эта версия macOS привязана к этому Mac. Это помогает предупредить атаки методом отката, как описано в разделе, посвященном высшему уровню безопасности на компьютере Mac с чипом Apple.

Политика загрузки «Средний уровень безопасности»

Политика загрузки «Средний уровень безопасности» в некоторой степени похожа на традиционную безопасную загрузку UEFI, когда поставщик (в данном случае Apple) генерирует цифровую подпись для кода, чтобы подтвердить, что он получен от поставщика. Это не позволяет злоумышленникам вставить неподписанный код. Мы называем эту подпись «глобальной», поскольку ее можно использовать на любом компьютере Mac в течение любого периода времени, если в настоящее время на компьютере установлена политика «Средний уровень безопасности». iOS, iPadOS и сам чип T2 не поддерживают глобальные подписи. При такой настройке не предпринимается никаких действий для предотвращения атак методом отката.

Политика загрузки с носителя

Политика загрузки с носителя существует только на компьютере Mac с процессором Intel и чипом T2 и не зависит от политики безопасной загрузки. Даже если пользователь отключает безопасную загрузку, это не влияет на заданный по умолчанию запрет Mac загрузки с любого устройства, кроме устройства хранения, напрямую подключенного к чипу T2. (Политика загрузки с носителя не требуется на компьютере Mac с чипом Apple.) См. раздел [Управление политикой безопасности Загрузочного диска](#).

Защита пароля прошивки на компьютере Mac с процессором Intel

macOS на компьютерах Mac с процессором Intel и чипом безопасности Apple T2 поддерживает использование пароля прошивки, что помогает предотвратить непреднамеренное изменение настроек прошивки на определенных компьютерах Mac. Пароль прошивки был создан для того, чтобы препятствовать выбору других режимов загрузки, таких как загрузка в режиме recoveryOS или однопользовательском режиме, загрузка из неразрешенного тома или загрузка в режиме внешнего диска.

Примечание. Пароль прошивки не требуется на компьютере Mac с чипом Apple, поскольку критически важные функциональные возможности прошивки перемещены в recoveryOS, в которой для доступа к критически важным функциям требуется аутентификация пользователя (если включена функция FileVault).

Базовый режим использования пароля прошивки доступен из Утилиты пароля прошивки в recoveryOS на компьютере Mac с процессором Intel без чипа T2 и из Утилиты безопасной загрузки на компьютере Mac с процессором Intel и чипом T2. Расширенные параметры (например запрос пароля при каждой загрузке) доступны через инструмент командной строки `firmwarepasswd` в macOS.

Установка пароля прошивки особенно важна для снижения риска атак на компьютеры Mac с процессором Intel без чипа T2, совершаемых при наличии физического доступа к компьютеру. Пароль прошивки может помешать злоумышленнику выполнить загрузку среды recoveryOS, чтобы иным способом выключить защиту целостности системы (SIP). А благодаря ограничению загрузки с других носителей злоумышленник не может запускать исполнение привилегированного кода из другой операционной системы для атаки на прошивки периферийных устройств.

Для помощи пользователям, которые забыли свой пароль, предусмотрен механизм сброса пароля прошивки. При загрузке требуется нажать особое сочетание клавиш, после чего будет показана уникальная для данной модели строка, которую нужно сообщить в AppleCare. AppleCare подписывает ресурс цифровой подписью, которая проверяется с помощью универсального идентификатора ресурса (URI). Если подпись подтверждена и содержимое относится к конкретному Mac, прошивка UEFI снимает пароль прошивки.

Если пользователь не хочет, чтобы кто-то другой мог программными средствами удалить его пароль прошивки, он может использовать параметр `-disable-reset-sarability` в инструменте командной строки `firmwarepasswd` в macOS 10.15. Перед установкой этого параметра пользователь должен подтвердить, что в случае, если он забудет пароль и потребуются удаление пароля, пользователь должен будет оплатить замену материнской платы, которая необходима для достижения этой цели. Если организация хочет защитить свои компьютеры Mac от злоумышленников и сотрудников, она должна установить пароль прошивки в принадлежащих ей системах. Это можно сделать на устройстве любым из следующих способов:

- вручную во время подготовки, используя инструмент командной строки `firmwarepasswd`;
- с помощью сторонних инструментов управления, которые используют инструмент командной строки `firmwarepasswd`;
- с помощью системы управления мобильными устройствами (MDM).

Среды recoveryOS и диагностики для компьютера Mac с процессором Intel

recoveryOS

Операционная система восстановления recoveryOS полностью отделена от основной macOS, и все ее содержимое хранится в файле образа диска с именем BaseSystem.dmg. Также имеется связанный с ним файл BaseSystem.chunklist, который используется для проверки целостности BaseSystem.dmg. Список фрагментов .chunklist представляет собой серию хэшей для 10-мегабайтных фрагментов BaseSystem.dmg. Прошивка унифицированного расширяемого интерфейса (UEFI) оценивает подпись файла списка фрагментов, а затем поочередно оценивает хэши фрагментов из файла BaseSystem.dmg, помогая убедиться, что они соответствуют подписанному содержимому списка фрагментов. Если один из хэшей не совпадает, загрузка из локальной среды recoveryOS прерывается и прошивка UEFI пытается выполнить загрузку из recoveryOS в интернете.

Если проверка пройдена успешно, прошивка UEFI подключает BaseSystem.dmg в качестве диска оперативной памяти и запускает содержащийся в нем файл boot.efi. Прошивке UEFI не нужно проверять boot.efi, а boot.efi не нужно проверять ядро, поскольку целостность всего содержимого операционной системы уже была проверена, а эти элементы составляют только ее часть.

Диагностика Apple

Процедура загрузки локальной диагностической среды в основном аналогична запуску recoveryOS. При этом используются отдельные файлы AppleDiagnostics.dmg и AppleDiagnostics.chunklist, однако их проверка выполняется так же, как и проверка файлов BaseSystem. Вместо запуска boot.efi прошивка UEFI запускает из образа диска (.dmg) файл с именем diags.efi, который отвечает за вызов ряда других драйверов UEFI, которые могут устанавливать соединение с оборудованием и проверять его на наличие ошибок.

Среды recoveryOS и среды диагностики, загружаемые из интернета

Если при запуске локальной среды восстановления или диагностики произошла ошибка, прошивка UEFI пытается загрузить образы из интернета. (Пользователь также может запросить загрузку образов из интернета, нажав при загрузке особое сочетание клавиш.) Проверка целостности образов диска и списков фрагментов, загруженных с сервера восстановления операционной системы, выполняется таким же способом, как для образов, извлеченных с устройства хранения.

Поскольку подключение к серверу восстановления операционной системы выполняется по протоколу HTTP, все полностью загруженные данные проверяются на целостность (как описано ранее). Таким образом они защищаются от манипуляций, если злоумышленник контролирует сеть. Если отдельный фрагмент не проходит проверку целостности, система запрашивает его 11 раз у сервера восстановления операционной системы, прежде чем прекратить попытки и выдать ошибку.

После того как в 2011 году на компьютеры Mac были добавлены режимы восстановления и диагностики, загружаемые из интернета, было принято решение использовать более простой транспортный протокол HTTP и использовать для аутентификации содержимого механизм списка фрагментов вместо реализации в прошивке UEFI более сложного транспорта HTTPS, что повышает уязвимость прошивки.

Безопасность подписанного системного тома в iOS, iPadOS и macOS

В macOS 10.15 компания Apple представила системный том только для чтения. Он изолирован и предназначен исключительно для содержимого системы. В macOS 11 и новее добавлены надежные средства криптографической защиты содержимого системы посредством *подписанного системного тома (SSV)*. SSV содержит механизм ядра, который проверяет целостность содержимого системы во время выполнения и отклоняет любые данные (код и некодовые данные) без действительной криптографической подписи Apple. Начиная с iOS 15 и iPadOS 15 системный том на устройствах iOS и iPadOS также имеет средства криптографической защиты подписанного системного тома.

SSV не только помогает предотвратить вмешательство в какое-либо программное обеспечение Apple, входящее в состав операционной системы, но также делает обновление программного обеспечения macOS более надежным и безопасным. И поскольку SSV использует снимки файловой системы Apple, то есть APFS (Apple File System), старую версию системы можно восстановить без переустановки, если обновление выполнить невозможно.

С момента своего внедрения APFS обеспечивает целостность метаданных файловой системы с помощью некриптографических контрольных сумм на внутреннем устройстве хранения. SSV позволяет усилить механизм обеспечения целостности путем использования криптографических хэшей, тем самым распространяя действие механизма на каждый бит данных файлов. Данные на внутреннем устройстве хранения (включая метаданные файловой системы) хэшируются криптографическим способом в пути чтения, после чего хэш сравнивается с ожидаемым значением в метаданных файловой системы. Если значения не совпадают, система делает вывод, что данные были изменены, и не возвращает их запросившей программе.

Каждый хэш SHA256 SSV хранится в основном дереве метаданных системы, которое хэшировано само. Поскольку каждый узел дерева рекурсивно проверяет целостность хэшей своих дочерних элементов, аналогично двоичному хэш-дереву (дереву Меркла), значение хэша корневого узла (называемое *печатью*) применяется к каждому биту данных на томе SSV. Это означает, что криптографическая подпись распространяется на весь системный том.

Во время установки и обновления macOS эта печать вычисляется заново для файловой системы на устройстве, а полученное измерение сравнивается с измерением, подписанным Apple. На компьютере Mac с чипом Apple загрузчик проверяет печать, прежде чем передать управление ядру. На компьютере Mac с процессором Intel и чипом безопасности Apple T2 загрузчик перенаправляет измерение и подпись в ядро, которое затем проверяет печать напрямую, прежде чем подключать корневую файловую систему. В обоих случаях при сбое проверки процесс загрузки останавливается и пользователю предлагается переустановить macOS. Эта процедура повторяется при каждой загрузке до тех пор, пока пользователь не выберет загрузку с применением политики безопасности более низкого уровня и не решит выключить подписанный системный том.

Во время обновления программного обеспечения iOS и iPadOS системный том схожим образом подготавливается и вычисляется заново. Перед тем как разрешить устройству запустить ядро, загрузчики iOS и iPadOS проверяют, что печать не повреждена и что она соответствует значению, подписанному Apple. Если при загрузке выявлены несоответствия, пользователь получает запрос на обновление системного программного обеспечения на устройстве. Пользователям не разрешено снимать защиту подписанного системного тома в iOS и iPadOS.

SSV и подпись кода

Ядро по-прежнему выполняет принудительное подписание кода. Подписанный системный том обеспечивает защиту во время чтения любого количества байтов с внутреннего устройства хранения, тогда как подпись кода обеспечивает защиту во время сопоставления памятью объектов Mach как исполняемых. Как SSV, так и подпись кода служат для защиты исполняемого кода во всех путях чтения и выполнения.

SSV и FileVault

В macOS 11 аналогичная защита содержимого системы во время хранения обеспечивается с помощью SSV, поэтому шифрование системного тома больше не требуется. Любые изменения, внесенные в файловую систему во время хранения, будут обнаружены файловой системой в процессе чтения данных. Если пользователь включил FileVault, содержимое пользователя на томе данных по-прежнему шифруется с помощью предоставленного пользователем секрета.

Если пользователь решит отключить SSV, система станет уязвимой для вмешательства во время хранения, и в результате такого вмешательства злоумышленник может извлечь зашифрованные данные пользователя при следующей загрузке системы. Поэтому система не позволит пользователю отключить SSV, если включена функция FileVault. Защиту данных во время хранения следует включать или отключать для обоих томов единообразно.

В macOS 10.15 и более ранних версиях функция FileVault служит для защиты операционной системы во время хранения путем шифрования пользовательского и системного содержимого с помощью ключа, защищенного предоставленным пользователем секретом. Таким образом обеспечивается защита от получения доступа к файловой системе с системным программным обеспечением или управления ею, если у злоумышленника есть физический доступ к устройству.

SSV и компьютер Mac с чипом безопасности Apple T2

На компьютере Mac с чипом безопасности Apple T2 с помощью SSV защищена только сама операционная система macOS. Программное обеспечение, которое выполняется на чипе T2 и проверяет macOS, защищено с помощью безопасной загрузки.

Безопасное обновление программного обеспечения

Безопасность требует постоянных усилий. Недостаточно просто обеспечить безопасную загрузку версии операционной системы, установленной на заводе. Также должен существовать механизм для быстрого и безопасного получения новейших обновлений безопасности. Apple регулярно выпускает обновления программного обеспечения в ответ на возникающие проблемы безопасности. Пользователи iOS и iPadOS получают уведомления о наличии обновлений прямо на устройстве. На Mac обновления доступны в Системных настройках. Обновления передаются по беспроводной сети, что ускоряет внедрение новейших исправлений, связанных с безопасностью.

Процесс обновления

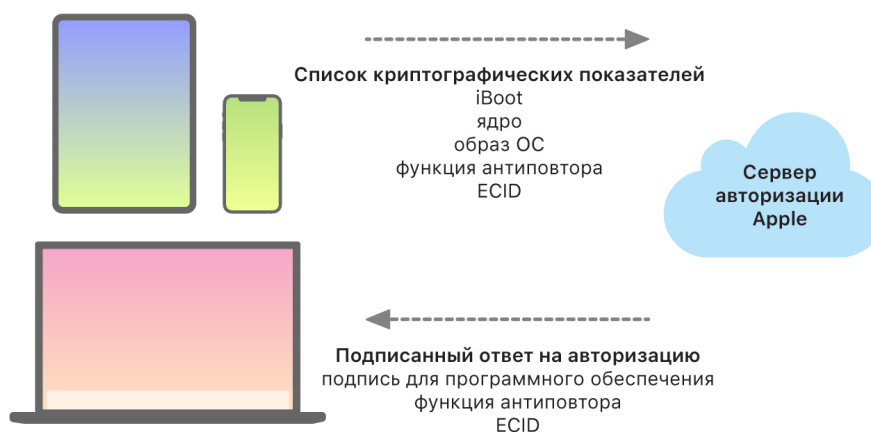
В процессе обновления используется тот же аппаратный корень доверия, что и используется при безопасной загрузке. Это помогает гарантировать, что устанавливается только код, подписанный Apple. Авторизация системного программного обеспечения во время обновления выполняет проверку, чтобы на устройствах iOS и iPadOS или на компьютерах Mac, на которых в Утилите безопасной загрузки выбрана политика безопасной загрузки «Высший уровень безопасности», можно было установить только копии операционных систем, специально подписанные Apple. Благодаря этим мерам предосторожности Apple может прекратить подписание более ранних версий операционных систем с известными уязвимостями и тем самым помочь предотвратить атаки через понижение версии.

Кроме того, для более надежной защиты во время обновления программного обеспечения при физическом подключении обновляемого устройства к компьютеру Mac загружается и устанавливается полная копия iOS или iPadOS. А при беспроводном обновлении загружаются *только те компоненты, которые необходимы для обновления системы*: тем самым оптимизируется расход трафика, так как не требуется загружать всю операционную систему. Кроме того, обновления ПО могут кэшироваться на компьютере Mac под управлением macOS 10.13 и новее с включенной функцией «Кэширование контента», чтобы устройствам iOS и iPadOS не пришлось заново загружать необходимые обновления из интернета. (Для завершения процесса обновления им по-прежнему нужно связаться с серверами Apple.)

Персонализированный процесс обновления

При обновлении устанавливается соединение с сервером авторизации установки Apple, которое включает список криптографических показателей для каждой части установочного пакета, которую предстоит установить (например, iBoot, ядро, образ ОС), случайное значение (nonce) для функции антиповтора и уникальный идентификатор устройства (ECID).

Сервер авторизации сверяет полученные измерения с версиями, установка которых разрешена. Если соответствие найдено, сервер добавляет ECID к измерениям и подписывает результат. В процессе обновления сервер передает на устройство полный комплект подписанных данных. Добавление ECID необходимо, чтобы сделать авторизацию запрашивающего устройства уникальной. Авторизация и подписание только при наличии установленных измерений помогают серверу гарантировать, что обновление будет происходить именно так, как предусмотрено Apple.



Проверка цепочки доверия в момент загрузки позволяет убедиться, что подпись получена от Apple, а значения измерений объекта, загруженного с устройства хранения, в сочетании с ECID устройства, совпадают с теми, на которые распространяется подпись. Все эти этапы направлены на то, чтобы убедиться, что на устройствах, поддерживающих функции персонализации, авторизация выполняется для данного конкретного устройства и что более старую версию операционной системы на одном из устройств не получится скопировать на другое устройство. Значение nonce способствует тому, чтобы злоумышленник не мог сохранить ответ сервера и использовать его для взлома устройства или изменения системного ПО иным образом.

Именно из-за процесса персонализации для обновления любого устройства с чипом Apple, включая компьютер Mac с процессором Intel и чипом безопасности Apple T2, требуется сетевое подключение к серверам Apple.

Наконец, том с пользовательскими данными отключается на время обновления программного обеспечения. Это помогает предотвратить чтение или запись каких-либо данных с этого тома во время обновления.

На устройствах с Secure Enclave этот аппаратный компонент аналогичным образом использует авторизацию системного ПО для проверки целостности своего программного обеспечения. Эта мера способствует защите от возврата к предыдущим версиям.

Целостность операционной системы

В основу операционных систем Apple заложены функции обеспечения безопасности. Аппаратный корень доверия используется для обеспечения безопасной загрузки, а процесс безопасного обновления ПО делает возможным быстрое и безопасное обновление системы безопасности. Операционные системы Apple также используют специальные аппаратные возможности чипа, что способствует предупреждению использования уязвимостей во время работы системы. Эти функции среды выполнения защищают целостность доверенного кода во время его выполнения. Если пояснять вкратце, операционная система Apple помогает смягчить последствия атак и использования уязвимостей независимо от того, исходят ли они от вредоносного приложения, из интернета или любого другого канала. Перечисленные здесь средства защиты доступны на устройствах с поддерживаемыми системами на кристалле, разработанными компанией Apple, включая iOS, iPadOS, tvOS, watchOS, а теперь и macOS на компьютере Mac с чипом Apple.

Функция	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	Семейство M1
Защита целостности ядра	✓	✓	✓	✓	✓	✓
Быстрые ограничения разрешений		✓	✓	✓	✓	✓
Защита целостности системного сопроцессора			✓	✓	✓	✓
Коды аутентификации указателя			✓	✓	✓	✓
Уровень защиты страниц		✓	✓	✓	✓	См. примечание ниже.

Примечание. Уровень защиты страниц (PPL) требует, чтобы платформа исполняла только подписанный и надежный код. Эта модель безопасности не применяется в macOS.

Защита целостности ядра

После завершения инициализации ядра операционной системы включается функция защиты целостности ядра (KIP), которая предотвращает внесение изменений в ядро и код драйвера. Контроллер памяти предоставляет защищенный регион физической памяти, который используется iBoot для загрузки ядра и расширений ядра. После завершения загрузки контроллер памяти отклоняет все запросы записи в защищенный регион физической памяти. Диспетчер памяти (MMU) процессора приложений настроен, чтобы способствовать предотвращению сопоставления привилегированного кода из физической памяти за пределами защищенного региона, а также чтобы способствовать предотвращению доступных для записи сопоставлений физической памяти внутри региона памяти ядра.

Чтобы предотвратить возможность перенастройки, оборудование, используемое для работы KIP, блокируется после завершения процесса загрузки.

Быстрые ограничения разрешений

В системах на кристалле Apple A11 Bionic и S3 был представлен новый аппаратный примитив. Этот примитив — быстрые ограничения разрешений — включает реестр ЦП для быстрого ограничения разрешений на уровне потока. Используя быстрые ограничения разрешений (также известные как регистры APRR), поддерживаемые операционные системы могут удалять из памяти разрешения на выполнение, не тратя время на системный вызов и проход по таблице страниц или ее сброс. Эти регистры обеспечивают дополнительный уровень защиты от сетевых атак, в частности компилируемых во время выполнения (точно в нужный момент), поскольку память не позволяет исполнять код в то время, когда происходит чтение или запись.

Защита целостности системного сопроцессора

Прошивка сопроцессоров, таких как Secure Enclave, процессор датчика изображений и сопроцессор движения, выполняет многие критически важные системные задачи. Поэтому ее безопасность имеет решающее значение для безопасности всей системы. Чтобы предотвратить изменение прошивки сопроцессора, Apple использует механизм, называемый *защитой целостности системного сопроцессора (SCIP)*.

Работа SCIP во многом похожа на работу функции защиты целостности ядра (KIP). Во время загрузки iBoot загружает прошивку каждого сопроцессора в защищенный регион памяти, который зарезервирован для этого сопроцессора и отделен от региона KIP. iBoot настраивает диспетчеры памяти каждого сопроцессора, чтобы помочь предотвращать следующие события:

- исполняемые сопоставления за пределами выделенной части защищенного региона памяти;
- доступные для записи сопоставления внутри выделенной части защищенного региона памяти.

Кроме того, операционная система Secure Enclave настраивает защиту целостности системного сопроцессора для Secure Enclave во время загрузки. После завершения процесса загрузки оборудование, используемое для работы SCIP, блокируется. Эта мера направлена на то, чтобы предотвратить возможность перенастройки.

Коды аутентификации указателя

Коды аутентификации указателя (PAC) используются для защиты от атак, связанных с использованием повреждения памяти. Системное программное обеспечение и встроенные приложения используют PAC, что помогает предотвращать изменения указателей функций и адресов возвратов (указателей кода). PAC использует пять секретных 128-битных значений для подписания инструкций и данных ядра, а каждый процесс пользовательского пространства имеет свои собственные ключи. К объектам добавляется случайное значение («соль») и подпись, как указано в таблице ниже.

Элемент	Ключ	Соль
Адрес возврата функции	IB	Адрес хранилища
Указатели функции	IA	0
Функция вызова блока	IA	Адрес хранилища
Кэш метода Objective-C	IB	Адрес хранилища + класс + вариант
Записи таблицы виртуальных методов C++	IA	Адрес хранилища + хэш (искаженное имя метода)
Вычисленная метка перехода	IA	Хэш (имя функции)
Состояние потока ядра	GA	.
Регистры состояния пользовательского потока	IA	Адрес хранилища
Указатели таблицы виртуальных методов C++	DA	0

Значение подписи хранится в неиспользуемых битах дополнения в верхних разрядах 64-битного указателя. Перед использованием указателя выполняется проверка подписи и восстановление битов дополнения. Это помогает убедиться, что указатель указывает на действительный адрес. В случае неудачной проверки действие прерывается. Такая проверка увеличивает сложность проведения многих атак, например, атаки методом возвратно-ориентированного программирования (ROP), при которой злоумышленник пытается обманным образом вынудить устройство выполнить существующий вредоносный код, манипулируя адресами возвратов функций в стеке.

Уровень защиты страниц

Уровень защиты страниц (PPL) в iOS, iPadOS и watchOS разработан для того, чтобы предупредить изменение кода в пользовательском пространстве после завершения проверки подписи кода. Уровень защиты страниц (PPL), в основе которого лежит защита целостности ядра и быстрые ограничения разрешений, управляет переопределениями разрешений таблицы страниц, гарантируя, что только PPL может изменять защищенные страницы, содержащие код пользователя и таблицы страниц. Система значительно сокращает уязвимую область, помогая обеспечить целостность кода в масштабе всей системы даже в условиях взлома ядра. Этого средства защиты нет в macOS, поскольку PPL применим только в системах, требующих подписания абсолютно всего исполняемого кода.

Дополнительные функции безопасности системы в macOS

Дополнительные функции безопасности системы в macOS

Диапазон устройств, на которых работает macOS, шире (например, устройства с процессорами Intel, или устройства с процессорами Intel в сочетании с чипом безопасности Apple T2 и устройства с системами на кристалле Apple). Кроме того, macOS поддерживает целый ряд универсальных сценариев использования компьютеров. Одним пользователям вполне достаточно основных предустановленных приложений и приложений из App Store, в то время как другим нужно вмешаться в работу ядра и выключить практически все средства защиты платформы, чтобы запускать и тестировать свой код как при наивысшем уровне доверия. Большинство пользователей находятся где-то посередине, и у многих из них есть периферийные устройства и программное обеспечение, требующие различных уровней доступа. При разработке платформы macOS компания Apple применила интегрированный подход к оборудованию, программному обеспечению и службам, который изначально ориентирован на обеспечение безопасности и упрощает настройку, развертывание и управление, но сохраняет необходимые пользователю возможности настройки. macOS также включает ключевые технологии безопасности, которые используют ИТ-специалисты для защиты корпоративных данных и интеграции в безопасные корпоративные сетевые среды.

Перечисленные ниже функции помогают безопасным образом удовлетворить различные потребности пользователей macOS. Функции безопасности:

- Безопасность подписанного системного тома
- Защита целостности системы
- Доверенные кэши
- Защита периферийных устройств
- Поддержка и безопасность Rosetta 2 (автоматическое преобразование) для компьютеров Mac с чипом Apple
- Поддержка и средства защиты прямого доступа к памяти (DMA)
- Поддержка и безопасность расширений ядра
- Поддержка и безопасность дополнительных ПЗУ
- Безопасность прошивки UEFI для компьютеров Mac с процессором Intel

Защита целостности системы

Функция *защиты целостности системы (SIP)* в macOS использует разрешения ядра для ограничения возможности записи в критически важные системные файлы. Это отдельная функция, и она дополняет функцию аппаратной защиты целостности ядра (KIP), доступную на компьютере Mac с чипом Apple, которая защищает от изменения ядра в памяти. Для предоставления этого средства защиты и ряда других на уровне ядра, включая песочницу и Data Vault, используются обязательные средства контроля доступа.

Обязательные средства контроля доступа

В macOS используются обязательные средства контроля доступа — заданные разработчиком политики безопасности, которые устанавливают определенные ограничения и которые нельзя обойти. Этот подход отличается от инициативного контроля доступа, при котором пользователь может переопределять политики безопасности по своему желанию.

Обязательные средства контроля доступа не видны пользователям, но являются базовой технологией, которая помогает реализовать несколько важных функций, включая песочницу, родительский контроль, управляемые настройки, расширения и защиту целостности системы.

Защита целостности системы

Защита целостности системы разрешает только чтение компонентов в определенных критических местах файловой системы, что помогает предотвратить их изменение вредоносным кодом. Защита целостности системы — это настройка компьютера, которая включается по умолчанию при обновлении до OS X 10.11 и новее. Отключение этой функции на компьютерах Mac с процессором Intel приводит к снятию защиты со всех разделов физического устройства хранения. macOS применяет эту политику безопасности ко всем процессам в системе, независимо от того, выполняются ли они в песочнице или с правами администратора.

Доверенные кэши

Одним из объектов, включенных в последовательность безопасной загрузки, является статический доверенный кэш. Это доверенная запись всех двоичных файлов Mach-O, которые размещены на подписанном системном томе. Каждый файл Mach-O представлен хэшем каталога кода. Перед вставкой в доверенный кэш выполняется сортировка хэшей для обеспечения эффективного поиска. Каталог кода является результатом подписания, выполненного `codesign(1)`. Для применения доверенного кэша необходимо, чтобы защита целостности системы (SIP) оставалась включена. Для отключения применения доверенного кэша на Mac с чипом Apple требуется настроить безопасную загрузку, установив низкий уровень безопасности.

При исполнении двоичного файла (в ходе создания нового процесса или сопоставления исполняемого кода с существующим процессом) его каталог кода извлекается и хэшируется. Если полученный хэш будет найден в доверенном кэше, то исполняемым сопоставлениям, созданным для двоичного файла, будут предоставлены полномочия платформы, то есть они могут обладать любыми правами и выполняться без дальнейшей проверки подлинности подписи. В этом состоит отличие от компьютера Mac с процессором Intel, где полномочия платформы передаются содержимому операционной системы с помощью сертификата Apple, который подписывает двоичные файлы. (Этот сертификат не ограничивает перечень прав, которыми может обладать двоичный файл.)

Для исполнения неплатформенных двоичных файлов (в том числе заверенного стороннего кода) у них должны быть действительные цепочки сертификатов, а права, которыми они могут обладать, ограничены профилем подписи, выданным разработчику в рамках программы Apple Developer Program.

Все двоичные файлы, поставляемые с macOS, подписаны с помощью *идентификатора платформы*. На компьютере Mac с чипом Apple этот идентификатор указывает, что, даже если двоичный файл подписан Apple, для исполнения такого файла его хэш каталога кода должен находиться в доверенном кэше. На компьютере Mac с процессором Intel идентификатор платформы используется для целевого отзыва конкретных двоичных файлов из более старой версии macOS. Этот целевой отзыв помогает предотвратить исполнение этих двоичных файлов в более новых версиях.

Статический доверенный кэш привязывает набор двоичных файлов к заданной версии macOS. Это помогает предотвратить перенос двоичных файлов, имеющих законную подпись Apple, из старых операционных систем в новые, чтобы злоумышленник не мог этим воспользоваться.

Код платформы, поставляемый вне операционной системы

Некоторые двоичные файлы от Apple, такие как для Xcode и стека инструментов разработчика, не подписаны с использованием идентификатора платформы. Несмотря на это, они могут исполняться с полномочиями платформы на компьютере Mac с чипом Apple и компьютере Mac с чипом Apple T2. Поскольку это программное обеспечение платформы поставляется независимо от macOS, на него не действует процедура отзыва, связанная со статическим доверенным кэшем.

Загружаемые доверенные кэши

Определенные программные пакеты Apple поставляются с *загружаемыми доверенными кэшами*. У этих кэшей такая же структура данных, как у статического доверенного кэша. При этом есть только один статический доверенный кэш, и после завершения ранней инициализации ядра содержимое этого кэша гарантированно находится в диапазонах памяти, доступных только для чтения, а загружаемые доверенные кэши добавляются в систему во время выполнения.

Эти доверенные кэши проходят аутентификацию либо с помощью того же механизма, который аутентифицирует загрузочную прошивку (персонализация с помощью службы доверенной подписи Apple), либо как объекты с глобальной подписью (такие подписи не привязывают их к конкретному устройству).

Примером персонализированного доверенного кэша может служить кэш, который поставляется с образом диска для выездной диагностики компьютера Mac с чипом Apple. Этот доверенный кэш персонализируется вместе с образом диска и загружается в ядро компьютера Mac, когда тот загружается в режиме диагностики. Благодаря этому доверенному кэшу программное обеспечение из образа диска может запускаться с полномочиями платформы.

Доверенный кэш с глобальной подписью поставляется, например, с обновлениями программного обеспечения macOS. Благодаря этому доверенному кэшу определенный фрагмент кода в обновлении программного обеспечения — *управляющий модуль обновления* — может запускаться с полномочиями платформы. Управляющий модуль обновления выполняет любые действия по обновлению программного обеспечения, которые операционная система не может выполнить согласованно в разных версиях.

Безопасность периферийных процессоров на компьютерах Mac

Все современные компьютерные системы оснащаются множеством встроенных периферийных процессоров, которые предназначены для таких задач, как подключение к сети, работа с графикой, управление питанием или управление шинами данных. Эти периферийные процессоры часто имеют узкое назначение и гораздо меньшую мощность, чем у основного ЦП. Встроенные периферийные устройства, не имеющие достаточных средств защиты, становятся мишенью для злоумышленников, которые ищут легкие способы заражать операционную систему. Заразив прошивку периферийного процессора, злоумышленник может атаковать программное обеспечение в главном процессоре или напрямую перехватить конфиденциальные данные (например, устройство Ethernet может видеть содержимое незашифрованных пакетов).

По возможности Apple ведет работу по уменьшению количества необходимых периферийных процессоров и стремится не использовать структуры, для которых требуется прошивка. А если использование отдельных процессоров с собственной прошивкой является обязательным, принимаются меры, направленные на то, чтобы не позволить злоумышленнику удержаться в этом процессоре. Это обеспечивается одним из двух способов:

- процессор запускается, чтобы загрузить проверенную прошивку из основного процессора при запуске;
- периферийный процессор реализует собственную безопасную последовательность загрузки, проверяя свою прошивку при каждой загрузке Mac.

Apple проверяет реализации сторонних поставщиков и улучшает их решения, следя за тем, чтобы те обладали требуемыми свойствами, например:

- обеспечение максимальной криптографической стойкости;
- отказ от использования прошивок с известными недостатками;
- отключение интерфейсов отладки;
- подписание прошивки с помощью криптографических ключей, которые хранятся в аппаратных модулях системы безопасности (HSM), контролируемых Apple.

В последние годы Apple помогает некоторым внешним поставщикам внедрить те же структуры данных манифеста Image4, код проверки и инфраструктуру подписей, которые используются чипом Apple.

Если невозможно обойтись без хранилища и невозможно реализовать хранилище с безопасной загрузкой, система требует, чтобы перед помещением в постоянное хранилище обновления прошивки были подписаны с использованием криптографических методов и проверены.

Rosetta 2 на компьютере Mac с чипом Apple

Компьютер Mac с чипом Apple способен запускать код, скомпилированный для набора инструкций x86_64, с помощью механизма преобразования под названием *Rosetta 2*. Предлагается два типа преобразования: точно в нужный момент и заблаговременно.

Преобразование точно в нужный момент

При использовании преобразования точно в нужный момент (JIT) идентификация объекта Mach x86_64 выполняется на раннем этапе исполнения образа. Встречая такие образы, ядро передает управление специальной заглушке преобразования Rosetta, а не динамическому редактору ссылок dyld(1). Заглушка преобразования выполняет преобразование страниц x86_64 во время исполнения образа.

Преобразование выполняется полностью внутри процесса. Ядро по-прежнему проверяет хэши кода каждой страницы x86_64 на соответствие подписи кода, прикрепленной к двоичному файлу, когда происходит сбой страницы. В случае несоответствия хэша ядро применяет соответствующую политику исправления, подходящую для этого процесса.

Заблаговременное преобразование

При использовании заблаговременного преобразования (AOT) чтение двоичных файлов x86_64 из хранилища выполняется в те моменты, которые система считает оптимальными для скорости отклика этого кода. Преобразованные артефакты записываются в хранилище как особый файл объекта Mach. Этот файл похож на исполняемый образ, но содержит пометку, что это результат преобразования другого образа.

В этой модели артефакт AOT получает всю свою идентификационную информацию из исходного исполняемого образа x86_64. Для обеспечения этой привязки привилегированный объект пользовательского пространства подписывает преобразованный артефакт с помощью ключа конкретного устройства, которым управляет Secure Enclave. Этот ключ выдается только привилегированному объекту пользовательского пространства, который идентифицируется в этом качестве с помощью ограниченного права. Каталог кода, созданный для артефакта преобразования, включает хэш каталога кода исходного исполняемого образа x86_64. Подпись самого артефакта преобразования называется *дополнительной подписью*.

Процесс AOT начинается аналогично процессу JIT, то есть ядро передает управление среде выполнения Rosetta, а не динамическому редактору ссылок dyld(1). Однако затем среда выполнения Rosetta отправляет в системную службу Rosetta запрос межпроцессного взаимодействия о том, доступно ли преобразование AOT для текущего исполняемого образа. Если такое преобразование найдено, служба Rosetta предоставляет дескриптор этого преобразования, после чего оно сопоставляется с процессом и выполняется. Во время исполнения ядро применяет хэши каталога кода артефакта преобразования, которые аутентифицируются подписью с корнем в ключе подписания конкретного устройства. Хэши каталога кода исходного образа x86_64 не участвуют в этом процессе.

Преобразованные артефакты находятся в хранилище Data Vault, которое во время выполнения недоступно для любых объектов, кроме службы Rosetta. Служба Rosetta управляет доступом к своему кэшу, выдавая доступные только для чтения файловые дескрипторы отдельным артефактам преобразования; это ограничивает доступ к кэшу артефакта AOT. Межпроцессное взаимодействие и зависимая область этой службы намеренно оставлены очень узкими, чтобы минимизировать атакуемую область.

Если хэш каталога кода исходного образа x86_64 не совпадает с хэшем, закодированным в подписи артефакта преобразования AOT, это равноценно недействительной подписи кода и приводит к принятию соответствующих принудительных мер.

Если удаленный процесс запрашивает у ядра права доступа или другие идентифицирующие свойства кода исполняемого файла, преобразованного AOT, ему возвращаются идентифицирующие свойства исходного образа x86_64.

Содержимое статического доверенного кэша

macOS 11 или новее поставляется с мультиархитектурными двоичными файлами Mach, которые содержат фрагменты кода x86_64 и arm64. Пользователь компьютера Mac с чипом Apple может выбрать исполнение фрагмента x86_64 системного двоичного файла через процесс Rosetta, например, чтобы загрузить подключаемый модуль, не имеющий нативной версии arm64. Для поддержки этого подхода статический доверенный кэш, который поставляется с macOS, в основном содержит три хэша каталога кода на каждый файл объекта Mach.

- Хэш каталога кода фрагмента arm64.
- Хэш каталога кода фрагмента x86_64.
- Хэш каталога кода фрагмента заблаговременного (AOT) преобразования x86_64.

Процедура преобразования AOT Rosetta детерминирована. Она дает одинаковый результат для любого отдельно взятого набора входных данных, независимо от того, когда или на каком устройстве было выполнено преобразование.

Во время сборки macOS каждый файл объекта Mach проходит через процесс преобразования AOT Rosetta, связанный с версией данной macOS, и полученный хэш каталога кода записывается в доверенный кэш. Из соображений эффективности фактические результаты преобразования не поставляются с операционной системой и воссоздаются по запросу, когда пользователь их запрашивает.

Когда на компьютере Mac с чипом Apple выполняется образ x86_64, то, если хэш каталога кода этого образа находится в статическом доверенном кэше, хэш каталога кода полученного артефакта AOT также должен находиться в статическом доверенном кэше. Такие продукты не подписываются ключом конкретного устройства, поскольку корень полномочий подписания находится в последовательности безопасной загрузки Apple.

Неподписанный код x86_64

Компьютер Mac с чипом Apple не разрешает исполнение нативного кода arm64 без прикрепленной подписи кода. Эта подпись может быть такой же простой, как специальная ad-hoc подпись кода (ср. с `codesign(1)`), не содержащая никакой идентификационной информации из секретной половины пары асимметричных ключей (это неаутентифицированное измерение двоичного файла).

Из соображений совместимости двоичных файлов преобразованному коду x86_64 разрешено исполняться через Rosetta, даже не имея никакой информации о подписи. Процедура подписи Secure Enclave для конкретного устройства никак не идентифицирует этот код, и он исполняется с теми же ограничениями, что и собственный неподписанный код, исполняемый на компьютере Mac с процессором Intel.

Средства защиты прямого доступа к памяти на компьютерах Mac

Для достижения высокой пропускной способности высокоскоростных интерфейсов, таких как PCIe, FireWire, Thunderbolt и USB, компьютеры должны поддерживать прямой доступ к памяти (DMA) с периферийных устройств. То есть им нужна возможность чтения оперативной памяти и записи в нее без постоянного участия основного процессора. Начиная с 2012 г. на компьютерах Mac реализовано множество технологий для защиты DMA, что позволило получить наиболее эффективный и полный набор средств защиты DMA по сравнению с любым другим ПК.

Средства защиты DMA для компьютера Mac с чипом Apple

В системе на кристалле Apple имеется [модуль управления памятью ввода-вывода \(IOMMU\)](#) для каждого агента DMA в системе, в том числе портов PCIe и Thunderbolt. Поскольку у каждого IOMMU есть свой набор таблиц преобразования адресов для преобразования запросов DMA, периферийные устройства, подключенные через порт PCIe или Thunderbolt, имеют доступ только к той области, которая явно сопоставлена для использования ими. Периферийным устройствам недоступны области памяти, принадлежащие другим компонентам системы, таким как ядро или прошивка, а также области памяти, назначенные другим периферийным устройствам. Как только модуль IOMMU выявляет попытку периферийного устройства получить доступ к области памяти, которая не предназначена для него, он выдает критическую ошибку ядра.

Средства защиты прямого доступа к памяти для компьютера Mac с процессором Intel

Компьютеры Mac с процессором Intel и технологией виртуализации Intel для направленного ввода-вывода (VT-d) инициализируют модуль IOMMU для повторного сопоставления DMA и прерывают сопоставление на очень раннем этапе процесса загрузки во избежание возникновения уязвимостей системы безопасности различных классов. Модуль IOMMU Apple начинает работу с политикой, налагающей запрет по умолчанию, поэтому как только подается питание на систему, она автоматически начинает блокировать любые запросы DMA от периферийных устройств. После инициализации программным обеспечением модули IOMMU начинают разрешать запросы DMA от периферийных устройств к областям памяти, которые явно сопоставлены для использования соответствующими периферийными устройствами.

Примечание. Прерывание повторного сопоставления для PCIe на компьютере Mac с чипом Apple не требуется, поскольку каждый модуль IOMMU обрабатывает MSI для своего периферийного устройства.

Начиная с macOS 11, на всех компьютерах Mac с чипом безопасности Apple T2 применяются драйверы UEFI, которые при создании пары с внешними устройствами используют DMA в ограниченной среде кольца 3. Это свойство позволяет снизить риск эксплуатации уязвимостей системы безопасности при нештатном взаимодействии вредоносных устройств с драйвером UEFI во время загрузки. В частности, снижается влияние уязвимостей в драйверах, которые обрабатывают буферы DMA.

Расширения ядра в macOS

Начиная с macOS 11, если сторонние расширения ядра разрешены, их невозможно загрузить в ядро по запросу. Вместо этого они объединяются во *вспомогательную коллекцию ядра (AuxKC)*, которая загружается в процессе загрузки компьютера. На компьютере Mac с чипом Apple измерение AuxKC прописывается в политике LocalPolicy (на оборудовании предыдущих поколений измерение AuxKC хранилось в томе данных). Перестроение AuxKC требует подтверждения пользователя и перезапуска macOS для загрузки внесенных изменений в ядро. Кроме того, для параметра безопасной загрузки должен быть выбран сниженный уровень безопасности.

Важно! В macOS больше не рекомендуется использовать расширения ядра. Расширения ядра подвергают риску целостность и надежность операционной системы, поэтому Apple рекомендует отдать предпочтение решениям, которые не требуют расширений.

Расширения ядра на компьютере Mac с чипом Apple

На компьютере Mac с чипом Apple расширения ядра должны быть разрешены явным образом с помощью длительного нажатия кнопки питания при запуске для перехода в режим одной истинной среды восстановления (1TR), последующего перехода на сниженный уровень безопасности и установки соответствующего флажка для активации расширений ядра. Для этого также требуется ввести пароль администратора для авторизации перехода в режим сниженной безопасности. Использование 1TR в сочетании с паролем усложняет для проникшего в macOS злоумышленника, использующего только программное обеспечение, внедрение расширений ядра в macOS, которые затем можно было бы использовать для получения прав уровня ядра.

После авторизации пользователем загрузки расширений ядра применяется поток утвержденной пользователем загрузки расширений ядра. Он предназначен для авторизации установки расширений ядра. Авторизация, используемая для указанного выше потока, также применяется для перехвата хэша SHA384 списка авторизованных пользователем расширений ядра (UAKL) в политике LocalPolicy. Затем процесс управления ядром (kmd) подтверждает включение в AuxKC только тех расширений ядра, которые указаны в списке UAKL.

- Если включена функция защиты целостности системы (SIP), выполняется проверка подписи каждого расширения ядра, прежде чем оно будет включено в AuxKC.
- Если функция SIP выключена, подпись расширения ядра не проверяется.

Этот подход позволяет выполнять потоки низкого уровня безопасности, с помощью которых разработчики или пользователи, не участвующие в программе Apple Developer Program, тестируют расширения ядра перед их подписью.

После создания AuxKC ее измерение отправляется в Secure Enclave на подпись и включение в структуру данных Image4, которая подлежит проверке загрузчиком iBoot во время загрузки. В процессе формирования AuxKC также создается ответ расширения ядра. Этот ответ содержит список расширений ядра, которые фактически были включены в AuxKC, поскольку набор может оказаться поднабором UAKL, если были обнаружены запрещенные расширения ядра. Хэш SHA384 структуры данных Image4 коллекции AuxKC и ответ расширения ядра включаются в файл LocalPolicy. Хэш Image4 AuxKC используется для дополнительной проверки загрузчиком iBoot во время загрузки, что помогает исключить загрузку старого файла Image4 AuxKC, подписанного Secure Enclave, с новой политикой LocalPolicy. Ответ расширения ядра используется такими подсистемами, как Apple Pay, для определения наличия любых загруженных расширений ядра, которые могут повлиять на достоверность macOS. Если такие расширения обнаруживаются, функциональные возможности Apple Pay могут быть отключены.

Альтернативы расширениям ядра (macOS 10.15 и новее)

В macOS 10.15 разработчики могут расширять возможности macOS, устанавливая и используя системные расширения, которые исполняются в пользовательском пространстве, а не на уровне ядра. Благодаря работе в пользовательском пространстве расширения системы повышают стабильность и безопасность macOS. Несмотря на то, что расширения ядра по определению имеют полный доступ ко всей операционной системе, расширениям, работающим в пользовательском пространстве, предоставляются только те права, которые необходимы для выполнения их конкретной функции.

Разработчики могут использовать доступные программные среды, включая DriverKit, EndpointSecurity и NetworkExtension, для создания драйверов USB и драйверов интерфейса пользователя, инструментов защиты конечных точек (например, агентов предотвращения потери данных и других агентов конечных точек), а также инструментов VPN и сетевых средств, причем для этого не потребуются расширения ядра. Сторонние агенты безопасности должны использоваться только в том случае, если они используют эти API или имеют продуманную схему перехода к ним от расширений ядра.

Загрузка расширений ядра, утвержденных пользователем

Для повышения безопасности перед загрузкой расширений ядра, устанавливаемых во время или после установки macOS 10.13, требуется согласие пользователя. Этот процесс называется *утвержденной пользователем загрузкой расширений ядра*. Для утверждения расширения ядра требуются права администратора. Расширения ядра не требуют утверждения в следующих случаях:

- расширения были установлены на Mac macOS 10.12 или более ранней версии;
- расширения заменяют ранее утвержденные расширения;
- их загрузка без согласия пользователя разрешена при помощи инструмента командной строки `srctl`, доступного при загрузке Mac в режиме `recoveryOS`;
- их загрузка разрешена через конфигурацию управления мобильными устройствами (MDM).

Начиная с macOS 10.13.2 через систему MDM можно задать список расширений ядра, загружаемых без разрешения пользователя. Для этого необходимо, чтобы Mac с macOS 10.13.2 был зарегистрирован в MDM через Apple School Manager или Apple Business Manager либо чтобы регистрация в MDM была совершена пользователем.

Безопасность дополнительных ПЗУ в macOS

Примечание. На компьютере Mac с чипом Apple в настоящее время не поддерживаются дополнительные ПЗУ.

Безопасность дополнительных ПЗУ на компьютере Mac с чипом безопасности Apple T2

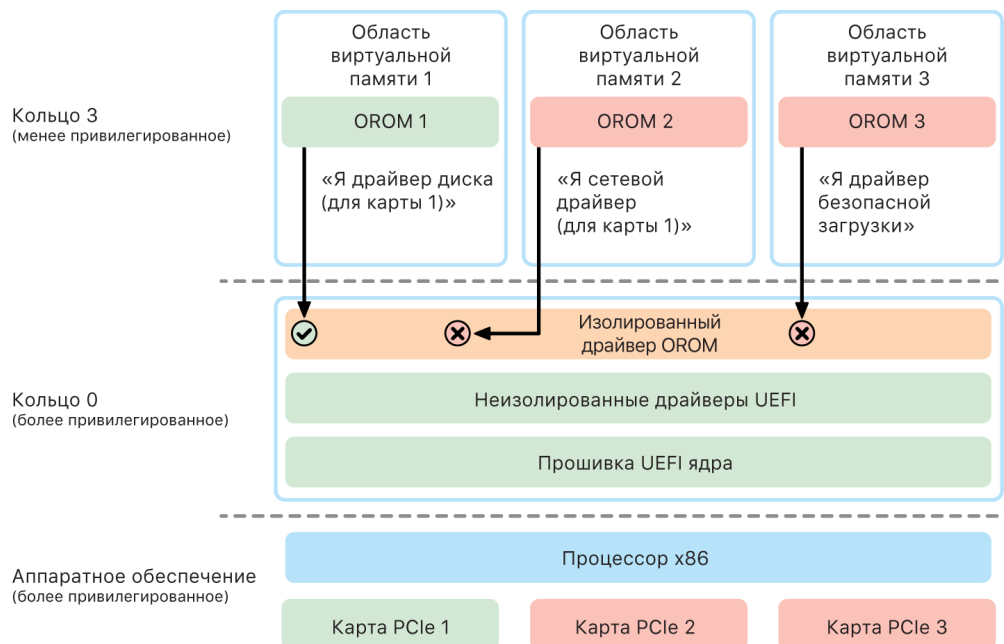
Устройства Thunderbolt и PCIe могут иметь дополнительное ПЗУ (OROM), физически подключенное к устройству. (Обычно это не настоящее ПЗУ, а перезаписываемый чип, в котором хранится прошивка.) В системах на основе UEFI эта прошивка обычно является драйвером UEFI, который считывается прошивкой UEFI и выполняется. Исполняемый код должен инициализировать и настроить оборудование, с которого он был извлечен, чтобы остальная часть прошивки могла использовать это оборудование. Благодаря этой функции специализированное оборудование сторонних производителей может загружаться и работать на самых ранних этапах процесса загрузки, что позволяет, например, выполнять загрузку с внешних массивов RAID.

Однако, поскольку устройства OROM обычно являются перезаписываемыми, если злоумышленник перезапишет OROM подлинного периферийного устройства, то код злоумышленника будет исполнен на раннем этапе процесса загрузки, и он сможет вмешаться в среду исполнения и нарушить целостность загружаемого впоследствии программного обеспечения. Кроме того, если злоумышленник подключит к системе вредоносное устройство, он также сможет исполнить вредоносный код.

На компьютерах Mac с macOS 10.12.3, продаваемых после 2011 г., OROM не выполняется по умолчанию во время загрузки Mac, если не было нажато специальное сочетание клавиш. Это сочетание клавиш защищало от непреднамеренного попадания вредоносного OROM в последовательность загрузки macOS. Стандартные настройки Утилиты пароля прошивки также были изменены. Теперь, если пользователь установил пароль прошивки, OROM не может выполняться, даже если нажато сочетание клавиш. Это не позволяло злоумышленнику, у которого есть физический доступ к компьютеру, преднамеренно добавить вредоносное OROM. Чтобы OROM исполнялось несмотря на установленный пароль прошивки, пользователь может задать другой параметр с помощью инструмента командной строки `firmwaterpasswd` в macOS.

Безопасность песочницы OROM

В прошивку UEFI в macOS 10.15 был добавлен механизм помещения OROM в изолированную среду (песочницу) и отмены полномочий OROM. Обычно прошивка UEFI исполняет весь код, в том числе OROM, с максимальным уровнем прав процессора, называемым «кольцо 0», и одним общим пространством виртуальной памяти для всего кода и данных. Кольцо 0 — это уровень прав, на котором работает ядро macOS, а минимальному уровню прав соответствует кольцо 3, где запускаются приложения. Песочница OROM отменяет полномочия OROM, используя разделение виртуальной памяти аналогично тому, как это делает ядро, и переводя OROM в кольцо 3.



Песочница также значительно ограничивает интерфейсы, которые разрешено вызывать OROM (аналогично фильтрации системных вызовов в ядрах), и типы устройств, в качестве которых может регистрироваться OROM (аналогично списку разрешенных приложений). Эта схема имеет важное преимущество: вредоносные OROM больше не могут выполнять запись напрямую в память кольца 0. Все потому, что они ограничены очень узким и четко определенным интерфейсом песочницы. Этот ограниченный интерфейс значительно сокращает уязвимую область и вынуждает злоумышленников сначала покинуть песочницу и расширить свои полномочия.

Безопасность прошивки UEFI на компьютере Mac с процессором Intel

На компьютере Mac с процессором Intel и чипом безопасности Apple T2 для обеспечения безопасности используется прошивка UEFI (Intel).

Обзор

Начиная с 2006 г. на компьютерах Mac с процессором Intel используется прошивка Intel на основе комплекта разработчика (EDK) расширяемого интерфейса прошивки (EFI) версии 1 или 2. Код на основе EDK2 соответствует спецификации Унифицированного расширяемого интерфейса прошивки (UEFI). В этом разделе прошивка Intel называется *прошивкой UEFI*. Прошивка UEFI была первым кодом, исполняемым на чипе Intel.

Для компьютера Mac с процессором Intel без чипа безопасности Apple T2 корнем доверия для прошивки UEFI является чип, в котором хранится прошивка. Обновления прошивки UEFI подписываются компанией Apple и проверяются прошивкой перед обновлением версии в хранилище. Версия обновления должна быть всегда новее текущей установленной версии. Это помогает предотвращать атаки методом отката. Однако злоумышленник с физическим доступом к Mac может подключиться к чипу хранилища прошивки с помощью аппаратных средств и обновить чип, записав в него вредоносный контент. Кроме того, если уязвимости будут обнаружены на раннем этапе процесса загрузки прошивки UEFI (до того, как она начинает ограничивать запись в чип хранилища), это также может привести к устойчивому заражению прошивки UEFI. Это аппаратное архитектурное ограничение, свойственное большинству ПК на базе процессоров Intel, имеется во всех компьютерах Mac с процессором Intel без чипа T2.

Чтобы защититься от физических атак на прошивку UEFI, компания Apple изменила архитектуру компьютеров Mac, заложив корень доверия в прошивку UEFI в чипе T2. На этих компьютерах Mac корнем доверия для прошивки UEFI является именно прошивка T2, как описано в разделе [Процесс загрузки компьютера Mac с процессором Intel](#).

Подсистема Intel Management Engine (ME)

Одной из подсистем, которые хранятся в прошивке UEFI, является прошивка *Intel Management Engine (ME)*. Подсистему ME, которая представляет собой отдельный процессор и подсистему в чипах Intel, можно использовать для удаленного управления, защищенной передачи аудио и видео и повышения безопасности на компьютере Mac, на котором установлен только графический процессор Intel. Для того чтобы сократить атакуемую поверхность подсистемы, компьютеры Mac с процессором Intel используют специальную прошивку ME, из которой было удалено большинство компонентов. Так как получаемая прошивка ME для компьютера Mac меньше, чем минимальная стандартная сборка, выпускаемая Intel, многие системы, которые ранее подвергались открытым атакам со стороны специалистов по обнаружению уязвимостей, теперь отсутствуют.

Режим управления системой (SMM)

У процессоров Intel есть специальный режим выполнения, который отличается от обычной работы. Этот режим, называемый *режимом управления системой (SMM)*, изначально разрабатывался для выполнения таких операций с жесткими временными ограничениями, как управление питанием. Однако для выполнения таких действий на компьютерах Mac всегда использовался отдельный микроконтроллер, называемый *контроллером управления системой (SMC)*. SMC больше не является отдельным микроконтроллером: он интегрирован в чип T2.

Безопасность системы watchOS

Часы Apple Watch используют многие из тех же аппаратных функций безопасности платформы, что и функции iOS и iPadOS. Например, часы Apple Watch:

- выполняют безопасную загрузку и безопасное обновление программного обеспечения;
- поддерживают целостность операционной системы;
- помогают защитить данные на устройстве и при обмене данными с объединенным в пару iPhone или интернетом.

К поддерживаемым технологиям относятся те, что перечислены в разделе о безопасности системы (например: KIP, SKP и SCIP), а также защита данных, связка ключей и сетевые технологии.

Обновление watchOS

watchOS может обновляться ночью, если изменить настройки. Подробные сведения о хранении код-пароля Apple Watch, используемого во время обновления, приведены в разделе [Хранилища ключей](#).

Распознавание запястья

Если функция распознавания запястья включена, устройство блокируется автоматически вскоре после того, как пользователь снимет часы с запястья. Если функция распознавания запястья выключена, Apple Watch можно заблокировать из Пункта управления. Когда часы Apple Watch заблокированы, Apple Pay можно использовать, только если ввести код-пароль на часах Apple Watch. Распознавание запястья можно отключить с помощью приложения Apple Watch на iPhone. Эту настройку также можно контролировать через систему управления мобильными устройствами (MDM).

Блокировка активации

Когда на iPhone включен Локатор, объединенные в пару часы Apple Watch могут использовать блокировку активации. Блокировка активации усложняет использование или продажу Apple Watch в случае их потери или кражи. После включения блокировки активации для разрыва пары, стирания или повторной активации Apple Watch необходимо ввести Apple ID и пароль пользователя.

Защищенное создание пары с iPhone

Apple Watch могут быть объединены в пару одновременно только с одним iPhone. При разрыве пары с Apple Watch iPhone передает инструкции для удаления всех материалов и данных с часов.

Для обмена открытыми ключами, а затем общим ключом канала Bluetooth Low Energy (BLE) при создании пары между Apple Watch и iPhone используется отдельное защищенное соединение. На экране Apple Watch отображается анимированный рисунок, который необходимо считать с помощью камеры iPhone. Этот рисунок содержит зашифрованный ключ, используемый для создания пары между устройствами по отдельному каналу BLE 4.1. При необходимости в качестве резервного способа создания пары используется стандартный ввод ключа доступа BLE.

После установления сеанса BLE и шифрования с использованием протокола максимальной защиты, описанного в спецификации ядра Bluetooth, Apple Watch и iPhone обмениваются ключами, используя один из следующих способов:

- Адаптированная процедура службы идентификации Apple (IDS), как описано в разделе [«Обзор безопасности iMessage»](#).
- Обмен ключами с помощью IKEv2/IPsec. Первоначальный обмен ключами аутентифицируется либо с помощью ключа сеанса Bluetooth (при создании пары), либо с помощью ключей IDS (при обновлении операционной системы). Каждое устройство генерирует случайную пару открытых и личных 256-битных ключей Ed25519. Во время первоначального обмена ключами выполняется обмен открытыми ключами.

Примечание. Механизм, используемый для обмена ключами и шифрования, отличается. Он зависит от версий операционных систем на устройствах iPhone и Apple Watch. При создании пары между устройствами iPhone под управлением iOS 13 или новее и Apple Watch под управлением watchOS 6 или новее для обмена ключами и шифрования используется только IKEv2/IPsec.

После обмена ключами:

- После обмена ключами ключ сеанса Bluetooth удаляется и вся информация, которой обмениваются iPhone и Apple Watch, шифруется с помощью одного из методов, указанных выше. При этом зашифрованные каналы Bluetooth, Wi-Fi и сотовой сети обеспечивают второй уровень шифрования.
- (Только IKEv2/IPsec) Ключи сохраняются в системной связке ключей и используются для аутентификации последующих сеансов IKEv2/IPsec между устройствами. Дальнейшие сеансы связи между этими устройствами шифруются по стандарту AES-256-GCM или ChaCha20-Poly1305 (256-битные ключи) для обеспечения их целостности на iPhone с iOS 15 или новее, объединенном в пару с часами Apple Watch Series 4 или новее с watchOS 8 или новее.

Адрес устройства Bluetooth Low Energy меняется каждые 15 минут, чтобы сократить риск локального отслеживания устройства, если кто-то транслирует постоянный идентификатор.

Для приложений, которые выполняют потоковую передачу данных, шифрование выполняется с помощью методов, описанных в разделе [Безопасность FaceTime](#), и посредством средств службы IDS компании Apple, используемых объединенным в пару iPhone или прямым подключением к интернету.

В Apple Watch реализовано хранилище с аппаратным шифрованием, а также защита файлов и элементов связки ключей на основе классов. Для элементов связки ключей также используются хранилища ключей с контролируемым доступом. Для защиты ключей, используемых для связи между Apple Watch и iPhone, также применяется защита на основе классов. Подробнее см. в разделе [Хранилища ключей для защиты данных](#).

Автоматическая разблокировка и Apple Watch

Для удобства пользования несколькими устройствами Apple некоторые устройства могут автоматически разблокировать другие устройства в определенных ситуациях. Предусмотрено три варианта использования автоматической разблокировки:

- Часы Apple Watch можно разблокировать с помощью iPhone.
- Компьютер Mac можно разблокировать с помощью часов Apple Watch.
- iPhone можно разблокировать с помощью часов Apple Watch, если нос и рот чехла закрыты.

Эти три варианта основаны на одном принципе: они используют протокол Station-to-Station (STS) для взаимной аутентификации, обмен статическими ключами, когда функция включена, и уникальные динамические ключи сеанса, согласованные для каждого запроса. Независимо от базового канала связи, туннель STS согласовывается непосредственно сопроцессорами Secure Enclave в обоих устройствах, и все криптографические данные хранятся в этом защищенном домене (за исключением компьютеров Mac без Secure Enclave, в которых туннель STS завершается в ядре).

Разблокировка

Полная последовательность разблокировки может быть разбита на два этапа. Сначала разблокируемое устройство (целевое устройство) генерирует криптографический ключ разблокировки и отправляет его на устройство, выполняющее разблокировку (инициатор). Затем инициатор выполняет разблокировку, используя ранее сгенерированный ключ.

Чтобы активировать автоматическую разблокировку, устройства подключаются друг к другу с помощью BLE-соединения. Затем 32-байтовый ключ разблокировки, случайным образом сгенерированный целевым устройством, передается инициатору по туннелю STS. Во время следующей биометрической разблокировки или разблокировки с помощью код-пароля целевое устройство защищает свой ключ на основе код-пароля (PDK), ключом разблокировки и удаляет ключ разблокировки из своей памяти.

Чтобы выполнить разблокировку, устройства создают новое BLE-соединение, а затем используют прямое соединение по Wi-Fi для безопасного определения приблизительного расстояния между ними. Если устройства находятся в заданном диапазоне и соблюдены необходимые политики безопасности, инициатор отправляет ключ разблокировки целевому устройству по туннелю STS. Затем целевое устройство генерирует новый 32-байтовый ключ разблокировки и возвращает его инициатору. Если текущий ключ разблокировки, отправленный инициатором, позволяет успешно расшифровать запись разблокировки, целевое устройство разблокируется, и PDK защищается новым ключом разблокировки. Наконец, новый ключ разблокировки и PDK удаляются из памяти целевого устройства.

Политики безопасности автоматической разблокировки часов Apple Watch

Для удобства часы Apple Watch можно разблокировать с помощью iPhone сразу после первоначального запуска, причем пользователю не придется вводить код-пароль на часах Apple Watch. Для обеспечения работы этой функции используется случайный ключ разблокировки (сгенерированный во время самой первой последовательности разблокировки после включения функции). С помощью этого ключа создается статическая запись о передаче, которая сохраняется в хранилище ключей часов Apple Watch. Ключ записи о передаче сохраняется в связке ключей iPhone и используется для инициализации нового сеанса после каждого перезапуска Apple Watch.

Политики безопасности автоматической разблокировки iPhone

К автоматической разблокировке iPhone с помощью Apple Watch применяются дополнительные политики безопасности. Часы Apple Watch нельзя использовать вместо Face ID на iPhone для других действий, таких как использование Apple Pay или авторизация в приложениях. После того как часы Apple Watch успешно разблокируют объединенный в пару iPhone, они отображают уведомление и воспроизводят тактильный отклик. Если пользователь нажимает кнопку блокировки iPhone в уведомлении, часы передают iPhone команду блокировки с помощью BLE-соединения. Когда iPhone получает команду блокировки, он блокируется, отключает Face ID и разблокировку с помощью Apple Watch. Для следующей разблокировки iPhone потребуется ввести код-пароль на iPhone.

Для успешной разблокировки объединенного в пару iPhone с помощью Apple Watch (если эта функция включена) требуется соблюдение следующих критериев:

- iPhone должен быть разблокирован другим способом как минимум один раз после того, как объединенные в пару часы Apple Watch были надеты на запястье и разблокированы.
- Датчики обнаружили, что нос и рот пользователя чем-то закрыты.
- Измеренное расстояние составляет не более 2–3 метров.
- Часы Apple Watch не находятся в режиме сна.
- Часы Apple Watch или iPhone были недавно разблокированы, или часы Apple Watch зафиксировали движения, указывающие на то, что пользователь активен (например, не спит).
- iPhone был разблокирован как минимум один раз за последние 6,5 часов.
- iPhone находится в состоянии, в котором разрешена разблокировка устройства с помощью Face ID. (Подробная информация приведена в разделе [Face ID, Touch ID, код-пароли и пароли](#).)

Подтверждение действий в macOS с помощью часов Apple Watch

Если включена автоматическая разблокировка с помощью часов Apple Watch, пользователь может использовать часы Apple Watch вместо или вместе с Touch ID для подтверждения запросов на авторизацию и аутентификацию от следующих приложений и функций:

- macOS и приложения Apple, требующие авторизации;
- приложения сторонних разработчиков, требующие аутентификации;
- сохраненные пароли Safari;
- секретные заметки.

Безопасное использование Wi-Fi, сети сотовой связи, iCloud и Gmail

Если Apple Watch находятся вне зоны действия Bluetooth, можно использовать Wi-Fi или сотовые данные. Часы Apple Watch автоматически подключаются к сетям Wi-Fi, к которым уже подключался объединенный в пару iPhone и учетные данные которых были синхронизированы с часами Apple Watch, когда оба устройства находились в зоне действия. Функцию автоподключения можно настроить отдельно для каждой сети, используя раздел «Wi-Fi» в приложении «Настройки» на Apple Watch. Если ни одно из устройств еще не подключалось к определенной сети Wi-Fi, к ней можно подключиться вручную в разделе «Wi-Fi» приложения «Настройки» на часах Apple Watch.

Если Apple Watch и iPhone находятся вне зоны действия сети, для получения почты Apple Watch подключаются напрямую к серверам iCloud и Gmail (вместо синхронизации данных Почты с iPhone, с которым создана пара, через интернет). В случае учетных записей Gmail пользователь должен пройти аутентификацию Google в разделе «Почта» приложения Apple Watch на iPhone. Полученный от Google токен OAuth будет передан на часы Apple Watch в зашифрованном формате через службу идентификации Apple (IDS), чтобы его можно было использовать для получения почты. Токен OAuth ни при каких обстоятельствах не будет использоваться для подключения к серверу Gmail с iPhone, с которым создана пара.

Генератор случайных чисел

Криптографически стойкие генераторы псевдослучайных чисел (КСГПСЧ) являются важным строительным блоком безопасного программного обеспечения. Поэтому Apple предоставляет надежный программный КСГПСЧ, работающий в ядре iOS, iPadOS, macOS, tvOS и watchOS. Используя в качестве источника энтропии саму систему, генератор предоставляет надежные случайные числа для ядра и пользовательского пространства.

Источники энтропии

КСГПСЧ ядра использует несколько источников энтропии во время загрузки и в течение всего срока службы устройства. Сюда входят (при наличии):

- аппаратный генератор истинных случайных чисел Secure Enclave;
- флуктуация времени во время загрузки;
- энтропия аппаратных прерываний;
- начальный файл, используемый для сохранения энтропии между загрузками;
- инструкции Intel для генерации случайных чисел, например RDSEED и RDRAND (только на компьютере Mac с процессором Intel).

КСГПСЧ ядра

КСГПСЧ ядра работает по алгоритму Fortuna, который ориентирован на 256-битный уровень защиты. Генератор предоставляет числа с высокой степенью случайности для пользовательского пространства через следующие API:

- системный вызов `getentropy(2)`;
- генератор случайных чисел (`/dev/random`).

КСГПСЧ ядра использует в качестве источника энтропии действия пользователя, которые сохраняются в генераторе случайных чисел.

Устройство Apple Security Research Device

Устройство Apple Security Research Device — это специально разработанный iPhone, с помощью которого специалисты по обнаружению уязвимостей исследуют iOS без необходимости обходить или выключать функции безопасности платформы iPhone. Данное устройство позволяет исследователям параллельно загружать содержимое, которое выполняется с разрешениями уровня платформы, тем самым проводя исследование на платформе, которая более точно моделирует реальные устройства.

Для того чтобы помочь избежать влияния политики выполнения устройства Security Research Device на устройства пользователей, изменения политики реализуются в виде варианта загрузчика iBoot и загрузочной коллекции ядра. Это исключает загрузку с использованием оборудования пользователя. Загрузчик iBoot для исследования проверяет новое состояние переключки и входит в цикл критической ошибки, если он запущен на оборудовании, которое не предназначено для исследования.

С помощью подсистемы cryptex исследователи могут загружать персонализированный [доверенный кэш](#) и образ диска с соответствующим содержимым. Имеется ряд средств углубленной защиты, направленных на то, чтобы эта подсистема не могла разрешить выполнение на устройствах пользователей:

- launchd не загружает список свойств launchd компонента cryptexd в случае обнаружения обычного пользовательского устройства.
- Выполнение cryptexd прерывается в случае обнаружения обычного пользовательского устройства.
- AppleImage4 не передает значение nonce, используемое для проверки исследовательской подсистемы cryptex на обычном пользовательском устройстве.
- Сервер подписания отказывает в персонализации образа диска cryptex для устройств, которые отсутствуют в списке явного предоставления разрешения.

Чтобы сохранить конфиденциальность специалиста по обнаружению уязвимостей, во время персонализации в компанию Apple отправляются только измерения (например, хэши) исполняемых элементов или кэш ядра и идентификаторы устройств, предназначенных для исследования. Apple не получает содержимое cryptex, загруженное на устройство.

Во избежание ситуаций, в которых злоумышленник пытается замаскировать устройство для исследования под устройство пользователя, чтобы обманом заставить объект атаки использовать его в своей повседневной деятельности, устройство Security Research Device отличается от обычного. Эти отличия описаны ниже.

- Устройство Apple Security Research Device загружается только во время зарядки с помощью кабеля Lightning или зарядного устройства стандарта Qi. Если устройство не заряжается во время загрузки, устройство входит в режим восстановления. Если пользователь начинает зарядку и перезагружает устройство, оно загружается в обычном режиме. После запуска XNU устройству не требуется зарядка для продолжения работы.
- Во время запуска загрузчика iBoot под логотипом Apple отображается надпись *Security Research Device*.
- Ядро XNU загружается в режиме подробного протоколирования загрузки.
- На боковой стороне устройства выгравирована надпись: «Property of Apple. Confidential and Proprietary. Call +1 877 595 1125».

Ниже указаны дополнительные меры, внедренные в программное обеспечение, которое отображается после загрузки.

- Надпись *Security Research Device*, которая отображается во время загрузки устройства.
- Надпись *Security Research Device*, которая отображается на экране блокировки и в приложении «Настройки».

На устройстве Security Research Device исследователи могут выполнять действия, которые невозможны на пользовательском устройстве. Исследователи могут:

- параллельно загружать исполняемый код на устройство с произвольными разрешениями того же уровня, что и у компонентов операционной системы Apple;
- запускать службы во время загрузки;
- сохранять содержимое между перезагрузками;
- использовать разрешение `research.com.apple.license-to-operate`, чтобы разрешать одному процессу отладку любого другого процесса системы, в том числе системных процессов.

Пространство имен `research.` учитывается только вариантом RESEARCH расширения ядра AppleMobileFileIntegrity; любой процесс с этим разрешением прерывается на пользовательском устройстве во время проверки подписи;

- персонализировать и восстанавливать настраиваемый кэш ядра.

Шифрование и защита данных

Обзор шифрования и защиты данных

Безопасная последовательность загрузки, а также функции обеспечения безопасности системы и приложений помогают следить за тем, чтобы на устройстве запускались только надежные приложения и фрагменты кода. В устройствах Apple также реализованы дополнительные функции шифрования для защиты данных пользователей даже в случае компрометации других частей системы безопасности (например, в случае пропажи устройства или запуска ненадежного кода). Все эти функции имеют большое значение для пользователей и ИТ-администраторов, поскольку они обеспечивают защиту личной и корпоративной информации, а также предоставляют средства для мгновенного и полного удаленного стирания в случае потери или кражи устройства.

На устройствах iOS и iPadOS используется технология шифрования файлов, также именуемая *технологией защиты данных*, в то время как для защиты данных на компьютере Mac с процессором Intel применяется технология шифрования томов под названием *FileVault*. На компьютерах Mac с чипом Apple используется гибридная модель, которая поддерживает технологию защиты данных, но с двумя оговорками. Самый низкий уровень защиты (класса D) не поддерживается, а используемый по умолчанию уровень защиты (класса C) использует ключ тома и работает так же, как и FileVault на Mac с процессором Intel. Во всех случаях основой иерархии ключей является специализированный процессор Secure Enclave, а выделенный модуль AES поддерживает шифрование на полной скорости и позволяет не раскрывать долговременные ключи шифрования ядру операционной системы или центральному процессору (где они могут быть скомпрометированы). (Для защиты ключей шифрования FileVault на Mac с процессором Intel и чипом T1 или без Secure Enclave не используется специализированный чип.)

Помимо использования функции защиты данных и FileVault, которые помогают предотвратить несанкционированный доступ к данным, *ядро операционной системы* Apple также обеспечивают защиту и безопасность. Ядро использует средства контроля доступа, чтобы помещать приложения в песочницу (что ограничивает доступ приложения к данным на основе установленных критериев). Ядро также использует механизм, который называется *Data Vault* (вместо того чтобы ограничивать запросы, которые может делать приложение, этот механизм ограничивает доступ к данным, которые находятся в одном приложении, но запрашиваются другим).

Код-пароли и пароли

Чтобы защитить данные пользователей от атак, Apple использует код-пароли в iOS и iPadOS и пароли в macOS. Чем длиннее код-пароль или пароль, тем он надежнее, а значит, он лучше противостоит атакам методом перебора. Чтобы еще больше повысить стойкость к атакам, Apple применяет задержки (в iOS и iPadOS) и ограничивает число попыток ввода пароля (на Mac).

В iOS и iPadOS защита данных включается автоматически, когда пользователь задает код-пароль или пароль. Защита данных также включается на других устройствах с системой на кристалле (SoC), таких как Mac с чипом Apple, Apple TV и Apple Watch. В macOS Apple использует встроенное приложение для шифрования томов, которое называется *FileVault*.

Как надежные код-пароли или пароли повышают безопасность

iOS и iPadOS поддерживают код-пароли из шести или четырех цифр и буквенно-цифровые код-пароли произвольной длины. Помимо разблокирования устройства, код-пароль или пароль является источником энтропии для некоторых ключей шифрования. Это означает, что злоумышленник, завладевший устройством, не сможет получить доступ к данным определенных классов защиты, не зная код-пароля.

Код-пароль или пароль привязывается к UID устройства, поэтому попытки перебора должны выполняться непосредственно на атакуемом устройстве. Для замедления каждой попытки используется счетчик повторений. Счетчик повторений настроен таким образом, что одна попытка занимает примерно 80 миллисекунд. Это означает, что для перебора всех сочетаний шестизначного код-пароля, состоящего из строчных букв и цифр, потребуется более пяти с половиной лет.

Чем надежнее код-пароль пользователя, тем надежнее ключ шифрования. Поэтому с Face ID или Touch ID пользователь может задать более надежный код-пароль, нежели тот, который было бы удобнее вводить в отсутствие данных технологий. Надежный код-пароль повышает эффективность энтропии, защищающей ключи шифрования, используемые для защиты данных, но не сказывается на удобстве пользователей, которым приходится по несколько раз в день разблокировать устройство.

Если введен длинный пароль, содержащий только цифры, вместо полной клавиатуры на экране блокировки отображается цифровая клавиатура. При аналогичном уровне безопасности вводить более длинный цифровой код-пароль может быть проще, чем короткий буквенно-цифровой.

Пользователи могут задать более длинный буквенно-цифровой код-пароль. Для этого нужно открыть «Настройки» > «Touch ID и код-пароль» или «Face ID и код-пароль» и выбрать вариант «Произвольный код (буквы + цифры)» в разделе «Параметры код-пароля».

Как увеличенные временные задержки препятствуют атакам методом перебора (iOS, iPadOS)

В iOS и iPadOS, чтобы еще больше усложнить атаки методом перебора, после ввода неправильного код-пароля на экране блокировки временные задержки увеличиваются. Время задержки указано в таблице далее.

Попытки	Принудительная задержка
1–4	Нет
5	1 минута
6	5 минут
7–8	15 минут
9	1 час

Если параметр «Стирать данные» включен («Настройки» > «Touch ID и код-пароль»), все данные на устройстве будут автоматически стерты после 10 неудачных попыток ввода код-пароля подряд. При подсчете не учитываются последовательные попытки ввода одного и того же неправильного код-пароля. Эта функция также доступна при настройке политики администрирования через систему управления мобильными устройствами (MDM) и через Exchange ActiveSync. Кроме того, можно установить более низкий порог ее срабатывания.

На устройствах с Secure Enclave за применение задержек отвечает Secure Enclave. Если в течение заданного времени задержки устройство перезапускается, задержка применяется еще раз, а таймер запускается заново.

Как увеличенные временные задержки препятствуют атакам методом перебора (macOS)

Для того чтобы помочь в предотвращении атак методом перебора, при загрузке Mac в окне входа или режиме внешнего диска дается не более 10 попыток ввода пароля, при этом каждый раз после ввода неправильного пароля время задержки перед новой попыткой увеличивается. За применение задержек отвечает Secure Enclave. Если в течение заданного времени задержки Mac перезапускается, задержка применяется еще раз, а таймер запускается заново.

В таблице ниже указаны задержки между попытками ввода пароля на компьютере Mac с чипом Apple и компьютере Mac с чипом T2.

Попытки	Принудительная задержка
5	1 минута
6	5 минут
7	15 минут
8	15 минут
9	1 час
10	Отключено

Чтобы помочь противодействовать необратимой потере данных из-за того, что вредоносное программное обеспечение атаковало пароль пользователя, эти ограничения снимаются после того, как пользователь успешно вошел в систему Mac, но вновь применяются после перезагрузки. Когда 10 попыток исчерпаны, можно выполнить загрузку в режиме recoveryOS, чтобы получить еще 10 попыток. Если и дополнительные попытки исчерпаны, каждому механизму восстановления FileVault (восстановление iCloud, ключ восстановления FileVault и корпоративный ключ) предоставляется по 10 дополнительных попыток, то есть всего доступно 30 дополнительных попыток. Если эти дополнительные попытки также исчерпаны, Secure Enclave перестанет обрабатывать запросы на дешифрование тома или проверку пароля, и данные на диске будут утрачены безвозвратно.

Чтобы помочь защитить данные в корпоративной среде, ИТ-отдел должен установить и внедрить политики конфигурации FileVault с помощью системы MDM. Организациям доступно несколько способов управления зашифрованными томами, включая корпоративные ключи восстановления, личные ключи восстановления (которые при желании можно передать в MDM для хранения) или их сочетание. В MDM также можно установить политику ротации ключей.

На компьютере Mac с чипом безопасности Apple T2 пароль выполняет схожую функцию, но сгенерированный ключ используется для шифрования FileVault, а не для технологии защиты данных. macOS также предлагает дополнительные варианты восстановления пароля:

- восстановление iCloud;
- восстановление FileVault;
- корпоративный ключ FileVault.

Защита данных

Обзор защиты данных

Apple использует специальную технологию, называемую защитой данных, чтобы защитить данные во флеш-памяти на устройствах с системой на кристалле Apple, таких как iPhone, iPad, Apple Watch, Apple TV и компьютер Mac с чипом Apple. Благодаря защите данных устройство может реагировать на типичные события, такие как входящие телефонные вызовы, вместе с тем обеспечивая более высокий уровень шифрования данных пользователей. Некоторые системные приложения, такие как Сообщения, Почта, Календарь, Контакты и Фото, а также медданные, используют технологию защиты данных по умолчанию, а приложения сторонних разработчиков получают ее автоматически.

Реализация

Технология защиты данных реализована путем построения и контроля иерархии ключей, и она основана на технологиях аппаратного шифрования, встроенных в устройства Apple. Защита данных организована на уровне файлов: каждому файлу назначается один из классов защиты, а доступность определяется разблокированием ключей класса. Файловая система Apple (APFS) позволяет дополнительно разделять ключи по диапазонам (различные фрагменты файла могут иметь разные ключи).

Каждый раз, когда в томе данных создается файл, защита данных создает новый 256-битный ключ (*ключ файла*) и передает его аппаратному AES-модулю, который использует этот ключ для шифрования файла при записи во флеш-память.

На устройствах с системой на кристалле A14 и A15 и устройствах семейства M1 для шифрования используется AES-256 в режиме XTS, где 256-битный ключ для каждого файла проходит через функцию формирования ключа (специальное издание NIST 800-108) для получения 256-битной поправки и 256-битного ключа шифрования. Поколения устройств с системами на кристалле от A9 до A13, S5, S6 и S7 используют AES-128 в режиме XTS, в котором 256-битный ключ файла разделяется для получения 128-битной поправки и 128-битного ключа шифрования.

На компьютере Mac с чипом Apple для технологии защиты данных по умолчанию установлен класс C (см. раздел [Классы защиты данных](#)), однако при этом используется ключ тома, а не ключ диапазона или ключ файла. Фактически это эффективно воспроизводит модель безопасности FileVault для защиты пользовательских данных. Однако, чтобы привязать иерархию ключей шифрования к паролю и получить полную защиту, пользователи все равно должны включить FileVault. Разработчики могут выбрать более высокий класс защиты, в котором используется ключ файла или ключ диапазона.

Защита данных на устройствах Apple

На устройствах Apple с технологией защиты данных каждый файл защищен уникальным ключом файла (или диапазона). Ключ, который защищен с помощью алгоритма защиты ключей NIST AED, дополнительно защищается одним из нескольких ключей класса в зависимости от того, доступ к какому файлу нужно получить. Затем защищенный ключ файла сохраняется в метаданных файла.

Устройства с файловой системой APFS могут поддерживать клонирование файлов (технология копирования при записи обеспечивает копирование с нулевыми затратами). Если файл клонируется, каждая из половин клона получает новый ключ для приема входящих операций записи, поэтому новые данные записываются на носитель с новым ключом. Со временем файл может разделиться на несколько диапазонов (или фрагментов), каждый из которых связан с отдельным ключом. Однако все диапазоны, составляющие файл, будут защищены одним и тем же ключом класса.

При открытии файла выполняется дешифрование его метаданных с помощью ключа файловой системы, которое приводит к раскрытию защищенного ключа файла и обозначения класса его защиты. Ключ файла (или диапазона) дешифруется с помощью ключа класса, а затем передается аппаратному модулю AES, который выполняет дешифрование файла при чтении из флеш-памяти. Вся обработка защищенного ключа файла выполняется в Secure Enclave; ключ файла никогда не раскрывается непосредственно процессору приложений. Во время загрузки компьютера процессор Secure Enclave согласовывает динамический ключ с модулем AES. Ключи файла расшифровываются в Secure Enclave, а затем снова защищаются с помощью динамического ключа и отправляются обратно процессору приложений.

Метаданные всех файлов файловой системы тома данных шифруются с помощью случайного ключа тома, который создается при первой установке операционной системы или при стирании данных на устройстве пользователем. Этот ключ шифруется и защищается для долгосрочного хранения с помощью ключа для упаковки ключа, который известен только Secure Enclave. Ключ для упаковки ключа изменяется каждый раз, когда пользователь стирает данные на устройстве. В системах на кристалле A9 и новее Secure Enclave использует энтропийное кодирование, подкрепленное системами антиповтора, а также другие методы для обеспечения возможности стирания и защиты ключа для упаковки ключа (наряду с другими ресурсами). Подробнее см. в разделе [Защищенное энергонезависимое хранилище](#).

Аналогично ключам файлов и диапазонов, ключ метаданных тома данных никогда не раскрывается процессору приложений напрямую; вместо этого Secure Enclave предоставляет динамическую версию для каждой загрузки. Во время хранения зашифрованный ключ файловой системы дополнительно защищается с помощью «стираемого ключа», хранящегося в стираемом накопителе, или с помощью ключа для упаковки ключа носителя, защищенного с помощью механизма антиповтора Secure Enclave. Этот ключ не обеспечивает дополнительную конфиденциальность данных. Он предназначен для быстрого стирания по запросу (запрос может быть инициирован пользователем с помощью пункта «Стереть контент и настройки» или администратором с помощью команды удаленного стирания от системы управления мобильными устройствами (MDM), сервера Microsoft Exchange ActiveSync или iCloud). Такой способ стирания ключа делает все файлы криптографически недоступными.

Содержимое файла может шифроваться с помощью одного или нескольких ключей файла (или диапазонов), которые защищаются с помощью ключа класса и сохраняются в метаданных файла, которые, в свою очередь, шифруются с помощью ключа файловой системы. Ключ класса защищен аппаратным UID. Кроме того, ключи некоторых классов защищены код-паролем пользователя. Такая иерархия обеспечивает и гибкость, и эффективность. Например, для изменения класса файла достаточно еще раз защитить его с помощью ключа файла, а изменение код-пароля приводит просто к повторной защите ключа класса.

Классы защиты данных

Когда приложение создает новый файл на устройствах, которые поддерживают защиту данных, оно назначает ему класс. Каждый класс использует различные политики для определения условий доступа к данным. Основные классы и политики описаны в следующих разделах. Компьютеры Mac с чипом Apple не поддерживают класс D «Без защиты», и границы зоны безопасности устанавливаются вокруг входа и выхода (а не блокировки и разблокировки, как на iPhone, iPad и iPod touch).

Класс	Тип защиты
Класс A. Полная защита	NSFileProtectionComplete
Класс B. Защищено, если не открыто	NSFileProtectionCompleteUnlessOpen
Класс C. Защищено до первой аутентификации пользователя	NSFileProtectionCompleteUntilFirstUserAuthentication
<i>Примечание.</i> macOS использует ключ тома для воссоздания характеристик защиты FileVault.	
Класс D. Без защиты	NSFileProtectionNone
<i>Примечание.</i> Не поддерживается в macOS.	

Полная защита

NSFileProtectionComplete. Ключ класса защищается с помощью ключа, полученного из код-пароля или пароля пользователя и UID устройства. Вскоре после того, как пользователь заблокирует устройство (через 10 секунд, если для параметра «Запрос пароля» задано значение «Сразу»), расшифрованный ключ класса удаляется, в результате чего все данные этого класса остаются недоступны, пока пользователь снова не введет код-пароль или не разблокирует устройство (войдет в систему) с помощью Face ID или Touch ID.

В macOS расшифрованный ключ класса удаляется вскоре после того, как последний пользователь выходит из системы, в результате чего все данные этого класса становятся недоступны, пока какой-либо пользователь снова не введет код-пароль или не выполнит вход на устройстве с помощью Touch ID.

Защищено, если не открыто

NSFileProtectionCompleteUnlessOpen. Иногда требуется записать определенные файлы, когда устройство заблокировано или пользователь вышел из системы. В качестве примера можно привести загрузку почтового вложения в фоновом режиме. Такое действие становится возможным благодаря использованию асимметричной эллиптической криптографии (ECDH по Curve25519). Для защиты обычного ключа файла используется ключ, полученный в результате однопроходного согласования ключей Диффи — Хеллмана, как описано в документе NIST SP 800-56A.

Динамический открытый ключ для согласования хранится вместе с защищенным ключом файла. В качестве KDF используется функция формирования ключа сцеплением (утвержденная альтернатива 1) согласно пункту 5.8.1 документа NIST SP 800-56A. *AlgorithmID* опускается. *PartyUInfo* и *PartyVInfo* — это динамический и статический открытые ключи соответственно. В качестве функции хэширования используется SHA256. Сразу после закрытия файла его ключ удаляется из памяти. Для повторного открытия файла снова создается открытый ключ на основе личного ключа класса «Защищено, если не открыто» и динамического открытого ключа; они используются для снятия защиты с ключа файла, который затем используется для дешифрования файла.

В macOS доступ к личной части ключа класса *NSFileProtectionCompleteUnlessOpen* предусмотрен до тех пор, пока пользователи системы находятся в системе или остаются аутентифицированными.

Защищено до первой аутентификации пользователя

NSFileProtectionCompleteUntilFirstUserAuthentication. Действие этого класса аналогично классу «Полная защита», однако расшифрованный ключ класса не удаляется из памяти при блокировке устройства или выходе пользователя из системы. Защита этого класса похожа на шифрование всего тома на настольных системах и защищает данные от атак, которые используют перезагрузку устройства. Этот класс по умолчанию используется для всех приложений сторонних разработчиков, которым не назначен класс защиты данных.

В macOS этот класс использует ключ тома, который доступен, пока подключен том, и он действует так же, как FileVault.

Без защиты

NSFileProtectionNone. Ключ этого класса защищен только с помощью UID и хранится в стираемом накопителе. Поскольку все ключи, необходимые для дешифрования файлов в этом классе, хранятся на устройстве, единственным преимуществом такого шифрования является возможность быстрого удаленного стирания. Даже если файлу не назначен класс защиты данных, он все равно хранится в зашифрованном виде (как и все данные на устройстве iOS и iPadOS).

Этот вариант не поддерживается в macOS.

Примечание. В macOS для томов, которые не используются для загрузки операционной системы, все классы защиты данных доступны, только пока подключен том. По умолчанию используется класс защиты данных *NSFileProtectionCompleteUntilFirstUserAuthentication*. Функция ключа диапазона доступна как в Rosetta 2, так и в собственных приложениях.

Хранилища ключей для защиты данных

В iOS, iPadOS, watchOS и tvOS ключи для классов файлов и классов защиты данных связки ключей организованы в хранилища ключей. В этих операционных системах используются следующие хранилища ключей: пользователь, устройство, резервная копия, передача и резервная копия iCloud.

Хранилище ключей пользователя

Хранилище ключей пользователя — это место хранения защищенных ключей класса, используемых при нормальном функционировании устройства. Например, при вводе код-пароля выполняется загрузка ключа *NSFileProtectionComplete* из хранилища ключей пользователя и дешифрование ключа. Хранилище ключей представляет собой двоичный файл списка свойств (.plist) с классом «Без защиты».

На устройствах с системой на кристалле до A9 содержимое файла .plist шифруется с помощью ключа, хранящегося в стираемом накопителе. Для повышения безопасности хранилищ ключей этот ключ стирается и генерируется снова каждый раз, когда пользователь меняет код-пароль.

На устройствах с системами на кристалле A9 или новее файл .plist содержит ключ, указывающий на то, что хранилище ключей помещено в сейф, который защищен с помощью значения попсе функции антиповтора, контролируемой Secure Enclave.

Сопроцессор Secure Enclave управляет хранилищем ключей пользователя и может получать запросы относительно состояния блокировки устройства. Он отвечает, что устройство разблокировано, только в том случае, если все ключи классов в хранилище ключей пользователя являются доступными и были успешно дешифрованы.

Хранилище ключей устройства

Хранилище ключей устройства предназначено для хранения защищенных ключей класса, используемых для выполнения операций с данными конкретного устройства. Устройства iPadOS, настроенные для совместного пользования, иногда нуждаются в доступе к учетным данным до того, как пользователь войдет в систему, поэтому необходимо хранилище ключей, не защищенное код-паролем пользователя.

iOS и iPadOS не поддерживают криптографическое разделение файловой системы разных пользователей, то есть для защиты ключей файлов система будет использовать ключи класса из хранилища ключей устройства. Однако для защиты элементов связки ключей пользователя используются ключи класса из хранилища ключей пользователя. На устройствах iOS и iPadOS, настроенных для использования одним пользователем (это конфигурация по умолчанию), хранилище ключей устройства и хранилище ключей пользователя совпадают и защищаются с помощью код-пароля пользователя.

Хранилище ключей в резервной копии

Хранилище ключей в резервной копии создается в тот момент, когда Finder (macOS 10.15 или новее) или iTunes (в macOS 10.14 и более ранних версиях) создает и сохраняет зашифрованную резервную копию на компьютере, куда передается резервная копия устройства. Новое хранилище ключей создается с новым набором ключей, и данные резервной копии повторно шифруются с использованием этих новых ключей. Как было объяснено ранее, элементы связки ключей «без возможности переноса» остаются защищенными ключом на основе UID; это позволяет восстанавливать их на исходном устройстве, но делает недоступными на другом устройстве.

Для защиты хранилища ключей используется заданный пароль, к которому применено 10 миллионов итераций функции формирования ключа PBKDF2. Несмотря на счетчик повторений, привязка к определенному устройству отсутствует, поэтому на хранилище ключей в резервной копии может быть совершена атака методом перебора с участием большого числа компьютеров. Для ослабления этой угрозы необходимо использовать достаточно надежный пароль.

Если пользователь решает не шифровать резервные копии, файлы резервных копий не шифруются независимо от класса защиты данных, однако связка ключей остается защищена ключом на основе UID. Поэтому элементы связки ключей переносятся на новое устройство, только если установлен пароль резервного копирования.

Хранилище ключей передачи

Хранилище ключей передачи используется для синхронизации с Finder (в macOS 10.15 и новее) или iTunes (в macOS 10.14 и более ранних версиях) через USB и систему управления мобильными устройствами (MDM). Благодаря этому хранилищу ключей приложение Finder или iTunes может выполнять резервное копирование и синхронизацию, не запрашивая у пользователя код-пароль, а система MDM может удаленно стирать код-пароль пользователя. Хранилище ключей находится на компьютере, который используется для синхронизации с Finder или iTunes, или в системе MDM, которая удаленно управляет устройством.

Хранилище ключей передачи упрощает работу пользователей при синхронизации устройства, которое может требовать доступа ко всем классам данных. Когда защищенное код-паролем устройство впервые подключается к Finder или iTunes, пользователю необходимо ввести код-пароль. Затем устройство создает хранилище ключей передачи, содержащее ключи того же класса, что и используемые на устройстве, но защищенные с помощью нового сгенерированного пароля. Хранилище ключей передачи и защищающий его ключ делятся между устройством и хостом или сервером, а данные сохраняются на устройстве с классом «Защищено до первой аутентификации пользователя». Поэтому для первого резервного копирования с помощью Finder или iTunes после перезагрузки пользователю необходимо ввести код-пароль устройства.

В случае беспроводного обновления программного обеспечения пользователь получает запрос на ввод код-пароля при запуске обновления. Это нужно для безопасного создания одноразового токена разблокировки, который разблокирует хранилище ключей пользователя после обновления. Этот токен невозможно сгенерировать без ввода код-пароля пользователем, а все ранее созданные токены становятся недействительными, если код-пароль пользователя меняется.

Одноразовые токены разблокировки бывают двух типов в зависимости от предназначения: для установки обновлений программного обеспечения либо с участием пользователя, либо без его участия. Они шифруются с помощью ключа, полученного из текущего значения монотонного счетчика, работающего в Secure Enclave, UUID хранилища ключей и UID Secure Enclave.

В системах на кристалле A9 (и новее) одноразовый токен разблокировки больше не зависит от счетчиков или стираемого накопителя. Для его защиты теперь используется значение поппе функции антиповтора, контролируемой сопроцессором Secure Enclave.

Срок действия одноразового токена разблокировки для установки обновлений программного обеспечения при участии пользователя истекает через 20 минут. В iOS 13 и iPadOS 13.1 или новее токен хранится в сейфе, который защищен сопроцессором Secure Enclave. В версиях, выпущенных ранее iOS 13, такой токен экспортировался из Secure Enclave и записывался в стираемый накопитель или защищался с помощью механизма антиповтора в сопроцессоре Secure Enclave. Таймер действия токена увеличивает значение счетчика, если устройство не перезагружалось в течение 20 минут.

Установка программного обеспечения без участия пользователя происходит, когда система обнаруживает наличие обновления и выполняется одно из следующих условий:

- в iOS 12 или новее настроено автоматическое обновление;
- пользователь выбирает вариант «Установить позже» в окне уведомления об обновлении.

После того как пользователь вводит код-пароль, генерируется одноразовый токен разблокировки, который может поддерживаться в Secure Enclave в действительном состоянии до 8 часов. Если обновление еще не произошло, этот одноразовый токен разблокировки уничтожается при каждой блокировке и заново создается при каждой последующей разблокировке. После каждой разблокировки отсчет 8 часов начинается с начала. По истечении 8 часов таймер действия токена аннулирует одноразовый токен разблокировки.

Хранилище ключей в резервной копии iCloud

Хранилище ключей в резервной копии iCloud похоже на хранилище ключей в резервной копии. Все ключи классов в этом хранилище являются асимметричными (используют Curve25519 так же, как и класс «Защищено, если не открыто»). Хранилище асимметричных ключей также используется для резервного копирования, необходимого для восстановления Связки ключей iCloud.

Защита ключей в других режимах загрузки

Функция защиты данных предоставляет доступ к пользовательским данным только после успешной аутентификации и только авторизованному пользователю. Классы защиты данных поддерживают различные ситуации, например возможность чтения и записи некоторых данных, даже когда устройство заблокировано (но после первой разблокировки). Дополнительные меры принимаются для защиты доступа к пользовательским данным в других режимах загрузки, например режимах, используемых для обновления прошивки устройства (DFU), восстановления, диагностики Apple или даже обновления программного обеспечения. Эти возможности основаны на сочетании аппаратных и программных функций и расширились по мере развития чипов Apple.

Функция	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, семейство M1
Восстановление: данные всех классов защиты защищены	✓	✓	✓	✓	✓
Режимы обновления прошивки устройства (DFU), восстановления и обновления программного обеспечения: защищены данные класса A, B и C		✓	✓	✓	✓

AES-модуль Secure Enclave имеет блокируемые программные начальные биты. При создании ключей из UID функция формирования ключа использует эти начальные биты для создания дополнительных иерархий ключей. Использование начального бита зависит от системы на кристалле:

- Начиная с систем на кристалле Apple A10 и S3 начальный бит предназначен для идентификации ключей, защищенных с помощью код-пароля пользователя. Начальный бит устанавливается для ключей, которым требуется код-пароль пользователя (включая ключи с классами защиты данных A, B и C), и очищается для ключей, которым не требуется код-пароль пользователя (включая ключ метаданных файловой системы и ключи класса D).
- В iOS 13 или новее и iPadOS 13.1 или новее на устройствах с A10 или новее при загрузке устройств в режиме диагностики все пользовательские данные становятся криптографически недоступными. Это достигается путем использования дополнительного начального бита, настройка которого определяет возможность доступа к ключу носителя, который необходим для доступа к метаданным и, следовательно, к содержимому всех файлов на томе данных, который зашифрован с помощью функции защиты данных. Эта защита распространяется на файлы всех классов защиты (A, B, C и D), а не только на те, которым требуется код-пароль пользователя.

- В системах на кристалле A12 загрузочное ПЗУ Secure Enclave блокирует начальный бит код-пароля, если процессор приложений переходит в режим обновления прошивки устройства (DFU) или Режим восстановления. Если начальный бит код-пароля заблокирован, все операции по его изменению запрещены. Эта мера направлена на то, чтобы предотвратить доступ к данным, защищенным с помощью код-пароля пользователя.

При восстановлении устройства после перехода в режим DFU выполняется возврат в известное исправное состояние, в котором гарантированно присутствует только неизменный код, который подписан компанией Apple. Переход в режим DFU можно выполнить вручную.

См. следующие статьи службы поддержки Apple, посвященные переводу устройства в режим DFU:

Устройство	Статья
iPhone, iPad, iPod touch	Если вы забыли код-пароль для iPhone
Apple TV	Если на Apple TV отображается символ предупреждения
Компьютер Mac с чипом Apple	Возобновление работы или восстановление компьютера Mac с чипом Apple (статья на английском языке)

Защита пользовательских данных в условиях атаки

Пытаясь получить пользовательские данные, злоумышленники могут использовать целый ряд методов: извлечение зашифрованных данных на другой носитель для атаки методом перебора, манипулирование версией операционной системы и другие способы изменения или ослабления политики безопасности устройства для облегчения атаки. Чтобы атаковать данные на устройстве, часто требуется связь с устройством через физический интерфейс, например Lightning или USB. В устройства Apple внедрены функции, помогающие предотвратить такие атаки.

Устройства Apple поддерживают технологию *защиты запечатыванием ключей (SKP)*, которая направлена на то, чтобы криптографические данные было нельзя обработать за пределами устройства и чтобы выявлять внесение изменений в версии операционных систем или в настройки безопасности без соответствующей авторизации пользователя. Эта функция *не* предоставляется сопроцессором Secure Enclave, а поддерживается аппаратными реестрами, которые работают на более низком уровне для обеспечения дополнительного уровня защиты ключей, необходимых для расшифровки пользовательских данных независимо от Secure Enclave.

Примечание. Технология SKP доступна только на устройствах с системами на кристалле Apple.

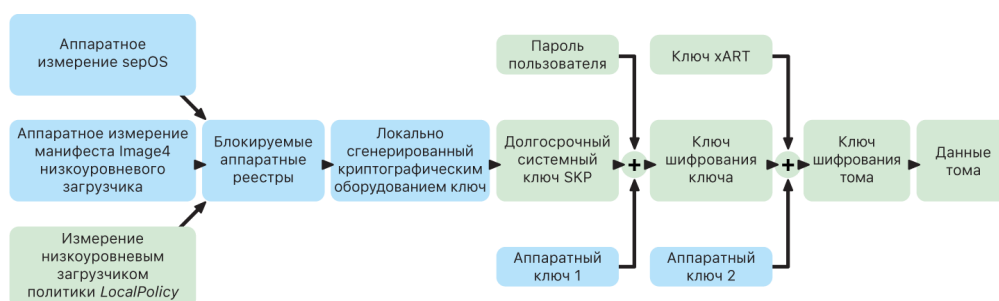
Функция	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, семейство M1
Технология защиты запечатыванием ключей	✓	✓	✓	✓	✓

Можно также настроить iPhone и iPad на активацию подключений для передачи данных только при наличии достаточных признаков того, что устройство остается под физическим контролем авторизованного владельца.

Технология защиты запечатыванием ключей (SKP)

На устройствах Apple, которые поддерживают защиту данных, ключ шифрования ключей (КЕК) защищен (или запечатан) измерениями программного обеспечения в системе, а также привязкой к UID, который доступен только из Secure Enclave. На компьютере Mac с чипом Apple для дополнительной защиты ключа шифрования ключей (КЕК) используется информация о политике безопасности системы, поскольку macOS поддерживает критически важные изменения политики безопасности (например, отключение безопасной загрузки или SIP), которые не поддерживаются на других платформах. На компьютере Mac с чипом Apple эта защита распространяется на ключи [FileVault](#), поскольку система FileVault реализована с использованием технологии защиты данных (класс C).

Ключ, полученный в результате связывания пароля пользователя, долгосрочного ключа SKP и аппаратного ключа 1 (UID из Secure Enclave), называется *ключом на основе пароля*. Этот ключ используется для защиты пользовательского хранилища ключей (на всех поддерживаемых платформах) и ключа KEK (только в macOS), а затем включает биометрическую или автоматическую разблокировку с помощью других устройств, таких как часы Apple Watch.



Монитор загрузки Secure Enclave фиксирует измерение загружаемой операционной системы Secure Enclave. Когда загрузочное ПЗУ процессора приложений измеряет манифест Image4, добавленный в низкоуровневый загрузчик, этот манифест также содержит измерение всех других загруженных парных системных прошивок. В политике LocalPolicy содержатся основные конфигурации безопасности для macOS, которые загружены. Кроме того, в ней содержится поле `ns1h`, в котором указан хэш манифеста Image4 macOS. Манифест Image4 в macOS содержит измерения всех парных прошивок macOS и основных объектов загрузки macOS, таких как загрузочная коллекция ядра или корневой хэш подписанного системного тома (SSV).

Если злоумышленнику удастся неожиданно изменить любой из измеренных компонентов прошивки, программного обеспечения или конфигурации безопасности, это приведет к изменению измерений, которые хранятся в реестрах оборудования. В результате изменения измерений *корневой ключ измерения системы (SMDK)*, сгенерированный криптографическим оборудованием, будет иметь другое значение, что ломает печать, наложенную на иерархию ключей. В результате этого станет невозможным доступ к *ключу измерения системы устройства (SMDK)*, что, в свою очередь, сделает невозможным доступ к ключу KEK и к данным.

Однако, когда система не подвергается атаке, в ней должны быть установлены подлинные обновления программного обеспечения, которые вносят соответствующие изменения в измерения прошивки и в поле `ns1h` политики LocalPolicy с учетом новых измерений macOS. В других системах, в которых предпринимается попытка внедрить измерения системы, но в которых отсутствует проверенный источник доверия, пользователю нужно выключить систему безопасности, обновить прошивку, а затем заново включить систему безопасности, чтобы можно было зафиксировать новое базовое измерение. Это значительно повышает риск стороннего вмешательства в прошивку во время обновления программного обеспечения. Дополнительная защита системы обеспечивается в результате того, что в манифесте Image4 содержатся все необходимые измерения. Оборудование, которое расшифровывает SMDK с помощью SMRK, когда во время обычной загрузки измерения совпадают, также может зашифровать SMDK для предполагаемого будущего SMRK. Путем указания измерений, которые ожидаются после обновления программного обеспечения, оборудование может зашифровать SMDK, доступ к которому имеется в текущей операционной системе, чтобы доступ сохранился в будущей операционной системе. Аналогично, когда клиент законным образом вносит изменения в настройки безопасности в политике LocalPolicy, SMDK должен быть зашифрован для будущего SMRK на основе измерения для LocalPolicy, которое низкоуровневый загрузчик вычисляет при следующей перезагрузке.

Безопасная активация подключений для передачи данных в iOS и iPadOS

Если на устройствах iOS или iPadOS давно не устанавливалось подключение для передачи данных, потребуется использовать Face ID, Touch ID или ввести код-пароль, чтобы активировать подключение для передачи данных, используя разъем Lightning, USB или Smart Connector. Это снижает уязвимость перед физически подключенными устройствами, такими как вредоносные зарядные устройства, и при этом позволяет использовать другие аксессуары с минимальными потерями времени. Если с момента блокировки устройства iOS или iPadOS или завершения соединения с аксессуаром прошло более часа, устройство не позволит установить новое соединение для передачи данных, пока устройство не будет разблокировано. В течение этого часового периода будут разрешены только соединения для передачи данных с аксессуарами, которые ранее подключались к устройству, когда оно было разблокировано. Информация об этих аксессуарах сохраняется в течение 30 дней после прошлого подключения. Если в этот период неизвестный аксессуар пытается установить подключение для передачи данных, все соединения для передачи данных с аксессуарами через Lightning, USB и Smart Connector разрываются до следующей разблокировки устройства. Преимущества использования часового периода:

- Он помогает гарантировать, что при частом подключении к Mac или ПК, аксессуарам USB или при проводном подключении к CarPlay пользователям не придется вводить код-пароль при каждом подсоединении.
- Он необходим, поскольку экосистема аксессуаров не предоставляет криптографически надежного способа идентификации аксессуаров перед установлением соединения для передачи.

Кроме того, если с момента установления соединения с аксессуаром для передачи данных прошло более трех дней, устройство запрещает новые соединения для передачи данных сразу после блокировки. Это увеличивает защищенность пользователей, которые редко пользуются такими аксессуарами. Передача данных через Lightning, USB и Smart Connector также останавливается, если устройство требует ввода код-пароля для возобновления биометрической аутентификации.

Пользователь также может включить передачу данных в Настройках, разрешив выполнять ее всегда (при настройке некоторых вспомогательных устройств это происходит автоматически).

Роль файловой системы Apple

Файловая система Apple (APFS) — собственная файловая система, которая была разработана с учетом новейших требований к шифрованию. APFS используется на всех платформах Apple — iPhone, iPad, iPod touch, Mac, Apple TV и Apple Watch. Она оптимизирована для использования флеш-памяти/SSD и имеет такие функции, как надежное шифрование, копирование при записи с использованием метаданных, совместное использование пространства, клонирование файлов и каталогов, снимки, быстрое определение размера каталогов, атомарные примитивы безопасного сохранения и усовершенствованные принципы файловой системы, а также уникальную технологию копирования при записи, которая использует объединение ввода/вывода для обеспечения максимальной производительности без ущерба для надежности данных.

Совместное использование пространства

APFS выделяет пространство для хранения по запросу. Если один контейнер APFS содержит несколько томов, свободное пространство контейнера используется совместно и может быть выделено любым томам по мере необходимости. Каждый том использует только часть контейнера, поэтому доступное пространство определяется как общий размер контейнера за вычетом пространства, используемого всеми томами контейнера.

Несколько томов

В macOS 10.15 или новее контейнер APFS, используемый для загрузки операционной системы на Mac, должен содержать как минимум пять томов, первые три из которых скрыты от пользователя.

- *Предзагрузочный том.* Этот том не зашифрован. Он содержит данные, необходимые для загрузки каждого системного тома в контейнере.
- *Том виртуальной памяти.* Этот том не зашифрован. Он используется macOS для хранения зашифрованных файлов подкачки.
- *Том восстановления.* Этот том не зашифрован. Он должен быть доступен без снятия защиты с системного тома, чтобы выполнять запуск recoveryOS.
- *Системный том.* Содержит следующие данные:
 - все необходимые файлы для загрузки Mac;
 - все встроенные нативные приложения macOS (эти приложения раньше находились в папке «/Программы», а теперь их можно найти в папке «/Система/Программы»).

Примечание. По умолчанию ни один процесс, даже системный процесс Apple, не имеет права записи в системный том.

- *Том данных.* Содержит изменяемые данные, например:
 - любые данные в папке пользователя, в том числе фото, музыку, видео и документы;
 - установленные пользователем приложения, включая AppleScript и Automator;
 - пользовательские программные среды и демоны, установленные пользователем, организацией или приложениями сторонних разработчиков;
 - другие папки, которые принадлежат пользователю и доступны ему для записи, например: «/Программы», «/Библиотеки», «/Пользователи», «/Volumes», «/usr/local», «/private», «/var» и «/tmp».

Для каждого дополнительного системного тома создается том данных.

Предзагрузочный том, том виртуальной памяти и том восстановления являются общими и не имеют дубликатов.

В macOS 11 или новее для системного тома создается снимок. Операционная система загружается со снимка системного тома, а не просто с изменяемого системного тома, подключенного только для чтения.

В iOS и iPadOS хранилище делится по крайней мере на два тома APFS:

- системный том;
- том данных.

Защита данных связки ключей

Многим приложениям для работы необходимы пароли и другие короткие, но конфиденциальные фрагменты данных, например ключи и токены входа. Связка ключей предоставляет безопасный способ хранения этих элементов. Различные операционные системы Apple используют разные механизмы для обеспечения уровней безопасности, связанных с разными классами защиты связки ключей. В macOS (включая компьютер Mac с чипом Apple) технология защиты данных не используется напрямую для обеспечения этих уровней безопасности.

Обзор

Для шифрования элементов связки ключей используются два разных ключа AES-256-GCM: ключ таблицы (метаданные) и ключ строки (секретный ключ). Метаданные связки ключей (все атрибуты, кроме `kSecValue`) шифруются с помощью ключа метаданных для ускорения поиска, а секретное значение (`kSecValueData`) шифруется с помощью отдельного секретного ключа. Ключ метаданных защищен сопроцессором Secure Enclave, однако кэшируется в процессоре приложений для быстрой отправки запросов к связке ключей. Для доступа к секретному ключу всегда требуется обращение к Secure Enclave.

Связка ключей реализована в виде базы данных SQLite, которая хранится в файловой системе. Существует только одна база данных, и демон `securityd` определяет, к каким элементам связки ключей может обращаться каждый процесс или каждое приложение. API доступа к связке ключей выдают вызовы демону, который запрашивает заданные для приложения права `Keychain-access-groups` (группы доступа к связке ключей), `application-identifier` (идентификатор приложения) и `application-group` (группа приложения). Группы доступа не ограничивают доступ одним процессом, а позволяют нескольким приложениям совместно использовать элементы связки ключей.

Элементы связки ключей могут использоваться совместно только приложениями одного и того же разработчика. Для совместного использования ключей приложения сторонних разработчиков используют группы доступа с префиксом, который был выделен им через программу Apple Developer Program путем распределения по группам приложений. Для принудительного использования префиксов и уникальных групп приложений используются подпись кода, профили обеспечения и [программа Apple Developer Program](#).

Для защиты данных связки ключей используется структура классов, аналогичная структуре, используемой для защиты данных в файлах. Работа этих классов аналогична работе классов защиты данных в файлах, но эти классы используют отдельные ключи и функции.

Доступность	Защита данных в файлах	Защита данных связки ключей
В разблокированном состоянии	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
В заблокированном состоянии	NSFileProtectionCompleteUnlessOpen	Недоступно
После первой разблокировки	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Всегда	NSFileProtectionNone	kSecAttrAccessibleAlways
При включении код-пароля	Недоступно	kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly

Если приложение пользуется службами фонового обновления, оно может использовать класс *kSecAttrAccessibleAfterFirstUnlock* для элементов связки ключей, которые необходимы во время фонового обновления.

Класс *kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly* работает так же, как и *kSecAttrAccessibleWhenUnlocked*, однако его можно использовать, только если на устройстве задан код-пароль. Элементы этого класса существуют только в системном хранилище ключей; они:

- не синхронизируются со Связкой ключей iCloud;
- не включаются в резервные копии;
- не включаются в хранилища ключей передачи.

В случае удаления или сброса код-пароля ключи класса становятся недействительными, что не позволяет использовать эти элементы.

Другие классы связки ключей имеют эквивалент «Только для этого устройства». При перемещении с устройства во время резервного копирования этот эквивалент защищается с помощью UID, что не позволяет восстановить его на другом устройстве. Apple достигла отличного баланса между безопасностью и удобством, выбирая классы связки ключей в зависимости от типа защищаемой информации и от того, когда эта информация необходима операционной системе iOS и iPadOS. Например, VPN-сертификат должен быть доступен постоянно, поэтому устройство поддерживает постоянное подключение, но он классифицируется как «без возможности переноса», поэтому не может быть перемещен на другое устройство.

Функции защиты класса для данных связки ключей

К элементам связки ключей применяются функции защиты следующих классов.

Элемент	Доступность
Пароли Wi-Fi	После первой разблокировки
Учетные записи Почты	После первой разблокировки
Учетные записи Microsoft Exchange ActiveSync	После первой разблокировки
Пароли VPN	После первой разблокировки
LDAP, CalDAV, CardDAV	После первой разблокировки
Токены учетных записей социальных сетей	После первой разблокировки
Ключи шифрования уведомлений Handoff	После первой разблокировки
Токен iCloud	После первой разблокировки
Ключи iMessage	После первой разблокировки
Пароль «Домашней коллекции»	В разблокированном состоянии
Пароли Safari	В разблокированном состоянии
Закладки Safari	В разблокированном состоянии
Резервное копирование с помощью Finder или iTunes	В разблокированном состоянии, без возможности переноса
Личные ключи, установленные профилем конфигурации	В разблокированном состоянии, без возможности переноса
Сертификаты VPN	Всегда, без возможности переноса
Ключи Bluetooth®	Всегда, без возможности переноса
Токен службы Apple Push Notification (APNs)	Всегда, без возможности переноса
Сертификаты и личный ключ iCloud	Всегда, без возможности переноса
PIN-код SIM-карты	Всегда, без возможности переноса
Сертификаты, установленные профилем конфигурации	Всегда
Токен Локатора	Всегда
Автоответчик	Всегда

Контроль доступа к связке ключей

Для установки политик доступа и требований аутентификации связки ключей могут использоваться списки контроля доступа (ACL). Элементы в связке могут задавать условия, требующие участия пользователя, запрещая доступ до тех пор, пока пользователь не выполнит аутентификацию с помощью Face ID, Touch ID либо не введет код-пароль или пароль устройства. Можно также ограничить доступ к элементам, указав, что регистрация с помощью Face ID или Touch ID не должна меняться с момента добавления элемента. Это ограничение направлено на то, чтобы злоумышленник не мог добавить собственный отпечаток пальца и получить доступ к элементу связки ключей. Списки контроля доступа оцениваются внутри Secure Enclave и передаются ядру только при соблюдении заданных ограничений.

Архитектура связки ключей в macOS

macOS также предоставляет доступ к связке ключей для удобного и безопасного хранения имен пользователей и паролей, цифровых удостоверений, ключей шифрования и секретных заметок. Для доступа к связке ключей необходимо открыть приложение «Связка ключей» в папке «/Программы/Утилиты». Использование связки ключей устраняет необходимость вводить — или даже запоминать — учетные данные для каждого ресурса. Для каждого пользователя Mac создается связка ключей по умолчанию. Также пользователи могут создавать другие связки ключей, предназначенные для определенных целей.

Помимо применения пользовательских связок ключей, в macOS используется ряд системных связок ключей, которые поддерживают ресурсы аутентификации, не зависящие от пользователя, такие как учетные данные сетей и идентификаторы инфраструктуры открытых ключей (PKI). Например, неизменяемая связка ключей System Roots хранит сертификаты корневого центра сертификации инфраструктуры открытых ключей интернета, упрощая такие распространенные задачи, как интернет-банкинг и электронная торговля. Аналогичным образом пользователь может развернуть внутренние сертификаты центра сертификации на управляемых компьютерах Mac, чтобы помочь в проверке внутренних веб-сайтов и служб.

FileVault

Шифрование тома с помощью FileVault в macOS

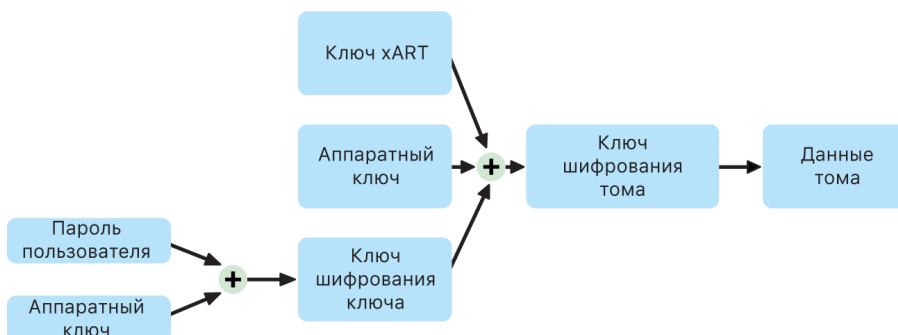
На компьютерах Mac имеется встроенная функция шифрования под названием FileVault, которая защищает все хранящиеся на компьютере данные. FileVault использует алгоритм шифрования данных AES-XTS для защиты всего тома на внутренних и съемных устройствах хранения.

Функция FileVault на компьютере Mac с чипом Apple реализована с использованием технологии защиты данных класса С и ключа тома. На компьютере Mac с чипом безопасности Apple T2 и на компьютере Mac с чипом Apple зашифрованные внутренние устройства хранения, напрямую подключенные к Secure Enclave, используют аппаратные функции безопасности, которые предоставляет этот сопроцессор, а также соответствующие функции модуля AES. Если пользователь включил FileVault на Mac, во время загрузки потребуются ввести учетные данные.

Внутреннее хранилище с включенной функцией FileVault

Без действительных учетных данных для входа или криптографического ключа восстановления внутренние тома APFS останутся зашифрованными и защищенными от несанкционированного доступа, даже если извлечь физическое устройство хранения из компьютера и подключить его к другому компьютеру. В macOS 10.15 это относится и к системному тому, и к тому данных. Начиная с macOS 11 для защиты системного тома применяется функция подписанного системного тома (SSV), однако для защиты томов данных по-прежнему используется шифрование. Шифрование внутреннего тома на компьютере Mac с чипом Apple и на компьютере Mac с чипом T2 осуществляется путем построения и контроля иерархии ключей, и оно основано на технологиях аппаратного шифрования, встроенных в чип. Эта иерархия ключей предназначена для одновременного решения следующих четырех задач:

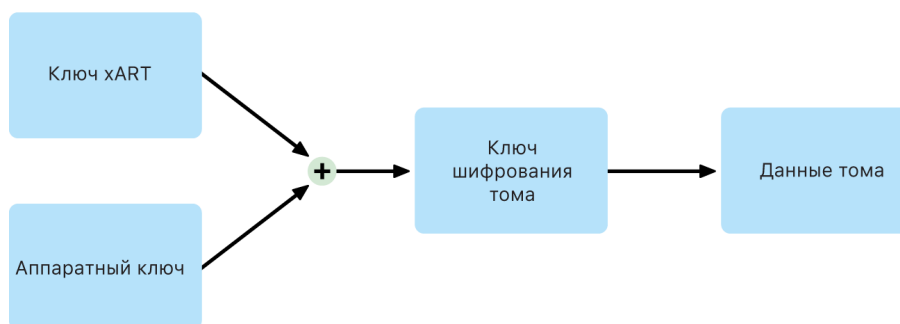
- требование пароля пользователя для дешифрования;
- защита системы от атаки методом перебора, выполняемой непосредственно на носителе информации, который был извлечен из Mac;
- предоставление возможности быстрого и надежного стирания данных путем удаления необходимых криптографических ключей;
- предоставление пользователю возможности изменить свой пароль (и, в свою очередь, криптографические ключи, используемые для защиты его файлов) без необходимости повторного шифрования всего тома.



На компьютере Mac с чипом Apple и компьютере Mac с чипом T2 вся обработка ключа FileVault выполняется в Secure Enclave; ключи шифрования никогда не раскрываются непосредственно процессору Intel. При создании любого тома APFS ему по умолчанию назначается ключ шифрования тома. Содержимое тома и метаданных шифруется с использованием этого ключа шифрования тома, который защищается с помощью ключа класса. При включении FileVault ключ класса защищается с помощью пароля пользователя и аппаратного идентификатора UID.

Внутреннее хранилище с отключенной функцией FileVault

Если на компьютере Mac с чипом Apple или компьютере Mac с чипом T2 в процессе начальной настройки в Ассистенте настройки не включить FileVault, том по-прежнему будет зашифрован, но ключ шифрования тома в Secure Enclave будет защищен только с помощью аппаратного UID.



Если включить FileVault позднее (что будет выполнено мгновенно, поскольку данные уже зашифрованы), механизм антиповтора позволяет предупредить использование старого ключа (основанный только на аппаратном UID) для дешифрования тома. Том будет защищен с помощью сочетания пароля пользователя и аппаратного UID, как было описано ранее.

Удаление томов FileVault

При удалении тома сопроцессор Secure Enclave безопасным образом удаляет его ключ шифрования тома. Данная мера позволяет предупредить дальнейший доступ с помощью этого ключа (даже для сопроцессора Secure Enclave). Кроме того, все ключи шифрования томов помещаются в упаковку в виде ключа носителя. Ключ носителя не обеспечивает дополнительную конфиденциальность данных. Он предназначен для быстрого и надежного удаления данных, поскольку без него дешифрование будет невозможным.

На компьютере Mac с чипом Apple и компьютере Mac с чипом T2 ключ носителя гарантированно стирается технологией, поддерживаемой [Secure Enclave](#), например командами удаленного стирания MDM. Такой способ стирания ключа носителя делает весь том криптографически недоступным.

Съемные устройства хранения

При шифровании съемных устройств хранения не используются функции безопасности Secure Enclave, а шифрование выполняется аналогично шифрованию на компьютере Mac с процессором Intel без чипа T2.

Управление FileVault в macOS

macOS позволяет организациям управлять FileVault с помощью безопасного токена или токена инициализации.

Использование безопасного токена

В файловой системе Apple (APFS) в macOS 10.13 и новее используется новый способ генерирования ключей шифрования FileVault. В предыдущих версиях macOS в томах CoreStorage создание ключей, используемых в процессе шифрования FileVault, происходило, когда пользователь или организация включали FileVault на Mac. В macOS в томах APFS ключи генерируются либо во время создания пользователя (при задании пароля первого пользователя), либо во время первого входа пользователя в систему Mac. Такая реализация ключей шифрования, время их создания и способ хранения составляют часть функции, называемой *безопасный токен*. Если говорить конкретнее, безопасный токен является версией ключа шифрования ключа (КЕК), защищенной с помощью пароля пользователя.

При развертывании FileVault в APFS пользователь сохраняет следующие возможности:

- использование существующих инструментов и процессов, таких как личный ключ восстановления (PRK), который может быть сохранен в системе управления мобильными устройствами (MDM);
- создание и использование корпоративного ключа восстановления (IRK);
- перенос включения FileVault на момент входа пользователя в систему или выхода из системы.

В macOS 11 при задании первоначального пароля первого пользователя на компьютере Mac этому пользователю предоставляется безопасный токен. В некоторых сценариях это может быть нежелательным, так как ранее для предоставления безопасного токена требовалось бы войти в учетную запись пользователя. Чтобы исключить это, добавьте параметр `;DisabledTags;SecureToken` в атрибут `AuthenticationAuthority` пользователя, прежде чем задавать пароль пользователя, как показано ниже.

```
sudo dscl . append /Users/<user name> AuthenticationAuthority  
";DisabledTags;SecureToken"
```

Использование токена инициализации

В macOS 10.15 представлена новая функция — *токен инициализации*. Она помогает предоставлять безопасные токены как для мобильных учетных записей, так и для дополнительной учетной записи администратора, созданной при регистрации устройства («управляемый администратор»). В macOS 11 с помощью токена инициализации можно предоставить безопасный токен любому пользователю, который выполняет вход в систему на компьютере Mac, включая учетные записи локальных пользователей. Для использования функции токена инициализации в macOS 10.15 или новее необходимо следующее:

- регистрация Mac в MDM через Apple School Manager или Apple Business Manager, в результате чего компьютер Mac становится контролируемым;
- поддержка этой функции системой MDM.

В macOS 10.15.4 или новее сгенерированный токен инициализации передается в систему MDM во время первого входа любого пользователя, чей безопасный токен включен (если система MDM поддерживает эту функцию). Токен инициализации также может быть сгенерирован и передан для хранения в систему MDM с использованием инструмента командной строки `profiles`, если необходимо.

В macOS 11 токен инициализации также можно использовать не только для предоставления безопасного токена учетным записям пользователей. На компьютере Mac с чипом Apple токен инициализации, если он имеется, можно использовать для авторизации установки как расширений ядра, так и обновлений программного обеспечения с помощью MDM.

Меры, принимаемые Apple для защиты персональных данных пользователей

Защита при доступе приложений к пользовательским данным

Помимо шифрования данных во время хранения, устройства Apple с использованием разных технологий, в том числе Data Vault, не позволяют приложениям получать доступ к персональной информации без разрешения пользователя. Пользователь может открыть Настройки в iOS и iPadOS или Системные настройки в macOS и посмотреть, какие приложения имеют доступ к определенной информации, а также предоставить или отменить доступ на будущее. Применяются следующие ограничения доступа:

- *iOS, iPadOS и macOS*: «Календари», «Камера», «Контакты», «Микрофон», «Фото», «Напоминания», «Распознавание речи».
- *iOS и iPadOS*: «Bluetooth», «Дом», «Медиа», «Медиа и Apple Music», «Движение и фитнес».
- *iOS и watchOS*: «Здоровье».
- *macOS*: «Монитор входа» (например, нажатие клавиш), «Запрос», «Запись экрана» (например, статические снимки и видеозапись экрана), «Системные настройки».

В iOS 13.4 или новее и iPadOS 13.4 или новее все сторонние приложения автоматически защищают свои данные с помощью Data Vault. Data Vault помогает защитить данные от несанкционированного доступа даже со стороны тех процессов, которые не имеют собственной песочницы. К дополнительным классам в iOS 15 или новее относятся: локальная сеть, функция «Дальномер», данные датчиков и использования, а также фокусирование.

Если пользователь входит в iCloud, приложения в iOS и iPadOS по умолчанию получают доступ к iCloud Drive. Пользователи могут управлять доступом отдельных приложений в разделе «iCloud» в Настройках. Кроме того, iOS и iPadOS позволяют настроить ограничения, которые помогают предупредить передачу данных между приложениями и учетными записями, установленными системой управления мобильными устройствами (MDM), и учетными записями, установленными пользователем.

Защита при доступе к медданным пользователя

HealthKit служит центральным репозиторием данных о состоянии здоровья и физической активности на устройствах iPhone и Apple Watch. HealthKit также напрямую взаимодействует с устройствами для спорта и здоровья, такими как совместимые пульсометры Bluetooth Low Energy (BLE), а также сопроцессор движения, встроенный во многие устройства iOS. Для любого взаимодействия HealthKit с приложениями и устройствами для здоровья и фитнеса, а также медицинскими учреждениями требуется разрешение пользователя. Эти данные имеют класс защиты «Защищено, если не открыто». Доступ к данным закрывается через 10 минут после блокировки устройства. Данные снова становятся доступны, как только пользователь вводит код-пароль или использует Face ID или Touch ID для разблокирования устройства.

Сбор и хранение данных о состоянии здоровья и физической активности

HealthKit также собирает и хранит управляющие данные, такие как таблицы доступа для приложений, имена устройств, подключенных к HealthKit, а также расписания, используемые для запуска приложений при появлении новых данных. Эти данные имеют класс защиты «Защищено до первой аутентификации пользователя». Для хранения медицинских записей, полученных, пока устройство заблокировано (например, во время тренировки пользователя), используются временные файлы журналов. Эти файлы имеют класс защиты «Защищено, если не открыто». При разблокировании устройства временные файлы журналов импортируются в основные базы медданных, после чего удаляются.

Медданные могут храниться в iCloud. Для сквозного шифрования данных приложения «Здоровье» требуется iOS 12 или новее, а также двухфакторная аутентификация. В ином случае данные пользователя по-прежнему шифруются при хранении и передаче, но без сквозного шифрования. При включении двухфакторной аутентификации и обновлении системы до iOS 12 или новее к медданным пользователя применяется сквозное шифрование.

При резервном копировании устройства через Finder (в macOS 10.15 и новее) или iTunes (в macOS 10.14 и более ранних версиях) медданные сохраняются только в том случае, если резервная копия зашифрована.

Данные о состоянии здоровья от медицинских учреждений

Пользователи могут войти в поддерживаемые системы медицинских учреждений через приложение «Здоровье» для получения копии записей о состоянии своего здоровья от этих медицинских учреждений. При подключении пользователя к системе медицинского учреждения он проходит аутентификацию с использованием учетных данных клиента OAuth 2. После подключения пользователя медицинские записи загружаются напрямую из системы медицинского учреждения через защищенное соединение TLS 1.3. После загрузки записи о состоянии здоровья безопасно хранятся вместе с другими медданными.

Целостность медданных

Вместе с блоками данных в базе данных хранятся метаданные, которые позволяют отследить источник каждой записи. Эти метаданные включают идентификатор приложений, которая сохранила запись. Кроме того, метаданные могут включать копию записи с цифровой подписью. Это позволяет обеспечить целостность записей, сгенерированных доверенным устройством. Формат хранения цифровой подписи использует синтаксис криптографических сообщений (CMS), заданный в [RFC 5652](#).

Доступ приложений сторонних разработчиков к медданным

Доступ к API HealthKit контролируется с помощью прав. Кроме того, приложения должны соблюдать ограничения по использованию данных. Например, приложениям запрещено использовать медданные для рекламных целей. Приложения также должны содержать ссылку на политику конфиденциальности, в которой подробно описывается использование медданных.

Доступ приложений к медданным регулируется настройками конфиденциальности пользователя. Когда приложению необходим доступ к медданным, пользователь получает запрос на предоставление доступа (аналогично доступу к Kontakтам, Фото и другим источникам данных iOS). Однако в случае медданных приложения получают доступ отдельно для чтения и записи, а также отдельно для каждого типа медданных. Пользователи могут просматривать и отзываться предоставленные ими разрешения на доступ к медданным, используя раздел «Настройки» > «Здоровье» > «Доступ к данным и устройства».

Если приложениям разрешено записывать данные, они также автоматически получают разрешение на чтение данных, которые они записали. Если у приложений есть доступ к чтению данных, они могут считывать данные, записанные любыми источниками. Однако приложения не могут определить уровень доступа, предоставленного другим приложениям. Кроме того, приложения не могут достоверно сообщить, разрешено ли им чтение медданных. Если у приложения нет доступа для чтения, все запросы возвращают пустые ответы — точно такие же ответы вернула бы пустая база данных. Эта мера направлена на то, чтобы не позволить приложениям анализировать состояние здоровья пользователя, узнав, какие типы данных отслеживает пользователь.

Медкарта для пользователей

Пользователи приложения «Здоровье» могут заполнить медкарту, указав информацию, которая может оказаться важной при оказании неотложной медицинской помощи. Эта информация вводится и обновляется вручную. Она не синхронизируется с информацией в базах медданных.

Для доступа к медкарте необходимо коснуться «SOS» на экране блокировки. Информация хранится на устройстве с классом «Без защиты», поэтому для получения доступа не нужно вводить код-пароль устройства. Пользователи сами решают, какую личную информацию внести в медкарту, с учетом возможной пользы и рисков. В iOS 13 и более ранних версиях эти данные сохраняются в резервных копиях iCloud. В iOS 14 медкарта синхронизируется между устройствами с помощью CloudKit; применяются те же характеристики шифрования, что и для остальных данных приложения «Здоровье».

Обмен данными из приложения «Здоровье»

В iOS 15 пользователи могут поделиться данными из приложения «Здоровье» с другими людьми. Данные приложения «Здоровье» передаются между двумя пользователями с использованием сквозного шифрования iCloud, и Apple не может получить доступ к данным, передаваемым при обмене данными из приложения «Здоровье». Чтобы использовать эту функцию, на устройстве получателя и отправителя должна быть установлена iOS 15 или новее и включена двухфакторная аутентификация.

Пользователи также могут делиться данными из приложения «Здоровье» с медицинским учреждением с помощью функции использования данных приложения «Здоровье» совместно с медицинским учреждением. Данные, передаваемые с использованием этой функции, защищены сквозным шифрованием и доступны только тем медицинским учреждениям, которые выбрал пользователь, и Apple не хранит ключи шифрования и не имеет доступа к ним, а значит, не может расшифровать или просмотреть данные из приложения «Здоровье», а также не может иным способом получить доступ к данным, передаваемым с помощью функции использования данных приложения «Здоровье» совместно с медицинским учреждением. Более подробную информацию о том, как механизмы этой службы защищают пользовательские данные приложения «Здоровье», можно найти в разделе о [безопасности и конфиденциальности](#) в руководстве Apple по регистрации для учреждений здравоохранения.

Цифровая подпись и шифрование

Списки контроля доступа

Данные связки ключей хранятся в отдельных разделах и защищены с помощью списков контроля доступа (ACL). Благодаря этому доступ к учетным данным, которые хранятся в приложениях сторонних разработчиков, не могут получить приложения с другими учетными данными (за исключением случаев, когда пользователь дал свое разрешение на это). Этот механизм защищает учетные данные на устройствах Apple, используемые для аутентификации в различных приложениях и службах внутри организации.

Почта

В приложении «Почта» можно отправлять зашифрованные сообщения, снабженные цифровой подписью. Почта автоматически находит соответствующий адрес электронной почты в формате [RFC 5322](#) (с учетом регистра) или дополнительные имена субъекта в сертификатах цифровой подписи и шифрования во вложенных токенах подтверждения личности (PIV) на совместимых смарт-картах. Если настроенная учетная запись электронной почты совпадает с адресом электронной почты в сертификате цифровой подписи или шифрования на вложенном токене PIV, Почта автоматически отображает кнопку подписи на панели инструментов в окне нового сообщения. Если у приложения «Почта» есть сертификат шифрования электронной почты получателя или оно нашло его в глобальном списке адресов (GAL) Microsoft Exchange, в панели инструментов нового сообщения отображается значок раскрытого замка. Значок закрытого замка означает, что перед отправкой сообщение будет зашифровано с помощью открытого ключа получателя.

Шифрование S/MIME отдельных сообщений

iOS, iPadOS и macOS поддерживают шифрование S/MIME отдельных сообщений. Это означает, что пользователи S/MIME могут по умолчанию подписывать и шифровать все сообщения или выборочно подписывать и шифровать отдельные сообщения.

Идентификационные данные, используемые для S/MIME, могут быть переданы на устройства Apple с помощью профилей конфигурации, системы управления мобильными устройствами (MDM), простого протокола регистрации сертификатов (SCEP) или центра сертификации Microsoft Active Directory.

Смарт-карты

В macOS 10.12 и новее встроена поддержка карт PIV. Эти карты широко используются в коммерческих и правительственных организациях для двухфакторной аутентификации, цифровой подписи и шифрования.

Смарт-карты содержат одно или несколько цифровых удостоверений, которые включают пару из открытого и личного ключей и связанный сертификат. Разблокирование смарт-карты с помощью PIN-кода предоставляет доступ к личным ключам, используемым для операций аутентификации, шифрования и подписания. Сертификат определяет, для чего может использоваться ключ, какие атрибуты с ним связаны и проверен (подписан) ли он сертификатом центра сертификации.

Смарт-карты могут использоваться для двухфакторной аутентификации. Для разблокировки карты необходимо два фактора: «что-то, что есть у пользователя» (карта) и «что-то, что пользователь знает» (PIN-код). В macOS 10.12 и новее также встроена поддержка аутентификации с помощью смарт-карты в окне входа в систему и аутентификации с помощью сертификата клиента на веб-сайтах Safari. Также поддерживается аутентификация Kerberos с использованием пар ключей (PKINIT) для реализации единого входа в службы, поддерживающие Kerberos. Чтобы узнать больше о смарт-картах и macOS, обратитесь к разделу [Вводная информация об интеграции смарт-карт](#) в документе *Развертывание платформы Apple*.

Зашифрованные образы дисков

В macOS зашифрованные образы дисков выступают в качестве безопасных контейнеров, которые пользователи могут использовать для хранения и передачи конфиденциальных документов и других файлов. Для создания зашифрованных образов дисков используется Дисковая утилита, расположенная в папке «/Программы/Утилиты». Образы дисков могут быть зашифрованы с использованием либо 128-битного, либо 256-битного шифрования AES. Поскольку подключенный образ диска рассматривается как локальный том, подключенный к Mac, пользователи могут копировать, перемещать и открывать файлы и папки, которые в нем хранятся. Как и в случае FileVault, шифрование и дешифрование содержимого образа диска выполняется в реальном времени. Используя зашифрованные образы дисков, пользователи могут безопасно обмениваться документами, файлами и папками: зашифрованный образ диска можно сохранить на съемном носителе, отправить в виде вложения в почтовое сообщение или сохранить на удаленном сервере. Подробнее о зашифрованных образах дисков см. в [Руководстве пользователя Дисковой утилиты](#).

Безопасность приложений

Обзор безопасности приложений

На сегодняшний день приложения являются одним из самых важных элементов архитектуры безопасности. Приложения не только значительно повышают продуктивность работы пользователей, но и, если не принять должных мер, могут негативно сказываться на безопасности системы, ее стабильности и пользовательских данных.

Поэтому Apple создает многоуровневую защиту, которая помогает оградить пользователя от приложений, которые содержат известное вредоносное ПО, и приложений, которые были взломаны. Дополнительные меры защиты обеспечивают тщательный контроль доступа приложений к пользовательским данным, выполняемого при посредничестве системы. Эти средства создают стабильную, безопасную платформу для работы приложений, позволяя тысячам разработчиков предлагать сотни тысяч приложений для iOS, iPadOS и macOS без ущерба для целостности системы. А пользователи могут получать доступ к этим приложениям со своих устройств Apple, не опасаясь вирусов, вредоносного ПО или атак.

Для обеспечения самого жесткого контроля все приложения на iPhone, iPad и iPod touch могут быть получены только из App Store — и каждое работает в своей изолированной среде.

Многие приложения на Mac доступны через App Store, однако пользователи Mac также загружают и используют приложения из интернета. Для безопасной загрузки из интернета в macOS предусмотрены дополнительные уровни защиты. Во-первых, по умолчанию в macOS 10.15 и новее все приложения для Mac должны быть заверены компанией Apple. Это требование помогает гарантировать, что приложения для Mac не содержат известного вредоносного ПО, и вместе с тем не ограничивать разработчиков рамками App Store. Кроме того, macOS включает передовые средства защиты от вирусов, которые предназначены для блокирования и, при необходимости, удаления вредоносного ПО.

Механизм песочниц, применяемый на всех платформах, помогает дополнительно защитить пользовательские данные от несанкционированного доступа со стороны приложений. Так как в macOS критически важные данные защищены сами по себе, пользователи могут контролировать доступ приложений к файлам на рабочем столе, в папках «Документы», «Загрузки» и других важных папках. Без согласия пользователя эти данные недоступны ни одному приложению, независимо от того, помещено ли оно в песочницу или нет.

Нативная возможность	Сторонний аналог
Список неодобренных плагинов, список неодобренных расширений Safari	База для обнаружения вирусов, а также известных вредоносных приложений и кода
Файлы на карантине	База для обнаружения вирусов, а также известных вредоносных приложений и кода
Сигнатуры XProtect/YARA	База для обнаружения вирусов, а также известных вредоносных приложений и кода; безопасность конечных устройств
Gatekeeper	Безопасность конечных устройств; требует подписания кода приложений, что помогает запускать только надежное программное обеспечение
efiheck (требуется для компьютера Mac без чипа безопасности Apple T2)	Безопасность конечных устройств; обнаружение пакета rootkit
Программный брандмауэр	Безопасность конечных устройств; применение брандмауэра
Брандмауэр Packet Filter (PF)	Решения для брандмауэров
Защита целостности системы	Встроено в macOS
Средства контроля доступа	Встроено в macOS
Список исключенных расширений ядра	Встроено в macOS
Обязательное подписание программного кода	Встроено в macOS
Заверение приложений	Встроено в macOS

Безопасность приложений в iOS и iPadOS

Безопасность приложений в iOS и iPadOS: введение

В отличие от других мобильных платформ, операционные системы iOS и iPadOS не позволяют пользователям устанавливать потенциально вредоносные неподписанные приложения с веб-сайтов или запускать ненадежные приложения. В процессе выполнения проводятся проверки подписей кода всех исполняемых страниц памяти по мере их загрузки. Это помогает проверить, что приложение не было изменено с момента установки или последнего обновления.

Убедившись, что приложение получено из надежного источника, iOS и iPadOS применяют специальные средства безопасности для защиты других приложений и остальной системы от взлома данным приложением.

Процесс подписания кода приложения в iOS и iPadOS

В iOS и iPadOS компания Apple предлагает такие средства обеспечения безопасности приложений, как обязательная подпись кода, строгий вход в систему для разработчиков и многие другие.

Обязательная подпись кода

После запуска ядро iOS или iPadOS определяет, какие процессы пользователей и приложения могут быть запущены в системе. Чтобы помочь проверить, что все приложения получены из известного и утвержденного источника и не подделаны, iOS и iPadOS требуют, чтобы весь исполняемый код был подписан с помощью выпущенного компанией Apple сертификата. Установленные на устройстве приложения, такие как Почта и Safari, подписаны Apple. Приложения сторонних разработчиков также должны быть проверены и подписаны с помощью выпущенного компанией Apple сертификата. Обязательная подпись кода расширяет концепцию цепочки доверия с операционной системы на приложения. Она помогает принять меры, чтобы приложения сторонних разработчиков не загружали неподписанные фрагменты кода или не использовали самомодифицирующийся код.

Процесс подписания приложений разработчиками

Разработчики могут подписывать свои приложения с помощью сертификатов (в рамках программы Apple Developer Program). Они также могут встраивать в свои приложения различные программные среды и использовать сертификаты, выданные Apple, для проверки кода (с помощью строки идентификатора команды).

- *Проверка сертификата.* Для разработки и установки приложений на устройствах iOS или iPadOS разработчики должны зарегистрироваться в Apple и присоединиться к программе Apple Developer Program. Перед выдачей сертификата компания Apple проверяет личность каждого разработчика, будь то частное лицо или компания, в реальном мире. Используя эти сертификаты, разработчики могут подписывать приложения и отправлять их в App Store для распространения. В результате все приложения в App Store отправляются идентифицированными людьми и организациями, что выступает в качестве сдерживающего фактора для создания вредоносных приложений. Кроме того, Apple проверяет все приложения, что помогает выявить явные ошибки или другие заметные проблемы и определить, соответствуют ли приложения своему описанию. Эта проверка дает пользователям дополнительную уверенность в качестве приложений, которые они покупают.
- *Проверка подписи кода.* Разработчики приложений для iOS и iPadOS могут встраивать в свои приложения различные программные среды, используемые самим приложением или встроенными в него расширениями. Чтобы защитить систему и другие приложения от загрузки стороннего кода в их адресное пространство, в момент загрузки система выполняет проверку подписи кода для всех динамических библиотек, на которые ссылается процесс. Эта проверка выполняется с помощью идентификатора команды (Team ID), который извлекается из выпущенного компанией Apple сертификата. Идентификатор команды представляет собой десятизначную буквенно-цифровую строку, например 1A2B3C4D5F. Приложение может ссылаться на любую библиотеку платформы, поставляемую вместе с системой, и любую библиотеку с таким же идентификатором команды в подписи кода, как у основного исполняемого модуля. Поскольку исполняемые модули, поставляемые с системой, не имеют идентификатора команды, они могут ссылаться только на библиотеки, которые также поставлялись с системой.

Проверка корпоративных приложений собственной разработки

У получивших разрешение компаний есть возможность разрабатывать корпоративные приложения для внутреннего пользования и распространять их среди своих сотрудников. Предприятия и организации могут подать заявку на участие в программе Apple Developer Enterprise Program (ADEP). Для получения дополнительной информации и ознакомления с условиями участия посетите [веб-сайт программы Apple Developer Enterprise Program](#). Став участником программы ADEP, организация может зарегистрироваться и получить профиль обеспечения, который разрешает запускать корпоративные приложения собственной разработки на указанных в профиле устройствах.

Для запуска этих приложений у пользователей должен быть установлен профиль обеспечения. Эта мера направлена на то, чтобы только санкционированные организацией лица могли загружать приложения на устройства iOS и iPadOS. Приложения, установленные через систему управления мобильными устройствами (MDM), по умолчанию считаются доверенными, поскольку взаимосвязь между организацией и устройством уже установлена. В противном случае пользователям необходимо авторизовать профиль обеспечения приложения в Настройках. Организации также могут запретить пользователям одобрять установку приложений неизвестных разработчиков. При первом запуске любого корпоративного приложения собственной разработки устройство должно получить подтверждение от Apple, что это приложение разрешено запускать.

Безопасность в процессе выполнения в iOS и iPadOS

iOS и iPadOS помогают обеспечить безопасность в процессе выполнения с помощью механизма песочницы, декларирования прав и технологии случайного расположения в адресном пространстве (ASLR).

Песочница

Все приложения сторонних разработчиков помещаются в песочницы, что ограничивает их доступ к файлам, хранящимся в других приложениях, и не позволяет вносить изменения в работу устройства. Песочницы были разработаны для того, чтобы не позволить приложениям собирать и изменять информацию, сохраняемую другими приложениями. Каждое приложение использует для своих файлов уникальную домашнюю папку, которая назначается случайным образом при установке приложения. Если приложению стороннего разработчика необходимо получить доступ к чужой информации, оно может сделать это только при помощи специальных служб iOS и iPadOS.

Системные файлы и ресурсы также отделены от приложений пользователей. Большинство системных файлов и ресурсов iOS и iPadOS, а также все приложения сторонних разработчиков работают с правами непривилегированного «мобильного» пользователя. Весь раздел операционной системы подключен только для чтения. Системное программное обеспечение не содержит ненужных инструментов, таких как службы удаленного входа, а API не позволяют приложениям расширять свои полномочия для изменения других приложений или самой iOS и iPadOS.

Использование прав

Для контроля доступа приложений сторонних разработчиков к информации пользователя и таким функциям, как iCloud и расширения, используется декларирование прав. Права — это пары ключ-значение, которые зарегистрированы в приложении и обеспечивают аутентификацию без привязки ко времени выполнения, аналогично идентификатору пользователя в UNIX. Поскольку права защищены цифровой подписью, их невозможно изменить. Системные приложения и демоны широко используют права для выполнения конкретных привилегированных операций — в противном случае для их выполнения требовалось бы использовать корневые процессы. Это значительно снижает вероятность передачи прав взломанным системным приложением или демоном.

Кроме того, приложения могут выполнять фоновую обработку только через системные API. Таким образом приложения продолжают работать без снижения производительности или значительного сокращения времени работы от аккумулятора.

Технология случайного расположения в адресном пространстве

Технология случайного расположения в адресном пространстве (ASLR) помогает защититься от атак, связанных с использованием повреждения памяти. Встроенные приложения используют ASLR, что помогает случайным образом перераспределять все регионы памяти при запуске. В дополнение к работе при запуске технология ASLR случайно располагает в памяти адреса исполняемого кода, системных библиотек и связанных с ними системных компонентов, снижая вероятность использования уязвимостей. Например, атака типа «возврат в библиотеку» пытается путем подмены вынудить устройство выполнить вредоносный код, манипулируя адресами стека и системных библиотек. Случайное размещение этих элементов повышает сложность проведения атаки, особенно при атаке на несколько устройств. Xcode, а также среда разработки iOS и iPadOS, автоматически включает поддержку ASLR в приложения сторонних разработчиков при их компиляции.

Функция Execute Never

Функция Execute Never (XN) архитектуры ARM в iOS и iPadOS помечает страницы памяти как неисполняемые, обеспечивая дополнительную защиту. Страницы памяти, помеченные как доступные для записи и исполняемые, могут использоваться только в жестко контролируемых условиях: ядро проверяет наличие права динамического подписания кода, которое предоставляется только Apple. Даже при его наличии можно выполнить только один вызов `mmap` для запроса исполняемой и доступной для записи страницы, которой присваивается случайный адрес. Safari использует эту функцию в своем компиляторе JavaScript Just-in-Time (JIT).

Поддержка расширений в iOS, iPadOS и macOS

Приложения в iOS, iPadOS и macOS могут предоставлять свои функции другим приложениям посредством расширений. Расширения — это специализированные подписанные исполняемые двоичные файлы, входящие в пакет приложения. Во время установки система автоматически обнаруживает расширения и делает их доступными для других приложений, использующих подходящую систему.

Точки расширения

Область системы, предназначенная для поддержки расширений, называется *точкой расширения*. Каждая точка расширения предоставляет API и обеспечивает применение политик в своей области. Система определяет доступные расширения на основе правил соответствия, заданных для конкретной точки расширения. Система автоматически запускает процессы расширений по мере необходимости и управляет их закрытием. Чтобы ограничить доступность расширений конкретному системному приложению, можно использовать права. Например, виджет «Сегодня» отображается только в Центре уведомлений, а расширение экспорта доступно только в панели общего доступа. Примерами точек расширения являются виджеты «Сегодня», кнопка «Поделиться», действия, редактирование фотографий, источник файлов и настраиваемая клавиатура.

Обмен данными между расширениями

Расширения работают в собственном адресном пространстве. Для обмена данными между расширением и приложением, которое его запустило, используется межпроцессная связь при посредничестве системной программной среды. У них нет доступа к файлам или адресному пространству друг друга. Расширения изолированы друг от друга, от содержащего их приложения и от приложений, которые их используют. Они исполняются в песочнице, как любые другие приложения сторонних разработчиков, а их контейнер отделен от контейнера, содержащего приложение. Однако им доступны те же настройки конфиденциальности, как у приложения-контейнера. Следовательно, если пользователь предоставил приложению доступ к Kontakтам, этот доступ также получают расширения, встроенные в приложение, но не получают расширения, запускаемые приложением.

Использование настраиваемых клавиатур

Настраиваемые клавиатуры являются особым типом расширений, поскольку они включаются пользователем сразу для всей системы. Если включено расширение клавиатуры, оно используется для всех текстовых полей, кроме поля код-пароля и любого поля безопасного ввода текста. Чтобы ограничить передачу данных пользователя, по умолчанию настраиваемые клавиатуры запускаются в песочнице с сильно ограниченными возможностями; эта песочница блокирует доступ к сети, к службам, которые выполняют сетевые операции от имени процесса, а также к интерфейсам API, которые могли бы позволить расширению извлекать вводимые данные. Разработчики настраиваемых клавиатур могут запросить для своего расширения открытый доступ, чтобы после получения согласия от пользователя система могла запускать расширение в песочнице, используемой по умолчанию.

MDM и расширения

На устройствах, которые зарегистрированы в системе управления мобильными устройствами (MDM), расширения для работы с документами и клавиатурами подчиняются правилам управления средой просмотра. Например, система MDM может принять меры, запретив пользователю экспортировать документ из управляемого приложения в неуправляемое хранилище документов или запретив использовать неуправляемую клавиатуру в управляемом приложении. Кроме того, разработчики приложений могут запретить использование сторонних расширений клавиатур в своем приложении.

Защита приложений и группы приложений в iOS и iPadOS

Организации могут использовать комплект SDK для iOS для надежной защиты приложений в iOS и iPadOS, а также вступить в группу обсуждения приложений (App Group) на портале разработчиков Apple (Apple Developer Portal).

Применение защиты данных в приложениях

Комплект разработчика ПО (SDK) для iOS и iPadOS предлагает полный набор API, которые упрощают внедрение технологии защиты данных для сторонних и корпоративных разработчиков, а также помогают им обеспечить высочайший уровень защиты в своих приложениях. Защита данных охватывает API для работы с файлами и базами данных, включая NSFileManager, CoreData, NSData и SQLite.

База данных приложения «Почта» (включая вложения), управляемые книги, закладки Safari, образы запуска приложений и данные о местоположении также хранятся в зашифрованном виде, а защита ключей обеспечивается посредством код-пароля, который задает пользователь. Календарь (без вложений), Контакты, Напоминания, Заметки, Сообщения и Фото имеют класс защиты данных «Защищено до первой аутентификации пользователя».

Установленные пользователем приложения, для которых не задан определенный класс защиты данных, по умолчанию получают класс «Защищено до первой аутентификации пользователя».

Присоединение к группе приложений

Приложения и расширения, принадлежащие учетной записи одного разработчика, могут совместно получать доступ к контенту, если они объединены в группу приложений. Для этого разработчик должен создать подходящие группы на портале разработчиков Apple и включить в них необходимые приложения и расширения. Приложения, настроенные как часть группы приложений, получают доступ к следующим данным:

- общий контейнер на томе, используемый в качестве хранилища, который остается на устройстве, пока на нем установлена хотя бы одно приложение из группы;
- общие настройки;
- общие элементы связки ключей.

Портал разработчиков Apple способствует тому, чтобы у каждой группы приложений был уникальный идентификатор группы (GID) в пределах всей экосистемы приложений.

Проверка аксессуаров в iOS и iPadOS

Программа лицензирования «Made for iPhone, iPad, and iPod touch» (MFi) предоставляет проверенным производителям аксессуаров доступ к протоколу iPod Accessories Protocol (iAP) и необходимым вспомогательным аппаратным компонентам.

Когда аксессуар MFi связывается с устройством iOS или iPadOS через разъем Lightning или USB-C или через Bluetooth, устройство просит его подтвердить, что он авторизован компанией Apple. Для этого аксессуар должен передать устройству предоставленный Apple сертификат, который проверяется устройством. Затем устройство направляет запрос, на который аксессуар должен отправить подписанный ответ. Вся процедура выполняется заказной интегральной микросхемой, которую компания Apple предоставляет утвержденным производителям аксессуаров, и незаметна для самого аксессуара.

Аксессуары могут запрашивать доступ к различным способам передачи и функциям, в том числе к цифровым аудиопотокам через кабель Lightning или USB-C, или к информации о местонахождении, передаваемой по Bluetooth. Интегральная микросхема аутентификации разработана таким образом, чтобы полный доступ к устройству получали только утвержденные аксессуары. Если аксессуар не поддерживает аутентификацию, его доступ ограничен аналоговым аудио и небольшим набором элементов управления воспроизведением через последовательный аудиопорт UART.

AirPlay также задействует интегральную микросхему аутентификации для подтверждения того, что устройства, на которые передаются данные, утверждены Apple. Аудиопотоки AirPlay и видеопотоки CarPlay используют протокол MFi-SAP (протокол сопоставления безопасности), который обеспечивает шифрование данных, передаваемых между аксессуаром и устройством, по алгоритму AES128 в режиме счетчика (CTR). Для обмена динамическими ключами используется алгоритм обмена ключами ECDH (Curve25519). Интегральная микросхема аутентификации подписывает ключи с помощью 1024-битного ключа RSA в рамках протокола Station-to-Station (STS).

Безопасность приложений в macOS

Безопасность приложений в macOS: введение

В macOS реализовано несколько перекрывающихся уровней безопасности приложений, первым из которых является возможность разрешить запуск только подписанных и надежных приложений из App Store. Кроме того, многоуровневая защита macOS помогает предотвратить работу с приложениями, которые загружаются из интернета и содержат известное вредоносное ПО. macOS располагает средствами обнаружения и удаления вредоносного ПО и обеспечивает дополнительные меры защиты, которые разработаны таким образом, чтобы предупредить доступ ненадежных приложений к пользовательским данным. Службы Apple, такие как служба заверения и служба обновлений XProtect, разработаны, чтобы предупредить установку вредоносного ПО. При необходимости эти службы находят вредоносное ПО, которое могло остаться незамеченным, а затем быстро и эффективно удаляют его. Кроме того, пользователи macOS могут выбрать любую модель безопасности, в том числе если она предусматривает запуск неподписанного и ненадежного кода.

Процесс подписи кода приложений в macOS

Все приложения в App Store подписаны Apple. Подписание помогает убедиться, что приложения не были подделаны или изменены. Apple также подписывает все приложения, поставляемые с устройствами Apple.

Чтобы пройти проверку Gatekeeper с настройками по умолчанию в macOS 10.15, все приложения, распространяемые не через App Store, должны быть подписаны разработчиком с помощью выпущенного компанией Apple сертификата идентификатора разработчика (и личного ключа) и заверены компанией Apple. Корпоративные приложения также должны быть подписаны выпущенным компанией Apple идентификатором разработчика, чтобы пользователи могли подтвердить целостность приложений.

В macOS подпись кода и заверение не связаны друг с другом. Они могут быть выполнены разными лицами для разных целей. Разработчик подписывает код с помощью своего сертификата, привязанного к уникальному идентификатору (сертификат выпускается компанией Apple). Благодаря проверке подписи пользователь может убедиться, что программное обеспечение разработчика не было изменено с тех пор, как разработчик выпустил и подписал его. Заверение может быть выполнено любым участником цепочки распространения программного обеспечения. Оно доказывает, что Apple получила копию кода для проверки на наличие вредоносного ПО и что известное вредоносное ПО обнаружено не было. Результатом заверения является билет, который хранится на серверах Apple и может быть при желании прикреплен к приложению (кем угодно), что не приведет к аннулированию подписи разработчика.

В соответствии с обязательными средствами контроля доступа (MAC) для получения прав, защищаемых системой, требуется подпись кода. Например, если приложению требуется доступ через брандмауэр, его код должен быть подписан с помощью соответствующего права MAC.

Gatekeeper и защита в процессе выполнения в macOS

В macOS встроена технология Gatekeeper и защита в процессе выполнения. Эти средства помогают убедиться, что на компьютере Mac пользователя запускается только надежное программное обеспечение.

Gatekeeper

В macOS встроена технология безопасности, называемая *Gatekeeper*. Она проверяет, что по умолчанию на компьютере Mac пользователя запускается только надежное программное обеспечение. Когда пользователь загружает и открывает приложение, плагин или пакет установщика, полученный не через App Store, Gatekeeper проверяет, получено ли это программное обеспечение от подтвержденного разработчика, заверено ли оно Apple как не содержащее известного вредоносного контента и не было ли оно изменено. Gatekeeper также запрашивает согласие пользователя перед первым открытием загруженного программного обеспечения, чтобы убедиться, что пользователь не был обманным образом вынужден запустить исполняемый код, который он считал простым файлом данных.

По умолчанию Gatekeeper работает таким образом, чтобы помочь убедиться, что все загруженное программное обеспечение было подписано App Store или было подписано зарегистрированным разработчиком и заверено Apple. Процесс проверки App Store и процесс заверения направлены на то, чтобы убедиться, что приложение не содержит известного вредоносного ПО. Следовательно, по умолчанию *все программное обеспечение в macOS проверяется на наличие известного вредоносного контента при первом открытии независимо от того, каким образом оно поступило на Mac.*

При желании пользователи и организации могут разрешить установку программного обеспечения только из App Store. Пользователи также могут изменить политики Gatekeeper, чтобы можно было открывать любое программное обеспечение, если эта возможность не ограничена системой управления мобильными устройствами (MDM). Организации могут использовать MDM для настройки параметров Gatekeeper, включая разрешение программного обеспечения, подписанного с помощью других идентификаторов. При необходимости Gatekeeper можно полностью отключить.

Gatekeeper также защищает от распространения вредоносных плагинов через обычные приложения. В некоторых случаях при использовании приложения запускается загрузка вредоносного плагина без ведома пользователя. При необходимости в работу вмешивается Gatekeeper. Он открывает приложения из случайных мест, доступных только для чтения. Эта мера направлена на то, чтобы предупредить автоматическую загрузку плагинов, распространяемых вместе с приложением.

Защита в процессе выполнения

Системные файлы, ресурсы и ядро отделены от пользовательского пространства приложений. Все приложения из App Store помещаются в песочницу, что ограничивает для них доступ к данным, хранящимся в других приложениях. Если приложению из App Store требуется доступ к данным другого приложения, оно может получить его только при помощи API и служб, предоставляемых macOS.

Защита от вредоносного ПО и кода в macOS

Apple использует процесс анализа угроз для быстрого выявления и блокировки вредоносного ПО.

Три уровня защиты

Средства защиты от вредоносного ПО действуют на трех уровнях:

1. *Предотвращение запуска или выполнения вредоносного ПО:* App Store или Gatekeeper в сочетании со службой заверения
2. *Блокировка работы вредоносного ПО в системах пользователя:* Gatekeeper, служба заверения и XProtect.
3. *Устранение вредоносного ПО, которое уже заразило систему:* XProtect

Первый уровень защиты предназначен для предотвращения распространения вредоносного ПО или его однократного запуска. За это отвечают App Store и Gatekeeper в сочетании со службой заверения.

Следующий уровень защиты помогает быстро обнаружить и заблокировать вредоносное ПО в случае его появления на компьютере Mac, что необходимо как для остановки распространения, так и для очистки систем Mac, в которые оно уже внедрилось. В дополнение к Gatekeeper и службе заверения на этом уровне подключается XProtect.

Наконец, XProtect занимается устранением вредоносного ПО, которое смогло успешно запуститься в системе.

В совокупности эти средства, как описано далее, обеспечивают соответствующую надлежащей практике защиту от вирусов и вредоносного ПО. Существуют и другие средства защиты, в частности на компьютере Mac с чипом Apple, для ограничения потенциального ущерба от вредоносного ПО, которому удалось запуститься в системе. macOS может помочь защитить пользовательские данные от вредоносного ПО (см. раздел [Защита при доступе приложений к пользовательским данным](#)) и может ограничивать действия, доступные вредоносному ПО в системе (см. раздел [Целостность операционной системы](#)).

Заверение

Заверение — это служба компании Apple, используемая для выявления вредоносного ПО. Разработчики, которые хотят распространять приложения для macOS не через App Store, отправляют свои приложения на проверку в рамках процесса распространения. Apple проверяет полученное программное обеспечение на наличие известного вредоносного ПО и, если оно не обнаружено, выдает билет заверения. Обычно разработчики прикрепляют этот билет к своим приложениям, чтобы технология Gatekeeper могла проверить и запустить приложение даже без подключения к интернету.

Apple также может выпустить билет аннуляции для приложения, если стало известно, что оно является вредоносным, даже если ранее оно получило заверение Apple. macOS регулярно проверяет наличие новых билетов аннуляции, так что Gatekeeper владеет самой актуальной информацией и может блокировать запуск таких файлов. Этот процесс позволяет очень быстро блокировать вредоносные приложения, поскольку обновления выполняются в фоновом режиме и гораздо чаще, чем даже фоновые обновления сигнатур XProtect. Кроме того, этот механизм защиты может применяться к приложениям, которые ранее были заверены компанией Apple, и к тем, которые не прошли этот процесс.

XProtect

В macOS встроена антивирусная система, которая называется *XProtect*. Она обнаруживает и удаляет вредоносное ПО путем его сравнения с базой сигнатур. Эта система использует сигнатуры YARA, чтобы обнаруживать вредоносное ПО путем сравнения подозрительных файлов с базой сигнатур, регулярно обновляемой Apple. Apple отслеживает новые случаи заражения и разновидности вирусов и автоматически — отдельно от системных обновлений — обновляет сигнатуры. Это позволяет предупредить заражение компьютера Mac вредоносным ПО. XProtect автоматически распознает и блокирует выполнение известного вредоносного ПО. В macOS 10.15 и новее XProtect проверяет программное обеспечение на наличие известного вредоносного контента в следующих ситуациях.

- Приложение запускается в первый раз.
- Приложение было изменено (в файловой системе).
- Сигнатуры XProtect были обновлены.

Когда XProtect распознает известное вредоносное программное обеспечение, оно блокируется, пользователь получает уведомление и может сразу переместить это программное обеспечение в корзину.

Примечание. Заверение эффективно в отношении известных файлов (или хэшей файлов) и может использоваться для приложений, которые ранее уже запускались. Правила анализа сигнатур XProtect являются более универсальными, чем хэш конкретного файла, поэтому данная технология может распознавать варианты, которые Apple еще не видела. XProtect сканирует только те приложения, которые были изменены или запускаются впервые.

Если вредоносное программное обеспечение проникнет на Mac, в этом случае XProtect применит технологию для устранения заражений. Например, ее модуль, предназначенный для устранения заражения, получает автоматические обновления от компании Apple (в автоматических обновлениях системных файлов и в обновлениях системы безопасности). Эта технология также удаляет вредоносное программное обеспечение по мере получения новой информации и периодически выполняет проверку. XProtect не перезагружает Mac автоматически.

Автоматические обновления системы безопасности XProtect

Apple автоматически выпускает обновления для XProtect на основе актуальной доступной информации об угрозах. По умолчанию macOS проверяет наличие таких обновлений ежедневно. Обновления службы заверения, которые распространяются с использованием синхронизации CloudKit, происходят намного чаще.

Реагирование Apple на обнаружение нового вредоносного ПО

Обнаружение нового вредоносного ПО приводит к принятию ряда мер.

- Отзываются любые связанные сертификаты, привязанные к идентификатору разработчика.
- Выпускаются билеты аннуляции заверения для всех файлов (приложений и связанных файлов).
- Разрабатываются и выпускаются сигнатуры XProtect.

Выявленные сигнатуры также применяются ретроактивно к ранее заверенному программному обеспечению, а любые новые случаи обнаружения приводят к выполнению одного или нескольких действий, описанных ранее.

В итоге обнаружение вредоносного ПО запускает ряд шагов, выполняемых в течение последующих секунд, часов и дней, чтобы защитить пользователей Mac, насколько это возможно.

Контроль доступа приложений к файлам в macOS

Компания Apple считает, что приложения могут использовать данные пользователя только с его согласия и только если он полностью понимает и контролирует такое использование. В macOS 10.15 этот подход реализован на уровне системы. Он помогает убедиться, что все приложения получают согласие пользователя перед получением доступа к файлам в папках «Документы» и «Загрузки», а также на рабочем столе, в iCloud Drive и в сетевых томах. В macOS 10.13 и новее приложения, которым требуется доступ ко всему устройству хранения, должны быть явным образом добавлены в Системных настройках. Кроме того, использование функций универсального доступа и автоматизации требует разрешения пользователя. Это помогает убедиться, что они не обходят другие средства защиты. В зависимости от политики доступа, пользователю предлагается или от него требуется изменить настройку в разделе «Системные настройки» > «Защита и безопасность» > «Конфиденциальность».

Элемент	Приложение выводит запрос для пользователя	Пользователь должен изменить системные настройки конфиденциальности
Универсальный доступ		✓
Полный доступ к внутреннему хранилищу		✓
Файлы и папки <i>Примечание.</i> В том числе папки «Рабочий стол», «Документы», «Загрузки», сетевые тома и съемные тома	✓	
Автоматизация (события Apple)	✓	

Приложения, имеющие полный доступ к диску, не имеют доступа к объектам в корзине пользователя и не запрашивают доступ к удаленным объектам. Чтобы эти файлы были доступны приложениям, данные файлы следует переместить из корзины в другое место.

Если пользователь включил FileVault на Mac, то перед продолжением процесса загрузки и получением доступа к специализированным режимам загрузки потребуется ввести действительные учетные данные. Без действительных учетных данных для входа или ключа восстановления том останется зашифрован и защищен от несанкционированного доступа, даже если извлечь физическое устройство хранения из компьютера и подключить его к другому компьютеру.

Чтобы защитить данные в корпоративной среде, ИТ-отдел должен задать политики конфигурации FileVault и включить их применение с помощью системы управления мобильными устройствами (MDM). Организациям доступно несколько способов управления зашифрованными томами, включая корпоративные ключи восстановления, личные ключи восстановления (которые при желании можно передать в MDM для хранения) или их сочетание. В MDM также можно установить политику ротации ключей.

Функции безопасности в приложении «Заметки»

В приложении «Заметки» есть функция «Секретные заметки» (на iPhone, iPad, Mac и веб-сайте iCloud), позволяющая защитить содержимое отдельных заметок. Пользователи также могут безопасно делиться заметками с другими.

Секретные заметки

Секретные заметки защищены с помощью сквозного шифрования с использованием придуманного пользователем пароля, без которого невозможно просмотреть эти заметки на устройствах iOS, iPadOS, macOS и на веб-сайте iCloud. Каждая учетная запись iCloud (включая учетные записи «На моем» устройстве) может иметь свой пароль.

Когда пользователь засекречивает заметку, создается 16-байтный ключ на основе введенного им пароля с использованием алгоритма PBKDF2 и SHA-256. Заметка и все ее вложения шифруются по алгоритму AES в режиме Galois/Counter Mode (AES-GCM). В CoreData и CloudKit создаются новые записи для хранения зашифрованной заметки, вложений, тега и вектора инициализации. После создания новых записей исходные незашифрованные данные удаляются. Следующие вложения поддерживают шифрование: изображения, зарисовки, таблицы, карты и веб-сайты. Заметки, содержащие другие типы вложений, нельзя зашифровать, а неподдерживаемые вложения нельзя добавить в секретные заметки.

Для просмотра секретной заметки пользователь должен ввести пароль или пройти аутентификацию с помощью Face ID или Touch ID. После успешной аутентификации пользователя для просмотра или создания секретной заметки приложение «Заметки» запускает безопасный сеанс. Во время безопасного сеанса пользователь может просматривать секретные заметки или защищать другие заметки, не проходя повторную аутентификацию. Однако безопасный сеанс распространяется только на заметки, защищенные с помощью того же пароля. Если заметки защищены с помощью другого пароля, потребуется аутентификация пользователя. Безопасный сеанс прекращается, если:

- пользователь касается кнопки «Заблокировать» в приложении «Заметки»;
- приложение «Заметки» находится в фоновом режиме более трех минут (восьми минут для macOS);
- устройство iOS или iPadOS блокируется.

Чтобы изменить пароль секретной заметки, пользователь должен ввести текущий пароль, так как для смены пароля нельзя использовать Face ID или Touch ID. После того как пользователь выбрал новый пароль, приложение «Заметки» повторно защищает ключи существующих заметок в той же учетной записи, зашифрованных с использованием предыдущего пароля.

Если пользователь неправильно вводит пароль три раза подряд, приложение «Заметки» показывает подсказку, заданную пользователем при настройке (если она была задана). Если пользователь по-прежнему не может вспомнить пароль, его можно сбросить в настройках Заметок. После этого пользователь сможет создавать новые секретные заметки с новым паролем, но не сможет просматривать секретные заметки, защищенные старым паролем. Если пользователь вспомнит старый пароль, то сможет просматривать старые секретные заметки даже после сброса пароля. Для сброса пароля необходимо знать пароль учетной записи iCloud пользователя.

Общие заметки

Если к заметке не применено сквозное шифрование с использованием пароля, можно предоставить доступ к такой заметке другим пользователям. Для любого текста и вложений, добавляемых пользователем в общую заметку, Apple использует тип зашифрованных данных CloudKit. Ресурсы всегда шифруются ключом, зашифрованным в CKRecord. Метаданные, например даты создания и изменения, не шифруются. CloudKit управляет процессом, используя который участники могут шифровать и дешифровать принадлежащие друг другу данные.

Функции безопасности в приложении «Быстрые команды»

При необходимости быстрые команды из приложения «Быстрые команды» могут быть синхронизированы между устройствами Apple с помощью iCloud. Можно также поделиться быстрыми командами с другими пользователями через iCloud. Быстрые команды хранятся локально в зашифрованном виде.

Пользовательские быстрые команды универсальны: они похожи на скрипты и приложения. При загрузке быстрых команд из интернета пользователь получает предупреждение о том, что быстрая команда не проверена Apple, и может проверить команду самостоятельно. Чтобы защитить пользователя от вредоносных быстрых команд, поддерживается актуальная база известных вредоносных приложений и кода, что позволяет выявлять вредоносные быстрые команды во время их выполнения.

Пользовательские быстрые команды позволяют запускать заданный пользователем код JavaScript на веб-сайтах в Safari при активации на странице экспорта. Чтобы защитить пользователя от вредоносного кода JavaScript, который может, например, обманным образом вынудить пользователя запустить скрипт на веб-сайте социальной сети, который будет собирать данные пользователя, выполняется проверка JavaScript по упомянутой выше базе определений вредоносных приложений. Когда пользователь в первый раз запускает JavaScript в определенном домене, ему предлагается разрешить выполнение быстрых команд, содержащих JavaScript, на текущей веб-странице этого домена.

Безопасность служб

Обзор безопасности служб

Apple предлагает широкий набор служб для повышения практичности и эффективности устройств. Эти службы предоставляют широкие возможности для облачного хранения, синхронизации, хранения паролей, аутентификации, оплаты, обмена сообщениями, связи и других задач, при этом обеспечивая конфиденциальность пользователей и безопасность их данных.

В этой главе рассказывается о технологиях обеспечения безопасности, используемых iCloud, функцией «Вход с Apple», а также Apple Pay, iMessage, Apple Messages for Business, FaceTime, Локатором и функцией непрерывности.

Примечание. Службы и контент Apple доступны не во всех странах и регионах.

Apple ID и управляемый Apple ID

Обзор безопасности Apple ID

Apple ID — это учетная запись, используемая для входа в сервисы и службы Apple. Пользователи должны безопасно хранить данные для входа в учетные записи Apple ID. Это поможет защитить учетные записи от несанкционированного доступа. Для этого Apple ID требует использовать надежные пароли, которые:

- должны содержать не менее восьми символов;
- должны включать буквы и цифры;
- не должны содержать три или более одинаковых символов подряд;
- не должны являться часто используемыми паролями.

Пользователям рекомендуется устанавливать еще более надежные пароли, добавляя дополнительные символы и знаки препинания.

Apple также уведомляет пользователей по электронной почте или в push-уведомлениях либо и тем и другим способом, если в учетную запись были внесены важные изменения, например, если были изменены платежные данные или пароль либо учетная запись Apple ID использовалась для входа на новом устройстве. Если что-то выглядит незнакомым, пользователям рекомендуется незамедлительно изменить пароль своего Apple ID.

Кроме того, Apple задействует целый ряд политик и процедур для защиты учетных записей пользователей. Сюда входит ограничение количества попыток входа и попыток сброса пароля, активный мониторинг мошеннических действий для помощи в обнаружении совершаемых атак, а также регулярный пересмотр политик с учетом любой новой информации, которая может повлиять на безопасность пользователей.

Примечание. Политика паролей для управляемых Apple ID задается администратором в Apple School Manager или Apple Business Manager.

Двухфакторная аутентификация

Чтобы помочь пользователям дополнительно защитить учетные записи, Apple по умолчанию использует *двухфакторную аутентификацию* — дополнительный уровень защиты Apple ID. Она помогает гарантировать, что доступ к учетной записи может получить только ее владелец, даже если кто-то другой знает пароль учетной записи. При использовании двухфакторной аутентификации доступ к учетной записи пользователя возможен только с доверенных устройств, таких как iPhone, iPad, iPod touch или Mac пользователя, а также с других устройств после их подтверждения с помощью одного из доверенных устройств или доверенных номеров телефона. Для первого входа в систему на любом новом устройстве требуется два фрагмента информации: пароль Apple ID и шестизначный цифровой проверочный код, который отображается на доверенных устройствах пользователя или отправляется на доверенный номер телефона. Указав данный код, пользователь подтверждает, что он доверяет новому устройству и что с этого устройства можно входить в систему. Теперь для получения доступа к учетной записи пользователя недостаточно одного пароля. Двухфакторная аутентификация повышает безопасность Apple ID и всей личной информации пользователя, которая хранится в Apple. Эта функция интегрирована в iOS, iPadOS, macOS, tvOS, watchOS и системы аутентификации, используемые на веб-сайтах Apple.

Когда пользователь выполняет вход на веб-сайте Apple, используя веб-браузер, на все доверенные устройства, связанные с учетной записью iCloud пользователя, передается запрос подтверждения веб-сеанса (второй фактор аутентификации). Если пользователь входит в систему веб-сайта Apple через веб-браузер на доверенном устройстве, код проверки отображается локально на этом доверенном устройстве. После ввода кода на этом устройстве пользователь подтверждает веб-сеанс.

Сброс пароля и восстановление доступа к учетной записи

Если пользователь забыл пароль учетной записи Apple ID, он может сбросить его на доверенном устройстве. Если доверенное устройство недоступно, но пользователь знает пароль, можно выполнить аутентификацию путем отправки кода проверки на номер телефона, используемый доверенным устройством. Кроме того, для быстрого восстановления доступа к Apple ID можно выполнить сброс, введя код-пароль, который использовался ранее, и код проверки из сообщения. Если проблему нельзя решить указанными способами, необходимо следовать процедуре восстановления доступа к учетной записи. Дополнительная информация приведена в статье службы поддержки Apple: [Восстановление учетной записи в случае, если сбросить пароль Apple ID не удастся](#).

Безопасность управляемых Apple ID

Управляемые Apple ID функционируют во многом аналогично обычным Apple ID, но принадлежат компании или образовательному учреждению, которые ими управляют. Эти организации могут сбрасывать пароли, ограничивать покупки и возможности связи, например выключать FaceTime и Сообщения, а также устанавливать права доступа на основе ролей для сотрудников, преподавателей и учащихся.

Для управляемых Apple ID выключены некоторые службы (например, Apple Pay, Связка ключей iCloud, HomeKit и Локатор).

Контроль управляемых Apple ID

Управляемые Apple ID поддерживают возможность *контроля*, что позволяет организациям соблюдать требования законодательства и нормативы в области конфиденциальности. Администратор Apple School Manager, менеджер или преподаватель могут проверять определенные управляемые Apple ID в рамках контроля.

Инспекторы могут проводить проверку только учетных записей, расположенных в иерархии организации ниже, чем они сами. Например, преподаватели могут контролировать учащихся, руководители могут контролировать преподавателей и учащихся, а администраторы могут контролировать руководителей, преподавателей и учащихся.

Если через Apple School Manager запросить учетные данные для контрольной проверки, будет создана специальная учетная запись с доступом только к тому управляемому Apple ID, для которого запрошена контрольная проверка. Инспектор может читать и изменять контент пользователя, хранящийся в iCloud или приложениях с поддержкой CloudKit. Все запросы на получение аудиторского доступа сохраняются в журнале Apple School Manager. В журналах содержится следующая информация: кто был инспектором; управляемый Apple ID, к которому инспектор запросил доступ; время запроса и факт проведения инспекции.

Управляемые Apple ID и личные устройства

Управляемые Apple ID также можно использовать на личных устройствах iOS, устройствах iPadOS и компьютерах Mac, принадлежащих пользователям. В этом случае учащиеся входят в iCloud с использованием управляемого Apple ID, выданного учреждением, и дополнительного пароля, который выступает в качестве второго фактора двухфакторной аутентификации Apple ID. Пока учащиеся используют на своих личных устройствах управляемый Apple ID, Связка ключей iCloud недоступна; контролирующее учреждение также может ограничить использование других функций, например FaceTime или Сообщений. Любые документы iCloud, созданные учащимися во время работы под управляемым Apple ID, могут быть подвергнуты аудиту, как описано выше в этом разделе.

iCloud

Обзор безопасности iCloud

iCloud хранит контакты, календари, фотографии, документы и другие данные пользователя и автоматически поддерживает их актуальность на всех устройствах пользователя. Кроме того, приложения сторонних разработчиков могут использовать iCloud для хранения и синхронизации документов, а также значений ключей для приложений в соответствии с настройками разработчика. Для настройки iCloud пользователям необходимо выполнить вход со своим Apple ID и выбрать нужные службы. Некоторые функции iCloud, такие как iCloud Drive и Резервное копирование iCloud, могут быть выключены ИТ-администратором с помощью профилей конфигурации [системы управления мобильными устройствами \(MDM\)](#).

Для защиты пользовательских данных iCloud применяет надежные методы защиты и строгие политики. Большинство данных iCloud сначала шифруются на устройстве пользователя с помощью ключей iCloud, сгенерированных устройством, и лишь затем выгружаются на серверы iCloud. Для тех данных, которые не защищены сквозным шифрованием, устройство пользователя безопасно выгружает эти ключи iCloud в аппаратные модули системы безопасности iCloud, находящиеся в центрах обработки данных Apple. Это позволяет Apple помогать пользователям с восстановлением данных и расшифровывать данные от имени пользователей, когда им это необходимо (например, при входе на новое устройство, восстановлении из резервной копии или доступе к данным iCloud в интернете). Данные, передаваемые между устройствами пользователя и серверами iCloud, отдельно шифруются при передаче посредством TLS, а серверы iCloud хранят данные пользователей с дополнительным уровнем шифрования при хранении.

Ключи шифрования, когда они доступны Apple, надежно хранятся в центрах обработки данных Apple. При обработке данных, хранящихся в стороннем центре обработки данных, эти ключи шифрования доступны только программному обеспечению Apple, запущенному на защищенных серверах, причем только тогда, когда выполняется требуемая обработка. В качестве дополнительной меры обеспечения конфиденциальности и безопасности многие службы Apple используют сквозное шифрование. Благодаря этому доступ к пользовательским данным iCloud может получить только сам пользователь и только с доверенных устройств, на которых пользователь выполнил вход со своим Apple ID.

Apple также предлагает пользователям два варианта шифрования и защиты данных, хранящихся в iCloud.

- **Стандартная защита данных (выбрана по умолчанию).** Пользовательские данные iCloud зашифрованы, ключи шифрования надежно хранятся в центрах обработки данных Apple, а Apple может помогать с восстановлением данных и учетной записи. Сквозным шифрованием защищены лишь некоторые данные iCloud — 14 категорий данных, в том числе данные Здоровья и пароли в Связке ключей iCloud.
- **Расширенная защита данных для iCloud.** Необязательная настройка, которая обеспечивает наивысший уровень защиты облачных данных, предлагаемый Apple. Если пользователь включает Расширенную защиту данных, то доступ к ключам шифрования большей части данных iCloud этого пользователя остается только у доверенных устройств пользователя, при этом данные защищены сквозным шифрованием. Когда у Вас включена Расширенная защита данных, сквозным шифрованием защищены 23 категории Ваших данных, в том числе резервные копии iCloud, Фото, Заметки и другие данные.

Конкретные категории данных iCloud, защищенных сквозным шифрованием, перечислены в статье службы поддержки Apple [Обзор системы защиты данных в iCloud](#).

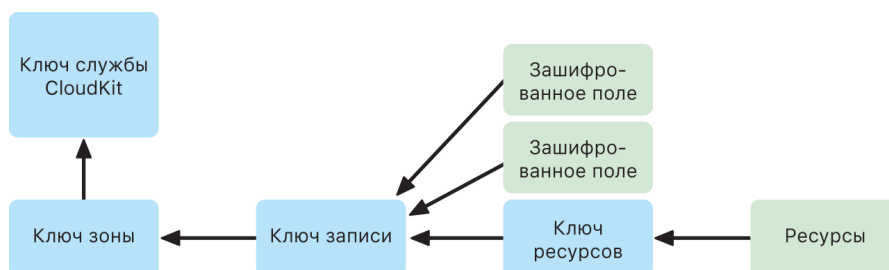
Шифрование в iCloud

Шифрование данных в iCloud тесно связано с моделью защиты данных, начиная с программных сред CloudKit и интерфейсов API, которые позволяют приложениям и системному ПО хранить пользовательские данные в iCloud и поддерживать актуальность всех данных на различных устройствах и в интернете.

Шифрование в CloudKit

[CloudKit](#) — это программная среда, с помощью которой разработчики приложений могут хранить в iCloud данные типа ключ-значение, структурированные данные и ресурсы (крупные массивы данных, хранящиеся отдельно от базы данных, например изображения или видео). CloudKit поддерживает как открытые, так и личные базы данных, объединенные в контейнеры. К личным базам данных предоставляется глобальный доступ, обычно они используются общими ресурсами и не шифруются. В личных базах данных хранятся данные iCloud каждого пользователя.

CloudKit использует иерархию ключей, которая соответствует структуре данных. Личная база данных каждого контейнера защищена иерархией ключей с корнем в асимметричном ключе, который называется *ключом службы CloudKit*. Эти ключи уникальны для каждого пользователя iCloud и генерируются на их доверенных устройствах. Когда данные записываются в CloudKit, ключи всех записей генерируются на доверенном устройстве пользователя и привязываются к соответствующей иерархии ключей перед выгрузкой любых данных.



Многие службы Apple, перечисленные в статье службы поддержки Apple [Обзор системы защиты данных в iCloud](#), используют сквозное шифрование с помощью ключа службы CloudKit, который защищен посредством синхронизации Связки ключей iCloud. Для таких контейнеров CloudKit ключи служб хранятся в Связке ключей iCloud пользователя и обладают такими же характеристиками безопасности, как Связка ключей iCloud; ключи служб доступны только на доверенных устройствах пользователя и недоступны Apple и любым третьим сторонам. В случае утери устройства пользователь может восстановить данные своей Связки ключей iCloud, используя [Безопасное восстановление Связки ключей iCloud, контакты для восстановления доступа](#) или ключ восстановления учетной записи.

Управление ключами шифрования

Безопасность защищенных данных в CloudKit основана на надежности соответствующих ключей шифрования. Ключ службы CloudKit разделены на две категории: защищенные сквозным шифрованием и доступные после аутентификации.

- **Ключи служб, защищенные сквозным шифрованием.** Для служб iCloud, защищенных сквозным шифрованием, соответствующие частные ключи службы CloudKit никогда не становятся доступны для серверов Apple. Пары ключей служб, в том числе частные ключи, создаются локально на доверенном устройстве пользователя и передаются на другие устройства пользователя в соответствии с нормами [безопасности Связки ключей iCloud](#). Несмотря на то, что восстановление Связки ключей iCloud и процессы синхронизации выполняются через серверы Apple, эти серверы не могут получить доступ к любым данным связки ключей пользователя благодаря ее шифрованию. В наихудшем сценарии потери доступа к Связке ключей iCloud и всем механизмам ее восстановления данные в CloudKit, защищенные сквозным шифрованием, окажутся потеряны. Apple не может помочь в восстановлении этих данных.
- **Ключи служб, доступные после аутентификации.** Для других служб, таких как Фото и iCloud Drive, ключи служб хранятся в аппаратных модулях системы безопасности iCloud, находящихся в центрах обработки данных Apple, и к ним могут получать доступ некоторые службы Apple. Когда пользователь входит в iCloud на новом устройстве и аутентифицирует свой Apple ID, серверы Apple могут получать доступ к этим ключам без дальнейших действий пользователя. Например, после входа на сайт [iCloud.com](#) пользователь может сразу просматривать свои фото онлайн. Эти ключи служб являются ключами, доступными после аутентификации.

Расширенная защита данных для iCloud

Расширенная защита данных для iCloud — это необязательная настройка, которая обеспечивает наивысший уровень защиты облачных данных, предлагаемый Apple. Когда пользователь включает Расширенную защиту данных, доступ к ключам шифрования большей части данных iCloud этого пользователя остается только у доверенных устройств пользователя, при этом данные защищены *сквозным шифрованием*. У пользователей, включивших Расширенную защиту данных, сквозным шифрованием защищены не 14, а 23 категории данных, в том числе резервные копии iCloud, Фото, Заметки и другие данные.

Расширенная защита данных для iCloud станет доступна пользователям в США к концу 2022 года и начнет становиться доступной в других странах мира с начала 2023 года.

Концепция Расширенной защиты данных проста. Все ключи служб CloudKit, которые были сгенерированы на устройстве и затем выгружены в *доступные после аутентификации* аппаратные модули системы безопасности (HSM) iCloud, находящиеся в центрах обработки данных Apple, удаляются из этих HSM и остаются только в домене защиты Связки ключей iCloud данной учетной записи. Они обрабатываются так же, как имеющиеся ключи служб, *защищенные сквозным шифрованием*. Это означает, что Apple больше не может получать доступ к этим ключам.

Расширенная защита данных также автоматически защищает поля CloudKit, которые отмечены как зашифрованные сторонними разработчиками, и все ресурсы CloudKit.

Включение Расширенной защиты данных

Когда пользователь включает Расширенную защиту данных, доверенная платформа этого пользователя выполняет два действия. Сначала она передает намерение пользователя включить Расширенную защиту данных для других устройств этого пользователя, защищенных сквозным шифрованием. Для этого она записывает новое значение, подписанное локальными ключами устройств, в метаданные устройств в Связке ключей iCloud. Серверы Apple не могут удалить или изменить эту информацию, и она синхронизируется с другими устройствами пользователя.

Затем устройство запускает удаление ключей служб, *доступных после аутентификации*, из центров обработки данных Apple. Поскольку эти ключи защищены HSM iCloud, они удаляются немедленно, навсегда и без возможности восстановления. После удаления этих ключей Apple больше не может получить доступ к *любым* данным, защищенным ключами служб пользователя. В этот момент устройство начинает процедуру асинхронной ротации ключей, в ходе которой создается новый ключ службы для каждой из служб, ключи которых ранее были доступны для серверов Apple. Если выполнить ротацию ключей не удастся из-за сбоя сетевого соединения или другой ошибки, устройство повторяет попытки ротации ключей до ее успешного выполнения.

После успешной ротации ключей служб новые данные, записанные в службу, становятся невозможно расшифровать с помощью старого ключа службы. Эти данные защищены новым ключом, который управляется только доверенными устройствами пользователя и никогда не был доступен для Apple.

Расширенная защита данных и веб-доступ к iCloud.com

Когда пользователь впервые включает Расширенную защиту данных, веб-доступ к данным этого пользователя на iCloud.com автоматически выключается. Причиной является то, что у веб-серверов iCloud больше нет доступ к ключам, необходимым для расшифровки и отображения данных пользователя. При желании пользователь может снова включить веб-доступ и использовать свое доверенное устройства для доступа к своим зашифрованным данным iCloud через интернет.

После включения веб-доступа пользователь должен авторизовать онлайн-вход в систему на одном из своих доверенных устройств при каждом посещении сайта iCloud.com. Такая авторизация дает устройству право на веб-доступ. В течение следующего часа это устройство принимает от определенных серверов Apple запросы на загрузку отдельных ключей служб, но только тех, которые соответствуют списку разрешенных служб, обычно доступных на iCloud.com. Иными словами, даже после того, как пользователь авторизует онлайн-вход в систему, запрос сервера не сможет вынудить устройство пользователя выгрузить ключи служб для данных, которые не предназначены для просмотра на iCloud.com (например, данных Здоровья или паролей в Связке ключей iCloud). Серверы Apple запрашивают только те ключи служб, которые необходимы для расшифровки конкретных данных, к которым пользователь запрашивает доступ в интернете. При каждой выгрузке ключа службы этот ключ шифруется с использованием кратковременного ключа, привязанного к веб-сеансу, который авторизован пользователем, а на устройстве пользователя отображается уведомление с указанием службы iCloud, данные которой временно становятся доступными для серверов Apple.

Сохранение выбора пользователя

Настройки Расширенной защиты данных и веб-доступа к iCloud.com могут быть изменены только пользователем. Эти значения хранятся в метаданных устройства в Связке ключей iCloud пользователя и могут быть изменены только с одного из доверенных устройств пользователя. Серверы Apple не могут изменять эти настройки от имени пользователя и не могут возвращать их к предыдущим конфигурациям.

Возможные угрозы для безопасности при общем доступе и совместной работе

В большинстве случаев, когда пользователи делятся контентом для совместной работы (например, настраивают общие заметки, общие напоминания, общие папки в iCloud Drive или общую медиатеку iCloud) и у всех участников включена Расширенная защита данных, серверы Apple используются только для настройки общего доступа, но не имеют доступа к ключам шифрования общих данных. Контент по-прежнему защищен сквозным шифрованием и доступен только на доверенных устройствах участников. При открытии общего доступа к каждому объекту Apple может сохранять заголовок и информативную миниатюру этого объекта со стандартной защитой данных, чтобы предоставлять получателям возможность предварительного просмотра.

Если при включении общего доступа пользователь выбирает вариант «всем, у кого есть ссылка», контент становится доступным для серверов Apple со стандартной защитой данных, так как серверам необходима возможность предоставлять доступ всем, кто открывает URL-ссылку.

Функция совместной работы в iWork и функция «Общие альбомы» в приложении «Фото» не поддерживают Расширенную защиту данных. Когда пользователи совместно работают над документом iWork или открывают документ iWork из общей папки в iCloud Drive, ключи шифрования этого документа безопасно выгружаются на серверы iWork в центрах обработки данных Apple. Причиной этого является то, что при совместной работе в iWork в режиме реального времени изменения документа синхронизируются между участниками через сервер. Фото, добавленные в функцию «Общие альбомы», хранятся со стандартной защитой данных, так как эта функция разрешает делать альбомы общедоступными в интернете.

Выключение Расширенной защиты данных

Пользователь может в любое время выключить Расширенную защиту данных. Если пользователь это делает:

1. Устройство пользователя сначала записывает новый выбор в метаданные участия в Связке ключей iCloud, и эта настройки безопасно синхронизируется на все устройства пользователя.
2. Устройство пользователя безопасно выгружает ключи служб для всех служб, доступных после аутентификации, в HSM iCloud в центрах обработки данных Apple. При этом никогда не выгружаются ключи служб, защищенных сквозным шифрованием со стандартной защитой данных, таких как Связка ключей iCloud и Здоровье.

Устройство выгружает как исходные ключи служб, сгенерированные до включения Расширенной защиты данных, так и новые ключи служб, сгенерированные после включения этой функции. При этом все данные в этих службах становятся доступными после аутентификации, а для учетной записи снова начинает действовать стандартная защита данных, при которой Apple может помогать пользователю восстанавливать большинство данных, если пользователь потеряет доступ к своей учетной записи.

Данные iCloud, для которых не действует Расширенная защита данных

Из-за необходимости взаимодействия с глобальными системами электронной почты, контактов и календарей Почта iCloud, Контакты iCloud и Календарь iCloud не защищены сквозным шифрованием.

iCloud хранит некоторые данные без защиты уникальных для пользователя ключей служб CloudKit, даже когда включена Расширенная защита данных. Чтобы данные были защищены, поля записей CloudKit должны быть явным образом объявлены как «зашифрованные» в схеме контейнера, а для зашифрованных полей чтения и записи требуется использовать специальные [API](#). Дата и время изменения файлов или объектов используются для сортировки информации пользователя, а контрольные суммы файлов и данных фото помогают Apple устранять дублирование и оптимизировать хранилище данных пользователя в iCloud и на устройстве, не получая доступа к самим файлам и фото. Подробная информация о том, как применяется шифрование для конкретных категорий данных, приведена в статье службы поддержки Apple [Обзор системы защиты данных в iCloud](#).

Такие решения, как использование контрольных сумм для устранения дублирования данных (широко известная технология *конвергентного шифрования*) изначально были встроены в службы iCloud в момент их запуска. Эти метаданные всегда зашифрованы, но Apple хранит ключи шифрования со стандартной защитой данных. Продолжая работу по усилению защиты данных всех пользователей, Apple внедряет сквозное шифрование новых типов данных, в том числе этого типа метаданных, для пользователей, включивших Расширенную защиту данных.

Требования для Расширенной защиты данных

Чтобы включить Расширенную защиту данных для iCloud, необходимо соблюдение следующих требований.

- Учетная запись пользователя должна поддерживать сквозное шифрование. Для сквозного шифрования требуется двухфакторная аутентификация Apple ID пользователя, а на доверенных устройствах пользователя должен быть задан пароль или код-пароль. Подробная информация приведена в статье службы поддержки Apple [Двухфакторная аутентификация для идентификатора Apple ID](#).
- Устройства, на которых пользователь выполнил вход со своим Apple ID должны быть обновлены до iOS 16.2, iPadOS 16.2, macOS 13.1, tvOS 16.2, watchOS 9.2 и новейшей версии iCloud для Windows. Это необходимо для того, чтобы исключить возможность неправильной обработки новых созданных ключей в iOS, iPadOS, macOS, tvOS или watchOS: система может повторно выгрузить их в HSM, *доступные после аутентификации*, ошибочно пытаясь восстановить состояние учетной записи.
- Пользователь должен настроить как минимум один альтернативный способ восстановления (один или несколько контактов для восстановления доступа или ключ восстановления), с помощью которого пользователь сможет восстановить свои данные iCloud, если потеряет доступ к своей учетной записи.

Если способы восстановления не сработают (например, данные контакта для восстановления доступа устарели или пользователь их забыл), Apple не сможет помочь с восстановлением пользовательских данных iCloud, защищенных сквозным шифрованием.

Расширенную защиту данных для iCloud можно включать только для Apple ID. Управляемые Apple ID и детские учетные записи (зависит от страны или региона) не поддерживаются.

Безопасность резервного копирования iCloud

Используя Wi-Fi, iCloud ежедневно выполняет резервное копирование информации, включая настройки устройства, данные приложений, фото и видео из альбома «Фотоплёнка» и разговоры из приложения «Сообщения». Резервное копирование iCloud выполняется только в том случае, если устройство заблокировано, подключено к источнику питания и подключено к интернету по Wi-Fi. Учитывая шифрование хранилища данных в iOS и iPadOS, резервное копирование iCloud обеспечивает защиту данных и при этом позволяет выполнять инкрементное резервное копирование и восстановление без участия пользователя. По умолчанию в аппаратных модулях системы безопасности iCloud в центрах обработки данных Apple хранится резервная копия ключа службы резервного копирования в iCloud. Этот ключ относится к категории данных, доступных после аутентификации. Для пользователей, включивших Расширенную защиту данных для iCloud, ключ службы резервного копирования в iCloud защищен сквозным шифрованием и доступен только самим пользователям на их доверенных устройствах.

Если созданные файлы имеют такие классы защиты данных, которые недоступны при заблокированном устройстве, их ключи файлов шифруются с использованием ключей классов из хранилища ключей резервного копирования в iCloud, а файлы включаются в резервные копии iCloud в исходном (зашифрованном) состоянии. Все файлы шифруются во время передачи, а во время хранения все файлы шифруются с использованием ключей на основе учетных записей, как описано в разделе [о шифровании в CloudKit](#).

Хранилище ключей резервного копирования в iCloud содержит асимметричные ключи (Curve25519) для таких классов защиты данных, доступ к которым запрещен, когда устройство заблокировано. Комплект резервной копии хранится в учетной записи iCloud пользователя и состоит из копии файлов пользователя и хранилища ключей резервного копирования в iCloud. Хранилище ключей резервного копирования в iCloud защищено случайным ключом, который также сохраняется в комплекте резервной копии. (Пользовательский пароль iCloud не используется для шифрования, поэтому изменение пароля iCloud не приводит к аннулированию имеющихся резервных копий.)

При восстановлении из пользовательской учетной записи iCloud извлекаются резервные копии файлов, хранилища ключей резервного копирования в iCloud и ключа от этого хранилища ключей. Сначала с помощью этого ключа дешифруется хранилище ключей резервного копирования в iCloud, а затем с помощью ключей файлов из хранилища ключей дешифруются файлы, хранившиеся в комплекте резервной копии. Эти файлы записываются в файловую систему как новые файлы, поэтому они повторно шифруются в соответствии со своим классом защиты данных.

При резервном копировании в iCloud создаются резервные копии следующего контента:

- Информация о приобретенной музыке, фильмах, телешоу, приложениях и книгах. Резервная копия iCloud включает информацию о приобретенном контенте, который находится на принадлежащем пользователю устройстве, но не сам приобретенный контент. Когда пользователь восстанавливает данные из резервной копии iCloud, приобретенный контент автоматически загружается из iTunes Store, App Store, приложения Apple TV или Apple Books. Некоторые виды контента загружаются автоматически не во всех странах и регионах. Кроме того, покупки могут быть недоступны, если пользователь вернул за них уплаченные средства или они больше не представлены в соответствующем магазине. Полная история покупок связана с Apple ID пользователя.
- Фотографии и видео на устройствах пользователя. Обратите внимание, что если пользователь включил Фото iCloud в iOS 8.1, iPadOS 13.1 либо OS X 10.10.3 или новее, фото и видео пользователя уже хранятся в iCloud, поэтому они не включены в резервную копию iCloud.
- Контакты, события календаря, напоминания и заметки.
- Настройки устройства.
- Данные приложений.
- Экран «Домой» и местоположение приложений.
- Конфигурация HomeKit.
- Данные медкарты.

- Пароль голосовых записей (если это необходимо, требуется физическая SIM-карта, которая использовалась при резервном копировании).
- Сообщения, Apple Messages for Business, текстовые сообщения (SMS) и MMS (если это необходимо, требуется физическая SIM-карта, которая использовалась при резервном копировании).

Функция «Резервное копирование iCloud» также используется для резервного копирования локальной связки ключей устройства. При этом она защищена ключом на основе корневого криптографического ключа UID Secure Enclave устройства. Этот ключ уникален для устройства и неизвестен Apple. Благодаря этому восстановить базу данных можно только на том устройстве, с которого она получена, и никто другой, включая Apple, не может ее прочитать. Подробнее см. в разделе [Secure Enclave](#).

Сообщения в iCloud

Функция «Сообщения в iCloud» поддерживает актуальность и доступность всей истории сообщений на всех устройствах пользователя.

При стандартной защите данных Сообщения в iCloud защищены сквозным шифрованием, когда резервное копирование в iCloud выключено. Когда резервное копирование в iCloud включено, в состав резервной копии входит копия ключа шифрования Сообщений в iCloud, что позволяет Apple помогать пользователям с восстановлением их сообщений даже в случае потери доступа к Связке ключей iCloud и доверенным устройствам. Если пользователь выключает резервное копирование в iCloud, на устройстве пользователя генерируется новый ключ для защиты будущих сообщений в iCloud. Новый ключ хранится только в Связке ключей iCloud и доступен только пользователю на его доверенных устройствах, а новые данные, записанные в этот контейнер, будет невозможно расшифровать старым ключом контейнера.

Когда включена Расширенная защита данных, Сообщения в iCloud всегда защищены сквозным шифрованием. Когда включено резервное копирование в iCloud, сквозным шифрованием защищено все содержимое резервной копии, в том числе ключи шифрования Сообщений в iCloud. Ключ службы резервного копирования в iCloud и ключ контейнера Сообщений в iCloud сбрасываются, когда пользователь включает Расширенную защиту данных. Подробная информация приведена в статье службы поддержки Apple [Обзор системы защиты данных в iCloud](#).

Обеспечение безопасности и контакты для восстановления доступа

Пользователи могут добавлять до пяти людей, которым они доверяют, в качестве контактов для восстановления доступа. Эти контакты помогут восстановить доступ к учетной записи и данным iCloud, в том числе всем данным, которые защищены сквозным шифрованием, независимо от того, включена ли Расширенная защита данных. Ни Apple, ни контакт для восстановления доступа сами по себе не обладают информацией, необходимой для восстановления пользовательских данных iCloud, защищенных сквозным шифрованием.

Функционирование контактов для восстановления доступа обеспечивает полную конфиденциальность данных. Apple не знает, кого пользователь назначил контактами для восстановления доступа. Серверы Apple получают информацию о контакте для восстановления доступа только в ходе попытки восстановления, после того как пользователь запрашивает помощь и соответствующий контакт начинает процесс восстановления. После восстановления эта информация не сохраняется.

Процесс обеспечения безопасности с помощью контактов для восстановления доступа

Когда пользователь настраивает контакт для восстановления доступа, ключ для доступа к пользовательским данным iCloud (в том числе данным CloudKit, которые защищены сквозным шифрованием) шифруется надежным случайным ключом. Затем этот случайный ключ разделяется между контактом для восстановления доступа и Apple. Восстановление исходного ключа и доступ к пользовательским данным iCloud возможны только после того, как обе части ключа объединяются в процессе восстановления доступа.

При настройке контакта для восстановления доступа устройство пользователя обменивается данными с серверами Apple, чтобы выгрузить ту часть данных ключа, которая будет храниться у Apple. Затем устройство создает защищенный сквозным шифрованием контейнер CloudKit с контактом для восстановления доступа и использует этот контейнер для отправки той части ключа, которая необходима контакту для восстановления доступа. Кроме того, Apple и контакт для восстановления доступа получают от пользователя один и тот же секретный код авторизации. Этот код позднее потребуется для восстановления доступа. Обмен данными, необходимый, чтобы пригласить контакты для восстановления доступа и получить от них одобрение запроса, происходит через взаимно удостоверенному каналу IDS. Контакт для восстановления доступа автоматически сохраняет полученные данные в своей связке ключей iCloud. Apple не может получить доступ ни к содержимому контейнера CloudKit, ни к связке ключей iCloud, в которых хранятся эти данные. При обмене данными серверы Apple могут прочитать только анонимный идентификатор контакта для восстановления доступа.

Позднее, если пользователю потребуется восстановить доступ к своей учетной записи и данным iCloud, пользователь может запросить помощь у контакта для восстановления доступа. В этот момент на устройстве контакта для восстановления доступа генерируется код восстановления. Контакт для восстановления доступа передает этот код пользователю не в электронном виде (например, сообщает лично или по телефону). Затем пользователь вводит этот код восстановления на своем устройстве, чтобы установить безопасное соединение между устройствами по протоколу SPAKE2+, содержимое которого Apple не может прочитать. За организацию этого процесса отвечают серверы Apple, но Apple не может запустить процесс восстановления.

После установления безопасного соединения и выполнения всех необходимых проверок безопасности устройство контакта для восстановления доступа возвращает свою часть данных ключа и ранее предоставленный секретный код авторизации пользователю, запросившему восстановление. Пользователь передает этот секретный код авторизации на серверы Apple, которые разрешают ему получить доступ к данным ключа, хранящимся у Apple. Предоставив секретный код для авторизации, также можно сбросить пароль учетной записи, чтобы восстановить доступ к ней.

Наконец, устройство пользователя объединяет данные ключа, полученные от Apple и от контакта для восстановления доступа, а затем использует их, чтобы расшифровать и восстановить данные iCloud.

Определенные меры безопасности, в том числе проверка активности учетной записи пользователя, не позволяют контакту для восстановления доступа запустить процесс восстановления без согласия пользователя. Если учетная запись активна, контакту для восстановления доступа также потребуется указать недавний код-пароль устройства или код безопасности iCloud.

Обеспечение безопасности и цифровые наследники

В учетной записи можно назначить цифровых наследников, чтобы передать им свои данные iCloud после смерти. Цифровой наследник получает доступ ко всем данным iCloud умершего пользователя, включая почти все данные, защищенные сквозным шифрованием, но не включая данные Связки ключей iCloud, такие как пароли учетных записей. Технология функционирования цифровых наследников аналогична технологии функционирования контактов для восстановления доступа: надежный случайный ключ, который разделяется между Apple и цифровым наследником, чтобы ни одна из сторон не могла расшифровать данные самостоятельно. Цифровой наследник получает одинаковый набор данных независимо от того, включил ли пользователь Расширенную защиту данных.

Данные ключа, который получает цифровой наследник, в пользовательской документации называется ключом доступа. Эти данные сохраняются на поддерживаемых устройствах автоматически, но их можно распечатать и хранить не в цифровой форме. Дополнительная информация приведена в статье службы поддержки Apple: [Как добавить цифрового наследника для вашего идентификатора Apple ID](#).

После смерти пользователя его цифровые наследники могут запросить доступ, выполнив вход на сайте Apple для заявлений. Для этого требуется предоставить свидетельство о смерти и выполнить частичную авторизацию с помощью секретного кода, упомянутого в предыдущем разделе. После всех проверок безопасности Apple выдает имя пользователя и пароль новой учетной записи и передает необходимые данные ключа цифровому наследнику.

Для более удобного ввода ключа доступа этот ключ предоставляется в виде буквенно-цифрового кода со связанным QR-кодом. После ввода ключа доступ к данным iCloud умершего человека восстанавливается. Это можно сделать на устройстве или в интернете. Подробная информация приведена в статье службы поддержки Apple [Запрос доступа к учетной записи Apple в качестве цифрового наследника](#).

Безопасность Частного узла iCloud

Частный узел iCloud не только помогает защищать пользователя при просмотре веб-сайтов Safari, но и содержит все запросы на разрешение имен в DNS. Благодаря этому никто, даже Apple, не может сопоставить IP-адрес пользователя с его действиями в интернете. Такой результат достигается путем использования разных прокси-серверов: прокси-сервера входящего трафика, управляемого Apple, и прокси-сервера исходящего трафика, управляемого поставщиком контента. Чтобы использовать Частный узел iCloud, требуется iOS 15, iPadOS 15 либо macOS 12.0.1 или новее, а также должен быть выполнен вход в iCloud+ с помощью Apple ID. После этого можно включить Частный узел iCloud, выбрав «Настройки» > «iCloud» или «Системные настройки» > «iCloud».

Подробная информация приведена в [обзоре Частного узла iCloud](#).

Управление код-паролями и паролями

Обзор безопасности пароля

В iOS, iPadOS и macOS для пользователей упрощен процесс безопасной и удобной аутентификации в сторонних приложениях и на веб-сайтах с использованием пароля. Проще всего управлять паролями, если использовать одну учетную запись для входа в разные системы. Используя функцию «Вход с Apple», пользователи могут выполнять вход в приложениях и на веб-сайтах сторонних разработчиков, не создавая дополнительные учетные записи и не запоминая пароли, а пользуясь учетной записью Apple ID, которая защищена двухфакторной аутентификацией. Если веб-сайт не поддерживает функцию «Вход с Apple», можно воспользоваться функцией автоматического создания надежных паролей. Благодаря этой функции устройства пользователя могут автоматически создавать, синхронизировать и вводить уникальные надежные пароли для веб-сайтов и приложений. В iOS и iPadOS пароли сохраняются в специальной связке ключей Автозаполнения паролей. Пользователь может управлять этой связкой ключей в приложении «Настройки» > «Пароли».

Для управления сохраненными паролями в macOS откройте Настройки в Safari и выберите раздел «Пароли». Систему синхронизации также можно использовать для синхронизации паролей, которые были вручную созданы пользователем.

Безопасность функции «Вход с Apple»

Функция «Вход с Apple» предлагает более конфиденциальную, прозрачную и удобную альтернативу другим технологиям единого входа. Пользователь получает возможность контролировать распространение личной информации и может одним касанием выполнять вход в разные системы.

Функция «Вход с Apple» позволяет создавать учетные записи и входить в приложения и на веб-сайты с помощью имеющегося Apple ID, при этом предоставляя пользователю дополнительный контроль личной информации. При создании учетной записи приложения могут запрашивать только имя и адрес электронной почты пользователя, при этом у пользователя всегда есть выбор. Можно сообщить приложению свой адрес электронной почты или не раскрывать его, а вместо этого использовать новую службу ретрансляции частных почтовых адресов Apple. Эта служба создает уникальный анонимный адрес электронной почты, письма с которого будут перенаправляться на личный адрес пользователя. Благодаря этому пользователь сможет получать полезные сообщения от разработчика, при этом защитив личное пространство и контролируя использование персональных данных.

Функция «Вход с Apple» создана для обеспечения безопасности. У каждого пользователя функции «Вход с Apple» должна быть включена двухфакторная аутентификация для его Apple ID. Двухфакторная аутентификация помогает защитить не только Apple ID пользователя, но и учетные записи, которые пользователь создает в приложениях. Кроме того, компания Apple разработала и внедрила в функцию «Вход с Apple» особую меру для борьбы с мошенничеством, которая не нарушает конфиденциальность пользовательских данных. Благодаря этой мере разработчики могут быть уверены в том, что новые пользователи — это реальные люди, а не боты или управляемые скриптами учетные записи.

Автоматическое создание надежных паролей

Если включена Связка ключей iCloud, при регистрации пользователя или изменении пароля на веб-сайте в Safari операционные системы iOS, iPadOS и macOS автоматически создают надежные случайные уникальные пароли. В iOS и iPadOS автоматическое создание надежных паролей также доступно в приложениях. Пользователь должен отказаться от использования надежных паролей, если это не требуется. Созданные пароли сохраняются в связке ключей и синхронизируются между устройствами с помощью Связки ключей iCloud, если она включена.

По умолчанию iOS и iPadOS генерируют пароли длиной 20 символов. Они содержат одну цифру, один символ в верхнем регистре, два дефиса и 16 символов в нижнем регистре. Сложность сгенерированных паролей составляет 71 бит энтропии, что соответствует высокому уровню надежности.

Пароли генерируются на основе эвристической системы, которая определяет, что пользователь обращается к полю пароля для создания пароля. Если эвристической системе не удастся определить, что выполняется создание пароля, разработчики приложения могут установить для своего текстового поля `UITextContentType.newPassword`, а веб-разработчики могут установить для элементов `<input>` значение `autocomplete= "new-password"`.

Приложения и веб-сайты могут сообщать правила, которым должны соответствовать пароли. Это помогает обеспечивать совместимость сгенерированных паролей с соответствующей службой. Для передачи этих правил разработчики должны использовать `UITextInputPasswordRules` или атрибут `passwordrules` в элементах `input`. Устройства будут генерировать самый надежный пароль, соответствующий этим правилам.

Безопасность функции «Автозаполнение паролей»

Функция «Автозаполнение пароля» автоматически вводит учетные данные, которые хранятся в связке ключей. Менеджер паролей Связки ключей iCloud и Автозаполнение пароля предоставляют следующие возможности:

- заполнение учетных данных в приложениях и на веб-сайтах;
- генерирование надежных паролей;
- сохранение паролей в приложениях и на веб-сайтах в Safari;
- безопасная передача паролей контактам пользователя;
- предоставление паролей находящемуся поблизости Apple TV, который запрашивает учетные данные.

Создание и сохранение паролей в приложениях, а также предоставление паролей Apple TV доступно только в iOS и iPadOS.

Автозаполнение пароля в приложениях

Пользователи iOS и iPadOS могут вводить сохраненные имена пользователей и пароли в полях для ввода учетных данных в приложениях аналогично использованию функции «Автозаполнение пароля» в Safari. В iOS и iPadOS пользователям нужно коснуться кнопки с изображением ключа в панели QuickType виртуальной клавиатуры. В macOS, в приложениях, созданных с помощью Mac Catalyst, под полями для ввода учетных данных, отображается раскрывающееся меню «Пароли».

Если приложение надежно связано с веб-сайтом, который использует тот же механизм связывания на основе того же файла apple-app-site-association, в панели QuickType в iOS и iPadOS, а также в раскрывающемся меню macOS отображаются предлагаемые учетные данные приложения, если они сохранены в связке ключей Автозаполнения пароля. Это дает пользователям возможность разрешать раскрытие учетных данных, сохраненных в Safari, приложениям с такими же свойствами безопасности, но без внедрения API в приложения.

Автозаполнение пароля не раскрывает приложению никаких сведений об учетных данных, пока пользователь не разрешит раскрывать учетные данные этому приложению. Списки учетных данных отображаются за пределами процесса приложения.

Если между приложением и веб-сайтом установлены отношения доверия и пользователь вводит учетные данные в приложении, iOS и iPadOS могут выдать запрос на сохранение этих учетных данных в связке ключей Автозаполнения паролей для дальнейшего использования.

Доступ приложений к сохраненным паролям

Когда пользователь пытается выполнить вход, приложения iOS, iPadOS и macOS могут запрашивать помощь связки ключей через `ASAuthorizationPasswordProvider` и `SecAddSharedWebCredential`, чтобы автоматически заполнять пароли. Параметры поставщика пароля и его запроса можно использовать совместно с функцией «Вход с Apple». В результате вызов одного и того же API позволит пользователю войти в приложение независимо от того, был пароль учетной записи задан пользователем или учетная запись была создана с помощью функции «Вход с Apple».

Приложения могут получить доступ к сохраненным паролям только в том случае, если разработчик приложения, администратор веб-сайта и пользователь дали на это согласие. Разработчики приложений выражают свое намерение использовать пароли, сохраненные в Safari, включая в свое приложение соответствующие права. Список прав представляет собой список полных доменных имен соответствующих веб-сайтов. Веб-сайты должны разместить на своем сервере файл со списком уникальных идентификаторов разрешенных Apple приложений.

При установке приложения с правом `com.apple.developer.associated-domains` операционные системы iOS и iPadOS отправляют каждому из перечисленных в списке веб-сайтов TLS-запрос на один из следующих файлов:

- `apple-app-site-association`
- `.well-known/apple-app-site-association`

Если в файле указан идентификатор устанавливаемого приложения, то iOS и iPadOS помечают, что между веб-сайтом и приложением существуют доверительные отношения. Только при наличии доверительных отношений вызовы этих двух API приводят к отображению запроса, в ответ на который пользователь должен согласиться на передачу паролей приложению, их обновление или удаление, прежде чем пароли будут переданы приложению.

Рекомендации по безопасности паролей

В списке паролей автозаполнения в iOS, iPadOS и macOS указывается, какой из сохраненных паролей пользователя *неоднократно используется* на разных веб-сайтах, а также выделяются пароли, которые считаются *ненадежными* или которые были скомпрометированы или украдены в результате *утечки данных*.

Обзор

Использование одного и того же пароля в нескольких службах может сделать эти учетные записи уязвимыми для атаки с использованием украденных учетных данных. Если одна из служб будет взломана, а пароли похищены, злоумышленники смогут использовать те же учетные данные в других службах для взлома дополнительных учетных записей.

- Пароль помечается как *неоднократно использованный*, если один и тот же пароль используется в качестве сохраненного пароля в разных доменах.
- Пароли помечаются как *ненадежные*, если они могут быть легко угаданы злоумышленником. iOS, iPadOS и macOS распознают распространенные шаблоны, используемые для создания легко запоминающихся паролей, например, использование слов из словаря, распространенные подстановки символов (например, использование «p4ssw0rd» вместо «password»), расположенные рядом клавиши (например, «q12we34r» на клавиатуре QWERTY) или повторяющиеся последовательности (например, «123123»). Эти шаблоны часто используются для создания паролей, удовлетворяющих минимальные требования служб, однако они также часто используются злоумышленниками, пытающимися получить пароль методом перебора.

Поскольку многие службы требуют использования именно PIN-кода из четырех или шести цифр, эти короткие код-пароли оцениваются по другим правилам. PIN-коды считаются ненадежными, если они совпадают с часто используемыми PIN-кодами, представляют собой возрастающую или убывающую последовательность, например «1234» или «8765», или следуют повторяющемуся шаблону, например «123123» или «123321».

- Пароли помечаются как *похищенные*, если по сведениям функции мониторинга паролей они были найдены в массивах данных, которые были украдены в результате утечки данных. Подробнее см. в разделе [Мониторинг паролей](#).

Ненадежные, повторно использованные и похищенные пароли либо помечаются соответствующим образом в списке паролей (macOS), либо указываются в соответствующем интерфейсе рекомендаций по безопасности (iOS и iPadOS). Если пользователь выполняет вход на веб-сайте в Safari с использованием ранее сохраненного пароля, который является очень ненадежным или был украден в результате утечки данных, отображается предупреждение, в котором настоятельно рекомендуется автоматически создать новый надежный пароль.

Повышение безопасности для аутентификации учетной записи в iOS и iPadOS

Приложения, которые используют расширение для изменения аутентификации учетной записи (в программной среде служб аутентификации), могут быстро повышать уровень защиты учетных записей, защищенных паролем, в одно касание кнопки. Например, они могут предлагать использовать функцию «Вход с Apple» или автоматическое создание надежного пароля. Эта точка расширения доступна в iOS и iPadOS.

Если приложение, в котором реализована точка расширения, установлено на устройстве, для пользователей отображаются варианты повышения уровня безопасности (в настройках в менеджере паролей Связки ключей iCloud, раздел рекомендаций по обеспечению безопасности учетных данных для приложения). Повышение уровня безопасности также предлагается во время входа пользователя в приложение с использованием ненадежных учетных данных. Приложения могут передавать системе информацию о том, что не следует предлагать варианты повышения уровня безопасности после входа в систему. С помощью нового API AuthenticationServices приложения также могут самостоятельно вызывать расширения и повышать уровень безопасности, предпочтительно в настройках учетной записи или на экране управления учетной записью в приложении.

Приложения могут поддерживать создание надежных паролей, функцию «Вход с Apple» либо обе эти функции. При использовании функции создания надежных паролей система генерирует для пользователя надежный пароль. При необходимости в приложении могут содержаться настраиваемые правила создания паролей для генерирования новых паролей. Когда пользователь учетной записи переключается с использования пароля на функцию «Вход с Apple», система предоставляет новые учетные данные «Вход с Apple», которые расширение связывает с этой учетной записью. В учетных данных не указывается адрес электронной почты Apple ID пользователя. После успешного перехода на использование функции «Вход с Apple» система удаляет из связки ключей пользователя использовавшийся ранее пароль, если он был там сохранен.

Расширения для изменения аутентификации учетной записи могут выполнить дополнительную аутентификацию пользователя, прежде чем повышать уровень безопасности. В случае повышения уровня безопасности с помощью менеджера паролей или после входа в приложение расширение предоставляет имя пользователя и пароль для учетной записи, уровень безопасности которой следует повысить. При повышении уровня безопасности в приложении предоставляется только имя пользователя. Если расширению требуется дополнительная аутентификация пользователя, перед повышением уровня безопасности оно может запросить отображение настраиваемого интерфейса пользователя. Это необходимо для того, чтобы пользователь применил второй фактор аутентификации и разрешил повышение уровня безопасности.

Мониторинг паролей

Мониторинг паролей — это функция, которая сопоставляет пароли, хранящиеся в связке ключей Автозаполнения паролей, с паролями в постоянно обновляемом списке паролей, которые были похищены у различных онлайн-организаций в результате утечки данных. Если эта функция включена, протокол мониторинга непрерывно сопоставляет пароли в связке ключей Автозаполнения паролей пользователя с паролями в обновляемом списке.

Как работает мониторинг

Устройство постоянно проверяет пароли пользователя путем циклического перебора, отправляя запросы через интервал времени, который не зависит от паролей пользователя или того, как их использует менеджер паролей. Это помогает гарантировать актуальность состояний проверки в соответствии с текущим отслеживаемым списком похищенных паролей. Чтобы способствовать предупреждению утечки информации о том, сколько у пользователя уникальных паролей, запросы объединяются в пакеты и выполняются параллельно. Во время каждой проверки параллельно проверяется фиксированное количество паролей, и если у пользователя меньше паролей, генерируются случайные пароли, которые затем добавляются в запросы для устранения различий.

Как сопоставляются пароли

Сопоставление паролей выполняется в два этапа. Самые распространенные похищенные пароли содержатся в локальном списке на устройстве пользователя. Если пароль пользователя имеется в этом списке, сразу же отображается соответствующее уведомление без какого-либо внешнего взаимодействия. Эта функция направлена на то, чтобы исключить утечку информации об имеющихся у пользователя паролях, которые подвержены наиболее высокому риску из-за появления в списке скомпрометированных паролей.

Если пароль отсутствует в списке самых распространенных похищенных паролей, он сопоставляется с менее распространенными похищенными паролями.

Сравнение паролей пользователя с паролями в отслеживаемом списке

Проверка наличия в отслеживаемом списке пароля, которого нет в локальном списке, подразумевает некоторое взаимодействие с серверами Apple. Чтобы помочь предупредить отправку надежных паролей в Apple, применяется *пересечение закрытых наборов* шифрования, которое используется для сравнения паролей пользователя с большим набором похищенных паролей. Эта функция направлена на то, чтобы передавать в компанию Apple незначительный объем информации в отношении паролей, менее подверженных взлому. Для пароля пользователя эта информация ограничена 15-битным префиксом криптографического хэша. Удаление из этого интерактивного процесса наиболее часто похищаемых паролей с использованием локального списка самых распространенных похищенных паролей приводит к снижению относительной частоты, с которой пароли встречаются в сегментах веб-служб. Благодаря этому на основе выполненного поиска не удастся сделать какие-либо выводы в отношении паролей пользователя.

Лежащий в основе протокол разделяет список отслеживаемых паролей, в котором на момент написания данного документа содержалось порядка 1,5 миллиарда паролей, на 2^{15} различных сегментов. Сегмент, в который входит пароль, основан на первых 15 битах значения хэша SHA256 пароля. Кроме того, каждый похищенный пароль (pw) связан с точкой эллиптической кривой на кривой NIST P256: $P_{pw} = \alpha \cdot H_{SWU}(pw)$, где α — это секретный случайный ключ, известный только Apple, а H_{SWU} — это случайная функция прогнозирования, которая сопоставляет пароли с точками на кривой по методу Шелью — ван де Вустейне — Уласа. Данное преобразование призвано скрыть значения паролей путем вычислений и предотвратить отображение новых похищенных паролей при использовании мониторинга паролей.

Чтобы вычислить пересечение закрытых наборов, устройство пользователя определяет сегмент, в который входит пароль пользователя, с помощью параметра λ , 15-битного префикса SHA256(upw), где upw — это один из паролей пользователя. Устройство генерирует свою собственную случайную константу, β , и отправляет точку $P_c = \beta \cdot H_{SWU}(upw)$ на сервер вместе с запросом сегмента, соответствующего λ . Здесь β скрывает информацию о пароле пользователя и ограничивает информацию, предоставляемую Apple о пароле, до λ . Наконец, сервер принимает точку, отправленную устройством пользователя, вычисляет $\alpha P_c = \alpha \beta \cdot H_{SWU}(upw)$, а затем возвращает его вместе с соответствующим сегментом точек $B_\lambda = \{ P_{pw} \mid \text{SHA256}(pw) \text{ начинается с префикса } \lambda \}$ для устройства.

На основе возвращенной информации устройство вычисляет $B'_\lambda = \{ \beta \cdot P_{pw} \mid P_{pw} \in B_\lambda \}$, а затем определяет, что пароль пользователя был похищен, если $\alpha P_c \in B'_\lambda$.

Отправка паролей другим пользователям или на другие устройства Apple

Apple безопасно отправляет пароли другим пользователям или на другие устройства Apple с помощью AirDrop, а также на Apple TV.

Сохранение учетных данных на другом устройстве с помощью AirDrop

Когда функция iCloud включена, пользователи могут отправлять сохраненные учетные данные на другое устройство с помощью AirDrop. Учетные данные — это имя пользователя, пароль и веб-сайт, для которого они сохранены. Отправка учетных данных с помощью AirDrop всегда выполняется в режиме «Только для контактов» независимо от настроек пользователя. После получения согласия пользователя на принимающем устройстве учетные данные сохраняются в связке ключей автозаполнения пароля, которая принадлежит пользователю.

Заполнение учетных данных в приложениях на Apple TV

Функция «Автозаполнение пароля» может использоваться для ввода учетных данных в приложениях на Apple TV. Когда пользователь выбирает текстовое поле имени пользователя или пароля в tvOS, Apple TV начинает передавать запрос Автозаполнения пароля по протоколу Bluetooth Low Energy (BLE).

На находящихся поблизости iPhone, iPad или iPod touch отображается запрос, предлагающий пользователю поделиться учетными данными с Apple TV. Способ установления зашифрованного соединения зависит от следующих факторов.

- Если устройство и Apple TV используют одну и ту же учетную запись iCloud, между ними автоматически устанавливается зашифрованное соединение.
- Если устройство и Apple TV используют разные учетные записи iCloud, пользователю предлагается установить зашифрованное соединение путем ввода PIN-кода. Для получения этого запроса iPhone должен быть разблокирован и находиться в непосредственной близости от пульта Siri Remote, связанного с этим Apple TV.

После установления зашифрованного соединения BLE учетные данные передаются на Apple TV и автоматически вводятся в соответствующие текстовые поля в приложении.

Расширения поставщиков учетных данных

В iOS, iPadOS и macOS пользователь может назначить приложение стороннего разработчика, соответствующее требованиям, в качестве поставщика учетных данных для функции «Автозаполнение паролей», используя раздел Настроек «Пароли» (iOS и iPadOS) или раздел «Расширения» Системных настроек (macOS). Этот механизм основан на расширениях приложений. Расширение поставщика учетных данных должно предоставлять визуальный интерфейс для выбора учетных данных, а также может предоставлять метаданные сохраненных учетных данных, чтобы они предлагались прямо в панели QuickType (iOS и iPadOS) или в качестве предложения автозаполнения (macOS). В состав метаданных входит веб-сайт, для которого сохранены учетные данные, и имя пользователя, но не входит сам пароль. iOS, iPadOS и macOS запрашивают пароль у расширения, когда пользователь хочет вставить его в приложении или на веб-сайте в Safari. Метаданные учетных данных хранятся в контейнере приложения поставщика учетных данных и автоматически удаляются при удалении приложения.

Связка ключей iCloud

Обзор безопасности Связки ключей iCloud

Связка ключей iCloud обеспечивает безопасную синхронизацию паролей пользователей между устройствами iOS, устройствами iPadOS и компьютерами Mac без передачи этой информации в компанию Apple. Помимо высокого уровня конфиденциальности и безопасности, при разработке дизайна и архитектуры Связки ключей iCloud учитывались такие аспекты, как простота использования и возможность восстановления связки ключей. Связка ключей iCloud состоит из двух служб: синхронизации связки ключей и восстановления связки ключей.

Связка ключей iCloud и восстановление связки ключей реализованы таким образом, что пароли пользователя остаются защищенными даже в следующих ситуациях:

- Учетная запись iCloud пользователя взломана.
- Служба iCloud взломана внешним злоумышленником или сотрудником.
- Третья сторона получает доступ к учетным записям пользователей.

Интеграция менеджера паролей со Связкой ключей iCloud

iOS, iPadOS и macOS могут автоматически генерировать криптографически стойкие случайные строки для использования в качестве паролей учетных записей в Safari. iOS и iPadOS также могут генерировать надежные пароли для приложений. Сгенерированные пароли хранятся в связке ключей и синхронизируются с другими устройствами. Элементы связки ключей передаются между устройствами и серверами Apple, однако они зашифрованы таким образом, чтобы компания Apple и другие устройства не могли прочитать их содержимое.

Безопасная синхронизация связки ключей

Когда пользователь впервые включает Связку ключей iCloud, устройство устанавливает круг доверия и создает для себя идентификатор синхронизации. Этот идентификатор синхронизации, состоящий из личного ключа и открытого ключа, хранится в связке ключей на устройстве. Открытый ключ идентификатора синхронизации помещается в круг, а сам круг подписывается дважды: в первый раз с помощью личного ключа идентификатора синхронизации, а во второй раз с помощью асимметричного эллиптического ключа (на основе P-256), полученного из пароля учетной записи iCloud пользователя. Вместе с кругом сохраняются параметры (случайное значение «соли» и число повторений), использованные для создания ключа из пароля учетной записи iCloud пользователя.

В случае учетных записей с двухфакторной аутентификацией создается дополнительный круг синхронизации, который сохраняется в CloudKit. Идентификаторы устройства в этой системе состоят из двух пар асимметричных эллиптических ключей (с использованием P-384), также сохраняемых в связке ключей. Каждое устройство ведет свой список доверенных идентификаторов и подписывает его одним из своих ключей идентификации.

Хранилище iCloud для круга синхронизации

Подписанный круг синхронизации хранится в хранилище типа ключ-значение в учетной записи iCloud пользователя. Его нельзя прочитать без пароля iCloud пользователя и нельзя изменить, не имея личного ключа идентификатора синхронизации одного из членов круга.

В случае учетных записей с двухфакторной аутентификацией список синхронизаций каждого устройства хранится в CloudKit. Эти списки устройств нельзя прочитать без пароля iCloud пользователя и нельзя изменить, не имея личных ключей владеющего устройства.

Порядок добавления других устройств пользователя в круг синхронизации

После входа в iCloud новые устройства добавляются в круг синхронизации связи ключей iCloud одним из двух способов: либо создав пару с зарегистрированным в iCloud устройством, с которого одобрено это новое устройство, либо используя восстановление Связки ключей iCloud.

Во время создания пары запрашивающее устройство создает новые идентификаторы синхронизации одновременно для круга синхронизации и списков синхронизации (в случае учетных записей с двухфакторной аутентификацией) и передает их одобренному устройству. Одобренное устройство добавляет в круг синхронизации открытый ключ нового члена и подписывает его еще раз с помощью своего идентификатора синхронизации и ключа, полученного из пароля iCloud пользователя. Новый круг синхронизации передается в iCloud, где его аналогичным образом подписывает новый член круга. В случае учетных записей с двухфакторной аутентификацией одобренное устройство также предоставляет присоединяющемуся устройству *ваучер*, подписанный ключами идентификации одобренного устройства, подтверждая, что присоединяющемуся устройству можно доверять. Затем это устройство обновляет свой отдельный список доверенных идентификаторов синхронизации, чтобы включить в него присоединяющееся устройство.

Теперь в круг входят два члена, и у каждого из них есть открытый ключ другого члена. Члены круга начинают обмениваться индивидуальными элементами связи ключей через хранилище iCloud типа ключ-значение или сохраняют эти элементы в CloudKit, что зависит от ситуации. Если оба члена круга хотят изменить один и тот же элемент, выбирается один или другой, чтобы остался только один элемент. Каждый синхронизируемый элемент шифруется таким образом, что его может расшифровать только устройство из круга доверия пользователя. Он не может быть расшифрован любыми другими устройствами или компанией Apple.

Когда к кругу присоединяются новые устройства, вся процедура повторяется. Например, при присоединении третьего устройства его можно объединить в пару с одним из других устройств пользователя. При добавлении нового члена круга выполняется его синхронизация с другими членами круга. Эта мера направлена на то, чтобы на всех устройствах хранились одинаковые элементы связи ключей.

Синхронизируются только определенные элементы

Некоторые элементы связи ключей, такие как ключи iMessage, относятся к конкретному устройству, поэтому они должны оставаться на устройстве. Поэтому каждый синхронизируемый объект должен быть явно обозначен атрибутом `kSecAttrSynchronizable`.

Apple устанавливает этот атрибут для пользовательских данных Safari (включая имена пользователей, пароли и номера кредитных карт), а также для паролей сетей Wi-Fi, ключей шифрования HomeKit и других элементов связи ключей, поддерживающих сквозное шифрование iCloud.

Кроме того, по умолчанию в синхронизации не участвуют элементы связи ключей, добавленные приложениями сторонних разработчиков. При добавлении элементов в связь ключей разработчики должны установить атрибут `kSecAttrSynchronizable`.

Безопасное восстановление Связки ключей iCloud

Связка ключей iCloud передает данные связки ключей пользователей в Apple, не позволяя Apple читать пароли и другие данные, которые там содержатся. Даже если у пользователя есть только одно устройство, функция восстановления связки ключей обеспечивает защиту от потери данных. Это особенно важно, если Safari генерирует для учетных записей веб-сайтов случайные, надежные пароли, поскольку единственный экземпляр этих паролей хранится в связке ключей.

Фундаментальным элементом восстановления связки ключей является служба дополнительной аутентификации и безопасного ответственного хранения, разработанная компанией Apple специально для поддержки этой функции. Связка ключей пользователя зашифрована с использованием надежного код-пароля, и служба ответственного хранения выдает копию этой связки ключей только при соблюдении строгого набора условий.

Использование дополнительной аутентификации

Есть несколько способов установить надежный код-пароль.

- Если для учетной записи пользователя включена двухфакторная аутентификация, для восстановления переданной на хранение связки ключей используется код-пароль устройства.
- Если двухфакторная аутентификация не настроена, пользователю предлагается создать код безопасности iCloud, введя код-пароль из 6 цифр. Либо, не используя двухфакторную аутентификацию, пользователи могут указать собственный, более длинный код или позволить устройствам создать криптографически случайный код, который они могут записать и хранить самостоятельно.

Процесс передачи связки ключей на хранение

После задания код-пароля связка ключей передается на ответственное хранение в Apple. Устройство iOS, iPadOS или macOS сначала экспортирует копию связки ключей пользователя, а затем шифрует ее с помощью ключей из хранилища асимметричных ключей и помещает в хранилище iCloud типа ключ-значение, причем само хранилище принадлежит пользователю. Хранилище ключей защищается с помощью кода безопасности iCloud и открытого ключа кластера аппаратного модуля системы безопасности (HSM), в котором хранится запись ответственного хранения. Эта запись становится записью *ответственного хранения iCloud* пользователя. В случае учетных записей с двухфакторной аутентификацией связка ключей также хранится в CloudKit. Она защищена с помощью промежуточных ключей, которые можно восстановить только с помощью содержимого записи ответственного хранения iCloud, что обеспечивает одинаковый уровень защиты.

С помощью содержимого записи ответственного хранения восстанавливающее устройство также может заново присоединиться к связке ключей iCloud, подтвердив для имеющихся устройств, что восстанавливающее устройство завершило процесс передачи, а следовательно, владелец учетной записи дал на это свое разрешение.

Примечание. Если вместо того, чтобы задавать свой собственный сложный или четырехзначный код, пользователь решит принять криптографически случайный код, запись ответственного хранения будет не нужна. Для защиты случайного ключа будет использован код безопасности iCloud.

Помимо установки кода безопасности, пользователи должны зарегистрировать номер телефона. Это обеспечивает второй уровень аутентификации при восстановлении связки ключей. Пользователь получает SMS и должен на него ответить, чтобы процесс восстановления был продолжен.

Безопасность ответственного хранения Связки ключей iCloud

Безопасная инфраструктура iCloud помогает гарантировать, что восстановление переданной связки ключей смогут выполнить только авторизованные пользователи и устройства. За iCloud расположены кластеры аппаратных модулей системы безопасности (HSM), которые защищают записи ответственного хранения. Как было описано ранее, каждый кластер имеет ключ, который используется для шифрования находящихся под его контролем записей ответственного хранения.

Чтобы восстановить связку ключей, пользователь должен пройти аутентификацию с использованием своей учетной записи и пароля iCloud, а также ответить на сообщение SMS, которое будет отправлено на зарегистрированный номер телефона. Затем пользователь должен ввести свой код безопасности iCloud. Чтобы убедиться, что пользователь знает свой код безопасности iCloud, кластер HSM использует протокол Secure Remote Password (SRP); сам код не пересылается в компанию Apple. Каждый член кластера независимо от других убеждается, что пользователь не превысил максимальное количество попыток извлечения своей записи (см. ниже). Если большинство членов кластера соглашаются с этим, кластер снимает защиту с записи ответственного хранения и отправляет ее на устройство пользователя.

Затем устройство с помощью кода безопасности iCloud дешифрует случайный ключ, который был использован для шифрования связки ключей пользователя. С помощью этого ключа выполняется дешифрование и восстановление на устройстве. Для этого используется связка ключей, извлеченная из хранилища значений ключей iCloud и CloudKit. iOS, iPadOS и macOS допускают только 10 попыток аутентификации и извлечения записи ответственного хранения. После нескольких неудавшихся попыток запись блокируется, и, чтобы получить право на дополнительные попытки, пользователь должен позвонить в службу поддержки Apple. После десятой неудавшейся попытки кластер HSM уничтожает запись ответственного хранения, и восстановить связку ключей невозможно. Такой подход защищает от попыток извлечь запись методом перебора, но жертвует связкой ключей.

Эти политики закодированы в прошивке HSM. Карты административного доступа, разрешающие вносить изменения в прошивку, уничтожены. Любая попытка изменения прошивки или доступа к личному ключу приводит к тому, что кластер HSM удаляет личный ключ. Если это происходит, владелец каждой связки ключей, защищенной этим кластером, получает сообщение о том, что его записи ответственного хранения были утеряны. При желании пользователи могут отправить записи на хранение повторно.

Apple Pay

Обзор безопасности Apple Pay

Технология Apple Pay позволяет пользователям поддерживаемых устройств iPhone, iPad, Mac и Apple Watch легко, безопасно и конфиденциально оплачивать покупки в магазинах, приложениях и на веб-сайтах через Safari. Пользователи также могут добавлять в Apple Wallet транспортные карты, студенческие билеты и карты доступа, если они поддерживают Apple Pay. Для пользователей это удобно, а защита, встроенная как в аппаратное, так и в программное обеспечение, гарантирует безопасность.

Кроме того, в Apple Pay предусмотрена защита личных данных пользователей. Apple Pay не собирает информацию о транзакциях, которую можно было бы связать с конкретным пользователем. Платежные операции выполняются исключительно между пользователем, продавцом и эмитентом платежной карты.

Безопасность компонентов Apple Pay

В Apple Pay используется несколько аппаратных и программных функций, предназначенных для безопасного и надежного совершения покупок.

Secure Element

Чип Secure Element представляет собой стандартную сертифицированную микросхему, работающую на платформе Java Card и совместимую с требованиями финансовой отрасли к электронным платежам. Чип Secure Element и платформа Java Card сертифицированы по стандарту оценки безопасности EMVCo. После успешного прохождения оценки безопасности EMVCo выдает уникальный сертификат интегральной микросхемы и платформы.

Чип Secure Element был сертифицирован на основе стандартов оценки по общим критериям. Подробная информация приведена в разделе [Сертификация безопасности процессора Secure Enclave](#) в документе «Сертификация платформы Apple».

Контроллер NFC

Контроллер NFC обрабатывает протоколы ближней бесконтактной связи и маршрутизирует данные, передаваемые между процессором приложений и чипом Secure Element, а также между Secure Element и терминалом, установленным в точке продажи.

Apple Wallet

Приложение Apple Wallet — удобный способ добавлять кредитные, дебетовые и магазинные карты, управлять ими и совершать платежи через Apple Pay. В Apple Wallet пользователи могут просматривать свои карты и дополнительную информацию, предоставленную эмитентом, например, о действующих политиках конфиденциальности, недавних транзакциях и многом другом. Кроме того, пользователи могут добавлять карты в Apple Pay через следующие приложения:

- Ассистент настройки и Настройки в iOS и iPadOS;
- приложение «Часы» на Apple Watch;
- раздел «Wallet & Apple Pay» в Системных настройках на Mac с Touch ID.

Кроме того, с Apple Wallet пользователи также могут добавлять транспортные карты, скидочные карты, посадочные талоны, билеты, подарочные карты, студенческие билеты, карты доступа и другие карты и управлять ими.

Secure Enclave

На iPhone, iPad, Apple Watch, а также компьютерах Mac с Touch ID и компьютерах Mac с чипом Apple и клавиатурой Magic Keyboard с Touch ID Secure Enclave управляет процессом аутентификации и позволяет продолжить выполнение платежа.

В случае с Apple Watch устройство должно быть разблокировано, а пользователь должен дважды нажать боковую кнопку. Информация об обнаружении двойного нажатия передается напрямую в чип Secure Element или Secure Enclave (при его наличии), не проходя через процессор приложений.

Серверы Apple Pay

Серверы Apple Pay управляют настройкой и добавлением кредитных, дебетовых, транспортных карт, студенческих билетов и карт доступа в Apple Wallet. Серверы также управляют учетными номерами устройств, которые хранятся в Secure Element. Эти серверы взаимодействуют как с устройством, так и с серверами платежной сети или эмитента карты. Кроме того, серверы Apple Pay отвечают за повторное шифрование платежных учетных данных при оплате в приложениях или в Интернете.

Как Apple Pay защищает покупки пользователей

Secure Element

В Secure Element хранится специально разработанный апплет для управления Apple Pay. Он также содержит апплеты, сертифицированные платежными сетями или эмитентами карт. Данные кредитной, дебетовой или предоплаченной карты отправляются из платежной сети или от эмитента карты этим апплетам — при этом данные зашифрованы с помощью ключей, известных только платежной сети или эмитенту карты и домену безопасности апплетов. Эти данные хранятся в апплетах и защищаются функциями обеспечения безопасности Secure Element. Во время транзакции терминал взаимодействует непосредственно с чипом Secure Element по специальной аппаратной шине с помощью контроллера NFC.

Контроллер NFC

Контроллер NFC выступает в качестве пункта доступа к Secure Element и помогает сделать так, чтобы все бесконтактные транзакции выполнялись с использованием установленного в точке продажи терминала, который находится вблизи устройства. Только запросы на оплату, поступающие от терминала на месте эксплуатации, отмечаются контроллером NFC как бесконтактные транзакции.

После того как владелец кредитной, дебетовой или предоплаченной карты (в том числе магазинных карт) авторизует платеж с помощью Face ID, Touch ID или код-пароля либо путем двойного нажатия боковой кнопки на разблокированных часах Apple Watch, бесконтактные ответы, подготовленные платежными апплетами в Secure Element, передаются контроллером только в диапазоне действия NFC. Следовательно, данные авторизации платежей при бесконтактных платежных транзакциях остаются в локальной области действия NFC и не раскрываются процессору приложений. При оплате покупок внутри приложений и на веб-сайтах данные авторизации платежей, наоборот, передаются в процессор приложений и только после шифрования чипом Secure Element — на сервер Apple Pay.

Кредитные, дебетовые и предоплаченные карты

Обзор безопасности подготовки карт

Когда пользователь добавляет кредитную, дебетовую или предоплаченную карту (в том числе магазинные карты) в Apple Wallet, компания Apple безопасно отправляет эмитенту карты или авторизованному им поставщику услуг информацию об этой карте вместе с другими сведениями об учетной записи пользователя и устройстве. Используя эту информацию, эмитент карты решает, разрешить ли добавление карты в Apple Wallet. В рамках процесса подготовки карты Apple Pay использует три вызова со стороны сервера для отправки и получения данных от эмитента карты или из сети:

- требуемые поля;
- проверка карты;
- привязка и подготовка.

Эмитент карты или сеть используют эти вызовы для проверки, утверждения и добавления карт в Apple Wallet. Передача данных во время этих сеансов связи «клиент-сервер» шифруется с использованием протокола TLS 1.2.

Полные номера карт не хранятся ни на устройстве, ни на серверах Apple Pay. Вместо этого создается учетный номер устройства, который шифруется и сохраняется в чипе Secure Element. Учетный номер устройства шифруется таким образом, что у Apple нет к нему доступа. Каждый учетный номер устройства уникален и отличается от большинства номеров кредитных и дебетовых карт. Эмитент карты или платежная сеть может запретить использование учетного номера устройства для оплаты физической картой с магнитной полосой, а также для оплаты по телефону или на веб-сайтах. Учетный номер устройства в чипе Secure Element никогда не хранится на серверах Apple Pay, и его резервная копия не создается в iCloud. Он также изолирован от устройств iOS, iPadOS, watchOS и компьютеров Mac с Touch ID.

Подготовка карт, используемых с Apple Watch для Apple Pay, выполняется с помощью приложения Apple Watch на iPhone или приложения для iPhone, разработанного эмитентом карты. Для добавления карты на Apple Watch необходимо, чтобы часы находились в зоне действия Bluetooth. Картам, зарегистрированным специально для использования с Apple Watch, назначаются собственные учетные номера устройства, которые хранятся в Secure Element на Apple Watch.

После добавления кредитных, дебетовых или предоплаченных карт (в том числе магазинных карт) они будут отображаться в списке карт в Ассистенте настройки на устройствах, на которых выполнен вход в ту же учетную запись iCloud. Эти карты остаются в списке, пока они активны хотя бы на одном устройстве. Карты удаляются из списка через семь дней после удаления с последнего устройства. Для работы этой функции в соответствующей учетной записи iCloud должна быть включена двухфакторная аутентификация.

Добавление кредитных или дебетовых карт в Apple Pay

Банковские карты можно добавлять вручную в Apple Pay на устройствах Apple.

Добавление кредитных или дебетовых карт вручную

Чтобы вручную добавить карту, в процессе подготовки необходимо указать имя владельца, номер карты, срок окончания ее действия и код CVV. В Настройках, в Apple Wallet или приложении Apple Watch пользователи могут сфотографировать карту камерой устройства или ввести данные карты. После съемки данных карты с помощью камеры Apple пытается заполнить поля имени владельца, номера карты и срока окончания ее действия. Фотоснимок не сохраняется на устройстве или в медиатеке. После заполнения всех полей их значения (кроме кода CVV) проверяются в рамках процесса проверки карты. Затем они шифруются и отправляются на сервер Apple Pay.

Если процесс проверки карты возвращает соответствующий идентификатор, Apple загружает и отображает положения и условия эмитента карты. Если пользователь принимает положения и условия, Apple отправляет идентификатор принятых условий и код CVV процессу привязки и подготовки. Кроме того, в рамках процесса привязки и подготовки Apple передает информацию с устройства эмитенту карты или сети. К такой информации относятся: (a) сведения об активности пользователя в учетной записи iTunes и App Store (например, много ли транзакций выполнялось в iTunes), (b) данные об устройстве пользователя (например, номер телефона, название и модель устройства и любых сопутствующих устройств Apple, необходимых для настройки Apple Pay) и (c) примерное местонахождение пользователя во время добавления карты (если включены Службы геолокации). Используя эту информацию, эмитент карты решает, разрешить ли добавление карты в Apple Pay.

В результате выполнения процесса привязки и подготовки происходят две вещи:

- Устройство начинает загружать файл кредитной или дебетовой карты для Apple Wallet.
- Устройство начинает привязку карты к Secure Element.

Файл карты содержит URL-адреса, перейдя по которым можно загрузить изображения карты, такие метаданные, как контактная информация, связанные приложения эмитента карты и поддерживаемые функции. Кроме того, он содержит различные данные о состоянии карты: была ли выполнена персонализация Secure Element, не приостановлено ли действие карты ее эмитентом, требуется ли дополнительная проверка, прежде чем карту можно будет использовать для оплаты с помощью Apple Pay, и так далее.

Добавление кредитных или дебетовых карт из учетной записи iTunes Store

Для добавления кредитных или дебетовых карт, зарегистрированных в iTunes, может потребоваться повторно ввести пароль Apple ID пользователя. После получения номера карты из iTunes выполняется проверка карты. Если карту можно использовать в Apple Pay, устройство загружает и показывает на экране положения и условия, а затем отправляет их идентификатор и код безопасности карты процессу привязки и подготовки. Для карт, зарегистрированных в учетной записи iTunes, может потребоваться дополнительная проверка.

Добавление кредитных или дебетовых карт из приложения эмитента карты

Если приложение зарегистрировано для использования с Apple Pay, этому приложению и серверу эмитента карты назначаются ключи. Эти ключи используются для шифрования данных карты, отправляемых эмитенту. Эта мера направлена на то, чтобы устройство Apple не могло прочитать эти данные. Процесс подготовки похож на используемый при добавлении карт вручную (см. выше), за исключением того, что вместо кода CVV используются одноразовые пароли.

Добавление кредитных или дебетовых карт на веб-сайте эмитента карты

Некоторые эмитенты карт дают возможность начать процесс подготовки карты для Apple Wallet на своем веб-сайте. В этом случае пользователь сначала выбирает на веб-сайте эмитента карты ту карту, которую нужно подготовить. Затем пользователь будет перенаправлен на независимую площадку Apple для входа (в домене Apple), где потребуется войти со своей учетной записью Apple ID. После успешного входа пользователь выберет одно или несколько устройств, чтобы подготовить карту, а затем подтвердит завершение подготовки на каждом отдельном целевом устройстве.

Добавление дополнительной проверки

Эмитент карты может решить, что для кредитной или дебетовой карты требуется дополнительная проверка. В зависимости от того, что предлагает эмитент карты, пользователь может выбирать между различными вариантами дополнительной проверки, например текстовым сообщением, электронным письмом, звонком из службы поддержки или завершением проверки в утвержденном приложении стороннего разработчика. Для отправки текстового сообщения или электронного письма пользователь должен выбрать контактные данные, зарегистрированные у эмитента карты. На выбранный адрес или номер телефона будет отправлен код, который потребуется ввести в Apple Wallet, Настройках или приложении Apple Watch. Если пользователь выбирает проверку через службу поддержки или приложение, выполняются действия, предусмотренные эмитентом.

Авторизация платежей при использовании Apple Pay

Если на устройстве есть Secure Enclave, оплату можно совершить только после ее авторизации со стороны Secure Enclave. На iPhone или iPad это включает подтверждение того, что пользователь прошел аутентификацию с помощью Face ID, Touch ID или код-пароля устройства. По умолчанию используется Face ID или Touch ID (при наличии), но вместо них также можно ввести код-пароль. Пользователю будет предложено ввести код-пароль после трех безуспешных попыток распознавания отпечатка пальца или двух безуспешных попыток распознавания лица. После пяти безуспешных попыток ввод код-пароля становится обязательным. Кроме того, код-пароль требуется, если функция Face ID или Touch ID не настроена или ее использование не включено для Apple Pay. Для совершения платежа на Apple Watch устройство должно быть разблокировано с помощью код-пароля, а пользователь должен дважды нажать боковую кнопку.

Использование общего ключа пары

Secure Enclave и чип Secure Element взаимодействуют через последовательный интерфейс. Чип Secure Element подключен к контроллеру NFC, который, в свою очередь, подключен к процессору приложений. Хотя они и не связаны напрямую, Secure Enclave и чип Secure Element могут безопасно взаимодействовать, используя общий ключ пары, который подготавливается при производстве устройства. Шифрование и аутентификация передаваемых данных выполняются на основе AES, и обе стороны используют криптографические значения nonce для защиты от атак с повторным использованием. Ключ пары генерируется в Secure Enclave из его ключа UID и уникального идентификатора Secure Element. Затем ключ пары безопасно передается из Secure Enclave в аппаратный модуль системы безопасности (HSM) на заводе, где есть необходимый материал для последующего внедрения ключа пары в Secure Element.

Авторизация безопасной транзакции

Когда пользователь авторизует транзакцию, что подтверждается физическим действием, передаваемым в Secure Enclave, Secure Enclave отправляет подписанные данные о типе аутентификации и сведения о типе транзакции (бесконтактная или в приложении) чипу Secure Element в связке со случайным значением авторизации (AR). Значение AR генерируется в Secure Enclave, когда пользователь впервые добавляет кредитную карту. Значение сохраняется, пока включена технология Apple Pay, и защищается шифрованием Secure Enclave и противооткатным механизмом. Оно безопасно передается чипу Secure Element с помощью ключа пары. При получении нового значения AR чип Secure Element помечает все ранее добавленные карты как удаленные.

Использование криптограммы платежа для динамической безопасности

Платежные транзакции, инициируемые платежными апплетами, содержат криптограмму платежа, а также учетный номер устройства. Эта криптограмма (одноразовый код) вычисляется с помощью счетчика транзакций и ключа. Значение счетчика транзакций увеличивается для каждой новой транзакции. Ключ подготавливается платежным апплетом в ходе персонализации, и он известен платежной сети или эмитенту карты или им обоим. В зависимости от схемы оплаты при расчете также могут использоваться другие данные, например:

- непредсказуемое число, формируемое терминалом (для NFC-транзакций);
- значение nonce сервера Apple Pay (для транзакций в приложениях).

Эти коды безопасности предоставляются платежной сети и эмитенту карты, что позволяет эмитенту проверять каждую транзакцию. Длина таких кодов безопасности может быть различной и зависит от типа транзакции.

Совершение платежей картами с помощью Apple Pay

Apple Pay можно использовать для оплаты покупок в магазинах, в приложениях и на веб-сайтах.

Оплата с помощью карт в магазинах

Если iPhone или Apple Watch включены и обнаруживают зону действия NFC, то предлагают пользователю запрошенную карту (если для этой карты включен автоматический выбор) либо карту по умолчанию (этим можно управлять в Настройках). Кроме того, пользователь также может открыть Apple Wallet и выбрать карту, а если устройство заблокировано, то:

- дважды нажать боковую кнопку на устройствах с Face ID;
- дважды нажать кнопку «Домой» на устройствах с Touch ID;
- использовать функции Универсального доступа, чтобы пользоваться Apple Pay, когда экран заблокирован.

Затем, прежде чем платежная информация будет передана, пользователь должен пройти аутентификацию, используя Face ID, Touch ID или введя код-пароль. Если Apple Watch разблокированы, при двойном нажатии боковой кнопки для оплаты активируется карта по умолчанию. Без аутентификации пользователя платежная информация не отправляется.

После аутентификации пользователя для обработки платежа используются учетный номер устройства и динамический код безопасности, назначаемый каждой транзакции. Ни Apple, ни устройство пользователя не отправляют продавцам полный номер кредитной или дебетовой карты. Apple может получать анонимные данные о транзакции, такие как примерное место и время ее выполнения. Это помогает улучшить работу Apple Pay и других продуктов и служб Apple.

Оплата с помощью карт в приложениях

Apple Pay также можно использовать для оплаты покупок в приложениях на iPhone, iPad, Mac и Apple Watch. Когда пользователи совершают платежи в приложениях, используя Apple Pay, компания Apple получает зашифрованную информацию о транзакции. Прежде чем отправить ее разработчику или продавцу, Apple заново шифрует ее с использованием ключа, назначаемого каждому разработчику. Apple Pay сохраняет анонимную информацию о транзакции, например примерную сумму покупки. Эта информация не может привести к пользователю и не содержит данных о том, что именно было куплено.

Когда приложение запускает платежную транзакцию Apple Pay, серверы Apple Pay получают зашифрованную транзакцию с устройства раньше, чем ее получит продавец. Затем серверы Apple Pay повторно шифруют транзакцию с использованием ключа, назначаемого каждому продавцу, после чего ретранслируют ее продавцу.

Когда приложение запрашивает оплату, оно вызывает API, чтобы определить, поддерживает ли устройство Apple Pay и есть ли у пользователя кредитные или дебетовые карты, которыми можно оплатить покупку в платежной сети, поддерживаемой продавцом. Приложение запрашивает всю информацию, необходимую для обработки и выполнения транзакции, например расчетный адрес, адрес доставки и контактные данные. Затем приложение подает iOS, iPadOS или watchOS запрос на предоставление листа Apple Pay, и система запрашивает информацию для приложения, а также другие необходимые сведения, например то, какую карту следует использовать.

В это время приложение получает данные о городе, регионе/штате и индексе, позволяющие вычислить итоговую стоимость доставки. Полный набор запрошенной информации не предоставляется приложению, пока пользователь не авторизует платеж с помощью Face ID, Touch ID или код-пароля устройства. После авторизации платежа информация, представленная в листе Apple Pay, передается продавцу.

Авторизация платежей в приложениях

Когда пользователь авторизует платеж, на серверы Apple Pay поступает запрос криптографического значения *nonce*, которое аналогично значению, возвращаемому терминалом NFC при выполнении транзакций в магазине. Значение *nonce* вместе с другими данными транзакции передается чипу Secure Element для вычисления учетных данных для оплаты, которые будут зашифрованы с помощью ключа Apple. Зашифрованные учетные данные для оплаты будут возвращены серверам Apple Pay, которые расшифруют их, сравнят значение *nonce* из учетных данных со значением *nonce*, изначально переданным серверами Apple Pay, и повторно зашифруют учетные данные для оплаты с помощью ключа продавца, связанного с идентификатором продавца. Затем учетные данные возвращаются на устройство, которое возвращает их приложению, используя API. Приложение передает их в систему продавца для обработки. Продавец может расшифровать учетные данные платежа, используя свой личный ключ, и обработать их. Это в сочетании с подписью серверов Apple позволяет продавцу проверить, что транзакция предназначена именно ему.

Интерфейсам API требуются права, в которых указаны идентификаторы поддерживаемых продавцов. Приложение также может отправить на подпись чипу Secure Element дополнительные данные, например номер заказа или удостоверение покупателя, чтобы гарантировать, что транзакция не будет связана с другим пользователем. Для этого разработчик приложения может задать данные `applicationData` в запросе `PKPaymentRequest`. Хэш этих данных включается в зашифрованные платежные данные. Затем продавец должен убедиться, что хэш его данных `applicationData` совпадает с включенным в платежные данные.

Оплата с помощью карт на веб-сайтах

Apple Pay можно использовать для оплаты покупок на веб-сайтах с помощью iPhone, iPad и Apple Watch, а также на компьютерах Mac с Touch ID. Транзакции Apple Pay также можно начать на Mac и закончить на iPhone, на котором включен Apple Pay, или на Apple Watch, если они используют ту же учетную запись iCloud.

Для использования Apple Pay на веб-сайте необходимо, чтобы он был зарегистрирован в Apple. После регистрации домена проверка доменного имени выполняется только после того, как Apple выдаст сертификат клиента TLS. Веб-сайты, поддерживающие Apple Pay, должны предоставлять свой контент через HTTPS. Для каждой платежной транзакции веб-сайт должен установить уникальный безопасный сеанс связи продавца с сервером Apple, используя выпущенный компанией Apple сертификат клиента TLS. Данные сеанса связи продавца подписываются компанией Apple. После того как подпись сеанса связи продавца подтверждена, веб-сайт может запросить, есть ли у пользователя устройство с поддержкой Apple Pay и активирована ли на устройстве кредитная, дебетовая или предоплаченная карта. Никакие другие данные не предоставляются. Если пользователь не хочет делиться этой информацией, можно отключить запросы о доступности Apple Pay в настройках конфиденциальности Safari на устройствах iPhone, iPad и Mac.

После подтверждения сеанса связи продавца применяются те же меры обеспечения конфиденциальности и безопасности, как и при оплате в приложении.

Если пользователь передает платежную информацию с компьютера Mac на iPhone или Apple Watch, то для передачи платежной информации между компьютером Mac и авторизованным устройством пользователя система Apple Pay Handoff использует протокол сквозного шифрования службы идентификации Apple (IDS). Служба IDS на Mac использует для шифрования ключи устройств пользователя, так что никакое другое устройство не может расшифровать эту информацию, а у Apple нет доступа к этим ключам. Запрос обнаружения устройств для передачи Apple Pay через Handoff содержит тип и уникальный идентификатор кредитных карт пользователя, а также ряд метаданных. Учетный номер устройства, назначенный карте пользователя, не передается: он продолжает надежно храниться на iPhone или Apple Watch пользователя. Apple также безопасно передает недавно использованные пользователем контактные данные, адреса доставки и адреса плательщика через Связку ключей iCloud.

Когда пользователь авторизует платеж с помощью Face ID, Touch ID, ввода код-пароля или двойного нажатия боковой кнопки на часах Apple Watch, платежный токен, уникально шифруемый для каждого сертификата веб-сайта продавца, безопасно передается с iPhone или Apple Watch пользователя на его Mac, а затем на веб-сайт продавца.

Запрашивать и совершать оплату могут только устройства, находящиеся поблизости друг от друга. Близость определяется с помощью оповещений Bluetooth Low Energy (BLE).

Бесконтактные карты в Apple Pay

Для передачи данных с поддерживаемых карт на совместимые терминалы NFC компания Apple использует протокол Apple VAS (Apple Value Added Services). Протокол VAS можно применять на бесконтактных терминалах или в приложениях для iPhone. Он использует NFC для взаимодействия с поддерживаемыми устройствами Apple. Протокол VAS работает на коротком расстоянии и может использоваться для предъявления бесконтактных карт независимо или в рамках выполнения транзакции Apple Pay.

Если поднести устройство к терминалу NFC, терминал инициирует получение информации о карте, отправив запрос о наличии карты. Если у пользователя есть карта с идентификатором поставщика карты, пользователю предлагается авторизовать ее использование с помощью Face ID, Touch ID или код-пароля. Информация о карте, временная метка и одноразовый случайный ключ ECDH P-256 вместе с открытым ключом поставщика карты используются, чтобы получить ключ шифрования для данных карты, которые передаются на терминал.

В версиях с iOS 12.0.1 и включительно по iOS 13 пользователи могут вручную выбрать карту перед ее считыванием терминалом NFC продавца. В iOS 13.1 и новее поставщики карты могут указывать, необходима ли аутентификация пользователя для выбранной вручную карты или карту можно использовать без аутентификации.

Отображение карт как недоступных в Apple Pay

Кредитные, дебетовые и предоплаченные карты, добавленные в Secure Element, можно использовать, только если Secure Element получает авторизацию с теми же ключом пары и случайным значением авторизации (AR), которые использовались при добавлении карты. При получении нового значения AR чип Secure Element помечает все ранее добавленные карты как удаленные. Это позволяет операционной системе сообщать Secure Enclave, какие карты следует делать недоступными для использования, отмечая свою копию значения AR как недействительную в следующих ситуациях.

Ситуация	Устройство
Запрос код-пароля выключен.	iPhone, iPad, Apple Watch
Запрос пароля выключен.	Mac
Пользователь вышел из iCloud.	iPhone, iPad, Mac, Apple Watch
Пользователь выбрал стирание всего контента и настроек.	iPhone, iPad, Mac, Apple Watch
Устройство было восстановлено в режиме восстановления.	iPhone, iPad, Mac, Apple Watch
Разрыв пары	Apple Watch

Приостановка действия, удаление и стирание карт

Пользователи могут приостановить действие Apple Pay на iPhone, iPad и Apple Watch, переведя устройства в режим пропажи с помощью Локатора. Кроме того, пользователи могут удалять и стирать свои карты из Apple Pay в Локаторе, на веб-сайте iCloud.com или прямо с устройства в Apple Wallet. Для удаления карт из Apple Watch можно использовать настройки iCloud, приложение Apple Watch на iPhone или интерфейс самих часов. Функция оплаты с помощью карт на устройстве будет приостановлена или удалена из Apple Pay эмитентом карты или соответствующей платежной сетью, даже если устройство не подключено к сети сотовой связи или Wi-Fi. Пользователи также могут позвонить эмитенту карты с просьбой приостановить действие или удалить карты из Apple Pay.

Когда пользователь стирает все данные с устройства с помощью функции «Стереть контент и настройки», Локатора или при восстановлении устройства, то iPhone, iPad, iPod touch, компьютер Mac и часы Apple Watch передают в Secure Element команду отметить все карты как удаленные. При этом все карты мгновенно переводятся в недействительное состояние, а после подключения к серверам Apple Pay полностью стираются из Secure Element. Независимо от этого процесса Secure Enclave помечает значение AR как недействительное, чтобы авторизация оплаты с использованием ранее зарегистрированных карт больше не была возможна. При подключении к сети устройство пытается связаться с серверами Apple Pay. Эта мера направлена на то, чтобы все карты были стерты из Secure Element.

Безопасность Apple Card

На поддерживаемых моделях iPhone и Mac пользователь может безопасно подать заявку на получение карты Apple Card.

Заявка на получение карты Apple Card

В iOS 12.4 и новее, macOS 10.14.6 и новее, а также watchOS 5.3 и новее карту Apple Card можно использовать для совершения платежей с Apple Pay в магазинах, приложениях и интернете.

Чтобы подать заявку на получение карты Apple Card, пользователь должен войти в свою учетную запись iCloud на устройстве iOS или iPadOS, совместимом с Apple Pay, а в его учетной записи iCloud должна быть настроена двухфакторная аутентификация. Когда заявка будет одобрена, карта Apple Card появится в Apple Wallet или в разделе «Настройки» > «Wallet и Apple Pay» на любом из поддерживаемых устройств, где пользователь выполнил вход со своей учетной записью Apple ID.

После того как пользователь подал заявку на Apple Card, партнеры Apple по работе с идентификационными данными безопасным образом проверяют идентификационную информацию пользователя, после чего она передается Goldman Sachs Bank USA для оценки идентификационных данных и кредитоспособности.

Информация, которая была предоставлена при подаче заявки, например номер социального страхования или фотография удостоверения личности, безопасно передается партнерам Apple по работе с идентификационными данными и/или Goldman Sachs Bank USA, зашифрованная с помощью ключа получателя. Apple не может расшифровать эти данные.

Информация о доходах, предоставленная при подаче заявки, а также информация о банковском счете, используемая для оплаты выставленных счетов, безопасно передается Goldman Sachs Bank USA в зашифрованном виде. Шифрование выполняется с помощью ключа получателя. Информация о банковском счете сохраняется в связке ключей. Apple не может расшифровать эти данные.

При добавлении Apple Card в Apple Wallet информация, аналогичная той, что предоставляется при добавлении кредитной или дебетовой карты, может быть отправлена банку-партнеру компании Apple, то есть в Goldman Sachs Bank USA и в Apple Payments Inc. Эта информация используется только для устранения неполадок, предотвращения мошенничества и соблюдения законодательства.

В iOS 14.6 или новее, iPadOS 14.6 или новее и watchOS 7.5 или новее организатор группы «Семья» в iCloud, у которого есть карта Apple Card, может делиться ею с другими членами группы «Семья» в iCloud, если они старше 13 лет.

Для подтверждения запроса в приглашении потребуется аутентификация. Apple Wallet использует ключ в Secure Enclave, чтобы вычислить подпись, которая связывает владельца и приглашенного пользователя. Эту подпись проверяют серверы Apple.

В дополнение к этому организатор может настроить лимит по операциям участников. Карты участников можно заблокировать в любое время, чтобы они не могли тратить средства через Apple Wallet. Когда совладелец или участник старше 18 лет примет приглашение и подаст заявку, этому человеку потребуется пройти через процесс рассмотрения заявки, описанный в разделе о подаче заявки на получение карты Apple Card в Apple Wallet.

Использование карты Apple Card

В разделе Apple Card в Apple Wallet можно заказать физическую карту. После того как пользователь получит физическую карту, она активируется с помощью метки NFC из конверта с физической картой. Эта метка уникальна для каждой карты и не может быть использована для активации карты другого пользователя. Карту также можно активировать вручную в настройках Apple Wallet. Кроме того, пользователь может в любое время заблокировать или разблокировать физическую карту в Apple Wallet.

Сведения о платежах с помощью карты Apple Card и картах в Apple Wallet

Платежи со счета Apple Card могут производиться из Apple Wallet в iOS с помощью Apple Cash и банковского счета. Можно запланировать повторные платежи или настроить одноразовый платеж в указанную дату с помощью Apple Cash и банковского счета. Когда пользователь совершает платеж, на серверы Apple Pay отправляется запрос криптографического значения nonce, как и в случае с Apple Cash. Значение nonce вместе с другими данными платежа передается в Secure Element для вычисления подписи. Затем эта подпись возвращается на серверы Apple Pay. Серверы Apple Pay проверяют аутентификацию, целостность и правильность платежа на основании подписи и значения nonce, после чего платеж поступает в банк Goldman Sachs Bank USA на обработку.

Apple Wallet извлекает номер карты Apple Card, предъявляя сертификат. Сервер Apple Pay проверяет сертификат, чтобы подтвердить, что ключ был сгенерирован в Secure Enclave. Затем он использует этот ключ, чтобы зашифровать номер карты Apple Card перед тем, как вернуть его в Apple Wallet, чтобы только iPhone, который запросил номер карты Apple Card, мог его расшифровать. После расшифровки номер Apple Card сохраняется в связке ключей iCloud.

Для отображения номера Apple Card на виртуальной карте в Apple Wallet требуется аутентификация пользователя с помощью Face ID, Touch ID или код-пароля. Пользователь может заменить эти данные в разделе информации о карте, отключив предыдущую карту.

Расширенная защита от мошенничества

В iOS 15 или новее и iPadOS 15 или новее пользователь карты Apple Card может включить функцию «Расширенная защита от мошенничества» в Apple Wallet. Когда функция включена, код безопасности карты обновляется каждые несколько дней.

Безопасность Apple Cash

В iOS 11.2 или новее, iPadOS 13.1 или новее и watchOS 4.2 или новее Apple Pay можно использовать на iPhone, iPad или Apple Watch для отправки, получения и запроса денежных средств от других пользователей. Когда пользователь получает денежные средства, они добавляются на счет Apple Cash, для доступа к которому можно перейти в Apple Wallet или раздел «Настройки» > «Wallet и Apple Pay» на любом из поддерживаемых устройств, где пользователь выполнил вход со своей учетной записью Apple ID.

В iOS 14, iPadOS 14 и watchOS 7 организатор группы «Семья» в iCloud, подтвердивший свою личность для Apple Cash, может включить Apple Cash для тех членов семьи, которым не исполнилось 18 лет. Также организатор может ограничить возможности таких пользователей по отправке денежных средств только членам семьи или только контактам. Если члену семьи в возрасте до 18 лет требуется восстановить учетную запись Apple ID, организатору группы «Семья» потребуется снова вручную активировать карту Apple Cash для этого пользователя. Если несовершеннолетний член семьи больше не входит в число пользователей Семейного доступа iCloud, средства со счета Apple Cash такого пользователя автоматически переводятся на счет организатора.

При настройке Apple Cash информация, аналогичная информации при добавлении кредитной или дебетовой карты, может быть отправлена в партнерский банк Green Dot Bank и в Apple Payments Inc. — дочернюю компанию в полной собственности Apple, созданную для защиты конфиденциальности пользователей. Она хранит и обрабатывает информацию отдельно от Apple таким образом, что Apple не имеет об этом сведений. Вышеуказанная информация используется только в целях устранения неполадок, предотвращения мошенничества и соблюдения нормативов.

Использование Apple Cash в iMessage

Для совершения межпользовательских платежей и использования Apple Cash пользователь должен войти в свою учетную запись iCloud на устройстве, совместимом с Apple Cash, а в его учетной записи iCloud должна быть настроена двухфакторная аутентификация. Пользователи могут инициировать запросы и переводы денежных средств из приложения «Сообщения» или попросив Siri. Когда пользователь пытается отправить денежные средства, в iMessage отображаются сведения Apple Pay. Сначала всегда отображается баланс Apple Cash. При необходимости дополнительные средства списываются со второй кредитной или дебетовой карты, которую пользователь добавил в Apple Wallet.

Использование Apple Cash в магазинах, приложениях и в интернете

Карту Apple Cash в Apple Wallet можно использовать для совершения платежей с Apple Pay в магазинах, приложениях и интернете. Можно также переводить денежные средства со счета Apple Cash на банковский счет. Помимо получения денежных средств от других пользователей, можно также вносить денежные средства на счет Apple Cash с дебетовых или предоплаченных карт в Apple Wallet.

После завершения транзакций между пользователями Apple Payments Inc. сохраняет и может использовать информацию об этих транзакциях в целях устранения неполадок, предотвращения мошенничества и соблюдения нормативов. Остальные подразделения Apple не располагают информацией о том, кому пользователь отправил денежные средства, от кого получил денежные средства или какую покупку оплатил картой Apple Cash.

Когда пользователь отправляет денежные средства с помощью Apple Pay, вносит денежные средства на счет Apple Cash или переводит денежные средства на банковский счет, на серверы Apple Pay отправляется запрос для получения криптографического значения nonce, аналогичного значению, возвращаемому Apple Pay в приложениях. Это значение nonce вместе с другими данными транзакции передается в Secure Element для вычисления подписи платежа. Затем эта подпись возвращается на серверы Apple Pay. Серверы Apple Pay проверяют аутентификацию, целостность и правильность транзакции, используя подпись платежа и значение nonce. После этого начинается перевод денежных средств, а пользователь уведомляется о завершении транзакции.

Если в транзакции используется:

- дебетовая карта для внесения денежных средств в Apple Cash;
- внесение дополнительных денежных средств в случае недостаточного баланса Apple Cash.

Также генерируются зашифрованные учетные данные платежа, которые затем отправляются на серверы Apple Pay. Эта процедура аналогична тому, как Apple Pay работает в приложениях и на веб-сайтах.

Если баланс счета Apple Cash превышает определенную сумму или система фиксирует подозрительную активность, пользователю предлагается подтвердить свою личность. Информация, предоставленная пользователем для подтверждения своей личности, например номер социального страхования или ответы на вопросы (такие как название улицы, на которой ранее жил пользователь), безопасно передается партнеру Apple и шифруется с помощью его ключа. Apple не может расшифровать эти данные. Пользователю будет предложено еще раз подтвердить свою личность при восстановлении учетной записи Apple ID, прежде чем он сможет снова получить доступ к своему счету Apple Cash.

Безопасность службы Tap to Pay on iPhone

Служба Tap to Pay on iPhone, доступная в iOS 15.4, дает возможность продавцам в США принимать Apple Pay и другие бесконтактные платежи с помощью iPhone и приложения iOS партнера. С помощью этой службы пользователи с поддерживаемыми устройствами iPhone могут безопасно принимать бесконтактные платежи и карты, поддерживающие NFC и добавленные в *Apple Pay*. При использовании службы Tap to Pay on iPhone продавцам не требуется дополнительное оборудование, чтобы принимать бесконтактные платежи.

Tap to Pay on iPhone предусматривает защиту личных данных плательщика. Эта служба не собирает никакой информации о транзакциях, которую можно связать с конкретным плательщиком. Информацию платежной карты, такую как номер кредитной или дебетовой карты (PAN), защищает Secure Element, и она недоступна продавцу. Информация платежной карты раскрывается только платежной системе продавца, плательщику и эмитенту карты. Кроме того, служба Tap to Pay on iPhone не собирает имена, адреса или номера телефонов плательщиков.

Служба Tap to Pay on iPhone была оценена сторонней организацией, а именно аккредитованной лабораторией по оценке безопасности, и получила аккредитацию от American Express, Discover, Mastercard и Visa.

Безопасность компонента для бесконтактных платежей

- *Secure Element*. Secure Element (подробную информацию о нем можно найти в разделе о Secure Element для Apple Pay) содержит обрабатывающие платежи ядра, которые считывают данные карт бесконтактной оплаты и обеспечивают их безопасность.
- *Контроллер NFC*. Контроллер NFC обрабатывает протоколы ближней бесконтактной связи и регулирует обмен данными, передаваемыми между процессором приложений и Secure Element, а также между Secure Element и картой бесконтактной оплаты.
- *Серверы службы Tap to Pay on iPhone*. Серверы службы Tap to Pay on iPhone управляют настройкой и подготовкой обрабатывающих платежи ядер на устройстве. Серверы также отслеживают безопасность устройств, использующих службу Tap to Pay on iPhone, в соответствии со стандартом CPoC для бесконтактных платежей на коммерческих мобильных устройствах, который выпущен Советом по стандартам безопасности индустрии платежных карт, а также в соответствии со стандартом безопасности индустрии платежных карт.

Как служба Tap to Pay on iPhone считывает кредитные, дебетовые и prepaid карты

Обзор безопасности в процессе подготовки

При первом использовании службы Tap to Pay on iPhone с приложением, у которого достаточно прав, сервер службы Tap to Pay on iPhone определяет, соответствует ли устройство необходимым критериям, таким как модель устройства, версия iOS, а также установлен ли код-пароль. После выполнения этой проверки апплет приема платежа загружается с сервера службы Tap to Pay on iPhone и устанавливается в Secure Element вместе со связанной конфигурацией платежного ядра. Эта операция выполняется безопасно между серверами службы Tap to Pay on iPhone и Secure Element. Secure Element проверяет целостность и подлинность этих данных перед установкой.

Обзор безопасности чтения карт

Когда приложение службы Tap to Pay on iPhone запрашивает чтение карты из программной среды ProximityReader, отображается лист, контролируемый iOS, а пользователю предлагается коснуться платежной карты. iOS инициализирует работу считывателя платежной карты, а затем отправляет запрос обрабатывающим платежные ядрам в Secure Element, чтобы они начали чтение карты.

На этом этапе Secure Element принимает контроль над контроллером NFC в режиме чтения. В этом режиме разрешен только обмен данными карты через контроллер NFC между платежной картой и Secure Element. Платежные карты можно считывать только в этом режиме.

После того как апплет приема платежа в Secure Element завершит чтение карты, он зашифрует и подпишет ее данные. Данные карты остаются защищены шифрованием и аутентификацией, пока они не будут переданы платежной системе. Расшифровать данные карты может только платежная система, используемая приложением для запроса чтения карт. Платежная система должна запросить ключ для дешифрования данных карты у сервера службы Tap to Pay on iPhone. Сервер службы Tap to Pay on iPhone передает платежной системе ключи расшифровки после проверки целостности и подлинности данных и подтверждения того, что карта была прочитана в течение 60 секунд после чтения карты на устройстве.

Эта модель помогает сделать так, чтобы данные карты не мог расшифровать никто, кроме платежной системы, которая обрабатывает эту транзакцию для продавца.

Использование Apple Wallet

Доступ через Apple Wallet

В Apple Wallet на поддерживаемых устройствах iPhone и часах Apple Watch пользователи могут хранить ключи от дома, ключи от автомобиля, а также гостиничные ключ-карты. Таким образом можно даже хранить пропуска на работу и студенческие билеты. Когда пользователь подходит к двери, автоматически предлагается нужный ключ, чтобы можно было войти по одному касанию благодаря технологии беспроводной связи малого радиуса действия (NFC).

Удобство использования

Экспресс-режим включается по умолчанию при добавлении ключа, ключ-карты, студенческого билета или пропуска на работу в Apple Wallet. Карты в экспресс-режиме работают с поддерживающими их терминалами без аутентификации с помощью Face ID, Touch ID, код-пароля или двойного нажатия боковой кнопки на часах Apple Watch. Чтобы выключить эту функцию, пользователи могут выключить Экспресс-режим, коснувшись кнопки «Еще» на лицевой стороне карты в Apple Wallet. Чтобы снова включить Экспресс-режим, потребуется Face ID, Touch ID или код-пароль.

Конфиденциальность и безопасность

Ключи в Apple Wallet максимально эффективно используют преимущества функций безопасности и конфиденциальности, встроенных в iPhone и Apple Watch. Данные о том, когда или где человек использует ключи из Apple Wallet, никогда не передаются в Apple и не сохраняются на серверах Apple, а учетные данные безопасно хранятся в Secure Element (SE) на поддерживаемых устройствах. Secure Element хранит специально разработанные апплеты, чтобы безопасно контролировать и хранить ключи доступа таким образом, чтобы их нельзя было извлечь.

Перед тем как подготовить ключи доступа, пользователю потребуется войти в свою учетную запись iCloud на совместимом iPhone и включить двухфакторную аутентификацию для учетной записи iCloud. Двухфакторную аутентификацию можно не включать для студенческих билетов.

Если пользователь начинает процесс подготовки, то последующие шаги схожи с процессом подготовки кредитных и дебетовых карт к использованию, как и в случае [привязки и подготовки](#). Во время транзакции считыватель обменивается данными непосредственно с чипом Secure Element по установленному безопасному каналу с помощью контроллера NFC, который работает в малом радиусе действия.

Количество устройств, включая iPhone и Apple Watch, которым можно предоставить ключ доступа, определяется и контролируется каждым партнером и может отличаться в зависимости от партнера. При таком подходе каждый партнер может управлять максимальным количеством ключей доступа, подготовленных для определенного типа устройства, в соответствии с его требованиями. Для этого Apple предоставляет партнерам информацию о типе устройств и их обезличенные идентификаторы. Идентификаторы отличаются у разных партнеров из соображений конфиденциальности и безопасности.

Ключи можно выключить или удалить следующими способами:

- удаленное стирание содержимого и настроек устройства с помощью приложения «Локатор»;
- перевод устройства в режим пропажи с помощью приложения «Локатор»;
- получение команды удаленного стирания от системы управления мобильными устройствами (MDM);
- удаление всех карт со страницы своей учетной записи Apple ID;
- удаление всех карт из iCloud.com;
- удаление всех карт из Apple Wallet;
- удаление карты из приложения эмитента.

В iOS 15.4 или новее, когда пользователь дважды нажимает боковую кнопку на iPhone с Face ID или дважды нажимает кнопку «Домой» на iPhone с Touch ID, ключи и данные карт доступа этого пользователя не отображаются, пока не выполнена аутентификация на устройстве. Перед тем как передать и отобразить определенную информацию, включая сведения о бронировании отеля, в Apple Wallet, требуется выполнить аутентификацию с помощью Face ID, Touch ID или код-пароля.

Виды получения доступа

Apple Wallet поддерживает различные способы доступа, в том числе гостиничные ключ-карты, пропуска на работу и студенческие билеты, а также ключи от дома и автомобиля.

Гостиницы

Гостиничные ключ-карты в Apple Wallet обеспечивают простой и бесконтактный доступ с момента заселения до выезда, предоставляя дополнительные преимущества в отношении конфиденциальности и безопасности гостей по сравнению со стандартными пластиковыми картами. Гости отелей, в которых используется эта функция, могут касанием отпирать двери номера с помощью ключей в Apple Wallet на совместимых устройствах [iPhone](#) и Apple Watch Series 4 или новее.

Возможности Apple Wallet созданы для максимального удобства пользователей:

- карта подготавливается через приложение отеля перед заездом, чтобы ее можно было добавить в Apple Wallet заранее;
- на устройство добавляются значки карт для заезда, позволяющие зарегистрироваться в отеле и получить номер через Apple Wallet;
- ключи обновляются после подготовки, чтобы изменять условия или продлевать время текущего пребывания;
- одной ключ-картой в Apple Wallet можно открывать несколько номеров;
- ключи с истекшим сроком действия автоматически архивируются в Apple Wallet.

Пропуска на работу

Ключ-карты сотрудников поддерживаемых компаний-партнеров можно добавить в Apple Wallet на iPhone и Apple Watch, предоставив сотрудникам по всему миру возможность получать бесконтактный доступ на работе. Чтобы добавить ключ-карту, у сотрудника должна быть включена многофакторная аутентификация для учетной записи, используемой для входа в приложение работодателя.

Ключ-карта сотрудника обладает всеми преимуществами функций доступа, разработанных компанией Apple. С ключ-картой пользователи могут:

- автоматически добавлять ключ-карты на объединенные в пару Apple Watch через push-уведомление о подготовке карты, для которого не требуется устанавливать приложение партнера;
- получать доступ к помещениям, используя экспресс-режим;
- получать доступ к рабочему месту, даже если iPhone разряжен.

Студенческие билеты

При использовании iOS 12 или новее учащиеся, преподаватели и сотрудники участвующих в программе учебных заведений могут добавить свои студенческие билеты в Apple Wallet на поддерживаемых моделях iPhone и Apple Watch, чтобы оплачивать покупки и проходить везде, где действует их билет.

Для добавления студенческого билета в Apple Wallet используется приложение эмитента карты или учебного заведения. С технической точки зрения процедура аналогична описанной в разделе «[Добавление кредитных или дебетовых карт из приложения эмитента карты](#)». Кроме того, приложения должны поддерживать двухфакторную аутентификацию для учетных записей, которые защищают доступ к студенческим билетам. Билет можно одновременно настроить на любых двух поддерживаемых устройствах Apple, на которых выполнен вход с одним и тем же Apple ID.

Многоквартирные дома и апартаменты

Квартиросъемщики и обслуживающий апартаменты персонал в зданиях поддерживаемых партнеров могут добавлять ключи от дома в Apple Wallet, чтобы входить в здание и посещать объекты его инфраструктуры. Ключи от дома могут быть подготовлены в приложении партнера. Если компании-партнеры поддерживают упрощенную подготовку, управляющие зданием могут отправить квартиросъемщикам ссылку, чтобы начать подготовку, любым привычным способом (например, по электронной почте или в SMS-сообщении), а квартиросъемщику останется только нажать на ссылку, чтобы активировать ключ. Блиц-приложения также работают безопасно и быстро: с их помощью можно подготовить ключ, не устанавливая приложение партнера. Дополнительная информация приведена в статье службы поддержки Apple: [Использование блиц-приложений на iPhone](#).

Ключ от дома

Ключ от дома, доступный в Apple Wallet, можно использовать с замками, поддерживающими технологию NFC, чтобы открывать эти замки простым касанием iPhone или часов Apple Watch. Дополнительная информация о том, как настроить и использовать ключ от дома, приведена в статье службы поддержки Apple: [Отпирание двери ключом от дома на iPhone](#).

Когда пользователь настраивает ключ от дома, его автоматически получают все жители этого дома. Чтобы поделиться ключом от дома или удалить пользователя из общего дома, владелец дома может открыть приложение «Дом» и изменить настройки для приглашений и участников. Когда пользователь примет приглашение присоединиться к дому и использовать ключ от него, начнется подготовка ключа от дома в Apple Wallet на устройстве этого пользователя. Если пользователь решит покинуть дом или если владелец отзовет доступ к дому, то ключ от дома будет удален из Apple Wallet.

Ключ от автомобиля

На поддерживаемых моделях iPhone и часах Apple Watch имеется встроенная поддержка хранения цифровых ключей от автомобиля в Apple Wallet. Ключи от автомобиля представлены в виде карт (созданных Apple от имени автопроизводителя) в Apple Wallet. Эти ключи поддерживают полный жизненный цикл карт Apple Pay (режим пропажи iCloud, удаленное стирание, локальное удаление карты, а также стирание всего контента и настроек). Помимо стандартного управления картами Apple Pay, общие ключи для автомобиля можно удалить с iPhone и Apple Watch владельца, а также из интерфейса оператора (HMI) транспортного средства.

Ключи от автомобиля можно использовать для блокировки и разблокировки транспортного средства, а также для запуска двигателя и перевода транспортного средства в режим вождения. Для взаимной аутентификации используется «стандартная транзакция», которая является обязательной для запуска двигателя. Для транзакций блокировки и разблокировки может применяться «быстрая транзакция», если это необходимо из соображений производительности.

Ключи создаются путем объединения в пару устройства iPhone с поддерживаемым транспортным средством пользователя. Все ключи создаются на встроенном чипе Secure Element с использованием встроенного механизма создания ключей на основе эллиптических кривых (NIST P-256) (ECC-OBKG), а личные ключи никогда не покидают чип Secure Element. Устройство и транспортное средство обмениваются данными с использованием либо технологии NFC, либо Bluetooth LE и технологии UWB, а для управления ключами используется API Apple и сервера автопроизводителя со взаимно аутентифицированным TLS-соединением. После создания пары между ключом и iPhone ключ также передается на любые Apple Watch, с которыми для этого iPhone создана пара. После удаления ключа с устройства или с транспортного средства через его интерфейс восстановить ключ не удастся. Работу ключей на утерянных или украденных устройствах можно приостановить и возобновить, однако для их повторной подготовки к использованию на новом устройстве требуется создать новую пару или заново предоставить к ним доступ.

Безопасность ключей от автомобиля в iOS

Разработчики могут обеспечивать безопасную поддержку электронных ключей от автомобиля на поддерживаемых iPhone и часах Apple Watch, с которыми создана пара.

Создание пары с владельцем

Владелец должен подтвердить, что транспортное средство принадлежит ему (способ подтверждения зависит от автопроизводителя), после чего он сможет начать процесс создания пары в приложении автопроизводителя с помощью ссылки в письме, отправленном автопроизводителем, или посредством меню транспортного средства. В любом случае при создании пары владелец должен ввести на iPhone секретный одноразовый пароль, который используется для создания защищенного канала связи по протоколу SPAKE2+ на основе кривой NIST P-256. При использовании приложения или ссылки в письме пароль автоматически передается на iPhone. При создании пары из интерфейса транспортного средства пароль необходимо ввести вручную.

Совместное использование ключей

Владелец iPhone, объединенного в пару, может делиться ключами с совместимыми iPhone членов семьи и друзей (а затем передавать ключи на Apple Watch, с которыми создана пара). Для этого необходимо отправить соответствующее приглашение с помощью iMessage и службы идентификации Apple (IDS). Обмен всеми командами по предоставлению доступа осуществляется с использованием функции сквозного шифрования службы IDS. Объединенный в пару iPhone владельца препятствует изменению канала служб идентификации во время предоставления доступа, что защищает от переадресации приглашений.

После принятия приглашения iPhone члена семьи или друга создает цифровой ключ и отправляет цепочку сертификатов создания ключа обратно на устройство iPhone владельца, который объединен в пару, для подтверждения того, что ключ был создан на подлинном устройстве Apple. Устройство iPhone владельца, с которым создана пара, подписывает открытый ключ ECC устройства iPhone другого члена семьи или друга, а затем отправляет подпись обратно на устройство iPhone члена семьи или друга. Для подписи на устройстве владельца пользователю требуется пройти аутентификацию (с помощью Face ID, Touch ID или код-пароля) и безопасно подтвердить свое намерение, как описано в разделе [Использование Face ID и Touch ID](#). Авторизация запрашивается при отправке приглашения и хранится на чипе Secure Element для использования при возврате запроса на подписание устройством друга. Ключевые разрешения предоставляются автомобилю либо онлайн с сервера OEM автомобиля или во время первого использования общего ключа в автомобиле.

Удаление ключа

Удалить ключ с устройства, которому ключ был ранее предоставлен для использования, можно с устройства владельца или из интерфейса транспортного средства. Операции удаления с iPhone владельца выполняются незамедлительно, даже если в этот момент владелец использует ключ. В силу этого перед удалением отображается предупреждение, акцентирующее внимание пользователя на необратимости этого действия. Удаление ключей в автомобиле возможно в любое время либо только тогда, когда автомобиль находится онлайн.

В обоих случаях использовавшее предоставленный владельцем ключ устройство или транспортное средство передает информацию об удалении на сервер инвентаризации ключей (KIS) на стороне автопроизводителя, который регистрирует выданные ключи в целях страхования.

Владелец может запросить удаление, перейдя на обратную сторону своей карты владельца. Сначала запрос отправляется автопроизводителю, чтобы он удалил ключ с транспортного средства. Условия удаления ключа с транспортного средства определяет автопроизводитель. Только после удаления ключа с транспортного средства автопроизводитель отправляет на устройство, использовавшее предоставленный владельцем ключ, запрос на удаленное прекращение действия ключа.

После того как действие ключа на устройстве прекращено, апплет, который управляет цифровыми ключами от автомобилей, создает удостоверение прекращения действия ключа, заверенное криптографической подписью. Это удостоверение подтверждает удаление ключа автопроизводителем и используется для удаления ключа с сервера KIS.

Стандартные транзакции с использованием NFC

В автомобилях, поддерживающих ключи NFC, безопасный канал связи устанавливается между считывателем и iPhone путем создания пар динамических ключей на считывателе и iPhone. С помощью метода согласования ключей общий ключ можно сгенерировать на основе данных с обоих устройств, а затем использовать его для создания общего симметричного ключа с помощью алгоритма Диффи — Хеллмана, функции формирования ключей и подписей из статического ключа, заданного при создании пары.

Динамический открытый ключ, сгенерированный на транспортном средстве, подписывается с помощью статического личного ключа на считывающем устройстве, в результате чего iPhone выполняет аутентификацию считывающего устройства. С точки зрения iPhone этот протокол призван исключить раскрытие конфиденциальных данных злоумышленником, перехватившим канал связи.

Наконец, iPhone использует созданный безопасный канал для шифрования идентификатора своего открытого ключа вместе с подписью, вычисленной на основе запроса полученных данных считывающего устройства и ряда других дополнительных данных приложения. Такая проверка подписи iPhone считывающим устройством позволяет ему аутентифицировать iPhone.

Быстрые транзакции

iPhone генерирует криптограмму на основе общего ключа, предоставленного ранее во время стандартной транзакции. Это позволяет транспортному средству быстро аутентифицировать устройство для сохранения требуемого уровня производительности. Также между транспортным средством и устройством может быть создан безопасный канал связи путем получения ключей сеанса из ключа, предоставленного ранее во время стандартной транзакции, и новой динамической пары ключей. Способность транспортного средства создать безопасный канал служит для аутентификации транспортного средства для устройства iPhone.

Стандартные транзакции с использованием BLE и UWB

В автомобилях, поддерживающих ключи UWB, сеанс Bluetooth LE устанавливается между автомобилем и iPhone. Как и в случае транзакций с использованием NFC, общий ключ генерируется по обе стороны и используется, чтобы наладить безопасный сеанс. В этом сеансе поочередно генерируется и согласовывается секретный ключ UWB для измерения расстояния, сокращенно — ключ URSK. Ключ URSK передается на средства радиосвязи UWB в устройстве пользователя и в автомобиле, чтобы можно было с точностью установить местонахождение устройства пользователя рядом с автомобилем или внутри него. После этого автомобиль будет учитывать местонахождение устройства перед тем, как разрешить отпереть дверь или завести двигатель. У ключей URSK есть предопределенное значение TTL. Чтобы измерение расстояния не прервалось, когда срок действия TTL истечет, ключи URSK можно предварительно сгенерировать на устройстве SE и в автомобиле HSM/SE, пока безопасное измерение расстояния неактивно, но есть соединение BLE. Следовательно, нет необходимости получать новый ключ URSK во время стандартной транзакции, когда каждое мгновение на счету. Предварительно сгенерированный ключ URSK можно быстро передать на средства радиосвязи UWB в автомобиле и устройстве, чтобы не прерывать измерение расстояния с помощью технологии UWB.

Конфиденциальность

На сервере инвентаризации ключей (сервере KIS) у автопроизводителя не хранятся идентификаторы устройств, SEID или Apple ID. На этом сервере хранится только изменяемый идентификатор — идентификатор экземпляра центра сертификации. Этот идентификатор не привязан к каким-либо личным данным на устройстве или на сервере. Когда пользователь стирает все данные с устройства с помощью функции «Стереть контент и настройки», этот идентификатор удаляется вместе с остальными данными.

Добавление транспортных карт и карт eMoney в Apple Wallet

Во многих странах и регионах пользователи могут добавлять поддерживаемые транспортные карты и карты eMoney в Apple Wallet на поддерживаемых моделях iPhone и Apple Watch. В зависимости от оператора можно перевести денежную сумму или проездной билет (или и то и другое) с физической карты в цифровой аналог в Apple Wallet или подготовить новую транспортную карту или карту eMoney в Apple Wallet или приложении эмитента транспортной карты. Добавив транспортные карты в Apple Wallet, пользователи могут оплачивать поездки в общественном транспорте, просто поднося iPhone или Apple Watch к считывателю. Некоторые транспортные карты также можно использовать для платежей.

Как работают транспортные карты и карты eMoney

Добавленные транспортные карты и карты eMoney связываются с учетной записью iCloud, принадлежащей пользователю. Если пользователь добавляет в Apple Wallet несколько карт, Apple или эмитент карты может связывать личную информацию пользователя и личную информацию из его учетной записи с различными картами. Транспортные карты, карты eMoney и транзакции защищены набором иерархических криптографических ключей.

Для перевода средств с физической карты в Apple Wallet пользователь должен ввести данные карты. Также может потребоваться предоставить личную информацию для подтверждения владения картой. При передаче карт с iPhone на часы Apple Watch оба устройства должны находиться в сети.

Баланс можно пополнять средствами с кредитных, дебетовых и предоплаченных карт через Apple Wallet или приложение эмитента транспортной карты или карты eMoney. Подробная информация о безопасности процедуры пополнения средств с использованием Apple Pay приведена в разделе [Оплата с помощью карт в приложениях](#). Чтобы узнать больше о том, как подготовить карту в приложении эмитента карты, обратитесь к разделу [Добавление кредитных или дебетовых карт из приложения эмитента карты](#).

Если поддерживается подготовка с использованием физической карты, у эмитента транспортной карты или карты eMoney есть криптографические ключи, необходимые для аутентификации физической карты и проверки данных, введенных пользователем. После проверки данных система может создать учетный номер устройства для чипа Secure Element и активировать карту, только что добавленную в Apple Wallet, с внесенными средствами. В некоторых случаях физическая карта перестает действовать после завершения подготовки с ее использованием.

Если баланс карты хранится на устройстве, то при любом способе подготовки в конце процедуры баланс на карте шифруется и сохраняется в выделенном апплете чипа Secure Element. У оператора есть ключи, чтобы выполнять криптографические операции с данными на карте для перевода средств.

По умолчанию пользователи могут автоматически оплачивать проезд транспортной картой в экспресс-режиме без использования Face ID, Touch ID или ввода код-пароля. Когда включен экспресс-режим, такая информация, как сведения о недавно посещенных станциях, истории транзакций и дополнительных билетах, может быть доступна любым находящимся рядом устройствам считывания бесконтактных карт. Пользователи могут включить обязательную авторизацию с помощью Face ID, Touch ID или код-пароля в разделе настроек «Wallet и Apple Pay», выключив Экспресс-режим. Экспресс-режим не поддерживается картами eMoney.

Как и в случае с другими картами Apple Pay, пользователи могут приостанавливать действие карт eMoney и удалять их следующими способами:

- удаленное стирание содержимого и настроек устройства с помощью приложения «Локатор»;
- перевод устройства в режим пропажи с помощью приложения «Локатор»;
- ввод команды удаленного стирания от системы управления мобильными устройствами (MDM);
- удаление всех карт со страницы своей учетной записи Apple ID;
- удаление всех карт из iCloud.com;
- удаление всех карт из Apple Wallet;
- удаление карты из приложения эмитента.

Серверы Apple Pay уведомляют оператора карт о приостановке действия карт или их выключении. Если пользователь удаляет транспортную карту или карту eMoney с подключенного к интернету устройства, оставшиеся на карте средства можно отправить на устройство, на котором выполнен вход с той же учетной записью Apple ID. Если устройство отключено от интернета, выключено или находится в неработоспособном состоянии, возврат средств может оказаться невозможным.

Добавление транспортных карт и карт eMoney на часы Apple Watch члена семьи

В iOS 15 и watchOS 8 организатор группы «Семья» в iCloud может добавлять транспортные карты и карты eMoney на часы Apple Watch членов семьи через приложение Apple Watch на их устройствах iPhone. При подготовке одной из этих карт для часов Apple Watch члена семьи часы должны находиться рядом, и они должны быть подключены к iPhone организатора по сети Wi-Fi или через Bluetooth. Для всего этого процесса необходимо, чтобы для учетных записей Apple ID членов семьи была включена двухфакторная аутентификация.

Члены семьи могут со своих часов Apple Watch отправлять запросы через iMessage на пополнение транспортной карты или карты eMoney или перевод средств на нее. Содержимое сообщения защищено сквозным шифрованием, как описано в разделе [Обзор безопасности iMessage](#). Пополнить карту на часах Apple Watch члена семьи можно удаленно по сети Wi-Fi или сотовой сети. Находиться рядом не обязательно.

Примечание. Эта функция может быть доступна не во всех странах и регионах.

Кредитные и дебетовые карты

В общественном транспорте некоторых городов валидаторы поддерживают оплату проезда с помощью смарт-карт EMV. Когда пользователи прикладывают кредитную или дебетовую карту стандарта EMV к считывателю, требуется аутентификация пользователя, как описано в разделе об оплате покупок в магазинах с помощью кредитных и дебетовых карт.

В iOS 12.3 или новее некоторые кредитные или дебетовые карты стандарта EMV, имеющиеся в Apple Wallet, можно использовать в экспресс-режиме. В экспресс-режиме пользователи могут оплачивать проезд в общественном транспорте поддерживаемых операторов без использования Face ID, Touch ID или ввода код-пароля. При подготовке первой кредитной или дебетовой карты стандарта EMV в Apple Wallet для нее включается экспресс-режим. Пользователь может коснуться кнопки «Еще» на лицевой стороне карты в Apple Wallet и выключить Экспресс-режим для этой карты, задав для функции «Настроить экспресс-карты» параметр «Нет». Пользователь также может выбрать другую кредитную или дебетовую карту в Apple Wallet в качестве транспортной экспресс-карты. Чтобы снова включить экспресс-режим или выбрать другую транспортную экспресс-карту, требуется Face ID, Touch ID или код-пароль.

Apple Card и Apple Cash могут использоваться в качестве транспортной экспресс-карты.

Удостоверения личности в Apple Wallet

На iPhone 8 или новее с iOS 15.4 или новее и Apple Watch Series 4 или новее с watchOS 8.4 или новее пользователи могут добавлять удостоверения личности и водительские права в Apple Wallet, чтобы быстро и безопасно предъявлять их касанием iPhone или Apple Watch там, где это возможно.

Примечание. Эта функция доступна не во всех штатах США.

Идентификаторы в Apple Wallet используют функции безопасности, встроенные в аппаратное и программное обеспечение устройства, чтобы защищать личность пользователя и надежно хранить личную информацию.

Добавление водительских прав или удостоверения личности в Apple Wallet

На iPhone пользователи могут просто коснуться кнопки добавления (+) сверху экрана в Apple Wallet, чтобы начать добавление водительских прав или удостоверения личности. Если во время настройки у пользователей есть часы Apple Watch, объединенные в пару, им предлагается также добавить водительские права или удостоверение личности в Apple Wallet на часах Apple Watch.

Пользователям сначала предлагается воспользоваться своим iPhone, чтобы отсканировать водительские права или удостоверение личности с обеих сторон. iPhone оценивает качество и тип изображений: они должны соответствовать требованиям органа власти штата. Эти изображения удостоверений личности зашифровываются на устройстве с помощью ключа органа власти штата, а затем передаются этому органу власти.

Затем пользователю предлагается выполнить несколько движений головой и мимических движений. Устройство пользователя и Apple оценивают эти движения, снижая вероятность того, что кто-то воспользуется чужой фотографией, либо чужими видео или маской, чтобы добавить чужое удостоверение личности в Apple Wallet. Результаты анализа этих движений затем передаются органу власти штата. Само видео, на котором показаны движения, не отправляется.

Чтобы убедиться, что человек, добавивший удостоверение личности в Apple Wallet, именно тот, кому оно принадлежит, пользователю предлагается сделать селфи. Перед тем как отправить фото пользователя органу власти штата, серверы Apple и устройство пользователя сравнивают, насколько человек на фото похож с тем, кто выполнил движения головой и мимические движения. Таким образом можно проверить, что на отправленном фото и фото в удостоверении личности изображен один и тот же человек. После сравнения фото зашифровывается на устройстве, а затем передается органу власти штата для сопоставления с тем изображением в удостоверении личности, которое имеется у этого органа власти.

Наконец, пользователям предлагается выполнить аутентификацию с помощью Face ID или Touch ID. Устройство пользователя связывает эти биометрические данные Face ID или Touch ID одного совпадения с удостоверением личности. Это позволяет убедиться, что только человек, добавивший удостоверение личности на iPhone, может его предъявлять; другую зарегистрированную биометрическую информацию нельзя использовать для того, чтобы разрешить предъявление удостоверения личности. Весь процесс выполняется исключительно на устройстве, и его данные не передаются органу власти штата.

Орган власти штата получает только ту информацию, которая необходима для настройки цифрового удостоверения личности. К этой информации относятся: изображения удостоверения личности с обеих сторон; данные, считанные со штрихкода PDF417; селфи, снятое пользователем во время подтверждения личности. Штат-орган выдачи также получает одноцифровое значение, которое используется для предупреждения мошенничества. Это значение основано на модели того, как используется устройство, а также на данных настроек и личной информации из учетной записи Apple ID. Окончательное решение о том, можно ли добавить удостоверение личности в Apple Wallet, принимает орган власти штата.

После того как орган власти штата одобрит добавление удостоверения личности и водительских прав в Apple Wallet, в Secure Element на iPhone, на котором имеется удостоверение личности, будет сгенерирована пара ключей для этого конкретного устройства. При добавлении на Apple Watch пара ключей генерируется в Secure Element часами Apple Watch.

После того как удостоверение появится на iPhone, информация из удостоверения будет храниться в Apple Wallet в зашифрованном виде, и она будет защищена с помощью Secure Enclave.

Использование водительских прав или удостоверения личности в Apple Wallet

Чтобы использовать удостоверение личности в Apple Wallet, потребуется выполнить аутентификацию с помощью устройства с Face ID или Touch ID, связанного с удостоверением личности в Apple Wallet перед тем, как iPhone сможет предоставить информацию считывателю удостоверений личности.

Чтобы воспользоваться удостоверением личности из Apple Wallet на часах Apple Watch, потребуется разблокировать iPhone, выполнив аутентификацию с помощью Face ID или Touch ID. Аутентификация по внешнему виду или отпечатку пальца будет необходима каждый раз, когда пользователь надевает часы Apple Watch. Затем удостоверением личности из Apple Wallet можно будет пользоваться без аутентификации, пока пользователь снова не снимет часы Apple Watch. Эта возможность основана на основополагающих функциях автоматической разблокировки, которые подробно описаны в разделе [Безопасность системы watchOS](#).

Если удерживать iPhone или Apple Watch рядом со считывателем удостоверений личности, на устройстве отобразится подсказка о том, какая информация запрашивается, кем она запрашивается и будет ли она сохранена. После подтверждения с помощью связанного устройства с Face ID или Touch ID запрашиваемая информация о личности передается с устройства.

Важно! Чтобы предъявить удостоверение личности, не нужно разблокировать устройство, показывать или передавать его.

Если вместо Face ID или Touch ID включена какая-либо функция Универсального доступа, в том числе Управление голосом, Виртуальный контроллер или AssistiveTouch, то можно использовать код-пароль для доступа к информации и ее предъявления.

Передача данных о личности на считыватель удостоверений личности выполняется в соответствии со стандартом ISO/IEC 18013-5, который предусматривает несколько защитных механизмов для выявления и снижения рисков, связанных с безопасностью, а также противодействия им. К этим механизмам относятся обеспечение целостности данных удостоверения личности и противодействие его подделке, связывание с устройством, информированное согласие, а также обеспечение конфиденциальности данных при передаче по радиосвязи.

Целостность данных удостоверения личности и противодействие его подделке

Удостоверения личности в Apple Wallet используют подпись, предоставленную органом выдачи, чтобы любой считыватель, соответствующий стандарту ISO/IEC 18013-5, мог проверить удостоверение личности пользователя в Apple Wallet. Кроме того, все фрагменты данных в удостоверении личности в Wallet защищены по отдельности от подделки. Благодаря этому считыватель удостоверений личности может запросить определенный поднабор фрагментов данных из удостоверения личности в Apple Wallet, а в ответ Apple Wallet должен вернуть тот же поднабор. Таким образом передаются только запрашиваемые данные, что помогает обеспечить конфиденциальность пользователя.

Связывание с устройством

При аутентификации в Apple Wallet удостоверения личности используют подпись устройства, чтобы защищать удостоверения личности от клонирования и повторного использования. Поскольку личный ключ хранится в Secure Element на iPhone для выполнения аутентификации перед предъявлением удостоверения, удостоверение личности связано с тем устройством, для которого орган выдачи штата создал это удостоверение.

Информированное согласие

При аутентификации перед предъявлением удостоверения в Apple Wallet выполняется аутентификация считывателя удостоверений личности по протоколу, предусмотренному стандартом ISO/IEC 18013-5. Во время предъявления значок из сертификата считывателя отображается для того, чтобы сообщить пользователю о происходящем процессе с участием третьих лиц.

Обеспечение конфиденциальности данных при передаче по радиосвязи

Благодаря шифрованию сеанса вся позволяющая установить личность информация (PII), которая передается между удостоверением личности в Apple Wallet и считывателем удостоверений личности, зашифровывается. Шифрование выполняется на уровне приложений. Следовательно, безопасность шифрования сеанса не зависит от безопасности, обеспечиваемой на уровне передачи данных (например, NFC, Bluetooth и Wi-Fi).

Удостоверения личности в Apple Wallet способствуют сохранению конфиденциальности пользователей

Процесс извлечения данных удостоверения личности с устройства пользователя в Apple Wallet соответствует стандарту ISO/IEC 18013-5. При извлечении данных с устройства нет необходимости делать запросы на сервер во время предъявления, следовательно, пользователи защищены от отслеживания со стороны Apple и органа выдачи.

iMessage

Обзор безопасности iMessage

Apple iMessage — это служба обмена сообщениями для устройств iOS и iPadOS, Apple Watch и компьютеров Mac. С помощью iMessage можно передавать не только текст, но и различные вложения, включая фотографии, контакты, географические координаты и ссылки. Например, прямо в сообщение можно добавить значок с большим пальцем вверх. Сообщения отображаются на всех зарегистрированных устройствах пользователя, поэтому начатый диалог можно продолжить на любом своем устройстве. iMessage активно использует службу Apple Push Notification (APNs). Apple не сохраняет содержимое сообщений или вложений: оно защищено с помощью сквозного шифрования, поэтому никто, кроме отправителя и получателя, не может получить к нему доступ. Apple не может расшифровать данные.

Когда пользователь включает iMessage на устройстве, оно генерирует пару ключей шифрования и пару ключей подписания для работы со службой. Для шифрования используется 1280-битный ключ RSA, а также 256-битный ключ EC на основе кривой NIST P-256. Для подписей используются 256-битные ключи подписания алгоритма цифровой подписи на основе эллиптической кривой (ECDSA). Личные ключи сохраняются в связке ключей устройства и доступны только после первой разблокировки. Открытые ключи передаются в службу идентификации Apple (IDS), где они связываются с номером телефона или адресом электронной почты пользователя, а также с APNs-адресом устройства.

Когда пользователь включает iMessage на дополнительных устройствах, их открытые ключи шифрования и подписания, APNs-адреса и связанные номера телефонов добавляются в службу каталогов. Пользователь также может добавить дополнительные адреса электронной почты, которые проверяются путем отправки ссылки для подтверждения. Для проверки номеров телефона используется сеть оператора и SIM-карта. В некоторых сетях для этого требуется SMS-сообщение (если оно не является бесплатным, пользователю будет предложено подтвердить его). Помимо iMessage, проверка номера телефона может требоваться для некоторых системных служб, например FaceTime и iCloud. При добавлении нового устройства, номера телефона или адреса электронной почты на всех зарегистрированных устройствах пользователя отображается соответствующее сообщение.

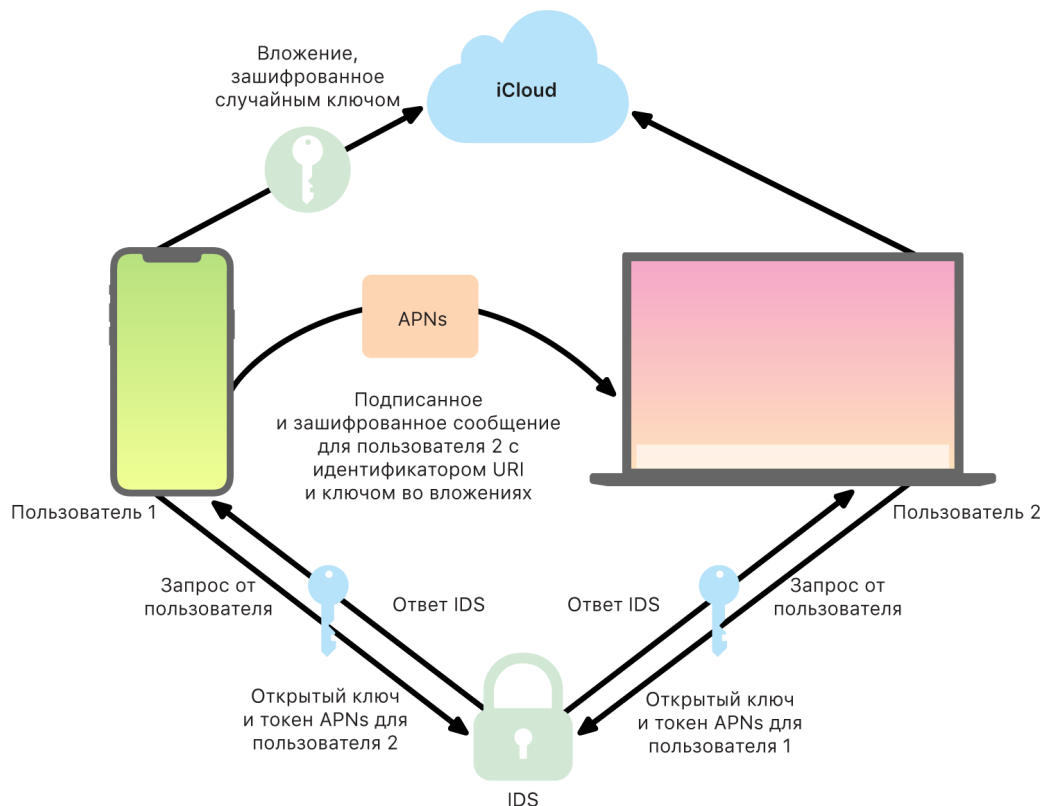
Процесс безопасной отправки и получения сообщений в iMessage

Чтобы начать новый разговор iMessage, пользователь вводит адрес или имя собеседника. Если пользователь вводит номер телефона или адрес электронной почты, устройство связывается со службой идентификации Apple (IDS) для получения открытых ключей и APNs-адресов для всех устройств, связанных с адресатом. Если пользователь вводит имя, устройство извлекает из приложения «Контакты» номера телефонов и адреса электронной почты, связанные с введенным именем, а затем получает открытые ключи и APNs-адреса из IDS.

Исходящие сообщения пользователя шифруются отдельно для каждого из устройств получателя. Открытые ключи шифрования и ключи подписания принимающих устройств извлекаются из IDS. Для каждого принимающего устройства отправляющее устройство генерирует случайное 88-битное значение и использует его в качестве ключа HMAC-SHA256 для создания 40-битного значения на основе открытых ключей отправителя и получателя, а также простого текста. Сцепление 88-битного и 40-битного значений дает 128-битный ключ, который используется для шифрования сообщения с применением алгоритма AES в режиме счетчика (CTR). 40-битное значение используется на стороне получателя для проверки целостности дешифрованного простого текста. Этот ключ AES отдельного сообщения шифруется по схеме RSA-OAEP с использованием открытого ключа принимающего устройства. Сочетание зашифрованного текста сообщения и зашифрованного ключа сообщения хэшируется с использованием SHA-1, затем хэш подписывается по алгоритму цифровой подписи на основе эллиптической кривой (ECDSA) с использованием личного ключа подписания передающего устройства. В iOS 13 или новее и iPadOS 13.1 или новее устройства могут использовать шифрование ECIES (интегрированная схема шифрования на эллиптических кривых) вместо шифрования RSA.

Результатом являются сообщения — по одному для каждого принимающего устройства — которые состоят из зашифрованного текста сообщения, зашифрованного ключа сообщения и цифровой подписи отправителя. Затем они передаются в APNs для доставки адресатам. Шифрование метаданных, таких как метка времени и информация о маршрутизации APNs, не выполняется. Связь с APNs шифруется с использованием канала TLS с прямой секретностью.

APNs может ретранслировать сообщения размером до 4 или 16 КБ в зависимости от версии iOS или iPadOS. Если текст сообщения слишком длинный либо к сообщению приложена фотография или другой большой объект, вложение шифруется по алгоритму AES в режиме CTR с использованием случайного 256-битного ключа и выгружается в iCloud. Затем в виде содержимого iMessage получателю пересылается ключ AES для вложения, его универсальный идентификатор ресурса (URI) и хэш SHA-1 для зашифрованной формы. За защиту их конфиденциальности и целостности отвечает стандартный процесс шифрования iMessage, который показан на рисунке ниже.



При отправке групповых сообщений эта процедура повторяется для каждого получателя и его устройств.

На принимающей стороне каждое устройство получает свою копию сообщения из APNs и, при необходимости, извлекает вложение из iCloud. Входящий номер телефона или адрес электронной почты отправителя сравнивается со списком контактов получателя, чтобы по возможности отобразить имя отправителя.

Как и все push-уведомления, сообщения удаляются из APNs после доставки. В отличие от других уведомлений APNs, если устройство отключено, сообщения iMessage ставятся в очередь для последующей отправки. Сообщения могут храниться на серверах Apple в течение 30 дней.

Безопасное отображение имени и фото пользователя iMessage для других пользователей

Пользователь может поделиться своим именем и фотографией в iMessage. Пользователь может выбрать информацию из своей карточки («Моя карточка») или изменить имя и добавить произвольное изображение. Если пользователь делится именем и фото в iMessage, используется двухэтапная система передачи имени и фотографии.

Данные разбиваются на поля, каждое из которых шифруется и аутентифицируется отдельно, а также аутентифицируется совместно с другими в соответствии с описанным ниже процессом. Имеется три поля:

- имя;
- фотография;
- имя файла фотографии.

На одном из первых шагов создания данных на устройстве генерируется случайный 128-битный ключ записи. Затем к этому ключу записи применяется HKDF-HMAC-SHA256 для создания трех производных подключей: Key 1:Key 2:Key 3 = HKDF(record key, "nicknames"). Для каждого поля генерируется случайный 96-битный вектор инициализации, затем выполняется шифрование данных с помощью AES-CTR и ключа Key 1. После этого по алгоритму HMAC-SHA256 с использованием ключа Key 2 вычисляется код аутентификации сообщения (MAC), включая имя поля, вектор инициализации поля и зашифрованный текст поля. Наконец, выполняется объединение набора значений MAC отдельных полей, и для них вычисляется значение MAC по алгоритму HMAC-SHA256 с использованием ключа Key 3. 256-битное значение MAC хранится вместе с зашифрованными данными. Первые 128 бит значения MAC используются в качестве идентификатора записи.

Затем эта зашифрованная запись сохраняется в открытой базе данных CloudKit под идентификатором записи. Эта запись никогда не подвергается изменениям. Когда пользователь решает изменить свои имя и фотографию, каждый раз создается новая зашифрованная запись. Когда пользователь 1 решает поделиться своими именем и фотографией с пользователем 2, он отправляет ключ записи вместе с идентификатором записи внутри своей полезной нагрузки iMessage, которая [зашифрована](#).

Когда устройство пользователя 2 получает эту полезную нагрузку iMessage, оно замечает, что сообщение содержит идентификатор записи и ключ имени и фотографии. Затем устройство пользователя 2 обращается к открытой базе данных CloudKit, чтобы получить зашифрованное имя и фотографию по идентификатору записи, и отправляет их в iMessage.

После извлечения сообщения устройство пользователя 2 расшифровывает полезную нагрузку и проверяет подпись, используя идентификатор записи. В случае успешной проверки пользователь 2 видит имя и фотографию и может добавить их в свои контакты или использовать в Сообщениях.

Безопасность Apple Messages for Business

Apple Messages for Business — это служба обмена сообщениями, с помощью которой пользователи могут общаться с компаниями через приложение «Сообщения». В Apple Messages for Business разговор всегда под контролем пользователя. Пользователь может удалить разговор и заблокировать компанию, чтобы в дальнейшем не получать от нее сообщений. В целях обеспечения конфиденциальности компания не получает номер телефона, адрес электронной почты или информацию учетной записи iCloud пользователя. Вместо этого службой идентификации Apple (IDS) генерируется, а затем предоставляется компании особый уникальный идентификатор, который называется *непрозрачным идентификатором*. Он является уникальным для взаимодействия между Apple ID пользователя и идентификатором компании. Для каждой компании, с которой пользователь общается в Apple Messages for Business, генерируется отдельный непрозрачный идентификатор пользователя. Пользователь сам решает, когда делиться с компанией личной информацией, а Apple Messages for Business никогда не хранит историю разговора.

Apple Messages for Business поддерживает управляемые Apple ID из Apple Business Manager и определяет, включены ли они для iMessage и FaceTime в Apple School Manager.

Каждое сообщение, отправленное компании, защищается шифрованием и передается с устройства пользователя на серверы обмена сообщениями Apple как сообщение iMessage с применением тех же функций безопасности. Серверы обмена сообщениями Apple расшифровывают сообщения в оперативной памяти и передают их компании по зашифрованному каналу связи с использованием протокола TLS 1.2. Сообщения никогда не хранятся в незашифрованном виде во время передачи через Apple Messages for Business. Ответы компаний аналогичным образом передаются по протоколу TLS 1.2 на серверы обмена сообщениями Apple, где они затем защищаются шифрованием с помощью уникальных открытых ключей устройств пользователей.

Если устройство пользователя в сети, сообщение доставляется мгновенно и не кэшируется на серверах обмена сообщениями Apple. Если устройство пользователя отсутствует в сети, зашифрованное сообщение помещается в кэш на срок до 30 дней, чтобы пользователь получил его, когда устройство снова подключится к сети. Как только устройство снова подключится к сети, сообщение доставляется и удаляется из кэша. По прошествии 30 дней недоставленное кэшированное сообщение удаляется без возможности восстановления.

Безопасность FaceTime

FaceTime — это служба Apple для совершения видео- и аудиозвонков. Подобно iMessage для установления первоначального соединения с зарегистрированными устройствами пользователя вызовы FaceTime используют службу Apple Push Notification (APNs). Содержимое вызовов FaceTime защищено с помощью сквозного шифрования, поэтому никто, кроме отправителя и получателя, не может получить к ним доступ. Apple не может расшифровать данные.

Изначальное соединение FaceTime устанавливается через серверную инфраструктуру Apple, которая ретранслирует пакеты данных между зарегистрированными устройствами пользователей. Передавая уведомления APNs и сообщения Утилиты прохождения сессий для NAT (STUN) через ретранслированное соединение, устройства проверяют свои сертификаты подлинности и выбирают общий ключ для каждого сеанса. Этот общий ключ используется для генерации ключей сеансов для медиаканалов, передаваемых в потоковом режиме через Secure Real-time Transport Protocol (SRTP). Пакеты SRTP шифруются с использованием алгоритма AES256 в режиме счетчика и аутентифицируются с помощью HMAC-SHA1. После первоначального соединения и настройки параметров безопасности FaceTime использует STUN и Internet Connectivity Establishment (ICE) для установления прямого соединения между устройствами, если это возможно.

Функция групповых вызовов по FaceTime обеспечивает поддержку одновременно до 33 участников. Как и при обычном вызове FaceTime, соединения между устройствами приглашенных участников группового вызова защищены с помощью сквозного шифрования. Несмотря на то, что для групповых вызовов FaceTime в значительной степени используются те же инженерные решения и разработки, что и для обычных вызовов, в групповых вызовах применяется механизм задания ключа, помимо средств проверки подлинности, обеспечиваемых службой идентификации Apple (IDS). Этот протокол обеспечивает прямую секретность: даже при взломе устройства пользователя данные прошлых вызовов останутся защищены. Ключи сеансов защищаются с помощью алгоритма AES-SIV и распределяются между участниками вызова с использованием построения ECIES с динамическими ключами ECDH P-256.

Когда в текущий групповой вызов по FaceTime добавляется новый номер телефона или адрес электронной почты, активные устройства назначают новые ключи сеансов для медиаканалов. Ранее использовавшиеся ключи никогда не предоставляются вновь добавленным устройствам.

Локатор

Безопасность Локатора

В приложении «Локатор» для устройств Apple используются передовые технологии криптографии с открытым ключом.

Обзор

Приложение Локатор для iOS, iPadOS и macOS объединяет в себе возможности приложений «Найти iPhone» и «Найти друзей». Локатор помогает найти пропавший Mac, даже если в момент поиска компьютер не подключен к интернету. Устройство, подключенное к интернету, может просто сообщить о своем местонахождении через iCloud. Локатор работает без подключения к интернету, отправляя сигналы Bluetooth с пропавшего устройства. Эти сигналы могут распознать устройства Apple, которые находятся поблизости. Затем эти устройства поблизости передают данные о местоположении пропавшего устройства в iCloud, благодаря чему владелец пропавшего устройства может найти его с помощью приложения Локатор. В течение всего процесса поиска все личные данные всех участников поиска не раскрываются и остаются защищены. Локатор также может определить местоположение компьютера Mac, который отключен от сети и находится в режиме сна.

Используя Bluetooth и сотни миллионов активных устройств iOS, iPadOS и macOS по всему миру, пользователь может найти пропавшее устройство, даже если оно не может подключиться к сети Wi-Fi или сотовой сети. В поиске может участвовать любое устройство iOS, iPadOS и macOS, на котором в настройках Локатора включен офлайн-поиск. Это означает, что устройство может обнаружить присутствие другого пропавшего устройства, которое отключено от сети, с помощью Bluetooth, а затем сообщить владельцу пропавшего устройства его примерное местонахождение, используя свое сетевое соединение. Кроме того, если на устройстве включен офлайн-поиск, оно может быть аналогичным образом найдено другими участниками. Весь этот процесс защищен сквозным шифрованием, анонимизирован и разработан таким образом, чтобы эффективно расходовать заряд аккумулятора и трафик данных. При минимальном влиянии на расход заряда и трафик сотовых данных обеспечивается большая конфиденциальность пользователя.

Примечание. Локатор доступен не во всех странах и регионах.

Сквозное шифрование

В Локаторе используются современные технологии криптографии с открытым ключом. Когда пользователь включает офлайн-поиск в настройках Локатора, непосредственно на устройстве генерируется пара личных ключей шифрования на основе эллиптических кривых (EC) P-224, обозначенные как $\{d, P\}$, где d — это личный ключ, а P — это открытый ключ. Кроме того, 256-битный секретный ключ SK_0 и счетчик i инициализируются нулями. Эта пара личных ключей и секретный ключ никогда не передаются в Apple и синхронизируются только между другими устройствами пользователя с использованием сквозного шифрования и Связки ключей iCloud. Секретный ключ и счетчик используются для получения текущего симметричного ключа SK_i при помощи следующей рекурсивной схемы: $SK_i = \text{KDF}(SK_{i-1}, \text{«update»})$.

На основе ключа SK_i вычисляется два больших целых числа u_i и v_i по формуле $(u_i, v_i) = \text{KDF}(SK_i, \text{diversify})$. Затем к личному ключу P-224, обозначенному как d_i , и соответствующему открытому ключу, обозначенному как P_i , применяется аффинное преобразование, включающее два целых числа, для вычисления краткосрочной пары ключей: производного личного ключа d_i , где $d_i = u_i * d + v_i$ (модуль коэффициента кривой P-224) и соответствующего открытого ключа P_i с подтверждением $P_i = u_i * P + v_i * G$.

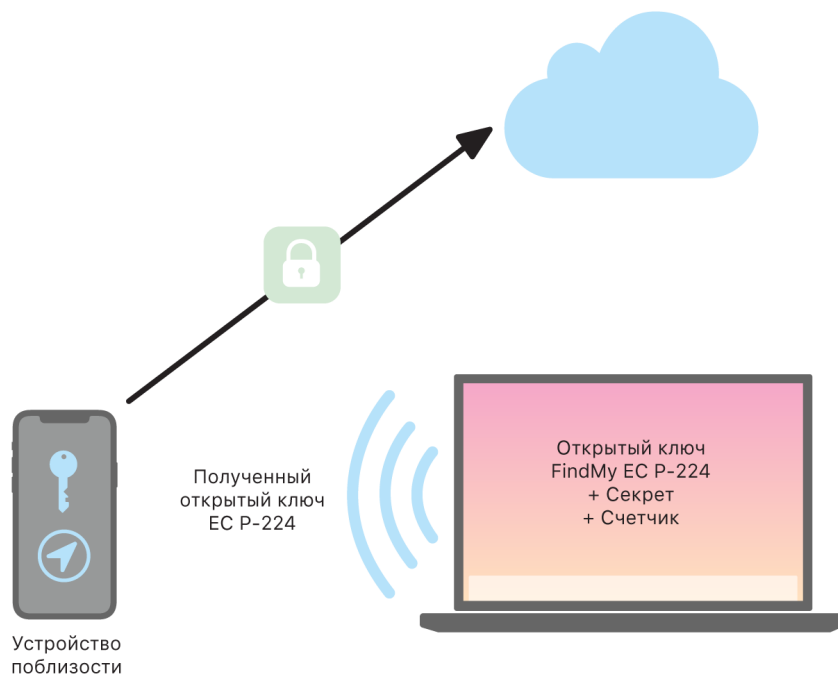
Если устройство пропало и не может подключиться к сети Wi-Fi или сотовой сети — например, пользователь оставил MacBook Pro на скамейке в парке, — устройство начинает периодически транслировать производный открытый ключ P_i в течение ограниченного времени через полезную нагрузку Bluetooth. Благодаря использованию P-224 представление открытого ключа помещается в полезную нагрузку одного пакета Bluetooth. Окружающие устройства могут помочь в обнаружении отключенного от сети устройства, зашифровав свое местоположение с помощью открытого ключа. Примерно каждые 15 минут открытый ключ заменяется новым ключом с использованием увеличенного значения счетчика и описанного выше процесса, чтобы пользователя было невозможно отследить по постоянному идентификатору. Механизм получения производных ключей направлен на то, чтобы предотвратить связывание различных открытых ключей P_i с одним и тем же устройством.

Сохранение анонимности пользователей и устройств

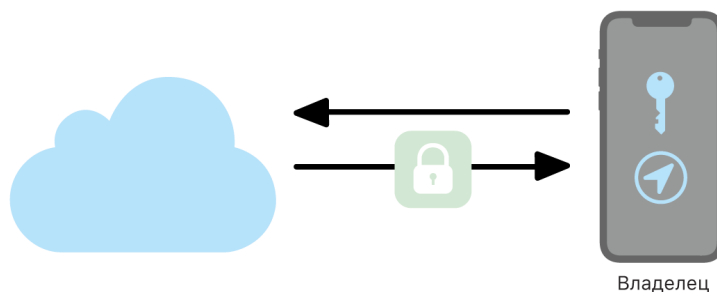
Помимо полного шифрования информации о местоположении и других данных, приложение скрывает личность участников от других участников и от Apple. В содержимом и заголовках пакетов, которые пересылаются в Apple участвующими в поиске устройствами, не содержится никакой информации для аутентификации. В результате Apple не знает, кто участвует в поиске или чье устройство было найдено. Кроме того, Apple не сохраняет информацию, которая позволила бы раскрыть личность участников поиска или установить взаимосвязь между участниками поиска и владельцем. Владелец устройства получает зашифрованную информацию о местоположении, которая расшифровывается и отображается в приложении Локатор без указания того, кто нашел устройство.

Использование Локатора для поиска пропавших устройств Apple

Любые устройства Apple, которые находятся в зоне действия Bluetooth и на которых включен офлайн-поиск, могут распознать сигнал от другого устройства Apple, на котором включен Локатор, и прочесть текущий ключ широковещательной передачи P_i . Используя схему ECIES и открытый ключ P_i из широковещательной передачи, участвующие в поиске устройства шифруют информацию о своем текущем местонахождении и передают ее в Apple. Зашифрованное местоположение связывается с индексом на сервере, который вычисляется как хэш SHA256 открытого ключа $P-224 P_i$, полученного из полезной нагрузки Bluetooth. У компании Apple нет ключа дешифрования и, следовательно, она не может узнать местонахождение устройства, участвующего в поиске. Владелец пропавшего устройства может восстановить индекс и расшифровать зашифрованное местоположение.



При попытке найти пропавшее устройство приблизительно оценивается ожидаемый диапазон значений счетчика для требуемого периода поиска. Зная исходный личный ключ P -224 d и секретные значения SK_i в диапазоне значений счетчика за период поиска, владелец может восстановить набор значений $\{d_i, \text{SHA256}(P_i)\}$ за весь период поиска. Затем устройство владельца, используемое для поиска пропавшего устройства, запрашивает у сервера информацию по набору значений индексов $\text{SHA256}(P_i)$ и загружает зашифрованные местоположения с сервера. После этого приложение Локатор выполняет локальное дешифрование зашифрованных местоположений с помощью соответствующих личных ключей d_i и показывает приблизительное местоположение пропавшего устройства в приложении. Приложение владельца объединяет информацию о местоположении, полученную от нескольких участвующих в поиске устройств, для более точного определения местоположения.



Поиск устройств, которые находятся офлайн

Если на устройстве пользователя была включена функция Найти iPhone, то при обновлении устройства до iOS 13 и новее, iPadOS 13.1 и новее или macOS 10.15 и новее на нем по умолчанию включается офлайн-поиск. Эта мера направлена на то, чтобы повысить шансы каждого пользователя найти свое устройство, если оно пропадет. Однако если пользователь решит не участвовать в программе, он в любое время может отключить офлайн-поиск в настройках Локатора на своем устройстве. Если офлайн-поиск отключен, устройство больше не участвует в поиске других устройств, а также не может быть обнаружено другими устройствами, участвующими в офлайн-поиске. Однако пользователь по-прежнему может найти устройство, если к устройству можно подключиться через сеть Wi-Fi или сотовую сеть.

Когда удастся определить местонахождение пропавшего отключенного устройства, пользователь получает уведомление и электронное письмо с информацией о том, что его устройство было найдено. Чтобы увидеть, где находится пропавшее устройство, пользователь должен открыть приложение Локатор и перейти на вкладку «Устройства». До обнаружения устройства оно отображается на пустой карте, а после обнаружения Локатор показывает его местонахождение на карте вместе с приблизительным адресом и информацией о том, как давно оно было обнаружено. Если поступает новая информация о местоположении, текущее местоположение и отметка времени автоматически обновляются. Пользователи не могут воспроизводить звук на выключенном устройстве или выполнить его удаленное стирание, однако они могут сопоставить информацию о местоположении со своим маршрутом или предпринять другие действия, чтобы вернуть свое устройство.

Непрерывность

Безопасность функции непрерывности

Функция «Непрерывность» задействует возможности таких технологий, как iCloud, Bluetooth и Wi-Fi, чтобы пользователи могли начинать действия на одном устройстве, а заканчивать их на другом. Например, таким образом можно совершать и принимать телефонные вызовы, отправлять и получать текстовые сообщения и совместно использовать подключение к интернету по сотовой сети.

Безопасность Handoff

Apple обеспечивает безопасную передачу данных как с одного устройства на другое, так и между нативным приложением и веб-сайтом, даже если объем передаваемых данных велик.

Безопасность работы Handoff

Если устройства iOS, iPadOS и macOS находятся близко друг к другу, то пользователь может автоматически передавать незавершенные задачи с одного устройства на другое с помощью Handoff. Handoff позволяет пользователю переключаться между устройствами и мгновенно продолжать свою работу.

Если пользователь входит в iCloud на втором устройстве с поддержкой Handoff, два устройства создают пару через отдельное соединение Bluetooth Low Energy (BLE) 4.2 при помощи службы APNs. Отдельные сообщения шифруются во многом так же, как сообщения в iMessage. После объединения в пару каждое из устройств генерирует симметричный 256-битный ключ AES, который сохраняется в связке ключей устройства. Этот ключ может использоваться для шифрования и аутентификации оповещений BLE, которые сообщают о текущем действии устройства другим объединенным в пару устройствам iCloud, используя AES256 в режиме GCM с защитой от повторной передачи перехваченных сообщений.

Когда устройство в первый раз получает оповещение от нового ключа, оно устанавливает соединение стандарта BLE с вызывающим устройством и обменивается с ним ключами шифрования оповещений. Для защиты этого соединения используется шифрование BLE 4.2, а также шифрование отдельных сообщений, которое похоже на шифрование сообщений iMessage. В некоторых случаях эти сообщения передаются не через BLE, а через APNs. Для защиты и передачи информации о выполняемых пользователем действиях используются такие же методы, как в iMessage.

Переключение между нативными приложениями и веб-сайтами с помощью Handoff

Благодаря Handoff нативные приложения iOS, iPadOS и macOS могут возобновлять активность пользователя на веб-странице в доменах, которые на законных основаниях контролируются разработчиком приложения. Кроме того, нативные приложения могут возобновлять действия пользователя в веб-браузере.

Приложение должно продемонстрировать наличие законного контроля над веб-доменами, которые оно хочет использовать для возобновления. Это способствует тому, чтобы нативные приложения не могли запросить возобновление веб-сайтов, которые не контролируются разработчиком. Для доказательства контроля над доменом веб-сайта используется такой же механизм, как для общего доступа к учетным данным веб-сайтов. Подробнее см. [Доступ приложений к сохраненным паролям](#). Прежде чем приложению будет разрешено принять действия пользователя через Handoff, система должна подтвердить, что приложение контролирует доменное имя.

Источником передачи веб-страницы может быть любой браузер с интерфейсами Handoff API. Когда пользователь просматривает веб-страницу, система передает ее доменное имя с помощью зашифрованных байтов оповещения Handoff. Расшифровать байты оповещения могут только другие устройства пользователя.

Система принимающего устройства распознает, что установленное нативное приложение принимает информацию Handoff от переданного доменного имени, и отображает значок этой нативного приложения в меню Handoff. При запуске нативное приложение получает полный URL-адрес и заголовок веб-страницы. Никакая другая информация из браузера не передается в нативное приложение.

При передаче информации в обратном направлении нативное приложение может указать резервный URL-адрес на тот случай, если на принимающем устройстве не установлено то же нативное приложение. В этом случае вместо приложения в меню Handoff отображается браузер по умолчанию (если этот браузер поддерживает интерфейсы Handoff API). При вызове Handoff отображается этот браузер и в него передается резервный URL-адрес, предоставленный исходным приложением. Резервный URL-адрес не обязательно должен принадлежать доменным именам, которые контролируются разработчиком нативного приложения.

Передача больших объемов данных с помощью Handoff

Помимо основной функции Handoff некоторые приложения могут использовать API, которые поддерживают отправку больших объемов данных через технологию прямого соединения Wi-Fi, разработанную компанией Apple (во многом похожую на AirDrop). Например, приложение «Почта» использует эти интерфейсы API для передачи черновиков писем, которые могут включать большие вложения.

Когда приложение использует эти интерфейсы API, между двумя устройствами начинается обмен данными, как при использовании Handoff. Однако после получения первоначальной полезной нагрузки по Bluetooth Low Energy (BLE) принимающее устройство устанавливает новое подключение по сети Wi-Fi. Это подключение шифруется (с помощью TLS) и получает объект доверия из удостоверения, отправленного через Связку ключей iCloud. Удостоверение в сертификатах сверяется с удостоверением пользователя. Вся дальнейшая информация полезной нагрузки пересылается по этому зашифрованному подключению, пока передача не будет завершена.

Универсальный буфер обмена

Универсальный буфер обмена задействует функцию Handoff для безопасной передачи содержимого буфера обмена между различными устройствами пользователя, позволяя скопировать контент на одном устройстве и вставить его на другом. Для защиты контента используются те же методы, как и для других данных Handoff. По умолчанию, если разработчик приложения не выключил общий доступ, контент передается в универсальный буфер обмена.

Приложения имеют доступ к данным в буфере обмена независимо от того, вставил ли пользователь эти данные в приложении. При наличии универсального буфера обмена такой доступ получают также приложения, запущенные на других устройствах пользователя (в соответствии с регистрацией iCloud).

Безопасность ретрансляции сотовых вызовов через iPhone

Если Mac, iPad, iPod touch или HomePod пользователя подключены к той же сети Wi-Fi, что и iPhone, они могут совершать и принимать телефонные вызовы через сотовое подключение iPhone. Для этого необходимо, чтобы на устройствах был выполнен вход в iCloud и FaceTime под одним и тем же Apple ID.

При поступлении входящего вызова все настроенные устройства получают уведомление через службу Apple Push Notification (APNs), при этом для каждого уведомления используется такое же сквозное шифрование, как в iMessage. На экранах устройств, подключенных к одной сети, появляется уведомление о входящем вызове. Когда пользователь отвечает на вызов, аудиопоток начинает транслироваться с iPhone через безопасное прямое соединение между двумя устройствами.

Если ответить на вызов на одном устройстве, выдача звукового сигнала на находящихся поблизости связанных с iCloud устройствах прекращается после передачи короткого оповещения через Bluetooth Low Energy (BLE). Байты оповещения шифруются тем же методом, который используется для оповещений Handoff.

Исходящие вызовы также ретранслируются на iPhone через службу APNs, а аудиопоток аналогичным образом передается через безопасное прямое соединение между устройствами. Для отключения ретрансляции телефонных вызовов пользователям необходимо отключить «Сотовые вызовы iPhone» в настройках FaceTime.

Безопасность переадресации сообщений через iPhone

Функция переадресации сообщений выполняет автоматическую пересылку SMS, полученных на iPhone, на зарегистрированные устройства iPad, iPod touch или Mac. На всех устройствах необходимо выполнить вход в iMessage с одним и тем же Apple ID. При включении переадресации сообщений регистрация выполняется автоматически на устройствах, входящих в круг доверия пользователя, если включена двухфакторная аутентификация. В ином случае необходимо подтвердить регистрацию каждого устройства, введя случайный шестизначный цифровой код, сгенерированный iPhone.

После завершения привязки устройств друг к другу iPhone начинает шифровать и переадресовывать входящие SMS на каждое из устройств, используя методы, описанные в разделе «[Обзор безопасности iMessage](#)». Ответы пересылаются обратно на iPhone аналогичным способом, после чего iPhone отправляет ответ в виде SMS, используя механизм передачи SMS оператора. Включить и выключить переадресацию сообщений можно в настройках приложения «Сообщения».

Безопасность Instant Hotspot

Instant Hotspot служит для подключения других устройств Apple с помощью режима модема в iOS или iPadOS. Устройства iOS и iPadOS, поддерживающие Instant Hotspot, используют Bluetooth Low Energy (BLE) для поиска других устройств, на которых выполнен вход в ту же личную учетную запись iCloud или учетную запись, используемую в рамках Семейного доступа (в iOS 13 и iPadOS). По окончании поиска BLE также используется для передачи данных между устройствами. Совместимые компьютеры Mac с операционной системой OS X 10.10 или новее используют эту же технологию для обнаружения устройств iOS и iPadOS с поддержкой Instant Hotspot и установления соединения с этими устройствами.

После того как пользователь вводит настройки Wi-Fi на устройстве, устройство передает оповещение BLE, содержащее идентификатор, который был подписан всеми устройствами, использующими одну и ту же учетную запись iCloud. Идентификатор генерируется из идентификатора связи с адресатом (DSID), который привязан к учетной записи iCloud и периодически меняется. Если в непосредственной близости от устройства оказываются другие устройства, использующие ту же учетную запись iCloud и поддерживающие режим модема, они распознают сигнал и отвечают на него, сигнализируя о том, что можно использовать Instant Hotspot.

Если пользователь, у которого нет Семейного доступа, выбирает iPhone или iPad для режима модема, на это устройство отправляется запрос о включении функции «Режим модема». Запрос передается по зашифрованному каналу BLE, а сам запрос зашифровывается так же, как в iMessage. Устройство отвечает на запрос по тому же каналу BLE, используя тот же способ шифрования отдельных сообщений, и передает информацию о подключении к модему.

Для пользователей, у которых есть Семейный доступ, информация о безопасном подключении с помощью функции «Режим модема» надежно передается посредством механизма, схожего с тем, который используют устройства HomeKit для синхронизации данных. Точнее, соединение, через которое между пользователями передается информация о точке доступа, защищено с помощью временного ключа ECDH (Curve25519), который аутентифицируется посредством соответствующих назначенных устройству открытых ключей Ed25519 пользователей. Используются те открытые ключи, которые ранее синхронизировались пользователями Семейного доступа посредством службы идентификации Apple, когда был настроен Семейный доступ.

Безопасность сети

Обзор безопасности сети

Помимо встроенных средств, используемых Apple для защиты данных на устройствах Apple, организации могут принять целый ряд мер для защиты информации при передаче между устройствами. Все эти средства и меры относятся к безопасности сети.

Поскольку пользователям необходимо иметь доступ к корпоративным сетям, в какой бы стране они ни оказались, необходимо принять меры, направленные на то, чтобы к корпоративной сети подключались только авторизованные пользователи и чтобы их данные были защищены во время передачи. Для обеспечения необходимой защиты в iOS, iPadOS и macOS встроены проверенные технологии и новейшие стандарты подключения к сетям Wi-Fi и сотовым сетям передачи данных. Поэтому для аутентификации, авторизации и шифрования при передаче данных наши операционные системы используют стандартные сетевые протоколы и предоставляют разработчикам доступ к ним.

Безопасность TLS

iOS, iPadOS и macOS поддерживают протокол Transport Layer Security (TLS 1.0, TLS 1.1, TLS 1.2 и TLS 1.3) и Datagram Transport Layer Security (DTLS). Протокол TLS поддерживает AES-128 и AES-256, предпочитая наборы шифров с прямой секретностью. Интернет-приложения, например Safari, Календарь и Почта, автоматически используют этот протокол для установления зашифрованного канала связи между устройством и сетевыми службами. Высокоуровневые API (такие как CFNetwork) упрощают внедрение TLS в приложениях сторонних разработчиков, а низкоуровневые API (такие как Network.framework) предоставляют детальный контроль. CFNetwork не разрешает использовать SSL 3, а приложениям, использующим WebKit (например, Safari), запрещается устанавливать подключения с использованием SSL 3.

В iOS 11 или новее и macOS 10.13 или новее сертификаты SHA-1 нельзя использовать для TLS-соединений, если им не доверяет пользователь. Также не разрешены сертификаты с ключами RSA короче 2048 бит. Набор симметричных шифров RC4 в iOS 10 и macOS 10.12 считается устаревшим. По умолчанию клиенты и серверы TLS, реализованные с использованием API SecureTransport, не имеют наборов шифров RC4 (их поддержка отключена) и не могут установить соединение, если единственным доступным набором шифров является RC4. Для повышения безопасности необходимо обновить службы и приложения, требующие использования RC4, чтобы в них использовались безопасные наборы шифров. В iOS 12.1 сертификаты, выпущенные после 15 октября 2018 г. от имеющего доверие в системе корневого сертификата, для установления TLS-соединений должны быть внесены в доверенный журнал прозрачности сертификатов. В iOS 12.2 стандарт TLS 1.3 по умолчанию включен для Network.framework и API NSURLSession. Клиенты TLS, использующие API SecureTransport, не могут использовать TLS 1.3.

App Transport Security

Протокол App Transport Security предоставляет используемые по умолчанию требования к подключению, чтобы приложения работали с защищенными подключениями при использовании API NSURLConnection, CFURL и NSURLSession. По умолчанию протокол App Transport Security ограничивает возможность выбора шифра только теми наборами, которые обеспечивают прямую секретность, в частности следующие:

- ECDHE_ECDSA_AES и ECDHE_RSA_AES в режиме Galois/Counter Mode (GCM)
- Режим поблочной передачи зашифрованного текста (CBC)

Приложения могут отключить требование обязательной прямой секретности на уровне домена; в этом случае к набору доступных шифров добавляется RSA_AES.

Серверы должны поддерживать TLS 1.2 и прямую секретность, а сертификаты должны быть действительны и подписаны с использованием шифрования SHA256 (или более надежного) с ключом уровня не ниже, чем 2048-битный ключ RSA или 256-битный ключ на основе эллиптических кривых.

Сетевые подключения, не отвечающие этим требованиям, будут прерваны, если только в приложении не предусмотрен обход протокола App Transport Security. Использование недействительных сертификатов всегда приводит к постоянному отказу и отсутствию подключения. Протокол App Transport Security автоматически применяется для приложений, скомпилированных для iOS 9 или новее и macOS 10.11 или новее.

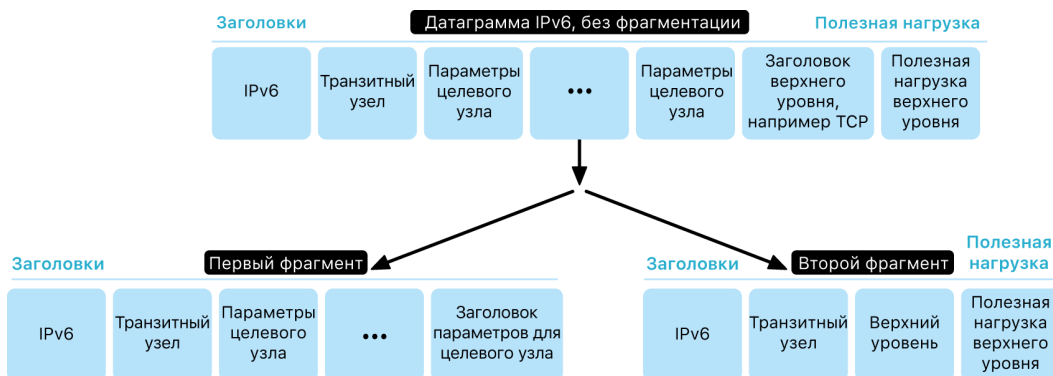
Проверка действительности сертификата

Оценка доверенного статуса сертификата TLS выполняется в соответствии с отраслевыми стандартами, установленными в [RFC 5280](#), и новыми стандартами, такими как [RFC 6962](#) (прозрачность сертификатов). В iOS 11 или новее и macOS 10.13 или новее устройства Apple периодически получают актуальный список отозванных и ограниченных сертификатов. Список обобщает списки отзыва сертификатов (CRL), публикуемые всеми встроенными корневыми центрами сертификации, которым доверяет Apple, а также их подчиненными центрами сертификации. Список также может включать в себя и другие ограничения по усмотрению Apple. Эта информация используется каждый раз, когда для установления безопасного соединения используется функция сетевого API. Если было отозвано слишком много сертификатов центра сертификации, чтобы перечислять их по отдельности, вместо сертификата для оценки доверия может использоваться ответ по протоколу состояния сетевого сертификата (OCSP). Если ответ не получен, тест на оценку доверия не будет пройден.

Безопасность протокола IPv6

Все операционные системы Apple поддерживают протокол IPv6, реализуя ряд механизмов для защиты конфиденциальности пользователей и обеспечения стабильной работы сетевого стека. При использовании автоматической настройки адресов без сохранения состояния (SLAAC) IPv6-адреса всех интерфейсов генерируются таким способом, который помогает препятствовать отслеживанию устройств в сетях и обеспечивать удобство для пользователей путем обеспечения стабильности адресов при отсутствии изменений в сети. В основе алгоритма генерирования адресов лежат криптографически сгенерированные адреса, как указано в требованиях стандарта [RFC 3972](#), дополненных модификаторами для каждого отдельного интерфейса, что гарантирует создание разных адресов для разных интерфейсов в одной и той же сети. Кроме того, создаются временные адреса с предпочтительным сроком действия 24 часа, и они по умолчанию используются для любых новых подключений. В соответствии с функцией частных адресов Wi-Fi, реализованной в iOS 14, iPadOS 14 и watchOS 7, для каждой сети Wi-Fi, к которой подключается устройство, создается уникальный локальный адрес канала. SSID сети используется в качестве дополнительного элемента для создания адреса, аналогично параметру Network_ID в соответствии со стандартом [RFC 7217](#). Такой подход применяется в iOS 14, iPadOS 14 и watchOS 7.

Для защиты от атак с использованием заголовков расширений и фрагментации IPv6 на устройствах Apple реализованы средства защиты в соответствии с требованиями стандартов [RFC 6980](#), [RFC 7112](#) и [RFC 8021](#). Наряду с другими мерами, это позволяет предотвратить атаки, в которых заголовок верхнего уровня содержится только во втором фрагменте (как показано ниже), что, в свою очередь, может привести к нарушениям в работе средств безопасности, таких как фильтры пакетов без сохранения состояния.



Кроме того, чтобы помочь обеспечить надежную работу стека IPv6 операционных систем Apple, устройства Apple накладывают различные ограничения в отношении структур данных IPv6, таких как количество префиксов на интерфейс.

Безопасность виртуальной частной сети (VPN)

Безопасные сетевые службы, такие как виртуальные частные сети, обычно требуют минимальной настройки и конфигурирования для работы с устройствами iOS, iPadOS и macOS.

Поддерживаемые протоколы

Эти устройства могут работать с VPN-серверами, которые поддерживают следующие протоколы и способы аутентификации:

- IKEv2/IPsec с аутентификацией по общему ключу, сертификатам RSA, сертификатам алгоритма цифровой подписи на основе эллиптической кривой (ECDSA), EAP-MSCHAPv2 или EAP-TLS;
- SSL-VPN с использованием соответствующего клиентского приложения из App Store;
- L2TP/IPsec с аутентификацией пользователя по паролю MS-CHAPv2, а также автоматической аутентификацией с помощью общего ключа (iOS, iPadOS и macOS) и RSA SecurID или CRYPTOCARD (только для macOS);
- Cisco IPsec с аутентификацией пользователя по паролю, RSA SecurID или CRYPTOCARD, а также автоматической аутентификацией с помощью общего ключа и сертификатов (только для macOS).

Поддерживаемые функции VPN

iOS, iPadOS и macOS поддерживают следующее:

- *VPN по запросу.* Для сетей, в которых аутентификация выполняется на основе сертификатов. Для указания доменов, требующих VPN-подключения, используется профиль конфигурации.
- *Раздельное подключение приложений к VPN.* Для повышения детализации установления VPN-соединений. Система управления мобильными устройствами (MDM) позволяет настроить подключение для каждого управляемого приложения и конкретных доменов в Safari. Это помогает гарантировать, что защищенные данные не выйдут за пределы корпоративной сети, а личные данные пользователя в нее не попадут.

iOS и iPadOS поддерживают следующее:

- *VPN всегда вкл.* Для устройств, управляемых через систему MDM и контролируемых с помощью Apple Configurator для Mac, Apple School Manager или Apple Business Manager. Эта функция избавляет пользователей от необходимости включать VPN для обеспечения защиты при подключении к сетям сотовой связи или Wi-Fi. С помощью этой функции организация получает полный доступ к контролю трафика устройства благодаря туннелированию всего IP-трафика обратно в организацию. По умолчанию при обмене параметрами и ключами для последующего шифрования используется IKEv2, который обеспечивает передачу трафика с шифрованием данных. Организация может контролировать и фильтровать входящий и исходящий трафик своих устройств, защитить данные в сети и ограничить доступ устройств к интернету.

Безопасность Wi-Fi

Безопасный доступ к беспроводным сетям

Все платформы Apple поддерживают стандартные протоколы аутентификации и шифрования Wi-Fi для обеспечения аутентификации и конфиденциальности при подключении к защищенным беспроводным сетям, перечисленным далее.

- Личный WPA2
- Корпоративный WPA2
- Переходный WPA2/WPA3
- Личный WPA3
- Корпоративный WPA3
- Корпоративный WPA3 со 192-битным ключом

WPA2 и WPA3 выполняют аутентификацию каждого подключения и обеспечивают 128-битное шифрование AES, чтобы способствовать конфиденциальной передаче данных по беспроводной сети. Это гарантирует высочайший уровень защиты при отправке или получении пользовательских данных по сети Wi-Fi.

Поддержка WPA3

WPA3 поддерживается в следующих устройствах Apple:

- iPhone 7 или новее;
- iPad 5-го поколения и новее;
- Apple TV 4K и новее;
- Apple Watch Series 3 и новее;
- компьютеры Mac (выпущенные в конце 2013 г. и позже, с 802.11ac и новее).

Более новые устройства поддерживают аутентификацию по протоколу «Корпоративный WPA3 со 192-битным ключом», включая 256-битное шифрование AES при подключении к совместимым точкам беспроводного доступа. Это обеспечивает еще более надежную защиту конфиденциальности при передаче трафика по беспроводной сети. Корпоративный WPA3 со 192-битным ключом поддерживается на iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max и более новых устройствах iOS и iPadOS.

Поддержка PMF

В дополнение к защите данных, передаваемых по беспроводной сети, платформы Apple распространяют средства защиты WPA2 и WPA3 на одноадресные и многоадресные кадры управления, используя для этого службу защищенных кадров управления (PMF), описанную в стандарте 802.11w. Поддержка PMF доступна в следующих устройствах Apple:

- iPhone 6 и новее
- iPad Air 2 и новее;
- Apple TV HD или новее;
- Apple Watch Series 3 и новее;
- компьютеры Mac (выпущенные в конце 2013 г. и позже, с 802.11ac и новее).

Благодаря поддержке 802.1X устройства Apple можно интегрировать в широкий набор сред, где используется аутентификация RADIUS. Поддерживаемые методы аутентификации в беспроводных сетях 802.1X включают EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0 и PEAPv1.

Средства защиты платформы

Операционные системы Apple обеспечивают защиту устройства от уязвимостей в прошивке сетевого процессора. Это означает, что сетевым контроллерам с Wi-Fi предоставляется ограниченный доступ к памяти процессора приложений.

- Когда для соединения с сетевым процессором используется USB или SDIO (безопасный цифровой ввод-вывод), сетевой процессор не может инициировать транзакции прямого доступа к памяти процессора приложений.
- Когда используется PCIe, каждый из сетевых процессоров подключен к собственной изолированной шине PCIe. Модуль управления памятью ввода-вывода (IOMMU) на каждой шине PCIe дополнительно ограничивает прямой доступ сетевого процессора, предоставляя его только к блокам памяти и ресурсам, содержащим его сетевые пакеты или управляющие структуры.

Устаревшие протоколы

Продукты Apple поддерживают следующие устаревшие протоколы аутентификации и шифрования Wi-Fi:

- открытый WEP с 40-битными и 104-битными ключами;
- WEP общего доступа с 40-битными и 104-битными ключами;
- динамический WEP;
- протокол целостности временного ключа (TKIP);
- WPA;
- переходный WPA/WPA2.

Эти протоколы больше не считаются безопасными. Их использование крайне не рекомендовано из соображений совместимости, надежности, производительности и безопасности. Они поддерживаются только для обеспечения обратной совместимости и могут быть исключены из будущих версий программного обеспечения.

Все сети Wi-Fi настоятельно рекомендуется перевести на Личный WPA3 или Корпоративный WPA3, чтобы обеспечить максимальную надежность, безопасность и совместимость подключений Wi-Fi.

Конфиденциальность Wi-Fi

Использование случайных MAC-адресов

Если устройства Apple не связаны с сетью Wi-Fi, при поиске доступных сетей Wi-Fi они используют случайный MAC-адрес. Поиск может выполняться для нахождения известной сети Wi-Fi и подключения к ней, а также для работы служб геолокации с приложениями, использующими геопозиции, например, для отправки напоминаний на основе местоположения или для исправления информации о местоположении в Картах Apple. Учтите, что сканирование Wi-Fi, выполняемое при попытке подключения к предпочитаемой сети Wi-Fi, имеет неслучайный характер. Использование случайных MAC-адресов для Wi-Fi поддерживается на iPhone 5 и новее.

Кроме того, если устройство не связано с сетью Wi-Fi или его процессор находится в режиме сна, платформа Apple также выполняет расширенный поиск предпочитаемой сети для выгрузки данных (ePNO), используя случайный MAC-адрес. Поиск ePNO выполняется, когда устройство использует службы геолокации для приложений, использующих геозоны, например, для выдачи напоминаний при приближении устройства к определенному местоположению.

Поскольку MAC-адрес устройства изменяется, когда устройство отключается от сети Wi-Fi, пассивные наблюдатели за трафиком Wi-Fi не могут использовать его для постоянного слежения за устройством, даже если устройство подключено к сотовой сети. Компания Apple сообщила производителям оборудования Wi-Fi, что для сканирования Wi-Fi операционные системы iOS и iPadOS используют случайный MAC-адрес и что ни Apple, ни производители не могут предсказать эти случайные MAC-адреса.

В iOS 14 или новее, iPadOS 14 или новее и watchOS 7 или новее, когда iPhone, iPad, iPod touch или часы Apple Watch, подключаются к сети Wi-Fi, они идентифицируют себя с помощью уникального (случайного) MAC-адреса в сети. Эта функция может быть отключена либо пользователем, либо с помощью нового параметра в полезной нагрузке Wi-Fi. При определенных обстоятельствах устройство вернется к фактическому MAC-адресу.

Подробнее см. в статье Службы поддержки Apple [Использование частных адресов Wi-Fi на iPhone, iPad, iPod touch и Apple Watch](#).

Использование случайных порядковых номеров кадров Wi-Fi

В состав кадров Wi-Fi входит порядковый номер, используемый низкоуровневым протоколом 802.11 для обеспечения эффективной и надежной связи через Wi-Fi. Поскольку эти порядковые номера увеличиваются с каждым переданным кадром, их можно использовать для сопоставления информации, передаваемой во время сканирования Wi-Fi, с другими кадрами, передаваемыми тем же устройством.

Чтобы избежать этого, устройства Apple используют новый случайный порядковый номер при каждой смене MAC-адреса на новый случайный адрес. Сюда входит использование нового случайного порядкового номера для каждого нового запроса сканирования, который инициируется, пока устройство не связано с сетью Wi-Fi. Использование случайных порядковых номеров поддерживается на следующих устройствах:

- iPhone 7 или новее;
- iPad 5-го поколения и новее;
- Apple TV 4K и новее;
- Apple Watch Series 3 и новее;
- iMac Pro (Retina 5K, 27 дюймов, 2017 г.) и новее;
- MacBook Pro (13 дюймов, 2018 г.) или новее;
- MacBook Pro (15 дюймов, 2018 г.) и новее;
- MacBook Air (Retina, 13 дюймов, 2018 г.) и новее;
- Mac mini (2018 г.) и новее;
- iMac (Retina 4K, 21,5 дюймов, 2019 г.) и новее;
- iMac (Retina 5K, 27 дюймов, 2019 г.) или новее;
- Mac Pro (2019 г.) и новее.

Подключения Wi-Fi

Apple генерирует случайные MAC-адреса для создания прямых соединений между устройствами по Wi-Fi, чтобы использовать их для AirDrop и AirPlay. Случайные адреса также используются для режима модема в iOS и iPadOS (с SIM-картой) и общего интернета в macOS.

Новые случайные адреса генерируются при каждом запуске этих сетевых интерфейсов; для каждого интерфейса по мере необходимости генерируются свои уникальные адреса.

Скрытые сети

Для идентификации сети Wi-Fi используется ее сетевое имя, известное как *идентификатор набора служб (SSID)*. Для некоторых сетей Wi-Fi настроено скрытие SSID, в результате чего на устройстве не отображается имя сети. Такие сети называются *скрытыми*. Устройства iPhone 6s и новее автоматически распознают, скрыта ли сеть. Если сеть скрыта, устройство iOS или iPadOS отправляет пробный запрос и идентификатор SSID. Если не указать имя сети, запрос отправлен не будет. Эта мера направлена на то, чтобы устройство не сообщало имена скрытых ранее сетей, к которым подключался пользователь, что обеспечивает дополнительную конфиденциальность.

Безопасность Bluetooth

В устройствах Apple используется две версии протоколов Bluetooth: Bluetooth Classic и Bluetooth Low Energy (BLE). Модель безопасности Bluetooth обеих версий включает следующие отдельные функции безопасности:

- *Создание пары.* Процесс создания одного или нескольких общих ключей.
- *Связывание.* Сохранение ключей, сгенерированных при создании пары, для использования во время последующих подключений, чтобы сформировать пару доверенных устройств.
- *Аутентификация.* Контроль того, что у обоих устройств имеются одинаковые ключи.
- *Шифрование.* Конфиденциальность сообщений.
- *Целостность сообщений.* Защита от подделки сообщений.
- *Безопасное простое создание пары:* Защита от пассивного прослушивания и защита от атак типа «человек посередине».

В Bluetooth версии 4.1 на уровне передачи Bluetooth Classic BR/EDR добавлена функция безопасных соединений.

В следующей таблице приведены функции безопасности для каждого типа Bluetooth.

Поддержка	Bluetooth Classic	Bluetooth Low Energy
Создание пары	Эллиптическая кривая P-256	Алгоритмы, одобренные FIPS (AES-CMAC и эллиптическая кривая P-256)
Связывание	Информация о создании пары, хранящаяся в безопасном месте на устройствах iOS, iPadOS, macOS, tvOS и watchOS	Информация о создании пары, хранящаяся в безопасном месте на устройствах iOS, iPadOS, macOS, tvOS и watchOS
Аутентификация	Алгоритмы, одобренные FIPS (HMAC-SHA256 и AES-CTR)	Алгоритмы, одобренные FIPS
Шифрование	Криптографические операции алгоритма AES-CCM, выполняемые в контроллере	Криптографические операции алгоритма AES-CCM, выполняемые в контроллере
Целостность сообщений	Алгоритм AES-CCM, используемый для обеспечения целостности сообщений	Алгоритм AES-CCM, используемый для обеспечения целостности сообщений
Безопасное простое создание пары: защита от пассивного прослушивания	Протокол обмена Диффи — Хеллмана на эллиптических кривых (ECDHE)	Протокол обмена Диффи — Хеллмана на эллиптических кривых (ECDHE)
Безопасное простое создание пары: защита от атак типа «человек посередине» (MITM)	Два числовых метода с участием пользователя: числовое сравнение или ввод пароля	Два числовых метода с участием пользователя: числовое сравнение или ввод пароля Для создания пары требуется ответ пользователя, включая все режимы создания пары без человека посередине

Поддержка	Bluetooth Classic	Bluetooth Low Energy
Bluetooth 4.1 и новее	iMac, выпущенный в конце 2015 г. и позже MacBook Pro, выпущенный в начале 2015 г. и позже	iOS 9 и новее iPadOS 13.1 и новее macOS 10.12 и новее tvOS 9 и новее watchOS 2.0 и новее
Bluetooth 4.2 и новее	iPhone 6 и новее	iOS 9 и новее iPadOS 13.1 и новее macOS 10.12 и новее tvOS 9 и новее watchOS 2.0 и новее

Конфиденциальность Bluetooth Low Energy

Для защиты конфиденциальности пользователей в состав BLE включены следующие две функции: использование случайных адресов и получение производных ключей для нескольких видов связи.

Использование случайных адресов снижает вероятность отслеживания устройства BLE в течение определенного периода времени благодаря частому изменению адреса устройства Bluetooth. Чтобы устройство, использующее эту функцию защиты конфиденциальности, могло повторно подключиться к обнаруженным ранее устройствам, необходимо, чтобы другие устройства могли получить адрес устройства, называемый *частным адресом*. Для генерации частного адреса используется ключ расшифровки, которым устройства обменялись при создании пары.

iOS 13 или новее и iPadOS 13.1 или новее могут *получать производные ключи каналов для нескольких видов связи*. Например, ключ канала, созданный для BLE, можно использовать для получения производного ключа канала Bluetooth Classic. Кроме того, Apple добавила Bluetooth Classic к поддержке BLE для устройств, которые поддерживают функцию безопасных соединений, представленную в базовой спецификации Bluetooth версии 4.1 (см. [базовую спецификацию Bluetooth версии 5.1](#)).

Безопасность сверхширокополосной технологии в iOS

В новом чипе U1, разработанном компанией Apple, используется сверхширокополосная технология для ориентации в пространстве. Благодаря этой технологии устройства iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max и более новые модели iPhone могут определять точное местоположение других устройств Apple, оснащенных U1. Сверхширокополосная технология использует те же методы рандомизации данных, которые используются в других поддерживаемых устройствах Apple:

- Использование случайных MAC-адресов
- использование случайных порядковых номеров кадров Wi-Fi.

Единый вход

Безопасность единого входа

Единый вход

iOS и iPadOS поддерживают аутентификацию в корпоративных сетях посредством единого входа в систему (SSO). Технология SSO работает с сетями на основе протокола Kerberos, обеспечивая аутентификацию пользователей в службах, к которым у них есть доступ. SSO можно использовать для целого ряда различных сетевых операций, начиная с безопасных сеансов Safari и заканчивая приложениями сторонних разработчиков. Также поддерживается аутентификация на основе сертификатов, такая как PKINIT.

macOS поддерживает аутентификацию в корпоративных сетях посредством Kerberos. Приложения могут использовать Kerberos для аутентификации пользователей в службах, к которым им разрешен доступ. Kerberos также можно использовать для целого ряда различных сетевых операций, начиная с безопасных сеансов Safari и аутентификации в сетевых файловых системах и заканчивая приложениями сторонних разработчиков. Поддерживается аутентификация на основе сертификатов, однако для этого приложение должно задействовать API разработчика.

Для взаимодействия со шлюзами аутентификации на основе Kerberos и системами встроенной аутентификации Windows, которые поддерживают билеты Kerberos, технология SSO в iOS, iPadOS и macOS использует токены SPNEGO и протокол HTTP Negotiate. Поддержка SSO основана на проекте с открытым кодом Heimdal.

В iOS, iPadOS и macOS поддерживаются следующие типы шифрования:

- AES-128-CTS-HMAC-SHA1-96
- AES-256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari поддерживает SSO. Кроме того, на использование этой технологии можно настроить приложения сторонних разработчиков, которые используют стандартные сетевые API в iOS и iPadOS. Для конфигурирования SSO в iOS и iPadOS используется полезная нагрузка профиля конфигурации, позволяющая системам управления мобильными устройствами (MDM) передавать необходимые настройки на устройства. Сюда входит настройка главного имени пользователя (которым является учетная запись пользователя Active Directory) и настройки областей Kerberos, а также настройка приложений и веб-адресов Safari, которым разрешено использовать SSO.

Чтобы настроить Kerberos в macOS, необходимо получить билеты через приложение «Просмотр билетов», войти в домен Windows Active Directory или воспользоваться инструментом командной строки kinit.

Расширяемая технология единого входа

Разработчики приложений могут предоставлять собственные реализации технологии единого входа на основе расширений SSO. Расширения SSO вызываются, когда нативному приложению или веб-приложению необходимо обратиться к какому-либо поставщику услуг идентификации для аутентификации пользователя. Разработчики могут предоставлять два типа расширений: расширения, которые перенаправляют на HTTPS, и расширения, которые используют механизм запроса-ответа, например Kerberos. Благодаря этому расширяемая технология единого входа поддерживает схемы аутентификации OpenID, OAuth, SAML2 и Kerberos.

Для использования расширения единого входа приложение может использовать либо API AuthenticationServices, либо механизм перехвата URL-адресов, предлагаемый операционной системой. WebKit и CFNetwork предоставляют уровень перехвата, который обеспечивает автоматическую поддержку единого входа для любого нативного приложения или приложения WebKit. Для вызова расширения единого входа необходимо установить предоставленную администратором конфигурацию, используя профиль управления мобильными устройствами (MDM). Кроме того, расширения перенаправления должны использовать полезную нагрузку ассоциированных доменов для подтверждения того, что поддерживаемый ими сервер идентификации знает об их существовании.

Вместе с операционной системой предоставляется только одно расширение: Kerberos SSO.

Безопасность AirDrop

Устройства Apple, поддерживающие AirDrop, используют Bluetooth Low Energy (BLE) и разработанную компанией Apple технологию прямого соединения по Wi-Fi, чтобы отправлять файлы и информацию на находящиеся поблизости устройства, включая устройства iOS и iPad с поддержкой AirDrop и операционной системой iOS 7 или новее и компьютеры Mac с операционной системой OS X 10.11 или новее. Для прямого обмена информацией между устройствами используется радиосвязь Wi-Fi — подключение к интернету или точке беспроводного доступа не требуется. Это подключение шифруется с помощью TLS.

По умолчанию функция AirDrop настроена на предоставление доступа «Только для контактов». Пользователи также могут настроить AirDrop на доступ «Для всех» или полностью отключить эту функцию. Организации могут запретить использование AirDrop на устройствах или в приложениях, управляемых с помощью системы управления мобильными устройствами (MDM).

Работа AirDrop

AirDrop использует службы iCloud для упрощения аутентификации пользователей. Когда пользователь выполняет вход в iCloud, на устройстве сохраняется 2048-битный идентификатор RSA, а когда пользователь включает AirDrop, создается хэш краткого идентификатора AirDrop на основе адресов электронной почты и номеров телефона, связанных с учетной записью Apple ID пользователя.

Когда пользователь экспортирует объект через AirDrop, отправляющее устройство передает по каналу BLE сигнал AirDrop, содержащий хэш краткого идентификатора AirDrop. Если поблизости есть другие устройства Apple, которые не находятся в режиме сна и на которых включена функция AirDrop, они распознают сигнал и отвечают на него, используя технологию прямого соединения Wi-Fi, чтобы передающее устройство могло распознать идентификаторы всех отвечающих устройств.

В режиме «Только для контактов» полученный хэш краткого идентификатора AirDrop сравнивается с хэшами пользователей в приложении «Контакты» на устройстве получателя. Если найдено соответствие, принимающее устройство отвечает по прямому соединению Wi-Fi и отправляет свой идентификатор. Если соответствие не найдено, устройство не отвечает.

В режиме «Для всех» используется аналогичная процедура. Однако принимающее устройство отвечает даже в том случае, если соответствие в приложении «Контакты» на устройстве не найдено.

Затем передающее устройство инициирует соединение AirDrop, используя прямое соединение Wi-Fi, и по этому соединению отправляет принимающему устройству хэш полного идентификатора. Если хэш полного идентификатора соответствует хэшу известного пользователя в приложении «Контакты» получателя, то получатель отправляет в ответ хэши своих полных идентификаторов.

Если хэши прошли проверку, в списке общего доступа AirDrop на устройстве отправителя отображается имя получателя и его фотография (при ее наличии в приложении «Контакты»). В iOS и iPadOS они отображаются в разделе «Люди» или «Устройства». Если устройства не прошли проверку или аутентификацию, они отображаются в списке общего доступа AirDrop на устройстве отправителя со значком силуэта и именем устройства, заданным в поле «Настройки» > «Основные» > «Об устройстве» > «Имя». В iOS и iPadOS они помещаются в раздел «Другие люди» в списке общего доступа AirDrop.

Затем отправитель может выбрать пользователя, которому он хочет передать файлы. После выбора пользователя передающее устройство инициирует зашифрованное TLS-соединение с принимающим устройством, для чего устройства обмениваются сертификатами удостоверения iCloud. Удостоверение в сертификатах проверяется по приложению «Контакты» каждого пользователя.

Если сертификаты прошли проверку, получатель должен принять запрос на входящую передачу от идентифицированного пользователя или устройства. Если выбрано несколько получателей, этот процесс повторяется на каждом целевом устройстве.

Безопасность предоставления доступа к паролям Wi-Fi на iPhone и iPad

Устройства iOS и iPadOS, поддерживающие предоставление паролей к Wi-Fi, используют механизм, аналогичный AirDrop, для передачи пароля к Wi-Fi между устройствами.

Когда пользователь выбирает сеть Wi-Fi (запрашивающая сторона) или пользователю предлагается ввести пароль к Wi-Fi, устройство Apple начинает оповещение Bluetooth Low Energy (BLE) с указанием на то, что ему требуется пароль к Wi-Fi. Другие устройства Apple, находящиеся поблизости, не находящиеся в режиме сна и располагающие паролем к выбранной сети Wi-Fi, подключаются к запрашивающему устройству через BLE.

Устройство, располагающее паролем к Wi-Fi (предоставляющая сторона), требует контактную информацию запрашивающей стороны. Запрашивающая сторона должна предоставить свой идентификатор, используя механизм, аналогичный AirDrop. После подтверждения идентификатора предоставляющая сторона отправляет запрашивающей стороне код-пароль, который может использоваться для подключения к сети.

Организации могут ограничить обмен паролями от Wi-Fi на устройствах или в приложениях, управляемых с помощью системы управления мобильными устройствами (MDM).

Безопасность брандмауэра в macOS

В macOS встроен брандмауэр для защиты Mac от сетевых атак и атак типа «отказ в обслуживании». Конфигурация брандмауэра настраивается в разделе «Защита и безопасность» Системных настроек. Поддерживаются следующие конфигурации:

- блокирование всех входящих подключений независимо от приложения;
- автоматическое разрешение встроенному программному обеспечению принимать входящие подключения;
- автоматическое разрешение загруженному и подписанному программному обеспечению принимать входящие подключения;
- разрешение или запрет доступа на основе указанных пользователем приложений;
- запрет компьютеру Mac отвечать на зондирующие запросы и запросы сканирования портов по протоколу межсетевых управляющих сообщений (ICMP).

Безопасность комплекта разработчика

Обзор безопасности комплекта разработчика

Apple предоставляет ряд программных сред, с помощью которых сторонние разработчики могут расширять возможности служб Apple. Конфиденциальность и безопасность заложены в основу следующих программных сред:

- HomeKit
- CloudKit
- SiriKit
- DriverKit
- ReplayKit
- ARKit

Безопасность HomeKit

Безопасность обмена данными HomeKit

HomeKit предоставляет инфраструктуру «умного дома», которая использует функции безопасности iCloud и iOS, iPadOS и macOS для защиты и синхронизации личных данных без передачи этой информации в компанию Apple.

Идентификация и защита в HomeKit реализованы на базе пар открытых и личных ключей. Устройство iOS, iPadOS и macOS генерирует пару ключей Ed25519 для каждого пользователя HomeKit, и эта пара ключей становится идентификатором пользователя в HomeKit. Он используется для аутентификации обмена данными между устройствами iOS, iPadOS и macOS, а также между устройствами iOS, iPadOS и macOS и аксессуарами.

Ключи хранятся в связке ключей и добавляются только в зашифрованные резервные копии Связки ключей. Для синхронизации ключей между устройствами используется Связка ключей iCloud (если доступно). HomePod и Apple TV получают ключи через настройку касанием или режим настройки, описанный ниже. Ключи передаются с iPhone на Apple Watch, с которыми создана пара, через службу идентификации Apple (IDS).

Связь между аксессуарами HomeKit

Аксессуары HomeKit генерируют собственные пары ключей Ed25519 для связи с устройствами iOS, iPadOS и macOS. При восстановлении заводских настроек аксессуара генерируется новая пара ключей.

Для установления связи между устройством iOS, iPadOS и macOS и аксессуаром HomeKit выполняется обмен ключами по 3072-битному протоколу Secure Remote Password: производитель аксессуара предоставляет восьмизначный цифровой код, который пользователь вводит на устройстве iOS или iPadOS; затем этот код шифруется по алгоритму ChaCha20-Poly1305 AEAD с использованием производных ключей HKDF-SHA512. Во время настройки также выполняется проверка сертификата MFi устройства. Аксессуары без чипа MFi могут обладать встроенной поддержкой аутентификации программного обеспечения в iOS 11.3 и новее.

Если в процессе эксплуатации устройству iOS, iPadOS или macOS и аксессуару HomeKit необходимо обменяться данными, каждый из них аутентифицирует вторую сторону, используя ключи, которыми они обменялись ранее (см. выше). Каждый сеанс связи устанавливается с использованием протокола Station-to-Station и шифруется с использованием производных ключей HKDF-SHA512, полученных из сеансовых ключей Curve25519. Этот метод применяется как для IP-аксессуаров, так и для аксессуаров стандарта Bluetooth Low Energy (BLE).

При работе с устройствами BLE, которые поддерживают ширококвещательные уведомления, аксессуар получает ключ шифрования ширококвещательной передачи от связанного устройства iOS, iPadOS или macOS в ходе безопасного сеанса. Ключ используется для шифрования данных об изменении состояния аксессуара, которые передаются с помощью оповещений BLE. Ключ шифрования ширококвещательной передачи является производным ключом HKDF-SHA512, а для шифрования данных используется алгоритм ChaCha20-Poly1305 AEAD. Ключ шифрования ширококвещательной передачи периодически изменяется устройством iOS, iPadOS или macOS и обновляется на других устройствах с помощью iCloud, как описано в разделе [«Безопасность данных HomeKit»](#).

HomeKit и Siri

С помощью Siri можно отправлять запросы аксессуарам, управлять ими и включать сценарии. Siri получает минимальный объем анонимной информации о конфигурации дома, включая имена комнат, аксессуаров и сценариев, необходимые для распознавания команд. Аудиоданные, отправляемые в Siri, могут включать упоминания определенных аксессуаров или команд, но такие данные Siri не связываются с другими функциями Apple, такими как HomeKit.

Аксессуары HomeKit с поддержкой Siri

Пользователи могут включить такие новые функции, как Siri, а также другие функции HomePod, в том числе таймеры, будильники, интерком и дверной звонок, на аксессуарах с поддержкой Siri в приложении «Дом». Когда эти функции включены, аксессуар связывается с объединенным в пару HomePod в локальной сети, который поддерживает эти функции Apple. Аудио передается между устройствами по зашифрованным каналам, одновременно используя протокол HomeKit и протокол AirPlay.

Когда функция «Слушать "Привет, Siri"» включена, аксессуар ожидает, когда будет произнесена фраза «Привет, Siri», используя модуль распознавания ключевой фразы. Если этот модуль распознает ее, он отправляет фрагменты аудио напрямую на объединенное в пару устройство HomePod, используя HomeKit. HomePod во второй раз проверяет аудио, чтобы отменить его отправку, если фрагмент не содержит ключевой фразы.

Когда функция «Siri: коснуться и удерживать» включена, пользователь может нажать кнопку на аксессуаре, чтобы вызвать Siri. Фрагменты аудио отправляются напрямую на объединенное в пару устройство HomePod.

Когда будет установлено, что был совершен вызов Siri, HomePod отправит аудио на серверы Siri и выполнит команду пользователя, используя те меры обеспечения безопасности, конфиденциальности и средства шифрования, которые применяет HomePod, когда к нему обращается пользователь. Если у Siri есть аудиоответ, тогда ответ Siri будет передан аксессуару по аудиоканалу AirPlay. Иногда для запросов к Siri требуется дополнительная информация от пользователя (например, нужно ли огласить другие параметры). В таком случае аксессуар получает указание о том, что нужно спросить пользователя, и дополнительная аудиозапись передается в потоковом режиме на HomePod.

У аксессуара должен быть индикатор, включающийся, когда устройство ожидает ключевую фразу (например, светодиодный индикатор). Аксессуару неизвестно содержание запроса к Siri, но ему доступны аудиопотоки. При этом никакие данные пользователя не хранятся аксессуаром.

Безопасность данных HomeKit

Данные HomeKit можно безопасно синхронизировать между устройствами iOS, iPadOS и macOS пользователя с помощью iCloud и связки ключей iCloud. В ходе этого процесса данные HomeKit шифруются с помощью ключей, полученных из ключей идентификации пользователя в HomeKit, а также случайного значения попсо.

Эти данные обрабатываются как непрозрачный большой двоичный объект, также называемый *blob*. Самый последний объект сохраняется в iCloud, но не используется для каких-либо других целей. Поскольку он зашифрован с помощью ключей, доступ к которым возможен только на принадлежащих пользователю устройствах iOS, iPadOS и macOS, его содержимое недоступно при передаче и хранении в iCloud.

Данные HomeKit синхронизируются между различными пользователями одного «умного дома». Используемые при этом методы аутентификации и шифрования аналогичны методам, используемым для синхронизации между устройством iOS, iPadOS и macOS и аксессуаром HomeKit. Аутентификация выполняется на основе открытых ключей Ed25519, которыми обмениваются устройства при добавлении нового пользователя «умного дома». После добавления нового пользователя для аутентификации и шифрования всех дальнейших сеансов связи используется протокол Station-to-Station и сеансовые ключи.

Новых пользователей может добавлять тот пользователь, который изначально создал дом в HomeKit, а также другие пользователи с правами редактирования. Устройство владельца настраивает аксессуары с использованием открытого ключа нового пользователя для того, чтобы аксессуары могли аутентифицировать нового пользователя и принимать команды от него. Когда нового пользователя добавляет пользователь с правами редактирования, этот процесс делегируется домашнему центру аксессуаров.

HomeKit и Apple TV

Процесс подготовки Apple TV для использования с HomeKit выполняется автоматически, когда пользователь входит в iCloud. Необходимо, чтобы для учетной записи iCloud была включена двухфакторная аутентификация. Apple TV и устройство владельца обмениваются временными открытыми ключами Ed25519 через iCloud. Если устройство владельца и Apple TV находятся в одной локальной сети, временные ключи используются для защиты соединения по локальной сети с использованием протокола Station-to-Station и сеансовых ключей. Используемые при этом методы аутентификации и шифрования аналогичны методам, используемым для синхронизации между устройством iOS, iPadOS и macOS и аксессуаром HomeKit. Устройство владельца передает по защищенному локальному соединению пары открытых и личных ключей Ed25519 пользователя на Apple TV. Эти ключи используются для защиты соединения между Apple TV и аксессуарами HomeKit, а также между Apple TV и другими устройствами iOS, iPadOS и macOS входящими в состав дома HomeKit.

Если у пользователя только одно устройство и он не предоставил доступ к своему дому другим пользователям, передача данных HomeKit в iCloud не выполняется.

Домашние данные и приложения

Доступ приложений к данным о доме регулируется настройками конфиденциальности пользователя. Когда приложению необходимы данные о доме, пользователь получает запрос на предоставление доступа (аналогично доступу к Контакты, Фото и другим источникам данных iOS, iPadOS и macOS). Если пользователь дает разрешение, приложение получает доступ к названиям комнат, названиям аксессуаров, распределению аксессуаров по комнатам и другой информации, которая подробно описана в документации разработчика HomeKit на веб-сайте <https://developer.apple.com/homekit/>.

Локальное хранилище

Данные о домах, аксессуарах, сценариях и пользователях HomeKit хранятся на принадлежащих пользователю устройствах iOS, iPadOS и macOS. Сохраненные данные шифруются с помощью ключей, полученных из ключей идентификации пользователя в HomeKit, а также случайного значения nonce. Кроме того, данные HomeKit имеют класс защиты данных «Защищено до первой аутентификации пользователя». Резервные копии данных HomeKit создаются только в зашифрованном виде, поэтому, например, незашифрованные резервные копии в Finder (в macOS 10.15 и более поздних версиях) или iTunes (в macOS 10.14 и более ранних версиях), созданные при подключении через USB, не содержат данных HomeKit.

Защита маршрутизаторов средствами HomeKit

Маршрутизаторы с поддержкой HomeKit повышают безопасность домашней сети, управляя доступом к Wi-Fi, который получают аксессуары HomeKit по локальной сети или через интернет. Маршрутизаторы также поддерживают аутентификацию с помощью личного предварительного ключа (PPSK). Следовательно, аксессуары можно добавлять в сеть Wi-Fi, используя ключ, который связан с аксессуаром и может быть отозван при необходимости. Благодаря этому обеспечивается более высокий уровень безопасности, потому что аксессуарам не передается основной пароль от сети Wi-Fi, а маршрутизатор может безопасно идентифицировать аксессуар даже при смене его MAC-адреса.

В приложении «Дом» можно задать ограничения доступа для групп аксессуаров. Примеры ограничений описаны далее.

- *Без ограничений.* Доступ к интернету и по локальной сети не ограничен.
- *Автоматически.* Этот параметр задан по умолчанию. Разрешен доступ к интернету и по локальной сети к веб-сайтам и локальным портам, указанным в списке, который передается в Apple производителем аксессуара. В списке должны быть указаны все веб-сайты и порты, которые нужны для работы аксессуара. Параметр «Без ограничений» включен до тех пор, пока такой список не получен.
- *Ограничить домом.* Доступ к интернету и по локальной сети запрещен для любых подключений, за исключением тех, которые были запрошены HomeKit для обнаружения аксессуара и управления им по локальной сети (в том числе с домашнего центра, обеспечивающего возможность удаленного управления).

Личный предварительный ключ (PPSK) — надежный пароль аксессуара, который сгенерирован HomeKit и защищен Личным WPA2. Пароль отзывается, как только пользователь удаляет аксессуар из приложения «Дом». PPSK используется, когда HomeKit добавляет аксессуар в сеть Wi-Fi из дома, который был настроен с помощью маршрутизатора HomeKit; это добавление обозначается как Учетные данные Wi-Fi: Управляется HomeKit на экране настроек аксессуара в приложении «Дом». Аксессуары, добавленные в сеть Wi-Fi раньше маршрутизатора, будут перенастроены на использование PPSK, если аксессуар поддерживает его; в противном случае они сохраняют свои изначальные учетные данные.

В качестве дополнительной меры безопасности пользователи должны настроить маршрутизатор HomeKit в приложении производителя маршрутизатора. Данное приложение может проверить, есть ли у пользователей доступ к маршрутизатору и могут ли пользователи добавить маршрутизатор в приложение «Дом».

Безопасность камеры HomeKit

Камеры, которым присвоен адрес протокола интернета (IP-адрес) в HomeKit, отправляют видео- и аудиопотоки напрямую на устройство iOS, iPadOS, tvOS или macOS в локальной сети, получающей доступ к потоку. Эти потоки шифруются с помощью случайным образом сгенерированных ключей на устройстве и камере протокола интернета (IP-камере). В ходе безопасного сеанса HomeKit эти данные отправляются на камеру. Когда устройство не находится в локальной сети, зашифрованные потоки данных ретранслируются на устройство через домашний центр. Он не расшифровывает потоки данных и служит только для ретрансляции данных между устройством и IP-камерой. Когда какое-либо приложение показывает пользователю видео с IP-камеры HomeKit, система HomeKit безопасно передает видеокadres из отдельного системного процесса, поэтому приложение не может получить доступ к видеопотоку или сохранить его. Приложениям также не разрешено делать снимки экрана из этого потока.

Защищенное видео HomeKit

HomeKit обеспечивает сквозное шифрование для безопасного механизма записи, анализа и просмотра видео с IP-камер HomeKit без передачи контента в компанию Apple или любым другим третьим лицам. Когда IP-камера обнаруживает движение, видеоклипы отправляются непосредственно на устройство Apple, которое выступает в качестве домашнего центра. Для передачи между IP-камерой и домашним центром используется выделенное локальное сетевое соединение. Локальное сетевое соединение зашифровывается с использованием сеансовых производных пар ключей HKDF-SHA512, которые согласовываются в ходе безопасного сеанса HomeKit между IP-камерой и домашним центром. HomeKit дешифрует потоки аудио и видео на домашнем центре и анализирует видеокadres для обнаружения значимых событий. В случае обнаружения значимого события HomeKit зашифровывает видеоклип с помощью AES-256-GCM и произвольно сгенерированного ключа AES256. HomeKit также выбирает обложку для каждого видео, и каждая обложка зашифровывается с помощью того же ключа AES256. Обложка, видео и аудио, которые защищены шифрованием, выгружаются на серверы iCloud. Метаданные каждого клипа, в том числе ключ шифрования, выгружаются в CloudKit с использованием сквозного шифрования iCloud.

Для классификации лиц HomeKit хранит все данные, используемые для классификации лица определенного человека, в CloudKit с помощью сквозного шифрования iCloud. К хранимым данным относятся сведения о каждом человеке, такие как имя, а также изображения лица этого человека. Изображения лица могут быть получены с фото пользователя в приложении «Фото», если он разрешил это, либо из проанализированного ранее видео с IP-камеры. Во время сеанса анализа защищенного видео HomeKit эти данные классификации используются для идентификации людей в потоке защищенного видео, который поступает напрямую с IP-камеры, и включаются в метаданные клипа, упомянутого ранее.

При просмотре видео с камеры в приложении «Дом» данные загружаются из iCloud, а ключи для дешифрования потоков распаковываются локально с использованием сквозного дешифрования iCloud. Защищенный поток видеоконтента передается на серверы и дешифруется локально на устройстве iOS перед отображением в окне просмотра. Каждый сеанс видеоклипа может быть разделен на несколько подсеансов, причем каждый такой подсеанс шифрует поток контента с помощью собственного уникального ключа.

Безопасность HomeKit на устройствах Apple TV

HomeKit безопасно подключает некоторые сторонние аксессуары к Apple TV и поддерживает добавление профилей пользователей на устройство Apple TV владельца дома.

Использование сторонних аксессуаров для дистанционного управления вместе с Apple TV

Некоторые сторонние аксессуары для дистанционного управления передают аудиоданные Siri и события, происходящие на устройствах взаимодействия с человеком (HID), на связанное устройство Apple TV, добавленное через приложение «Дом». Пульт отправляет события HID посредством безопасного сеанса на устройство Apple TV. Пульт с поддержкой Siri отправляет аудиоданные на Apple TV, когда пользователь явным образом активирует микрофон на пульте с помощью специальной кнопки Siri. Пульт отправляет фрагменты аудио напрямую на устройство Apple TV посредством выделенного локального сетевого соединения. Для шифрования локального сетевого соединения используется пара сеансовых производных ключей HKDF-SHA512, которые согласовываются в ходе безопасного сеанса HomeKit между Apple TV и пультом. HomeKit дешифрует фрагменты аудио на Apple TV и перенаправляет их в приложение Siri, где к ним применяются стандартные меры для защиты конфиденциальности входящих аудиоданных Siri.

Профили Apple TV для домов HomeKit

Когда пользователь дома HomeKit добавляет свой профиль на Apple TV владельца дома, этот пользователь получает доступ к телешоу, музыке и подкастам. Настройки каждого пользователя, касающиеся использования его профиля на Apple TV, передаются в учетную запись владельца iCloud с использованием сквозного шифрования iCloud. Данные принадлежат соответствующему пользователю и доступны владельцу только для чтения. Каждый пользователь дома может изменить эти значения в приложении «Дом», после чего Apple TV владельца будет использовать новые настройки.

При включении параметра учетная запись iTunes пользователя становится доступной на Apple TV. При выключении параметра все учетные записи и данные, относящиеся к этому пользователю, удаляются с Apple TV. Первоначальная общая запись в CloudKit инициализируется устройством пользователя, а токен для создания безопасной общей записи в CloudKit отправляется по тому же безопасному каналу, который используется для синхронизации данных между пользователями дома.

Безопасность SiriKit для iOS, iPadOS и watchOS

Для связи с приложениями сторонних разработчиков Siri использует механизм расширений приложения. На устройстве Siri имеет доступ к контактной информации пользователя и данным о текущем местонахождении устройства. Однако прежде чем передавать защищенные данные другому приложению, Siri проверяет, какие права доступа были предоставлены этому приложению пользователем. В соответствии с этими правами Siri передает расширению только тот фрагмент исходного голосового запроса пользователя, который имеет к нему отношение. Например, если у приложения нет доступа к контактной информации, Siri не передаст ему, о ком говорится в запросе пользователя «Переведи моей маме 1000 рублей через "Платежное приложение"». В этом случае приложение увидит только слово «маме».

Однако если пользователь предоставил приложению доступ к контактной информации, приложение получит информацию о матери пользователя. Если отношение или степень родства упоминается в тексте сообщения, например «Напиши моей маме через приложение "Удобные сообщения", что мой брат круче всех», Siri не будет анализировать и преобразовывать фразу «мой брат» независимо от прав доступа, которые есть у приложения.

Приложения с поддержкой SiriKit могут отправить в Siri словарь приложения или пользователя, включающий, например, имена контактов пользователя. Эта информация, связанная со случайным идентификатором, позволяет функции Siri, предназначенной для распознавания речи и обработки естественного языка, пополнять лексикон, связанный с этим приложением. Пользовательская информация остается доступной, пока идентификатор используется, пока пользователь не отключит интеграцию приложения с Siri в Настройках или пока приложение с поддержкой SiriKit не будет удалено.

В таких фразах, как «Найди машину в RideShare до дома моей мамы», для выполнения запроса требуется информация о местонахождении из списка контактов пользователя. Только для выполнения данного запроса Siri предоставляет требуемую информацию расширению приложения, независимо от назначенных пользователем прав доступа приложения к контактам и данным о местонахождении.

Безопасность DriverKit для macOS

Программная среда DriverKit позволяет разработчикам создавать драйверы устройств, устанавливаемые пользователем на свой Mac. Драйверы, созданные с помощью DriverKit, работают в пользовательском пространстве, а не как расширения ядра, что повышает безопасность и стабильность системы. Это упрощает установку и повышает стабильность и безопасность macOS.

Пользователь просто загружает приложение (при использовании расширений системы или DriverKit установщики можно не использовать), и расширение включается только при необходимости. Во многих ситуациях расширения системы заменяют собой расширения ядра, требующие прав администратора для установки в папку «/Система/Библиотеки» или «/Библиотеки».

ИТ-администраторам, которые используют драйверы устройств, облачные хранилища, сети и приложения для обеспечения безопасности на основе расширений ядра, рекомендуется переходить на более новые версии, основанные на расширениях системы. Эти новые версии значительно снижают вероятность возникновения критических ошибок ядра на Mac, а также сокращают уязвимую область. Эти новые расширения работают в пользовательском пространстве, не требуют специальных прав для установки и автоматически удаляются при переносе связанного приложения в корзину.

Программная среда DriverKit предоставляет классы C++ для служб ввода-вывода, сопоставления устройств, дескрипторов памяти и очередей диспетчеризации. Она также задает типы чисел, коллекций, строк и другие распространенные типы для работы со вводом-выводом. Пользователь использует их с программными средами драйверов определенного семейства, такими как USBDriverKit и HIDDriverKit. Используйте программную среду расширений системы для установки и обновления драйвера.

Безопасность ReplayKit в iOS и iPadOS

ReplayKit — это программная среда, которая позволяет разработчикам добавлять в свои приложения функции записи и проведения прямых трансляций. Кроме того, она позволяет пользователям комментировать свои записи и трансляции, используя фронтальную камеру устройства и микрофон.

Запись фильмов

При записи фильмов используется многоуровневая система безопасности.

- *Диалоговое окно разрешений.* Перед началом записи ReplayKit предлагает пользователю подтвердить свое согласие на запись содержимого экрана, звука с микрофона и изображения с фронтальной камеры. Предупреждение отображается однократно в рамках одного процесса приложения. Если приложение остается в фоновом режиме более 8 минут, предупреждение отображается повторно.
- *Запись содержимого экрана и звука.* Запись содержимого экрана и звука выполняется вне процесса приложения — в демоне ReplayKit replayd. Эта мера направлена на то, чтобы процесс приложения не смог получить доступ к записанным данным.

- *Запись содержимого экрана и звука внутри приложения.* Это позволяет приложению получать буферы видео и фрагментов после того, как пользователь дал согласие в диалоговом окне разрешений.
- *Создание и хранение фильма.* Файл фильма записывается в каталог, который доступен только подсистемам ReplayKit и не доступен никаким приложениям. Это помогает предотвратить использование записей третьими сторонами без согласия пользователя.
- *Просмотр конечным пользователем и публикация.* Пользователь может просмотреть и опубликовать фильм через интерфейс, предоставляемый ReplayKit. Интерфейс предоставляется отдельно от процесса через инфраструктуру расширений iOS и имеет доступ к полученному файлу фильма.

Прямая трансляция ReplayKit

При прямой трансляции используется многоуровневая система безопасности.

- *Запись содержимого экрана и звука.* Механизм записи содержимого экрана и звука во время прямой трансляции идентичен записи видео; запись выполняется в демоне `replayd`.
- *Расширения прямой трансляции.* Чтобы службы сторонних разработчиков могли принимать участие в прямой трансляции ReplayKit, они должны создать два новых расширения с конечной точкой `com.apple.broadcast-services`:
 - расширение интерфейса пользователя, чтобы пользователь мог настраивать прямую трансляцию;
 - расширение загрузки, которое будет обрабатывать загрузку видео- и аудиоданных на внутренние серверы службы.

Эта архитектура позволяет гарантировать, что хостинговые приложения не смогут получить доступ к передаваемым видео- и аудиоматериалам. Доступ есть только у ReplayKit и расширений прямой трансляции сторонних разработчиков.

- *Инструмент выбора для прямой трансляции.* С помощью этого инструмента пользователи могут запустить прямую трансляцию из приложения, используя тот же интерфейс пользователя, который доступен через Пункт управления. Интерфейс пользователя реализуется с помощью закрытого API и является расширением в рамках программной среды ReplayKit. Он существует отдельно от процесса приложения публикации.
- *Расширение загрузки.* Расширение, реализуемое сторонними службами прямой трансляции для обработки видео- и аудиоматериалов во время эфирного вещания, использует буферы необработанных закодированных фрагментов. В этом режиме видео- и аудиоданные преобразуются в последовательную форму и передаются стороннему расширению загрузки в реальном времени через прямое соединение XPC. Кодирование видеоданных выполняется следующим образом: объект `IOSurface` извлекается из буфера видеофрагментов, надежно кодируется как объект XPC, пересылается стороннему расширению через XPC, а затем снова декодируется в объект `IOSurface`.

Безопасность ARKit в iOS и iPadOS

ARKit — это программная среда, с помощью которой разработчики могут добавлять в свои приложения или игры элементы дополненной реальности. Разработчики могут добавлять двумерные или трехмерные элементы с использованием фронтальной камеры или камеры на обратной стороне устройства iOS или iPadOS.

Apple разрабатывает камеры с учетом требований конфиденциальности, и, чтобы получить доступ к камере, приложения сторонних разработчиков должны сначала получить согласие пользователя. В iOS и iPadOS приложения, которым пользователь предоставил доступ к камере, могут получать текущие изображения с передней и задней камер в реальном времени. Приложениям запрещено использовать камеру незаметно для пользователя.

Снятые на камеру фото и видео могут содержать другую информацию, например место и время съемки, глубину резкости и функцию *overcapture*. Если пользователи не хотят, чтобы фото и видео, снятые в приложении «Камера», содержали информацию о месте съемки, они могут изменить эту настройку в разделе «Настройки» > «Конфиденциальность» > «Службы геолокации» > «Камера». Если пользователи не хотят, чтобы при публикации фото и видео содержали информацию о месте съемки, они могут отключить геопозицию в меню «Параметры» на странице экспорта.

Для улучшения позиционирования объектов дополненной реальности приложения, использующие ARKit, могут обрабатывать информацию об отслеживании окружающей обстановки или лиц, полученную от другой камеры. Функция отслеживания окружающей обстановки использует специальные алгоритмы на устройстве пользователя для обработки информации от датчиков, чтобы определить их положение в физическом пространстве. Отслеживание окружающей обстановки позволяет использовать такие функции, как оптическое наведение в Картах.

Безопасное управление устройствами

Обзор безопасного управления устройствами

iOS, iPadOS, macOS и tvOS предлагают гибкие политики и конфигурации безопасности, которые легко применять и поддерживать. С их помощью организации могут защищать корпоративную информацию и следить за тем, чтобы сотрудники соблюдали корпоративные требования, даже если они используют собственные устройства, например, в рамках программы использования сотрудниками личных устройств на работе (BYOD).

Организации могут использовать такие средства, как защита паролем, профили конфигурации, удаленное стирание и системы управления мобильными устройствами (MDM) сторонних разработчиков, для управления большой группой устройств и защиты корпоративных данных даже в том случае, если сотрудники обращаются к этим данным со своих персональных устройств.

В iOS 13 или новее, iPadOS 13.1 или новее и macOS 10.15 или новее поддерживается новый способ регистрации пользователей устройств Apple, созданный специально для программ BYOD. Механизм регистрации пользователей предоставляет пользователям дополнительную свободу действий на своих собственных устройствах, одновременно повышая безопасность корпоративных данных благодаря хранению этих данных на отдельном томе файловой системы Apple (APFS) с криптографической защитой. Это обеспечивает оптимальный баланс безопасности, конфиденциальности и удобства для пользователей при использовании программ BYOD.

Безопасность модели создания пары для iPhone и iPad

Для управления доступом к устройству с компьютера-хоста в iOS и iPadOS используется модель создания пары. Создание пары устанавливает отношения доверия между устройством и подключенным к нему компьютером-хостом, которые выражаются в обмене открытыми ключами. iOS и iPadOS используют этот знак доверия для разрешения дополнительных действий с подключенным хостом, например синхронизации данных. В iOS 9 или новее:

- службы, требующие создания пары, не могут быть запущены до тех пор, пока устройство не будет разблокировано пользователем;
- службы не запускаются, если устройство не было недавно разблокировано;
- для запуска некоторых служб (например, синхронизации фотографий) может быть необходимо, чтобы устройство было разблокировано.

Для создания пары пользователь должен разблокировать устройство и принять запрос на создание пары от хоста. В iOS 9 и новее пользователь также должен ввести свой код-пароль, после чего хост и устройство обмениваются открытыми 2048-битными ключами RSA и сохраняют их. Затем хост получает 256-битный ключ для разблокировки хранилища ключей передачи, которое расположено на устройстве. Ключи, которыми обменялись хост и устройство, используются для инициирования сеанса связи, зашифрованного с использованием SSL. Пока такой сеанс не установлен, устройство не пересылает защищенные данные хосту и не запускает службы (синхронизация iTunes или Finder, пересылка файлов, разработка Xcode и т. д.). Чтобы этот зашифрованный сеанс использовался для всех подключений, устройство требует подключения хоста по Wi-Fi, поэтому сначала необходимо создать пару через USB. Создание пары также предоставляет несколько диагностических возможностей. В iOS 9, если запись создания пары не использовалась дольше 6 месяцев, ее действие прекращается. В iOS 11 или новее этот срок сокращен до 30 дней.

Некоторые службы диагностики, включая `com.apple.mobile.pcapd`, могут работать только через USB. Кроме того, для использования службы `com.apple.file_relay` на устройстве должен быть установлен профиль конфигурации, подписанный Apple. В iOS 11 или новее устройство Apple TV может использовать протокол Secure Remote Password для беспроводного создания пары.

Пользователь может очистить список доверенных узлов, выбрав «Сбросить настройки сети» или «Сбросить геонастройки».

Управление мобильными устройствами

Обзор безопасности управления мобильными устройствами

Операционные системы Apple поддерживают работу с системами управления мобильными устройствами (MDM), благодаря чему организации могут выполнять безопасную настройку и управлять масштабным развертыванием устройств Apple.

Безопасность работы системы MDM

Работа функций MDM основана на существующих технологиях операционной системы, таких как профили конфигурации, регистрация по беспроводной сети и служба Apple Push Notification (APNs). Например, APNs используется для вывода устройства из режима сна, чтобы оно могло напрямую связаться с системой MDM через безопасное соединение. Конфиденциальная или корпоративная информация через APNs не передается.

Используя MDM, отделы ИТ могут безопасно внедрять устройства Apple в корпоративную среду, устанавливать и обновлять настройки по беспроводной сети, следить за соответствием корпоративным политикам, управлять политиками обновления программного обеспечения и даже удаленно стирать данные или блокировать управляемые устройства.

Помимо стандартных способов регистрации устройств, поддерживаемых в iOS, iPadOS, macOS и tvOS, в операционных системах iOS 13 или новее, iPadOS 13.1 или новее и macOS 10.15 или новее был добавлен новый тип регистрации — регистрация пользователя. Регистрация пользователя — это регистрация в MDM, которая разработана для программы использования сотрудниками личных устройств на работе (BYOD), когда устройство принадлежит пользователю, но используется в управляемой среде. Регистрация пользователя предоставляет системе MDM меньше полномочий, чем регистрация неконтролируемых устройств, и обеспечивает криптографическое разделение пользовательских и корпоративных данных.

Типы регистрации

- *Автоматическая регистрация устройства.* Этот тип регистрации позволяет организациям настраивать устройства и управлять ими с момента извлечения из коробки (этот тип регистрации также называется *полностью автоматическим развертыванием*). Такие устройства также называются *контролируемыми*. На контролируемых устройствах можно запретить удаление профиля MDM пользователем. Автоматическая регистрация возможна только для устройств, принадлежащих организации.
- *Регистрация устройства.* Этот тип регистрации позволяет пользователям организаций вручную регистрировать устройства и управлять различными аспектами использования устройств, в том числе возможностью стирания данных на устройстве. Администратору доступен большой набор полезных нагрузок и ограничений, которые можно применять к устройству. Когда пользователь удаляет профиль регистрации, также удаляются все профили конфигурации, включая связанные с ними настройки и управляемые приложения, использующие этот профиль регистрации.

- *Регистрация пользователя.* Этот тип регистрации, предназначенный для личных устройств, используется совместно с управляемыми Apple ID для идентификации пользователя на устройстве. Управляемые Apple ID являются частью профиля регистрации пользователя, и для завершения процесса регистрации пользователь должен успешно пройти аутентификацию. Управляемые Apple ID можно использовать одновременно с личным Apple ID, с которым пользователь уже выполнил вход в систему ранее. Управляемые приложения и учетные записи используют управляемые Apple ID, а личные приложения и учетные записи — личные Apple ID.

Ограничения устройств

Администраторы могут накладывать (и иногда снимать) ограничения, чтобы запретить пользователям доступ к определенным приложениям, службам или функциям устройства iPhone, iPad, Mac или Apple TV, которые зарегистрированы в системе MDM. Ограничения отправляются на устройства в составе полезной нагрузки ограничений, которая входит в профиль конфигурации. Некоторые ограничения на iPhone можно накладывать на часы Apple Watch, с которыми создана пара.

Управление настройками код-паролей и паролей

По умолчанию код-пароль пользователя является цифровым. На устройствах iOS и iPadOS с Face ID или Touch ID минимальная длина код-пароля составляет четыре цифры. Рекомендуется использовать более длинные и сложные код-пароли, поскольку их труднее подобрать или взломать.

Для принудительного применения сложных код-паролей и других политик администраторы могут воспользоваться системой MDM или Microsoft Exchange ActiveSync, а также обязать пользователей вручную установить профили конфигурации. Для установки полезной нагрузки политики код-паролей macOS требуется пароль администратора. Некоторые политики код-паролей могут требовать задания код-паролей определенной длины, а также использования в них определенных символов и других атрибутов.

Применение профиля конфигурации

Профили конфигурации являются основным способом, с помощью которого решение MDM может применить политики и ограничения на управляемых устройствах и управлять этими политиками и ограничениями. Если требуется настроить большое количество устройств или задать значительный объем отдельных настроек электронной почты, параметров сети или сертификатов на большом количестве устройств, это можно легко и безопасно сделать с помощью профилей конфигурации.

Профили конфигурации

Профиль конфигурации представляет собой файл XML (с расширением MOBILECONFIG), состоящий из полезных нагрузок, которые загружают настройки и информацию об авторизации на устройства Apple. Профили конфигурации позволяют автоматизировать процесс настройки параметров, учетных записей, ограничений и учетных данных. Эти файлы могут быть созданы системой MDM или Apple Configurator для Mac. Кроме того, их можно создать вручную. Прежде чем отправлять профиль конфигурации на устройство Apple, устройство сначала необходимо зарегистрировать в решении MDM с помощью профиля регистрации.

Профили регистрации

Профиль регистрации — это профиль конфигурации с полезной нагрузкой MDM, который регистрирует устройство в системе MDM, указанной для этого устройства. После этого система MDM может отправлять на устройство команды и профили конфигурации, а также запрашивать определенную информацию с устройства. Когда пользователь удаляет профиль регистрации, также удаляются все профили конфигурации, включая связанные с ними настройки и управляемые приложения, использующие этот профиль регистрации. В каждый момент времени на устройстве может использоваться только один профиль регистрации.

Настройки профиля конфигурации

Профиль конфигурации содержит ряд настраиваемых параметров в определенных полезных нагрузках, включая следующие (но не ограничиваясь ими):

- политики код-паролей и паролей;
- ограничения возможностей устройства (например, отключение камеры);
- сетевые настройки и настройки VPN;
- настройки Microsoft Exchange;
- настройки Почты;
- настройки учетной записи;
- настройки служб каталогов LDAP;
- настройки служб календарей CalDAV;
- учетные данные и ключи;
- обновления программного обеспечения.

Подпись и шифрование профиля

Профили конфигурации можно подписать, чтобы подтвердить их источник, и зашифровать, что поможет обеспечить их целостность и защитить их содержимое. Для шифрования профилей конфигурации для iOS и iPadOS используется синтаксис криптографических сообщений (CMS), заданный в [RFC 5652](#), с поддержкой 3DES и AES128.

Установка профиля

Пользователи могут устанавливать профили конфигурации напрямую на устройства с помощью Apple Configurator для Mac. Профили также можно загружать через Safari, отправлять по электронной почте, через AirDrop или приложение «Файлы» в iOS и iPadOS или по беспроводной сети, используя систему управления мобильными устройствами (MDM). Когда пользователь настраивает устройство в Apple School Manager или Apple Business Manager, устройство загружает и устанавливает профиль для регистрации в системе MDM. Сведения об удалении профилей приведены в разделе [Управление мобильными устройствами: введение](#) в документе «Развертывание платформы Apple».

Примечание. За контролируемые устройства также можно закрепить профили конфигурации. За контролируемые устройства также можно закрепить профили конфигурации. Благодаря этому можно предотвратить удаление профилей или разрешить их удаление только при условии ввода код-пароля. Поскольку многие организации являются владельцами своих устройств iOS и iPadOS, они могут удалить профили конфигурации, которые привязывают устройство к системе MDM, но при этом также удаляются все управляемые настройки, данные и приложения.

Автоматическая регистрация устройства

Регистрацию устройств iOS, iPadOS, macOS и tvOS в системе управления мобильными устройствами (MDM) можно выполнить автоматически — организации не нужно будет физически настраивать или готовить устройства перед выдачей пользователям. После регистрации в одной из служб администратору необходимо войти в систему на веб-сайте службы и связать программу со своей системой MDM. Затем можно назначить приобретенные устройства пользователям через MDM. При настройке устройства можно повысить степень защиты конфиденциальных данных, обеспечив принятие соответствующих мер безопасности. Например:

- При активации устройства Apple сделать обязательной аутентификацию пользователей в процессе начальной настройки в Ассистенте настройки.
- Предоставить предварительную конфигурацию с ограниченными правами доступа и сделать так, чтобы для доступа к конфиденциальным данным, было необходимо сконфигурировать новое устройство.

После назначения пользователя выполняется автоматическая установка конфигурации, ограничений и параметров управления, заданных в MDM. В процессе передачи все данные, пересылаемые между устройствами и серверами Apple, шифруются по протоколу HTTPS (TLS).

Можно еще больше упростить процесс настройки для пользователей, убрав определенные шаги из приложения «Ассистент настройки», чтобы пользователи могли быстро приступить к работе. Администраторы также могут решить, смогут ли пользователи удалить профиль MDM с устройства, что способствует непрерывному действию ограничений в течение всего жизненного цикла устройства. После распаковки и активации устройство может зарегистрироваться в системе MDM данной организации, и все управляемые настройки, приложения и книги устанавливаются автоматически, как задано администратором MDM.

Apple School Manager, Apple Business Manager и Apple Business Essentials

Apple School Manager, Apple Business Manager и Apple Business Essentials — это службы для администраторов, предназначенные для развертывания устройств Apple, которые организация приобрела напрямую у компании Apple, а также авторизованных Apple реселлеров и операторов.

С помощью MDM администраторы могут упростить для пользователей процесс настройки, задавать настройки устройств и распространять приложения и книги, приобретенные в трех указанных выше службах. Apple School Manager также интегрируется со студенческими информационными системами (SIS) как напрямую, так и с помощью SFTP. Кроме того, все три службы могут использовать систему для междоменного управления удостоверениями (SCIM) или федеративную аутентификацию Microsoft Azure Active Directory (Azure AD), благодаря чему администраторы могут быстро создавать учетные записи.

Apple поддерживает сертификацию в соответствии со стандартами ISO/IEC 27001 и 27018. Благодаря этому клиенты Apple могут выполнить законодательные и контрактные обязательства со своей стороны. Благодаря сертификации покупатели получают независимую оценку политик компании Apple в отношении информационной безопасности и конфиденциальности сертифицированных систем. Подробная информация приведена в разделе [Сертификация безопасности интернет-сервисов Apple](#) в документе «Сертификация платформы Apple».

Примечание. Сведения о доступности программы Apple в странах или регионах приведены в статье службы поддержки Apple: [Доступность программ Apple и способов оплаты для предприятий и образовательных учреждений](#).

Контроль устройства

Контроль в целом означает, что устройством владеет организация, которой предоставлены дополнительные возможности управления конфигурацией устройства и ограничениями. Подробная информация приведена в разделе [о контроле устройств Apple](#) в документе «Развертывание платформы Apple».

Безопасность блокировки активации

То, как Apple реализует Блокировку активации, зависит от типа устройства, то есть iPhone это или iPad, компьютер Mac с чипом Apple или компьютер Mac с процессором Intel и чипом безопасности Apple T2.

Применение на устройствах iPhone и iPad

На устройствах iPhone и iPad функция Блокировки активации применяется в процессе активации после отображения экрана выбора сети Wi-Fi в Ассистенте настройки iOS и iPadOS. Когда устройство сообщает о своей активации, оно отправляет на сервер Apple запрос на получение сертификата активации. После этого на устройствах, активация которых заблокирована, появляется предложение ввести учетные данные пользователя iCloud, который включил Блокировку активации. Ассистент настройки iOS и iPadOS не будет продолжать настройку устройства, пока не будет получен действительный сертификат.

Применение на компьютере Mac с чипом Apple

На компьютере Mac с чипом Apple низкоуровневый загрузчик проверяет наличие действительной политики LocalPolicy для устройства, а также то, совпадают ли значения nonce политики LocalPolicy со значениями, которые хранятся в компоненте защищенного хранилища. Низкоуровневый загрузчик загружает recoveryOS в следующих случаях.

- Политики LocalPolicy нет в текущей версии macOS.
- Политика LocalPolicy недействительна для текущей версии macOS.
- Значения хэша nonce политики LocalPolicy не совпадают со значениями хэша, которые хранятся в компоненте защищенного хранилища.

recoveryOS определяет, что компьютер Mac не активирован, и обращается к серверу активации за соответствующим сертификатом. Если на компьютере включена функция Блокировки активации, recoveryOS предлагает ввести учетные данные пользователя iCloud, который включил Блокировку активации. После получения действительного сертификата активации ключ этого сертификата используется для получения сертификата RemotePolicy. Компьютер Mac использует ключ LocalPolicy и сертификат RemotePolicy для создания действительной политики LocalPolicy. Низкоуровневый загрузчик не позволит загрузить macOS, пока не будет получена действительная политика LocalPolicy.

Применение на компьютерах Mac с процессором Intel

На компьютере Mac с процессором Intel и чипом T2 перед загрузкой операционной системы macOS прошивка чипа T2 проверяет наличие действительного сертификата активации. Прошивка UEFI, загруженная чипом T2, запрашивает у чипа сведения о статусе активации и в случае отсутствия сертификата активации загружает recoveryOS вместо macOS. recoveryOS определяет, что компьютер Mac не активирован, и обращается к серверу активации за соответствующим сертификатом. Если на компьютере включена функция Блокировки активации, recoveryOS предлагает ввести учетные данные пользователя iCloud, который включил Блокировку активации. Прошивка UEFI не позволит загрузить macOS, пока не будет получен действительный сертификат активации.

Управляемый режим пропажи и удаленное стирание

Управляемый режим пропажи используется для поиска украденных контролируемых устройств. После того как местоположение устройства определено, его можно удаленно заблокировать или стереть.

Управляемый режим пропажи

В случае потери или кражи контролируемого устройства iOS или iPadOS с iOS 9 или новее администратор системы управления мобильными устройствами (MDM) может удаленно включить на устройстве режим пропажи (который называется управляемым режимом пропажи). После включения управляемого режима пропажи производится выход из учетной записи текущего пользователя системы, а устройство становится невозможно разблокировать. На экране отображается настроенное администратором сообщение, например номер телефона, по которому следует позвонить в случае обнаружения устройства. Кроме того, администратор может запросить у устройства его текущее местоположение (даже если Службы геолокации выключены) и при необходимости воспроизвести на нем звуковой сигнал. Единственный способ выйти из управляемого режима пропажи — выключение режима пропажи администратором. Пользователь получает уведомление об этом на экране блокировки или на экране «Домой».

Удаленное стирание

Администратор или пользователь может выполнить удаленное стирание данных с устройств iOS, iPadOS и macOS (мгновенное удаленное стирание доступно, только если на Mac включена функция FileVault). Мгновенное удаленное стирание реализуется путем надежного удаления ключа носителя из стираемого накопителя, в результате чего все данные становятся недоступными. При запуске удаленного стирания через Microsoft Exchange ActiveSync устройство сначала регистрируется на сервере Microsoft Exchange Server, а затем выполняет стирание.

Когда MDM или iCloud отдадут команду удаленного стирания, то iPhone, iPad, iPod touch или Mac отправляют подтверждение в MDM и выполняют стирание.

Удаленное стирание невозможно в следующих ситуациях:

- в случае регистрации пользователя;
- через Microsoft Exchange ActiveSync, если учетная запись установлена с помощью регистрации пользователя;
- через Microsoft Exchange ActiveSync, если устройство является контролируемым.

Для стирания данных со своего устройства iOS и iPadOS пользователи также могут использовать приложение «Настройки». Как уже упоминалось, на устройствах iOS и iPadOS можно настроить автоматическое стирание после ряда неудачных попыток ввода код-пароля.

Безопасность общего iPad в iPadOS

Общий iPad — это многопользовательский режим использования iPad. В этом режиме несколько человек могут использовать один iPad, не имея доступа к документам и данным друг друга. Каждый пользователь получает собственное хранилище, которое создается на томе файловой системы Apple (APFS), защищенном учетными данными пользователя. Для использования общего iPad нужен управляемый Apple ID, который выпускается организацией и принадлежит ей.

В режиме общего iPad пользователь может входить в систему на любом устройстве, принадлежащем организации, если оно настроено на использование несколькими пользователями. Данные пользователей хранятся в разных папках, каждая из которых находится в собственном домене защиты данных и защищена правами доступа UNIX и механизмом песочницы. В iPadOS 13.4 или новее пользователи также могут выполнить вход для временного сеанса. Когда пользователь завершает временный сеанс, том APFS этого пользователя удаляется, а зарезервированное пространство возвращается в систему.

Вход в систему общего iPad

При входе в систему общего iPad поддерживаются как собственные, так и федеративные управляемые Apple ID. При первом использовании федеративной учетной записи пользователь перенаправляется на портал входа поставщика услуг идентификации (IdP). После прохождения аутентификации выпускается краткосрочный токен доступа для управляемых Apple ID, после чего процесс входа продолжается аналогично процессу входа с собственным управляемым Apple ID. После входа в систему на общем iPad отображается Ассистент настройки, который предлагает пользователю установить код-пароль (учетные данные), который будет использоваться для защиты локальных данных на устройстве и последующей аутентификации на экране входа в систему. Аналогично однопользовательскому устройству, на котором пользователь один раз входит в свой управляемый Apple ID через свою федеративную учетную запись, а затем выполняет разблокировку устройства с помощью своего код-пароля, на общем iPad пользователь один раз входит в систему через свою федеративную учетную запись, а затем использует заданный код-пароль.

Когда пользователь входит в систему без федеративной аутентификации, служба идентификации Apple (IDS) выполняет аутентификацию управляемого Apple ID по протоколу SRP. В случае успешной аутентификации устройству предоставляется кратковременный токен доступа. Если пользователь ранее использовал данное устройство, выполнив вход с теми же учетными данными, учетная запись локального пользователя будет разблокирована.

Если пользователь еще не использовал данное устройство или начал временный сеанс, общий iPad создаст новый идентификатор пользователя в UNIX, том APFS для сохранения данных пользователя и локальную связку ключей. Поскольку во время создания тома APFS пользователю выделяется пространство (резервируется за ним), пространства, доступного на устройстве, может быть недостаточно для создания нового тома. В таком случае система идентифицирует текущего пользователя, данные которого синхронизированы с облаком, и выполняет выход из системы за этого пользователя, подготавливая устройство для нового пользователя. В редких случаях, если выгрузка данных всех текущих пользователей в облако не завершена, новый пользователь не сможет выполнить вход. Чтобы выполнить вход, новый пользователь должен дождаться окончания синхронизации или попросить системного администратора принудительно удалить данные, связанные с учетной записью текущего пользователя, что может привести к их потере.

Если устройство не подключено к интернету (например, когда у устройства нет точки доступа к Wi-Fi), аутентификация может выполняться по локальной учетной записи в течение ограниченного периода времени. В этой ситуации только пользователи, у которых ранее существовали локальные учетные записи, могут войти в систему. Второй вариант — начать временный сеанс. По достижении лимита времени пользователи должны пройти аутентификацию онлайн, даже если локальная учетная запись уже существует.

Если после разблокировки или создания локальной учетной записи выполнена удаленная аутентификация, краткосрочный токен, выданный серверами Apple, преобразуется в токен iCloud, позволяющий входить в iCloud. После этого выполняется восстановление настроек пользователя и синхронизация его документов и данных из iCloud.

Пока сеанс пользователя активен и устройство подключено к интернету, документы и данные сохраняются в iCloud сразу после создания или изменения. Кроме того, механизм фоновой синхронизации помогает обеспечить отправку изменений в iCloud или другие веб-службы с помощью фоновых сеансов NSURLSession после выхода пользователя из системы. После завершения фоновой синхронизации для этого пользователя его том APFS отключается и не может быть подключен снова, пока пользователь не войдет в систему.

В ходе временных сеансов данные не синхронизируются с iCloud. Несмотря на то, что при временном сеансе может выполняться вход в сторонние службы синхронизации, такие как Box или Google Drive, синхронизация данных прерывается по окончании сеанса.

Выход из системы общего iPad

Когда пользователь выходит из системы на общем iPad, хранилище ключей пользователя мгновенно блокируется, а все приложения закрываются. Чтобы ускорить вход нового пользователя, iPadOS временно откладывает некоторые стандартные действия по выходу из системы и отображает окно входа для нового пользователя. Если пользователь входит в систему в течение выделенного времени (приблизительно 30 секунд), общий iPad выполняет отложенную очистку в рамках входа в учетную запись нового пользователя. А если общий iPad не используется, он запускает отложенную очистку. В процессе очистки происходит перезапуск окна входа, как будто был выполнен еще один выход из системы.

Как только временный сеанс завершится, общий iPad выполняет полную последовательность действий для выхода из системы и незамедлительно удаляет том APFS временного сеанса.

Безопасность Apple Configurator

Apple Configurator для Mac — это гибкое, защищенное и ориентированное на устройства решение, с помощью которого администратор может быстро и легко настроить одно или несколько десятков устройств iOS, iPadOS и tvOS, подключенных к Mac через USB (или устройств tvOS, с которыми создана пара с помощью Bonjour), перед передачей их пользователям. С помощью Apple Configurator для Mac администратор может обновлять программное обеспечение, устанавливать приложения и профили конфигурации, переименовывать устройства, менять обои на устройствах, экспортировать информацию об устройствах и документы и выполнять множество других действий.

Apple Configurator для Mac также может возобновить работу или восстановить компьютеры Mac с чипом Apple и с чипом безопасности Apple T2. Когда работа будет возобновлена или компьютер Mac будет восстановлен, файл, содержащий новейшие небольшие обновления операционных систем (macOS, recoveryOS для чипа Apple или serOS для T2), безопасно загрузится с серверов Apple и установится напрямую на Mac. После успешного возобновления работы или восстановления этот файл будет удален с компьютера Mac, на котором запущен Apple Configurator. Пользователь никогда не сможет проверить или использовать этот файл вне Apple Configurator.

Администраторы также могут добавить устройства в Apple School Manager, Apple Business Manager или Apple Business Essentials, используя Apple Configurator для Mac или Apple Configurator для iPhone, даже если устройства не были куплены напрямую у компании Apple, авторизованного реселлера Apple или авторизованного оператора сотовой связи. Когда администратор настраивает устройство, которое было зарегистрировано вручную, оно ведет себя так же, как и любое другое устройство в этих службах с обязательным контролем и регистрацией в системе управления мобильными устройствами (MDM). Если устройство не было куплено напрямую, то в течение 30 дней пользователь может отменить регистрацию устройства в одной из вышеуказанных систем и системе MDM, а также отказаться от контроля.

Организации также могут использовать Apple Configurator для Mac, чтобы активировать устройства iOS, iPadOS и tvOS, которые не подключены к интернету, подключив их к компьютеру-хосту Mac с интернет-соединением на время настройки устройств. Администраторы могут восстанавливать, активировать и подготавливать устройства, используя требуемую конфигурацию, в том числе приложения, профили и документы, без необходимости подключаться к сети Wi-Fi или сотовым сетям. Данная функция не позволяет администраторам обходить существующие требования блокировки активации, которые применяются при активации без использования подключения к хосту.

Безопасность Экранного времени

Экранное время — это встроенная функция для просмотра отчетов о том, сколько времени взрослые и дети проводят в приложениях, на веб-сайтах и за устройством. Кроме того, с ее помощью можно управлять временем, проводимым за экраном устройства. Выделяют два типа пользователей: взрослые и дети (управляемые пользователи).

Несмотря на то что функция «Экранное время» не является новой функцией безопасности системы, важно понимать, каким образом она обеспечивает конфиденциальность и безопасность данных, собираемых на устройствах и передаваемых между ними. Функция «Экранное время» доступна в iOS 12 или новее, iPadOS 13.1 или новее, macOS 10.15 или новее, а некоторые ее функции представлены в watchOS 6 или новее.

В таблице ниже описаны основные возможности функции «Экранное время».

Функция	Поддерживаемая операционная система
Просмотр данных об использовании	iOS iPadOS macOS
Применение дополнительных ограничений	iOS iPadOS macOS watchOS
Настройка лимитов использования интернета	iOS iPadOS macOS
Настройка лимитов использования приложений	iOS iPadOS macOS watchOS
Настройка времени покоя	iOS iPadOS macOS watchOS

Если пользователи управляют собственными устройствами, элементы управления Экранным временем и данные об использовании могут быть синхронизированы между устройствами, связанными с одной и той же учетной записью iCloud, с использованием сквозного шифрования CloudKit. При этом необходимо, чтобы для учетной записи пользователя была включена двухфакторная аутентификация (по умолчанию синхронизация включена). Экранное время заменяет функцию «Ограничения», которая использовалась в предыдущих версиях iOS и iPadOS, и функцию «Родительский контроль», которая использовалась в предыдущих версиях macOS.

В iOS 13 или новее, iPadOS 13.1 или новее и macOS 10.15 или новее информация об использовании автоматически передается между устройствами пользователя Экранного времени или контролируемого ребенка, если для учетной записи iCloud включена двухфакторная аутентификация. Когда пользователь очищает историю Safari или удаляет приложение, соответствующие данные об использовании удаляются с устройства и всех синхронизированных с ним устройств.

Экранное время для родителей

Родители могут использовать функцию «Экранное время» на устройствах iOS, iPadOS и macOS, чтобы просматривать и контролировать использование устройств детьми. Если родитель является организатором семейного доступа (в Семейном доступе iCloud), он может просматривать данные об использовании и управлять настройками Экранного времени для своих детей. Дети получают уведомление о том, что родители включили Экранное время, и могут также следить за своим использованием устройств самостоятельно. При включении Экранного времени для ребенка родители устанавливают код-пароль, чтобы ребенок не мог внести изменения. При достижении совершеннолетия (возраст зависит от страны или региона) ребенок может отключить мониторинг.

Для передачи данных об использовании и параметров конфигурации между устройствами родителя и ребенка используется протокол сквозного шифрования службы идентификации Apple (IDS). Зашифрованные данные могут ненадолго сохраняться на серверах IDS, пока их не прочтает принимающее устройство (например, пока не будет включен iPhone, iPad или iPod touch, если он был выключен). Apple не может прочитать эти данные.

Анализ Экранного времени

Если пользователь включил параметр «Делиться для iPhone и часов», выполняется сбор следующих анонимизированных данных (и только их), которые помогают компании Apple лучше понять, как используется Экранное время:

- когда была включена функция «Экранное время»: в Ассистенте настройки или позднее в Настройках;
- как изменилось использование по категориям после установки лимита (в течение 90 дней);
- включена ли функция «Экранное время»;
- включена ли функция «В покое»;
- количество запросов дополнительного времени;
- количество лимитов приложений;
- количество просмотров использования устройства в настройках Экранного времени с разделением по типу пользователей и типу просмотра (локальный, удаленный, через виджет);
- сколько раз пользователи игнорировали лимит (с разделением по типу пользователей);
- сколько раз пользователи удаляли лимит (с разделением по типу пользователей).

Apple не собирает данные об использовании конкретных приложений или интернета. Когда пользователь видит информацию об использовании в окне «Экранного времени», значки для списка приложений извлекаются напрямую из App Store, в котором не сохраняется никаких данных из таких запросов.

Глоссарий

Авторизация системного ПО Процесс, который сочетает в себе использование встроенных в оборудование криптографических ключей и интернет-службы. В рамках этого процесса выполняется проверка, направленная на то, чтобы при обновлении устанавливалось только подлинное программное обеспечение Apple, подходящее для поддерживаемых устройств.

Алгоритм цифровой подписи на основе эллиптической кривой (ECDSA) Алгоритм цифровой подписи на основе эллиптической криптографии.

Аппаратный модуль системы безопасности (HSM) Специализированный, устойчивый к взлому компьютер, который защищает цифровые ключи и управляет ими.

Вознаграждение за обнаружение уязвимостей Apple Вознаграждение, которое компания Apple выплачивает исследователям за сообщение об уязвимостях, затрагивающих последние версии операционных систем или новейшее оборудование.

Защита данных Механизм защиты файлов и связки ключей для поддерживаемых устройств Apple. Это понятие также относится к API, используемым приложениями для защиты файлов и элементов связки ключей.

Защита ключа Шифрование одного ключа с помощью другого ключа. iOS и iPadOS используют защиту ключей с помощью шифрования NIST AES по алгоритму [RFC 3394](#).

Защита целостности системного сопроцессора (SCIP) Механизм, разработанный Apple, чтобы препятствовать изменению прошивки сопроцессора.

Значение nonce Уникальное одноразовое число, используемое различными протоколами защиты.

Идентификатор группы (GID) Похож на UID, но совпадает для всех процессоров одного класса.

Интегральная микросхема (IC) Также известна как *микрочип*.

Ключ на основе код-пароля (PDK) Ключ шифрования, полученный путем привязывания пароля пользователя к долгосрочному ключу SKP и UID Secure Enclave.

Ключ носителя Компонент архитектуры ключей шифрования, который позволяет выполнить безопасное мгновенное стирание. В iOS, iPadOS, tvOS и watchOS ключ носителя защищает метаданные тома данных (следовательно, без него невозможно получить доступ ко всем ключам файлов, а обрабатываемые файлы, которые обрабатываются технологией защиты данных, становятся недоступными). В macOS ключ носителя защищает данные ключа, все метаданные и данные тома, защищенного FileVault. В любом случае стирание ключа носителя приводит к утрате доступа к зашифрованным данным.

Ключ файла Ключ, используемый технологией защиты данных для шифрования файла в файловой системе. Ключ файла защищается с помощью ключа класса и хранится в метаданных файла.

Ключ файловой системы Ключ, используемый для шифрования метаданных каждого файла, включая его ключ класса. Ключ файловой системы хранится в стираемом накопителе для обеспечения быстрого стирания в ущерб конфиденциальности.

Компонент защищенного хранилища Он содержит неизменяемый код только для чтения, аппаратный генератор случайных чисел, криптографические модули и функцию обнаружения физического взлома. На поддерживаемых устройствах для хранения значения попсе функции антиповтора сопроцессор Secure Enclave объединяется в пару с компонентом защищенного хранилища. Для чтения и обновления значений попсе сопроцессор Secure Enclave и чип хранилища используют безопасный протокол, который помогает предоставить эксклюзивный доступ к значениям попсе. Существует несколько поколений этой технологии с разными уровнями безопасности.

Контроллер памяти Подсистема внутри системы на кристалле, управляющая интерфейсом между системой на кристалле и основной памятью.

Контроллер SSD Аппаратная подсистема, которая управляет носителем информации (твердотельным накопителем).

Криптографический модуль AES Выделенный аппаратный компонент, который реализует AES.

Модуль управления памятью для операций ввода-вывода (IOMMU) Модуль управления памятью для операций ввода-вывода. Подсистема, которая интегрирована в чип и контролирует доступ других устройств ввода-вывода и периферийных устройств к адресному пространству.

Низкоуровневый загрузчик (LLB) На компьютерах Mac с двухэтапной архитектурой загрузки низкоуровневый загрузчик содержит код, загружаемый загрузочным ПЗУ, который затем загружает iBoot как часть безопасной последовательности загрузки.

Привязка Процесс превращения код-пароля пользователя в криптографический ключ и его усиления с помощью UID устройства. Из-за этой меры атаки методом перебора необходимо проводить на конкретном устройстве, что ограничивает скорость перебора и не позволяет выполнять его параллельно. В качестве алгоритма привязки используется PBKDF2: в качестве псевдослучайной функции на каждой итерации используется AES, согласованный с UID устройства.

Программные начальные биты Специальные биты в AES-модуле Secure Enclave, которые добавляются к UID при генерации ключей из UID. Каждый программный начальный бит имеет соответствующий защитный бит. Загрузочное ПЗУ Secure Enclave и операционная система Secure Enclave могут независимо друг от друга изменять значение каждого программного начального бита, пока не установлен соответствующий защитный бит. Если защитный бит установлен, невозможно изменить ни программный начальный бит, ни защитный бит. Программные начальные биты и защитные биты сбрасываются при перезагрузке Secure Enclave.

Протокол обмена Диффи — Хеллмана на эллиптических кривых (ECDHE) Механизм обмена ключами на основе эллиптических кривых. ECDHE позволяет двум сторонам согласовать секретный ключ, предотвратив обнаружение ключа перехватывающим устройством, которое просматривает сообщения между двумя сторонами.

Профиль обеспечения Список свойств (файл .plist), который подписан компанией Apple и содержит набор субъектов и прав, позволяющих устанавливать и тестировать приложения на устройстве iOS или iPadOS. Профиль обеспечения разработки содержит список устройств, выбранных разработчиком для специализированного распространения, а профиль обеспечения распространения содержит идентификатор корпоративного приложения.

Прошивка унифицированного расширяемого интерфейса (UEFI) Технология, которая заменяет собой BIOS и обеспечивает взаимодействие прошивки и операционной системы.

Прямой доступ к памяти (DMA) Функция, которая позволяет аппаратным подсистемам обращаться к основной памяти напрямую, то есть в обход центрального процессора.

Расширенный последовательный периферийный интерфейс (eSPI) Универсальная шина, разработанная для синхронной последовательной связи.

Реестр процесса загрузки (BPR) Набор аппаратных флажков системы на кристалле (SoC), используемых программным обеспечением для отслеживания режимов загрузки, в которые вошло устройство, таких как режим обновления прошивки устройства (DFU) и режим восстановления. После того как флажок реестра процесса загрузки установлен, его уже нельзя снять. Благодаря этому запускаемое далее программное обеспечение имеет надежный индикатор состояния системы.

Режим восстановления Режим восстановления используется для восстановления многих устройств Apple, если не удастся распознать устройство пользователя, чтобы пользователь мог переустановить операционную систему.

Режим обновления прошивки устройства (DFU) Режим, в котором код Boot ROM устройства ожидает восстановления через USB. В режиме DFU экран остается черным, однако при подключении к компьютеру с запущенным приложением iTunes или Finder, отображается сообщение о том, что приложение iTunes (или Finder) обнаружило iPad, iPhone или iPod touch в режиме восстановления и что iPad, iPhone или iPod touch потребуется восстановить перед использованием с iTunes (или Finder).

Связка ключей Инфраструктура и набор API, используемые операционными системами Apple и приложениями сторонних разработчиков для хранения и извлечения паролей, ключей и других конфиденциальных учетных данных.

Система на кристалле (SoC) Интегральная микросхема (IC), которая объединяет несколько компонентов на одном чипе. Процессор приложений, Secure Enclave и другие сопроцессоры являются компонентами системы на кристалле.

Служба идентификации Apple (IDS) Каталог Apple, в котором хранятся открытые ключи iMessage, адреса APNs, а также номера телефонов и адреса электронной почты, используемые для поиска ключей и адресов устройств.

Служба Apple Push Notification (APNs) Доступная по всему миру служба Apple, которая обеспечивает доставку push-уведомлений на устройства Apple.

Стираемый накопитель Выделенная область в хранилище NAND, используемая для хранения криптографических ключей и поддерживающая прямую адресацию и безопасное стирание. Стираемый накопитель не обеспечивает защиту, если злоумышленник физически завладевает устройством, однако хранящиеся в нем ключи могут быть использованы как часть иерархии ключей для обеспечения быстрого стирания и повышения безопасности.

Технология защиты запечатыванием ключей (SKP) Технология защиты данных, которая защищает, или *запечатывает* ключи шифрования с помощью измерений программного обеспечения в системе и ключей, доступных только в аппаратном обеспечении (таком как UID Secure Enclave).

Технология случайного расположения в адресном пространстве (ASLR) Технология, используемая операционными системами для того, чтобы значительно усложнить использование программных ошибок для злоумышленников. Поскольку предсказать адреса памяти и смещения невозможно, вредоносный код не может задать для них конкретные значения.

Угловое представление дактилоскопического узора Математическое представление направления и толщины линий дактилоскопического узора, полученное из части отпечатка пальца.

Улучшенный стандарт шифрования (AES) Популярный мировой стандарт шифрования, используемый для сохранения конфиденциальности данных.

Универсальный идентификатор ресурса (URI) Символьная строка, которая идентифицирует веб-ресурс.

Уникальный идентификатор (UID) 256-битный ключ AES, вшитый в процессор на этапе производства. Этот ключ не может быть считан прошивкой или программным обеспечением, и он используется только аппаратным AES-модулем процессора. Для получения фактического ключа злоумышленнику необходимо провести крайне сложную и дорогостоящую физическую атаку на микросхему процессора. UID не связан ни с каким другим идентификатором на устройстве, включая UDID.

Уникальный идентификатор устройства (ECID) Уникальный 64-битный идентификатор процессора, установленного в устройстве iOS и iPadOS. Если ответить на вызов на одном устройстве, выдача звукового сигнала на находящихся поблизости связанных с iCloud устройствах прекращается после передачи короткого оповещения через Bluetooth Low Energy (BLE) 4.0. Байты оповещения шифруются тем же методом, который используется для оповещений Handoff. Используется как часть процедуры персонализации и не считается секретным.

Управление мобильными устройствами (MDM) Служба, которая позволяет администратору удаленно управлять зарегистрированными устройствами. После регистрации устройства администратор может настраивать параметры и выполнять другие действия с устройством по сети без участия пользователя, используя службу MDM.

Файловая система Apple (APFS) Файловая система по умолчанию для iOS, iPadOS, tvOS, watchOS и компьютеров Mac с macOS 10.13 или новее. APFS имеет такие функции, как надежное шифрование, совместное использование пространства, снимки, быстрое определение размера каталогов и усовершенствованные принципы файловой системы.

Хранилище ключей Структура данных, используемая для хранения коллекции ключей класса. Все типы (пользователь, устройство, система, резервная копия, хранилище и резервная копия iCloud) имеют одинаковый формат.

Заголовок, содержащий следующие элементы: версия (имеет значение 4, начиная с iOS 12); тип (система, резервная копия, хранилище и резервная копия iCloud); UUID хранилища ключей; HMAC, если хранилище ключей подписано; способ защиты ключей класса: привязка к UID или PBKDF2, а также случайное значение («соль») и счетчик повторений.

Список ключей класса: UUID ключа; класс (класс защиты данных файла или связки ключей); тип защиты (ключ на основе только UID; ключ на основе UID и код-пароля); защищенный ключ класса; открытый ключ для асимметричных классов.

AES-XTS Режим AES, определенный в стандарте IEEE 1619-2007, предназначен для шифрования носителей информации.

Apple Business Manager Простой веб-портал для ИТ-администраторов, который предоставляет организациям быстрый и оптимальный способ развертывания устройств Apple, приобретенных напрямую у Apple либо участвующих в программе авторизованных реселлеров Apple или операторов сотовых сетей. Регистрацию устройств в решении для управления мобильными устройствами (MDM) можно выполнить автоматически. В этом случае не потребуется физически настраивать или подготавливать устройства перед выдачей пользователям.

Apple School Manager Простой веб-портал для ИТ-администраторов, который предоставляет организациям быстрый и оптимальный способ развертывания устройств Apple, приобретенных напрямую у Apple либо участвующих в программе авторизованных реселлеров Apple или операторов сотовых сетей. Регистрацию устройств в решении для управления мобильными устройствами (MDM) можно выполнить автоматически. В этом случае не потребуется физически настраивать или подготавливать устройства перед выдачей пользователям.

Boot Camp Утилита для Mac, которая позволяет установить Microsoft Windows на поддерживаемых компьютерах Mac.

Boot ROM Самый первый код, исполняемый процессором устройства при первой загрузке. Этот код является неотъемлемой частью процессора и не может быть изменен компанией Apple или злоумышленником.

CKRecord Словарь пар ключ-значение, которые содержат данные, сохраненные в CloudKit или извлеченные из CloudKit.

Data Vault Этот механизм, реализованный на уровне ядра, обеспечивает защиту от несанкционированного доступа к данным независимо от того, помещено ли в песочницу приложение, которое запрашивает данные.

Gatekeeper Технология в macOS, которая помогает убедиться, что на компьютере Mac пользователя запускается только надежное программное обеспечение.

HMAC Код аутентификации сообщения на основе хэша, полученный с помощью функции криптографического хэша.

iBoot Загрузчик второго уровня для устройств Apple. Код, загружающий XNU как часть безопасной последовательности загрузки. В зависимости от поколения системы на кристалле (SoC) iBoot может загружаться низкоуровневым загрузчиком или напрямую загрузочным ПЗУ.

Joint Test Action Group (JTAG) Стандартное средство отладки оборудования, используемое программистами и разработчиками микросхем.

NAND Энергонезависимая флеш-память.

sePOS Прошивка Secure Enclave на основе версии микроядра L4, доработанной компанией Apple.

xART Аббревиатура, которая расшифровывается как eXtended Anti-Replay Technology, то есть расширенная технология антиповтора. Набор служб, которые предоставляют Secure Enclave зашифрованное постоянное хранилище с аутентификацией и возможностями антиповтора на основе архитектуры физического хранилища. Подробные сведения приведены в разделе «Компонент защищенного хранилища».

XNU Ядро, лежащее в основе операционных систем Apple. Это ядро считается доверенным, и оно обеспечивает применение специальных средств безопасности, таких как подпись кода, песочница, проверка прав и технология случайного расположения в адресном пространстве (ASLR).

XProtect Антивирусная технология в macOS для сигнатурного обнаружения и удаления вредоносного программного обеспечения.

История правок документа

История правок документа

Дата	Сводка
Декабрь 2022 г.	<p>Добавленные разделы:</p> <ul style="list-style-type: none">• Расширенная защита данных для iCloud <p>Обновленные разделы:</p> <ul style="list-style-type: none">• Обзор безопасности iCloud• Шифрование в iCloud• Безопасность резервного копирования iCloud• Обеспечение безопасности и контакты для восстановления доступа• Обеспечение безопасности и цифровые наследники

Дата	Сводка
Май 2022 г.	<p>Обновлено для:</p> <ul style="list-style-type: none"> • iOS 15.4 • iPadOS 15.4 • macOS 12.3 • tvOS 15.4 • watchOS 8.5 <p>Добавленные разделы:</p> <ul style="list-style-type: none"> • Ограничения для парных сред recoveryOS • Версия локальной операционной системы (значение love) • Обмен данными из приложения «Здоровье» • Обеспечение безопасности и контакты для восстановления доступа • Обеспечение безопасности и цифровые наследники • Безопасность службы Tap to Pay on iPhone • Доступ через Apple Wallet • Виды получения доступа • Удостоверения личности в Apple Wallet • Аксессуары HomeKit с поддержкой Siri <p>Обновленные разделы:</p> <ul style="list-style-type: none"> • Magic Keyboard с Touch ID • Face ID, Touch ID, код-пароли и пароли • Безопасность сопоставления лица • Экспресс-карты с резервным питанием • Режимы загрузки компьютера Mac с чипом Apple • Содержимое файла LocalPolicy для компьютера Mac с чипом Apple • Безопасность подписанного системного тома в iOS, iPadOS и macOS • Безопасность системы watchOS • Устройство Apple Security Research Device • Роль файловой системы Apple • Защита при доступе приложений к пользовательским данным • Безопасность приложений в macOS: введение • Защита от вредоносного ПО и кода в macOS • Обзор безопасности iCloud • Безопасная синхронизация связки ключей • Безопасное восстановление Связки ключей iCloud • Совершение платежей картами с помощью Apple Pay • Бесконтактные карты в Apple Pay • Отображение карт как недоступных в Apple Pay • Заявка на получение карты Apple Card • Безопасность Apple Cash • Добавление транспортных карт и карт eMoney в Apple Wallet • Безопасность Apple Messages for Business • Безопасность FaceTime • Безопасность ключей от автомобиля в iOS • Безопасность Apple Configurator <p>Удаленные разделы:</p> <ul style="list-style-type: none"> • Аксессуары HomeKit и iCloud

Дата	Сводка
Май 2021 г.	<p data-bbox="836 212 992 233">Обновлено для:</p> <ul data-bbox="836 247 976 407" style="list-style-type: none"><li data-bbox="836 247 938 268">• iOS 14.5<li data-bbox="836 283 971 304">• iPadOS 14.5<li data-bbox="836 319 971 340">• macOS 11.3<li data-bbox="836 354 954 375">• tvOS 14.5<li data-bbox="836 390 976 411">• watchOS 7.4 <p data-bbox="836 422 1062 443">Добавленные разделы:</p> <ul data-bbox="836 457 1414 606" style="list-style-type: none"><li data-bbox="836 457 1117 478">• Magic Keyboard с Touch ID.<li data-bbox="836 493 1414 537">• Безопасное подтверждение намерения и подключения к Secure Enclave.<li data-bbox="836 552 1317 573">• Автоматическая разблокировка и Apple Watch.<li data-bbox="836 588 1256 609">• Хэш манифеста Image4 CustomOS (coih). <p data-bbox="836 619 1052 640">Измененные разделы:</p> <ul data-bbox="836 655 1453 856" style="list-style-type: none"><li data-bbox="836 655 1453 699">• В раздел Экспресс-карты с резервным питанием добавлено описание двух новых транзакций в экспресс-режиме.<li data-bbox="836 714 1328 735">• Изменен раздел Обзор функций Secure Enclave.<li data-bbox="836 749 1406 793">• В раздел Безопасная мультизагрузка (smb3) добавлены сведения касательно обновления ПО.<li data-bbox="836 808 1393 852">• Дополнен раздел Технология защиты запечатыванием ключей (SKP).

Дата	Сводка
Февраль 2021 г.	<p>Обновлено для:</p> <ul style="list-style-type: none"> • iOS 14.3 • iPadOS 14.3 • macOS 11.1 • tvOS 14.3 • watchOS 7.2 <p>Добавленные разделы:</p> <ul style="list-style-type: none"> • Реализация iBoot, безопасная для памяти • Процесс загрузки компьютера Mac с чипом Apple • Режимы загрузки компьютера Mac с чипом Apple • Управление политикой безопасности Загрузочного диска на компьютере Mac с чипом Apple • Создание ключа подписания политики LocalPolicy и управление им • Содержимое файла LocalPolicy для компьютера Mac с чипом Apple • Безопасность подписанного системного тома в iOS, iPadOS и macOS • Устройство Apple Security Research Device • Мониторинг паролей • Безопасность протокола IPv6 • Безопасность ключей от автомобиля в iOS <p>Обновленные разделы:</p> <ul style="list-style-type: none"> • Secure Enclave • Аппаратное отключение микрофона • Среды recoveryOS и диагностики для компьютера Mac с процессором Intel • Средства защиты прямого доступа к памяти на компьютерах Mac • Расширения ядра в macOS • Защита целостности системы • Безопасность системы watchOS • Управление FileVault в macOS • Доступ приложений к сохраненным паролям • Рекомендации по безопасности паролей • Безопасность Apple Cash • Безопасность Apple Messages for Business • Конфиденциальность Wi-Fi • Безопасность блокировки активации • Безопасность Apple Configurator

Дата	Сводка
Апрель 2020 г.	<p>Обновлено для:</p> <ul style="list-style-type: none"> • iOS 13.4 • iPadOS 13.4 • macOS 10.15.4 • tvOS 13.4 • watchOS 6.2 <p>Обновления:</p> <ul style="list-style-type: none"> • Информация об отключении микрофона iPad добавлена в раздел Аппаратное отключение микрофона. • Сведения о Data Vault добавлены в раздел Защита при доступе приложений к пользовательским данным. • Внесены изменения в разделы Управление FileVault в macOS и «Использование инструментов командной строки». • Дополнена информация об инструменте удаления вредоносного ПО и кода в разделе Защита от вредоносного ПО и кода в macOS. • Внесены изменения в раздел Безопасность общего iPad в iPadOS.
Декабрь 2019 г.	<p>Объединение руководства по безопасности iOS, обзора безопасности macOS и обзора чипа безопасности Apple T2</p> <p>Обновлено для:</p> <ul style="list-style-type: none"> • iOS 13.3 • iPadOS 13.3 • macOS 10.15.2 • tvOS 13.3 • watchOS 6.1.1 <p>Разделы «Настройки конфиденциальности», «Siri», «Предложения Siri» и «Интеллектуальная защита от сбора данных в Safari» были удалены. Посетите https://www.apple.com/ru/privacy/, чтобы узнать больше об изменениях, касающихся этих продуктов и служб.</p>
Май 2019 г.	<p>Обновлено для iOS 12.3</p> <ul style="list-style-type: none"> • Поддержка TLS 1.3 • Обновлено описание безопасности AirDrop • Режим обновления прошивки устройства (DFU) и режим восстановления • Требования к код-паролям для подключения аксессуаров
Ноябрь 2018 г.	<p>Обновлено для iOS 12.1</p> <ul style="list-style-type: none"> • Групповые вызовы по FaceTime

Дата	Сводка
Сентябрь 2018 г.	Обновлено для iOS 12 Secure Enclave <ul style="list-style-type: none"> • Защита целостности операционной системы • Экспресс-карты с резервным питанием • Режим обновления прошивки устройства (DFU) и режим восстановления • Аксессуары для дистанционного управления HomeKit • Бесконтактные карты • Студенческие билеты • Предложения Siri • Быстрые команды в Siri • Приложение «Быстрые команды» • Управление паролями пользователей • Экранное время • Сертификаты и программы обеспечения безопасности
Июль 2018 г.	Обновлено для iOS 11.4 <ul style="list-style-type: none"> • Политики использования биометрических данных • HomeKit • Apple Pay • Деловой чат • Сообщения в iCloud • Apple Business Manager
Декабрь 2017 г.	Обновлено для iOS 11.2 <ul style="list-style-type: none"> • Apple Pay Cash
Октябрь 2017 г.	Обновлено для iOS 11.1 <ul style="list-style-type: none"> • Сертификаты и программы обеспечения безопасности • Touch ID/Face ID • Общие заметки • Сквозное шифрование CloudKit • Обновление TLS • Apple Pay, оплата покупок в интернете с помощью Apple Pay • Предложения Siri • Общий iPad
Июль 2017 г.	Обновлено для iOS 10.3 <ul style="list-style-type: none"> • Secure Enclave • Защита данных в файлах • Хранилища ключей • Сертификаты и программы обеспечения безопасности • SiriKit • HealthKit • Безопасность сети • Bluetooth • Общий iPad • Режим пропажи • Блокировка активации • Настройки конфиденциальности

Дата	Сводка
Март 2017 г.	<p>Обновлено для iOS 10 Безопасность системы</p> <ul style="list-style-type: none"> • Классы защиты данных • Сертификаты и программы обеспечения безопасности • HomeKit, ReplayKit, SiriKit • Apple Watch • Wi-Fi, VPN • Единый вход • Apple Pay, оплата покупок в интернете с помощью Apple Pay • Подготовка кредитных, дебетовых и предоплаченных карт • Предложения Safari
Май 2016 г.	<p>Обновлено для iOS 9.3</p> <ul style="list-style-type: none"> • Управляемые Apple ID • Двухфакторная аутентификация для Apple ID • Хранилища ключей • Сертификаты безопасности • Режим пропажи, блокировка активации • секретные заметки. • Apple School Manager • Общий iPad
Сентябрь 2015 г.	<p>Обновлено для iOS 9 Блокировка активации Apple Watch</p> <ul style="list-style-type: none"> • Политики код-паролей • Поддержка API Touch ID • Для защиты данных процессор A8 использует AES-XTS • Хранилища ключей для обновления программного обеспечения без участия пользователя • Обновления сертификации • Модель доверия для корпоративных приложений • Защита данных для закладок Safari • App Transport Security • Спецификации VPN • Удаленный доступ к iCloud для HomeKit • Скидочные карты в Apple Pay, приложение эмитента карты в Apple Pay • Индексирование содержимого устройства для поиска Spotlight • Модель создания пары iOS • Apple Configurator 2 • Ограничения

© 2022 Apple Inc. Все права защищены.

Использование «клавиатурного» логотипа Apple (Option-Shift-K) в коммерческих целях без предварительного письменного согласия Apple может являться посягательством на права владельца товарного знака и проявлением недобросовестной конкуренции, нарушающим государственные и местные законы.

Apple, логотип Apple, AirDrop, AirPlay, Apple Books, Apple Card, Apple Music, Apple Pay, Apple TV, Apple Wallet, Apple Watch, AppleScript, ARKit, Bonjour, Boot Camp, CarPlay, Face ID, FaceTime, FileVault, Finder, FireWire, Handoff, HealthKit, HomeKit, HomePod, HomePod mini, iMac, iMac Pro, iMessage, iPad, iPadOS, iPad Air, iPad Pro, iPhone, iPod touch, iTunes, Keychain, Lightning, Mac, Mac Catalyst, Mac mini, Mac Pro, MacBook, MacBook Air, MacBook Pro, macOS, Magic Keyboard, Objective-C, OS X, QuickType, Retina, Rosetta, Safari, Siri, Siri Remote, SiriKit, Swift, Spotlight, Touch ID, TrueDepth, tvOS, watchOS и Xcode являются товарными знаками Apple Inc., зарегистрированными в США и других странах и регионах.

App Clips, Find My и Touch Bar являются товарными знаками Apple Inc.

App Store, AppleCare, CloudKit, iCloud, iCloud Drive, iCloud Keychain и iTunes Store являются знаками обслуживания Apple Inc., зарегистрированными в США и других странах и регионах.

Apple Messages for Business является знаком обслуживания Apple Inc.

Apple
One Apple Park Way
Cupertino, CA 95014
apple.com

iOS является товарным знаком или зарегистрированным товарным знаком компании Cisco в США и других странах и используется по лицензии.

Словесный товарный знак и логотипы Bluetooth® являются зарегистрированными товарными знаками Bluetooth SIG, Inc. и используются компанией Apple по лицензии.

Java является зарегистрированным товарным знаком Oracle и/или ее дочерних компаний.

UNIX® является зарегистрированным товарным знаком The Open Group.

Другие названия продуктов и компаний, упомянутые в этом документе, могут являться товарными знаками соответствующих компаний.

Были приложены все усилия для того, чтобы информация в этом руководстве была точной. Apple не несет ответственности за опечатки или описки.

Некоторые приложения доступны не везде. Доступность приложений может меняться.

RS028-00625