ความปลอดภัยของแพลตฟอร์ม Apple

พฤษภาคม 2022

สารบัญ

ความปลอดภัยของแพลตฟอร์ม Apple

บทนำเกี่ยวกับความปลอดภัยของแพลตฟอร์ม Apple

Apple ออกแบบความปลอดภัยลงในหัวใจสำคัญของแพลตฟอร์ม Apple ได้สร้างสถาปัตยกรรมความปลอดภัยที่ตอบสนองความต้องการเฉพาะของอุปกรณ์เคลื่อนที่ นาฬิกา เดสก์ท็อป และบ้านโดยต่อยอดจากประสบการณ์ด้านการคิดค้นระบบปฏิบัติการอุปกรณ์เคลื่อนที่ที่ล้ำหน้าที่สุดในโลก

อุปกรณ์ Apple ทุกเครื่องประกอบด้วย**ฮาร์ดแวร์ ซอฟต์แวร์** และ**บริการ**ที่ออกแบบมาให้ใช้งานร่วมกันเพื่อความปลอดภัยสูงสุดและประสบการณ์การใช้งานที่โปร่งใสเพื่อให้เกิดเป้าหมายสูงสุดในการรักษาข้อมูลส่วนบุคคลให้ปลอดภัยอยู่เสมอ ตัวอย่างเช่น Silicon และฮาร์ดแวร์ด้านความปลอดภัยที่ Apple ออกแบบจะขับเคลื่อนคุณสมบัติด้านความปลอดภัยที่สำคัญต่างๆ การปกป้องซอฟต์แวร์ทำงานเพื่อให้ระบบปฏิบัติการและแอปของบุคคลหรือบริษัทอื่นได้รับการปกป้องอยู่เสมอ และสุดท้าย บริการต่างๆ จะมอบกลไกสำหรับการอัปเดตซอฟต์แวร์ที่ปลอดภัยและตรงเวลา ขับเคลื่อนระบบนิเวศแอปที่ได้รับการปกป้อง และอำนวยความสะดวกให้กับการสื่อสารและการชำระเงินที่ปลอดภัย ผลลัพธ์ที่ได้คือ อุปกรณ์ Apple ไม่เพียงปกป้องอุปกรณ์และข้อมูลในเครื่อง แต่ยังปกป้องระบบนิเวศทั้งหมด ซึ่งรวมถึงทุกอย่างที่ผู้ใช้ใช้งานในเครื่อง บนเครือข่าย และในบริการอินเทอร์เน็ตหลัก

เช่นเดียวกับที่เราออกแบบผลิตภัณฑ์ของเราให้เรียบง่าย เข้าใจได้ง่าย และมีความสามารถ เราก็ออกแบบให้ผลิตภัณฑ์ของเรามีความปลอดภัย คุณสมบัติด้านความปลอดภัยที่สำคัญ เช่น การเข้ารหัสอุปกรณ์ด้วยฮาร์ดแวร์ไม่สามารถปิดใช้งานโดยไม่ได้ตั้งใจได้ คุณสมบัติอื่นๆ เช่น Face ID และ Touch ID ช่วยปรับปรุงประสบการณ์ของผู้ใช้โดยทำให้การรักษาความปลอดภัยอุปกรณ์เรียบง่ายขึ้นและใช้งานได้ง่ายขึ้น และเนื่องจากคุณสมบัติเหล่านี้หลายอย่างจะเปิดใช้งานไว้ตามค่าเริ่มต้น ผู้ใช้หรือแผนก IT จึงไม่จำเป็นต้องปรับแต่งการกำหนดค่ามากมาย

เอกสารนี้ให้รายละเอียดเกี่ยวกับวิธีนำเทคโนโลยีและคุณสมบัติความปลอดภัยไปใช้งานภายในแพลตฟอร์ม Apple เอกสารนี้ยังช่วยองค์กรให้รวมเทคโนโลยีและคุณสมบัติความปลอดภัยของแพลตฟอร์ม Apple เข้ากับนโยบายและขั้นตอนการทำงานของตนเอง เพื่อตอบสนองความต้องการด้านความปลอดภัยขององค์กรอีกด้วย

เนื้อหาจะแบ่งออกเป็นส่วนหัวข้อต่างๆ ดังต่อไปนี้:

- **ความปลอดภัยของฮาร์ดแวร์และข้อมูลทางชีวมิติ:** Silicon และฮาร์ดแวร์ที่เป็นรากฐานสำหรับการรักษาความปลอดภัยบนอุปกรณ์ Apple ซึ่งรวมถึง Apple Silicon, Secure Enclave, กลไกการเข้ารหัส, Face ID และ Touch ID
- **ความปลอดภัยของระบบ:** การผสานฟังก์ชั่นของฮาร์ดแวร์และซอฟต์แวร์สำหรับการบูตอย่างปลอดภัย การอัปเดต และการทำงานที่ต่อเนื่องของระบบปฏิบัติการ Apple
- **การเข้ารหัสและการปกป้องข้อมูล:** สถาปัตยกรรมและการออกแบบที่ช่วยปกป้องข้อมูลของผู้ใช้หากอุปกรณ์สูญหายหรือถูกขโมย หรือหากคนหรือกระบวนการที่ไม่ได้รับอนุญาตพยายามใช้งานหรือแก้ไขข้อมูล
- **ความปลอดภัยของแอป:** ซอฟต์แวร์และบริการที่มอบระบบนิเวศของแอปที่ปลอดภัย และช่วยให้แอปสามารถทำงานได้อย่างปลอดภัยโดยไม่ทำให้ความสมบูรณ์ของแพลตฟอร์มบกพร่อง
- **ความปลอดภัยของบริการ:** บริการของ Apple สำหรับการระบุตัวตน การจัดการรหัสผ่าน การชำระเงิน การสื่อสาร และการค้นหาอุปกรณ์ที่สูญหาย

- **ความปลอดภัยของเครือข่าย:** โปรโตคอลเครือข่ายมาตรฐานอุตสาหกรรมที่มอบการตรวจสอบสิทธิ์ที่ปลอดภัยและการเข้ารหัสข้อมูลที่อยู่ระหว่างการส่ง
- **ความปลอดภัยของชุดสินค้านักพัฒนา:** เฟรมเวิร์ค "ชุดสินค้า" สำหรับการจัดการที่ปลอดภัยและเป็นส่วนตัวของบ้านและสุขภาพ เช่นเดียวกับส่วนขยายของอุปกรณ์ Apple และความสามารถในการบริการแอปของบริษัทอื่น
- **การจัดการอุปกรณ์อย่างปลอดภัย:** วิธีการที่ทำให้สามารถจัดการอุปกรณ์ Apple ช่วยป้องกันการใช้โดยไม่ได้รับอนุญาต และทำให้สามารถลบข้อมูลระยะไกลได้หากอุปกรณ์สูญหายหรือถูกขโมย

ความมุ่งมั่นทุ่มเทเพื่อความปลอดภัย

Apple มุ่งมั่นทุ่มเทเพื่อช่วยปกป้องลูกค้าด้วยเทคโนโลยีด้านความเป็นส่วนตัวและการรักษาความปลอดภัยชั้นนำ ซึ่งออกแบบมาเพื่อปกป้องข้อมูลส่วนบุคคล และวิธีการอันครอบคลุม เพื่อช่วยปกป้องข้อมูลขององค์กรในสภาพแวดล้อมแบบองค์กร Apple จะมอบรางวัลให้นักวิจัยสำหรับงานที่นักวิจัยทำเพื่อเปิดเผยช่องโหว่ โดยมอบเงินอุดหนุนด้านความปลอดภัยของ Apple อีกด้วย รายละเอียดของโปรแกรมและหมวดหมู่เงินอุดหนุนมีให้ดูได้ที่ https://developer.apple.com/security-bounty/

เรามีทีมงานด้านการรักษาความปลอดภัยแบบเฉพาะเพื่อรองรับผลิตภัณฑ์ทั้งหมดของ Apple ทีมงานนี้จะช่วยตรวจสอบการรักษาความปลอดภัยและการทดสอบผลิตภัณฑ์ ทั้งผลิตภัณฑ์ที่กำลังพัฒนาและผลิตภัณฑ์ที่วางจำหน่ายแล้ว ทีมงานของ Apple ยังมอบเครื่องมือรักษาความปลอดภัยและการฝึกอบรม และตรวจสอบภัยคุกคามและรายงานปัญหาด้านความปลอดภัยใหม่ๆ อยู่ตลอดเวลาอีกด้วย Apple เป็นสมาชิกของ Forum of Incident Response and Security Teams (FIRST)

Apple ยังคงขยายขอบเขตของความเป็นไปได้ในด้านความปลอดภัยและความเป็นส่วนตัวต่อไป Apple ใช้ Silicon แบบกำหนดเองในกลุ่มผลิตภัณฑ์ ตั้งแต่ Apple Watch ไปจนถึง iPhone และ iPad และไปจนถึงชิป T2 Security และ Apple Silicon ใน Mac ซึ่งไม่เพียงแต่ขับเคลื่อนการคำนวณที่มีประสิทธิภาพเท่านั้น แต่ยังรวมถึงการรักษาความปลอดภัยด้วย ตัวอย่างเช่น Apple Silicon ซึ่งเป็นรากฐานสำหรับการเริ่มต้นระบบอย่างปลอดภัย, Face ID และ Touch ID และการปกป้องข้อมูล นอกจากนี้ คุณสมบัติการรักษาความปลอดภัยบนอุปกรณ์ที่ขับเคลื่อนโดย Apple Silicon เช่น การปกป้องความสมบูรณ์ของเคอร์เนล รหัสการตรวจสอบสิทธิ์ตัวชี้ และการจำกัดสิทธิ์อย่างรวดเร็ว จะช่วยขัดขวางการโจมตีทางไซเบอร์ประเภทที่พบบ่อย ดังนั้น แม้ว่าโค้ดของผู้โจมตีจะทำงาน แต่ความเสียหายที่อาจเกิดขึ้นก็จะลดทอนลงไปอย่างมาก

เพื่อให้ได้ประโยชน์สูงสุดจากคุณสมบัติด้านความปลอดภัยในตัวแพลตฟอร์มของเรา ขอแนะนำให้องค์กรต่างๆ ตรวจทานนโยบายด้าน IT และด้านความปลอดภัยของตัวเองเพื่อให้มั่นใจได้ว่ากำลังใช้ประโยชน์สูงสุดจากเทคโนโลยีรักษาความปลอดภัยหลายชั้นที่แพลตฟอร์มเหล่านี้นำเสนอ

ในการเรียนรู้เพิ่มเติมเกี่ยวกับการแจ้งปัญหาให้กับ Apple และการสมัครรับการแจ้งเตือนความปลอดภัย ให้ดูที่ แจ้งช่องโหว่ด้านความปลอดภัยหรือความเป็นส่วนตัว

Apple เชื่อว่าความเป็นส่วนตัวคือสิทธิมนุษยชนขั้นพื้นฐาน และมีตัวควบคุมและตัวเลือกในตัวจำนวนมากที่ทำให้ผู้ใช้สามารถตัดสินใจได้ว่าแอปจะใช้ข้อมูลของผู้ใช้อย่างไรและเมื่อใด และข้อมูลใดที่จะถูกนำไปใช้ในการเรียนรู้เพิ่มเติมเกี่ยวกับแนวทางด้านความเป็นส่วนตัวของ Apple การควบคุมความเป็นส่วนตัวบนอุปกรณ์ Apple และนโยบายความเป็นส่วนตัวของ Apple ให้ดูที่ https://www.apple.com/th/privacy

หมายเหตุ: ยกเว้นว่าจะระบุไว้เป็นอย่างอื่น เอกสารประกอบฉบับนี้ครอบคลุมระบบปฏิบัติการเวอร์ชั่นต่อไปนี้: iOS 15.4, iPadOS 15.4, macOS 12.3, tvOS 15.4 และ watchOS 8.5

ความปลอดภัยของฮาร์ดแวร์และข้อมูลทางชีวมิติ

ภาพรวมความปลอดภัยของฮาร์ดแวร์

สำหรับการรักษาความปลอดภัยของซอฟต์แวร์ ซอฟต์แวร์จะต้องอยู่บนฮาร์ดแวร์ที่มีความปลอดภัยในตัว ซึ่งเป็นสาเหตุให้อุปกรณ์ Apple ที่ใช้ iOS, iPadOS, macOS, tvOS และ watchOS มีการออกแบบความสามารถด้านความปลอดภัยลงในซิลิคอน ความสามารถเหล่านี้รวมถึง CPU ซึ่งให้พลังงานแก่คุณสมบัติด้านความปลอดภัยของระบบ รวมถึง Silicon เพิ่มเติมที่มุ่งไปที่ฟังก์ชั่นด้านความปลอดภัย ฮาร์ดแวร์ที่มุ่งเน้นความปลอดภัยจะปฏิบัติตามหลักเกณฑ์ของการรองรับฟังก์ชั่นที่จำกัดและกำหนดอย่างชัดเจนเพื่อลดพื้นหน้าของการโจมตีให้เหลือน้อยที่สุด ส่วนประกอบดังกล่าว ได้แก่ Boot ROM ที่สร้างรากของความเชื่อถือฮาร์ดแวร์สำหรับการบูตอย่างปลอดภัย กลไก AES เฉพาะสำหรับการเข้ารหัสและการถอดรหัสที่มีประสิทธิภาพและปลอดภัย และ Secure Enclave **Secure Enclave** เป็นระบบบนชิป (SoC) ที่มีอยู่ในอุปกรณ์ iPhone, iPad, Apple Watch, Apple TV และ HomePod รุ่นล่าสุดทั้งหมด และบน Mac ที่ใช้ Apple Silicon รวมถึง Mac ที่มีชิป Apple T2 Security ตัวระบบ Secure Enclave เองก็ปฏิบัติตามหลักเกณฑ์การออกแบบเช่นเดียวกับ SoC โดยมี Boot ROM และกลไก AES ของตัวเองแบบแยกต่างหากอย่างชัดเจน Secure Enclave ยังมอบพื้นฐานสำหรับการสร้างความปลอดภัยและการจัดเก็บกุญแจที่จำเป็นต่อการเข้ารหัสข้อมูลในเครื่อง รวมถึงปกป้องและประเมินข้อมูลชีวมิติสำหรับ Face ID และ Touch ID

การเข้ารหัสพื้นที่จัดเก็บข้อมูลจะต้องรวดเร็วและมีประสิทธิภาพ ในขณะเดียวกันก็ไม่สามารถเปิดเผยข้อมูล (หรือ **ข้อมูลการป้อน**) ที่ใช้เพื่อสร้างความสัมพันธ์การป้อนที่เข้ารหัสได้ กลไกฮาร์ดแวร์ AES แก้ไขปัญหานี้โดยดำเนินการเข้ารหัสและถอดรหัสในบรรทัดอย่างรวดเร็ว**ขณะที่มีการเขียนหรืออ่านไฟล์** ช่องทางพิเศษจาก Secure Enclave จะให้ข้อมูลการป้อนที่จำเป็นกับกลไก AES โดยไม่เปิดเผยข้อมูลนี้กับหน่วยประมวลผลแอปพลิเคชัน (หรือ CPU) หรือระบบปฏิบัติการโดยรวม ซึ่งช่วยทำให้แน่ใจว่าการปกป้องข้อมูลของ Apple และเทคโนโลยี FileVault ปกป้องไฟล์ของผู้ใช้โดยไม่เปิดเผยกุญแจการเข้ารหัสระยะยาว

Apple ได้ออกแบบการบูตอย่างปลอดภัยเพื่อปกป้องระดับที่ต่ำที่สุดของซอฟต์แวร์ไม่ให้ถูกรบกวน และเพื่ออนุญาตเพียงซอฟต์แวร์ระบบปฏิบัติการที่เชื่อถือแล้วจาก Apple เท่านั้นที่จะสามารถโหลดได้เมื่อเริ่มต้นระบบ การบูตอย่างปลอดภัยจะเริ่มต้นในโค้ดที่เปลี่ยนไม่ได้ที่เรียกว่า Boot ROM ซึ่งจะมีการระบุระหว่างขั้นตอนการผลิต Apple SoC และเป็นที่รู้จักกันว่าเป็น**รากของความเชื่อถือฮาร์ดแวร์** บนคอมพิวเตอร์ Mac ที่มีชิป T2 ความเชื่อถือสำหรับการบูตอย่างปลอดภัยของ macOS จะเริ่มต้นด้วย T2 (ทั้งชิป T2 และ Secure Enclave ยังเรียกใช้กระบวนการบูตที่ปลอดภัยของตนเองโดยใช้ Boot ROM ที่แยกต่างหาก ซึ่งเป็นอนาล็อกที่ตรงกับวิธีที่ชิปซีรีส์ A และตระกูล M1 ดำเนินการบูตอย่างปลอดภัย)

Secure Enclave ยังประมวลผลข้อมูลใบหน้าและลายนิ้วมือจากเซ็นเซอร์ของ Face ID และ Touch ID ในอุปกรณ์ Apple อีกด้วย การทำงานนี้จะมอบการตรวจสอบสิทธิ์ที่ปลอดภัยขณะที่ยังรักษาข้อมูลทางชีวมิติของผู้ใช้ให้เป็นความลับและปลอดภัย กระบวนการนี้ยังทำให้ผู้ใช้ได้รับประโยชน์จากการรักษาความปลอดภัยด้วยรหัสและรหัสผ่านที่ยาวและซับซ้อนยิ่งขึ้น พร้อมด้วยการตรวจสอบสิทธิ์อย่างรวดเร็วเพื่อความสะดวกในการเข้าถึงหรือการซื้อในหลายๆ สถานการณ์

ความปลอดภัยของ Apple SoC

Silicon ที่ Apple ออกแบบเป็นสถาปัตยกรรมที่มีร่วมกันในผลิตภัณฑ์ทั้งหมดของ Apple และตอนนี้ได้ขับเคลื่อน Mac รวมถึง iPhone, iPad, Apple TV และ Apple Watch นับเป็นเวลากว่าทศวรรษที่ทีมออกแบบ Silicon ระดับโลกของ Apple ได้สร้างและปรับแต่งระบบบนชิป (SoC) ของ Apple ผลลัพธ์ที่ได้คือสถาปัตยกรรมที่วัดได้ ซึ่งออกแบบมาเพื่ออุปกรณ์ทั้งหมดที่ก้าวนำอุตสาหกรรมในความสามารถด้านความปลอดภัย รากฐานสำหรับคุณสมบัติด้านความปลอดภัยที่มีร่วมกันนี้จะเป็นไปได้ก็ต่อเมื่อมาจากบริษัทที่ออกแบบ Silicon ของตัวเองเพื่อทำงานกับซอฟต์แวร์ของตัวเอง

Apple Silicon ได้รับการออกแบบและคิดค้นเพื่อใช้งานคุณสมบัติความปลอดภัยของระบบตามรายละเอียดด้านล่างนี้โดยเฉพาะ:

คุณสมบัติ	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	ตระกูล M1
การปกป้องความสมบูรณ์ของเคอร์เนล	✓	✓	✓	✓	✓	✓
การจำกัดสิทธิ์อย่างรวดเร็ว		✓	✓	✓	✓	✓
การปกป้องความสมบูรณ์ของหน่วยประมวลผลร่วมของระบบ			✓	✓	✓	✓
รหัสการตรวจสอบสิทธิ์ตัวชี้			✓	✓	✓	✓
ระดับชั้นการปกป้องหน้า		✓	✓	✓	✓	ดูหมายเหตุด้านล่าง

หมายเหตุ: ระดับชั้นการปกป้องหน้า (PPL) กำหนดให้แพลตฟอร์มเรียกใช้**เฉพาะ**รหัสที่ลงชื่อและเชื่อถือได้ นี่คือรูปแบบการรักษาความปลอดภัยที่ไม่สามารถใช้งานได้บน macOS

Silicon ที่ Apple ออกแบบยังใช้งานความสามารถด้านการปกป้องข้อมูลตามรายละเอียดด้านล่างนี้โดยเฉพาะ

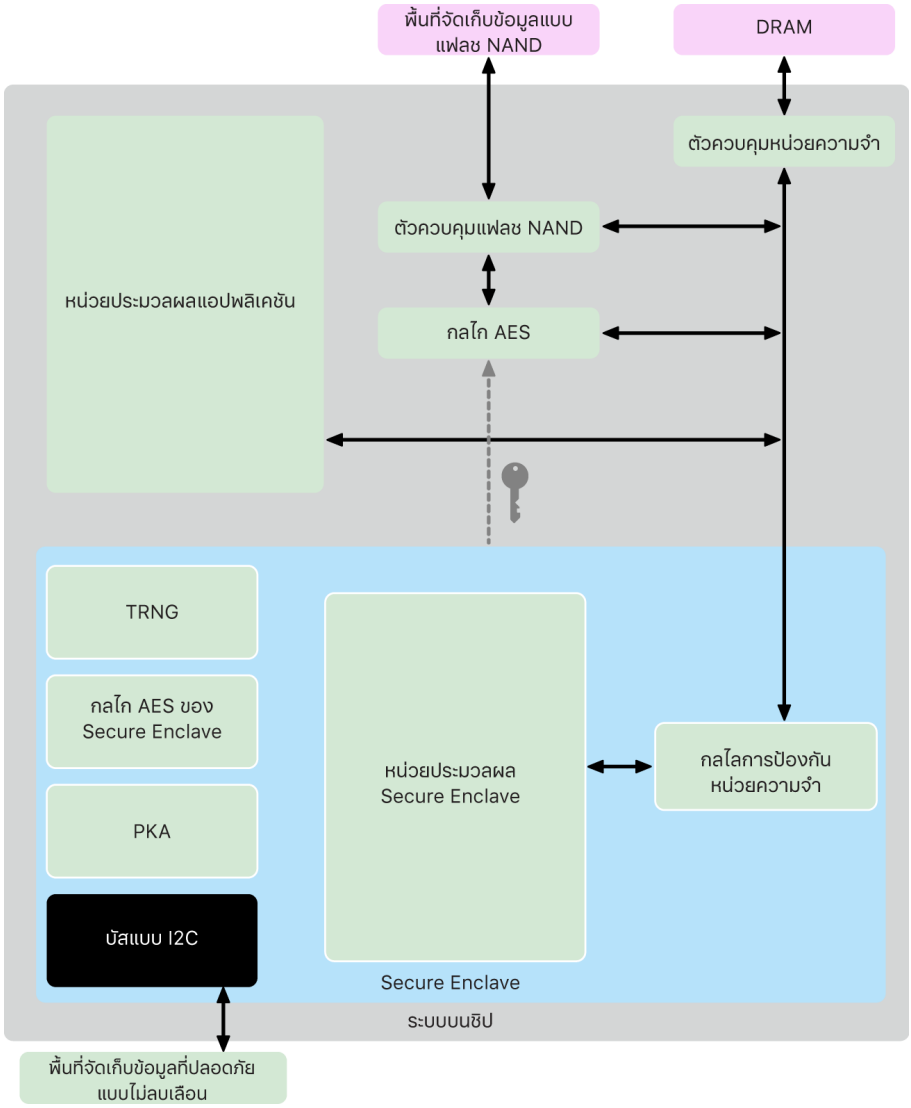
คุณสมบัติ	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, ตระกูล M1
Sealed Key Protection (SKP)	✓	✓	✓	✓	✓
recoveryOS - คลาสการปกป้องข้อมูลทุกคลาสที่ได้รับการปกป้อง	✓	✓	✓	✓	✓
การบูตอื่นๆ ของ DFU, การวินิจฉัย และการอัปเดต - คลาส A, B และ C ที่ได้รับการปกป้อง			✓	✓	✓

Secure Enclave

Secure Enclave เป็นระบบย่อยที่ปลอดภัยโดยเฉพาะใน iPhone, iPad, iPod touch, Mac, Apple TV, Apple Watch และ HomePod เวอร์ชั่นล่าสุด

ภาพรวม

Secure Enclave คือระบบย่อยเฉพาะที่ปลอดภัยซึ่งรวมอยู่ในระบบบนชิป (SoC) ของ Apple Secure Enclave จะแยกจากหน่วยประมวลผลหลักเพื่อให้การรักษาความปลอดภัยอีกขั้นหนึ่งและได้รับการออกแบบให้เก็บข้อมูลผู้ใช้ที่มีความอ่อนไหวอย่างปลอดภัยเมื่อเคอร์เนลของหน่วยประมวลผลแอปพลิเคชันถูกโจมตี ระบบใช้หลักเกณฑ์การออกแบบเดียวกันกับ SoC ซึ่งมี Boot ROM สำหรับสร้างรากของความเชื่อถือฮาร์ดแวร์, กลไก AES สำหรับการดำเนินการเข้ารหัสที่มีประสิทธิภาพและปลอดภัย และหน่วยความจำที่มีรหัสปกป้อง แม้ว่า Secure Enclave ไม่มีพื้นที่จัดเก็บข้อมูล แต่มีกลไกเพื่อจัดเก็บข้อมูลอย่างปลอดภัยบนพื้นที่จัดเก็บข้อมูลที่เชื่อมต่ออยู่ด้วยกัน ซึ่งแยกต่างหากจากพื้นที่จัดเก็บข้อมูลแบบแฟลช NAND ที่ใช้โดยหน่วยประมวลผลแอปพลิเคชันและระบบปฏิบัติการ



Secure Enclave คือคุณสมบัติฮาร์ดแวร์ของ iPhone, iPad, Mac, Apple TV, Apple Watch และ HomePod เกือบทุกเวอร์ชั่น ได้แก่:

- iPhone 5s ขึ้นไป
- iPad Air ขึ้นไป
- คอมพิวเตอร์ MacBook Pro ที่มี Touch Bar (2016 และ 2017) ที่มีชิป Apple T1
- คอมพิวเตอร์ Mac ที่ใช้ Intel ที่มีชิป Apple T2 Security
- คอมพิวเตอร์ Mac ที่ใช้ Apple Silicon
- Apple TV HD ขึ้นไป
- Apple Watch Series 1 ขึ้นไป
- HomePod และ HomePod mini

หน่วยประมวลผล Secure Enclave

หน่วยประมวลผล Secure Enclave มอบประสิทธิภาพในการคำนวณที่สำคัญกับ Secure Enclave ในการมอบการแยกที่ปลอดภัยที่สุด หน่วยประมวลผล Secure Enclave ได้รับการกำหนดให้ใช้งานกับ Secure Enclave เท่านั้น ซึ่งช่วยป้องกันการโจมตีแบบ side-channel ที่ขึ้นอยู่กับซอฟต์แวร์ที่ประสงค์ร้ายที่แชร์ core การทำงานเดียวกันในขณะที่ซอฟต์แวร์เป้าหมายถูกโจมตี

หน่วยประมวลผล Secure Enclave ทำงานด้วยไมโครเคอร์เนล L4 เวอร์ชั่นที่ Apple กำหนดเอง ซึ่งได้รับการออกแบบมาเพื่อทำงานอย่างมีประสิทธิภาพเมื่อความเร็วนาฬิกาอยู่ในระดับต่ำซึ่งจะช่วยปกป้องไม่ให้นาฬิกาและพลังงานถูกโจมตี หน่วยประมวลผล Secure Enclave ที่เริ่มตั้งแต่ A11 และ S4 เป็นต้นไปจะมีกลไกปกป้องหน่วยความจำและหน่วยความจำที่เข้ารหัสพร้อมกับความสามารถในการป้องกันการเล่นซ้ำ การบูตอย่างปลอดภัย ตัวสร้างหมายเลขแบบสุ่มเฉพาะ และกลไก AES ของตัวเอง

กลไกการปกป้องหน่วยความจำ

Secure Enclave ทำงานจากพื้นที่เฉพาะของหน่วยความจำ DRAM ของอุปกรณ์ การปกป้องหลายชั้นจะแยกหน่วยความจำที่ได้รับการปกป้องของ Secure Enclave ออกจากหน่วยประมวลผลแอปพลิเคชัน

เมื่อเริ่มต้นระบบอุปกรณ์ Secure Enclave Boot ROM จะสร้างกุญแจการปกป้องหน่วยความจำชั่วคราวแบบสุ่มสำหรับกลไกการปกป้องหน่วยความจำ ทุกครั้งที่ Secure Enclave เขียนไปยังพื้นที่หน่วยความจำเฉพาะ กลไกการปกป้องหน่วยความจำจะเข้ารหัสบล็อกของหน่วยความจำโดยใช้ AES ในโหมด Mac XEX (xor-encrypt-xor) แล้วคำนวณแท็กการตรวจสอบสิทธิ์รหัสการตรวจสอบสิทธิ์ข้อความแบบเข้ารหัส (CMAC) สำหรับหน่วยความจำนั้น กลไกการปกป้องหน่วยความจำจะจัดเก็บแท็กการตรวจสอบสิทธิ์พร้อมกับหน่วยความจำที่เข้ารหัส เมื่อ Secure Enclave อ่านหน่วยความจำ กลไกการปกป้องหน่วยความจำจะตรวจสอบยืนยันแท็กการตรวจสอบสิทธิ์ ถ้าแท็กการตรวจสอบสิทธิ์ตรงกัน กลไกการปกป้องหน่วยความจำจะถอดรหัสบล็อคหน่วยความจำ ถ้าแท็กไม่ตรงกัน กลไกการปกป้องหน่วยความจำจะส่งสัญญาณข้อผิดพลาดไปยัง Secure Enclave หลังจากพบข้อผิดพลาดการตรวจสอบสิทธิ์หน่วยความจำ Secure Enclave จะหยุดยอมรับคำขอจนกว่าจะมีการบูตระบบอีกครั้ง

เริ่มต้นด้วย A11 SoC และ S4 SoC ของ Apple กลไกการปกป้องหน่วยความจำจะเพิ่มการป้องกันการเล่นซ้ำสำหรับหน่วยความจำ Secure Enclave ในการช่วยป้องกันการเล่นซ้ำของข้อมูลด้านความปลอดภัยที่สำคัญ กลไกการปกป้องหน่วยความจำจะจัดเก็บหมายเลขครั้งเดียวที่ไม่ซ้ำกันซึ่งเรียกว่า **nonce** สำหรับบล็อกของหน่วยความจำควบคู่ไปกับแท็กการตรวจสอบสิทธิ์ Nonce จะถูกใช้ในรูปแบบการปรับปรุงเพิ่มเติมสำหรับแท็กการตรวจสอบสิทธิ์ CMAC Nonces สำหรับบล็อคหน่วยความจำทั้งหมดจะได้รับการปกป้องโดยใช้โครงสร้างความสมบูรณ์ที่มีรากฐานมาจาก SRAM เฉพาะภายใน Secure Enclave สำหรับการเขียนข้อมูล กลไกการปกป้องหน่วยความจำจะ**อัปเดต** Nonce และโครงสร้างความสมบูรณ์ในแต่ละระดับจนถึง SRAM สำหรับการอ่านข้อมูล กลไกการปกป้องหน่วยความจำจะ**ตรวจสอบยืนยัน** Nonce และโครงสร้างความสมบูรณ์ในแต่ละระดับจนถึง SRAM Nonce ที่ไม่ตรงกันจะได้รับการจัดการในลักษณะที่คล้ายกันกับแท็กการตรวจสอบสิทธิ์ที่ไม่ตรงกัน

ใน Apple A14, A15, ตระกูล M1 และ SoCS ที่ใหม่กว่านั้น กลไกการปกป้องหน่วยความจำจะรองรับคุณแจการปกป้องหน่วยความจำแบบชั่วคราวสองรายการ รายการแรกจะใช้กับข้อมูลส่วนตัวของ Secure Enclave และรายการที่สองจะใช้กับข้อมูลที่แชร์กับกลไกทางประสาทที่ปลอดภัย

กลไกการปกป้องหน่วยความจำทำงานแบบอินไลน์และโปร่งใสกับ Secure Enclave Secure Enclave จะอ่านและเขียนข้อมูลหน่วยความจำคล้ายกับเป็น DRAM ที่ไม่ได้เข้ารหัสตามปกติ ในขณะที่ผู้สังเกตการณ์ภายนอก Secure Enclave จะเห็นเฉพาะหน่วยความจำในเวอร์ชั่นที่เข้ารหัสและได้รับการตรวจสอบสิทธิ์แล้ว ผลคือการการปกป้องหน่วยความจำที่ปลอดภัยโดยไม่ต้องแลกกับประสิทธิภาพหรือความซับซ้อนของซอฟต์แวร์

Secure Enclave Boot ROM

Secure Enclave มี Secure Enclave Boot ROM ของตัวเองโดยเฉพาะ เช่นเดียวกันกับ Boot ROM ของหน่วยประมวลผลแอปพลิเคชัน Secure Enclave Boot ROM เป็นโค้ดที่เปลี่ยนไม่ได้ ซึ่งสร้างรากฐานของความเชื่อถือฮาร์ดแวร์สำหรับ Secure Enclave

บนการเริ่มต้นระบบของระบบ iBoot จะกำหนดพื้นที่เฉพาะของหน่วยความจำไปยั Secure Enclave ก่อนที่จะใช้หน่วยความจำ Secure Enclave Boot ROM จะเริ่มต้นการทำงานกลไกการปกป้องหน่วยความจำเพื่อมอบการปกป้องการเข้ารหัสหน่วยความจำที่ได้รับการปกป้องของ Secure Enclave

จากนั้นหน่วยประมวลผลแอปพลิเคชันจะส่งภาพดิสก์ sepOS ไปยัง Secure Enclave Boot ROM หลังจากคัดลอกภาพดิสก์ sepOS ไปยังหน่วยความจำที่มีรหัสปกป้องของ Secure Enclave แล้ว Enclave Boot ROM จะตรวจสอบแฮชการเข้ารหัสและลายเซ็นของภาพดิสก์เพื่อตรวจสอบยืนยันว่า sepOS ได้รับการอนุญาตในการทำงานบนอุปกรณ์นี้แล้ว ถ้าภาพดิสก์ sepOS ได้รับการเซ็นชื่ออย่างถูกต้องให้ทำงานบนอุปกรณ์นี้ Secure Enclave Boot ROM จะถ่ายโอนการควบคุมไปยัง sepOS ถ้าลายเซ็นไม่ถูกต้อง Secure Enclave Boot ROM ได้รับการออกแบบมาป้องกันไม่ให้มีการใช้งาน Secure Enclave เพิ่มเติมจนกว่าจะรีเซ็ตชิปในครั้งถัดไป

บน Apple SoC A10 ขึ้นไปนั้น Secure Enclave Boot ROM จะล็อคแฮชของ sepOS ในการลงทะเบียนเพื่อจุดประสงค์นี้เท่านั้น ตัวเร่งดำเนินการกุญแจสาธารณะใช้แฮชนี้กับกุญแจที่ผูกกับระบบปฏิบัติการ (ผูกกับ OS)

ตัวตรวจสอบการบูตของ Secure Enclave

บน Apple SoC A13 ขึ้นไป Secure Enclave จะรวมตัวตรวจสอบการบูตที่ได้รับการออกแบบมาเพื่อให้แน่ใจว่าความสมบูรณ์บนแฮชของ sepOS ที่บูตปลอดภัยขึ้น

เมื่อเริ่มต้นระบบของระบบ การกำหนดค่าการปกป้องความสมบูรณ์ของหน่วยประมวลผลร่วมของระบบ (SCIP) ของหน่วยประมวลผล Secure Enclave จะช่วยป้องกันไม่ให้หน่วยประมวลผล Secure Enclave เรียกใช้โค้ดใดๆ นอกเหนือจาก Secure Enclave Boot ROM ตัวตรวจสอบการบูตจะช่วยป้องกันไม่ให้ Secure Enclave แก้ไขการกำหนดค่า SCIP โดยตรง ในการทำให้ sepOS ที่โหลดปฏิบัติงานได้ Secure Enclave Boot ROM จะส่งคำขอที่มีที่อยู่และขนาดของ sepOS ที่โหลดไปยังตัวตรวจสอบการบูต เมื่อได้รับคำขอ ตัวตรวจสอบการบูตจะรีเซ็ตหน่วยประมวลผล Secure Enclave, แฮช sepOS ที่โหลด, อัปเดตการตั้งค่า SCIP เพื่ออนุญาตการทำงานของ sepOS ที่โหลด และเริ่มการทำงานภายในโค้ดที่โหลดใหม่ ในขณะที่ระบบทำการบูตต่อไป กระบวนการนี้จะถูกใช้ทุกครั้งที่มีการปฏิบัติงานของโค้ดใหม่ โดยในแต่ละครั้งตัวตรวจสอบการบูตจะอัปเดตแฮชของกระบวนการบูตที่ใช้งานอยู่ ตัวตรวจสอบการบูตยังรวมถึงพารามิเตอร์ความปลอดภัยที่สำคัญในแฮชที่ใช้งานด้วย

เมื่อบูตสำเร็จแล้ว ตัวตรวจสอบการบูตจะดำเนินการแฮชที่ใช้งานอยู่ให้เสร็จสมบูรณ์แล้วส่งไปยังตัวเร่งดำเนินการกุญแจสาธารณะเพื่อใช้กับกุญแจที่ผูกกับ OS กระบวนการนี้ออกแบบมาเพื่อให้กุญแจที่ผูกกับระบบปฏิบัติการไม่สามารถบายพาสได้แม้ว่าจะมีช่องโหว่ใน Secure Enclave Boot ROM

ตัวสร้างเลขสุ่มแท้

ตัวสร้างเลขสุ่มแท้ (True Random Number Generator หรือ TRNG) ใช้สำหรับสร้างข้อมูลแบบสุ่มที่ปลอดภัย Secure Enclave จะใช้ TRNG ทุกครั้งที่มีการสร้างกุญแจการเข้ารหัสแบบสุ่ม, Seed กุญแจแบบสุ่ม หรือการเข้ารหัสอื่นๆ TRNG จะอิงจากออสซิลเลเตอร์แบบวงแหวนหลายรายการที่ผ่านกระบวนการหลังจากเสร็จสิ้นกับ CTR_DRBG (อัลกอริทึมที่อิงจากชุดรหัสบล็อกในโหมดตัวนับ)

กุญแจการเข้ารหัสราก

Secure Enclave มีกุญแจการเข้ารหัสราก ID เฉพาะ (UID) UID จะไม่ซ้ำกันบนอุปกรณ์แต่ละเครื่องและไม่เกี่ยวข้องกับข้อมูลจำเพาะอื่นๆ บนอุปกรณ์

UID ที่สร้างขึ้นแบบสุ่มจะรวมเข้ากับ SoC ณ เวลาที่ผลิต เริ่มตั้งแต่ A9 SoC เป็นต้นไป UID จะมีการสร้างโดย TRNG ของ Secure Enclave ในระหว่างการผลิตและมีการเขียนไปยังฟิวส์โดยใช้กระบวนการซอฟต์แวร์ที่ทำงานทั้งหมดใน Secure Enclave กระบวนการนี้ปกป้อง UID จากการมองเห็นภายนอกอุปกรณ์ในระหว่างการผลิต ดังนั้น Apple หรือผู้จัดหารายใดๆ ของ Apple จึงไม่สามารถเข้าถึงหรือจัดเก็บ UID ได้

sepOS จะใช้ UID ในการปกป้องความลับเฉพาะของอุปกรณ์ ค่า UID อนุญาตให้ข้อมูลมีการผูกแบบเข้ารหัสกับอุปกรณ์เฉพาะเครื่อง ตัวอย่างเช่น ลำดับชั้นกุญแจที่ปกป้องระบบไฟล์จะมีค่า UID ดังนั้นถ้าพื้นที่จัดเก็บข้อมูล SSD ภายในถูกย้ายจากอุปกรณ์เครื่องหนึ่งไปอีกเครื่อง ไฟล์จะไม่สามารถเข้าถึงได้ ความลับเฉพาะของอุปกรณ์ที่ได้รับการปกป้องอื่นๆ ได้แก่ ข้อมูล Face ID หรือ Touch ID บน Mac เฉพาะพื้นที่จัดเก็บข้อมูลภายในแบบเต็มที่เชื่อมโยงกับกลไก AES เท่านั้นที่จะได้รับการเข้ารหัสในระดับนี้ ตัวอย่างเช่น อุปกรณ์จัดเก็บข้อมูลภายนอกที่เชื่อมต่อผ่าน USB และพื้นที่จัดเก็บข้อมูลแบบ PCIe ที่ถูกเพิ่มไปยัง Mac Pro รุ่นปี 2019 จะไม่ถูกเข้ารหัสในลักษณะนี้

อีกทั้ง Secure Enclave ยังมี ID กลุ่ม (GID) ของอุปกรณ์ ซึ่งมีอยู่ทั่วไปในอุปกรณ์ทั้งหมดที่ใช้ SoC ที่กำหนด (ตัวอย่างเช่น อุปกรณ์ทั้งหมดที่ใช้ A15 SoC ของ Apple จะแชร์ GID เดียวกัน)

ค่า UID และ GID ไม่สามารถใช้งานได้ผ่าน Joint Test Action Group (JTAG) หรืออินเทอร์เฟซการแก้ไขข้อผิดพลาดอื่นๆ

กลไก AES ของ Secure Enclave

กลไก AES ของ Secure Enclave คือบล็อคฮาร์ดแวร์ที่ใช้ในการเข้ารหัสแบบสมมาตรโดยอิงจากรหัส AES กลไก AES ออกแบบมาเพื่อต่อต้านการรั่วไหลของข้อมูลโดยใช้การจับเวลาและ Static Power Analysis (SPA) เริ่มต้นด้วย SoC A9 กลไก AES ยังมีการโต้ตอบแบบ Dynamic Power Analysis (DPA) ด้วยเช่นกัน

กลไก AES รองรับกุญแจฮาร์ดแวร์และซอฟต์แวร์ โดยกุญแจฮาร์ดแวร์มาจาก UID หรือ GID ของ Secure Enclave กุญแจเหล่านี้จะอยู่ภายในกลไก AES และจะไม่สามารถมองเห็นได้แม้กระทั่งกับซอฟต์แวร์ sepOS แม้ว่าซอฟต์แวร์สามารถขอให้มีการดำเนินการเข้ารหัสและถอดรหัสด้วยกุญแจฮาร์ดแวร์ได้ ซอฟต์แวร์จะไม่สามารถดึงข้อมูลกุญแจได้

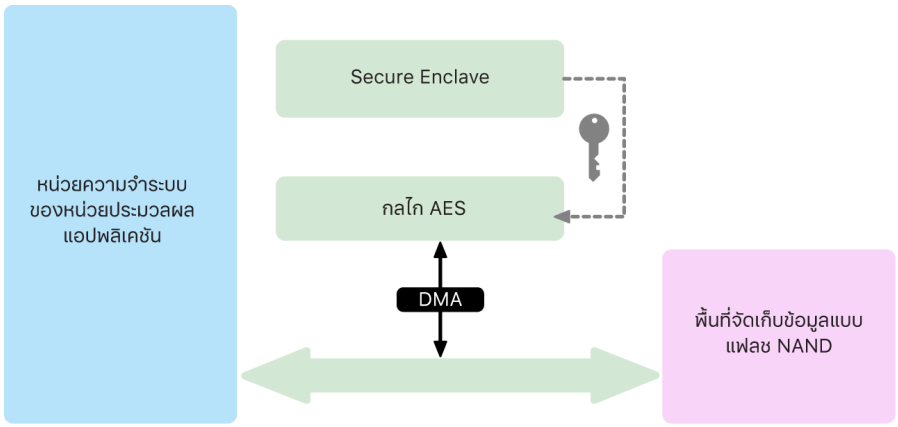
บน A10 SoC และเวอร์ชั่นที่ใหม่กว่าของ Apple กลไก AES จะมีบิต Seed ที่ล็อคได้ซึ่งทำให้กุญแจที่ได้มาจาก UID หรือ GID มีความหลากหลาย วิธีการนี้ทำให้การเข้าถึงข้อมูลมีเงื่อนไขบนโหมดการดำเนินการของอุปกรณ์นั้น ตัวอย่างเช่น บิต Seed ที่ล็อคได้จะใช้เพื่อปฏิเสธการเข้าถึงข้อมูลที่มีรหัสผ่านปกป้องเมื่อมีการบูตจากโหมดอัปเดตเฟิร์มแวร์อุปกรณ์ (DFU) โปรดดูที่ รหัสและรหัสผ่าน สำหรับข้อมูลเพิ่มเติม

กลไก AES

อุปกรณ์ Apple ทุกเครื่องที่มี Secure Enclave ยังมีกลไกการเข้ารหัส AES256 แบบเฉพาะ (หรือ “กลไก AES”) อีกด้วย ซึ่งมีมาให้ในเส้นทางการเข้าถึงหน่วยความจำโดยตรง (DMA) ระหว่างพื้นที่จัดเก็บข้อมูลแบบแฟลช NAND (แบบถาวร) และหน่วยความจำหลักของระบบ ซึ่งทำให้การเข้ารหัสไฟล์มีประสิทธิภาพเป็นอย่างยิ่ง บนหน่วยประมวลผลซีรีส์ A รุ่น A9 ขึ้นไป ระบบย่อยของพื้นที่จัดเก็บข้อมูลแบบแฟลชอยู่บนบัสที่จำกัด ซึ่งอนุญาตให้เข้าถึงเฉพาะหน่วยความจำที่มีข้อมูลผู้ใช้ผ่านกลไกการเข้ารหัส DMA เท่านั้น

ขณะบูต sepOS จะสร้างกุญแจการห่อแบบชั่วคราวโดยใช้ TRNG Secure Enclave จะส่งกุญแจนี้ไปที่กลไก AES โดยใช้สายไฟเฉพาะซึ่งได้รับการออกแบบมาเพื่อป้องกันไม่ให้ซอฟต์แวร์ใดๆ ภายนอก Secure Enclave สามารถเข้าถึงกุญแจได้ จากนั้น sepOS จะสามารถใช้กุญแจการห่อแบบชั่วคราวเพื่อห่อกุญแจไฟล์สำหรับใช้โดยไดรเวอร์ระบบไฟล์ของหน่วยประมวลผลแอปพลิเคชันได้ เมื่อไดรเวอร์ระบบไฟล์อ่านหรือเขียนไฟล์ ไดรเวอร์ระบบไฟล์จะส่งกุญแจที่ถูกห่อไปยังกลไก AES ซึ่งจะแกะห่อกุญแจนั้น กลไก AES จะไม่เปิดเผยกุญแจที่แกะห่อแล้วไปยังซอฟต์แวร์

หมายเหตุ: กลไก AES เป็นส่วนประกอบที่แยกต่างหากจากทั้ง Secure Enclave และกลไก Secure Enclave AES แต่การทำงานของกลไกนั้นสัมพันธ์กับ Secure Enclave อย่างใกล้ชิดดังที่แสดงด้านล่าง



ตัวเร่งดำเนินการกุญแจสาธารณะ

ตัวเร่งดำเนินการกุญแจสาธารณะ (PKA) เป็นบล็อคฮาร์ดแวร์ที่ใช้ในการดำเนินการการทำงานการเข้ารหัสแบบไม่สมมาตร PKA รองรับ RSA และการลงชื่อ ECC (การเข้ารหัสแบบเส้นโค้งรูปไข่) และอัลกอริทึมการเข้ารหัส PKA ออกแบบมาเพื่อป้องกันการรั่วไหลของข้อมูลโดยใช้การจับเวลาและการโจมตีแบบ side-channel เช่น SPA และ DPA

PKA รองรับกุญแจซอฟต์แวร์และฮาร์ดแวร์ โดยกุญแจฮาร์ดแวร์มาจาก UID หรือ GID ของ Secure Enclave กุญแจเหล่านี้จะอยู่ภายใน PKA และจะไม่สามารถมองเห็นได้แม้กระทั่งกับซอฟต์แวร์ sepOS

เริ่มต้นด้วย A13 SoC การปรับใช้การเข้ารหัสของ PKA จะได้รับการพิสูจน์เพื่อความถูกต้องเชิงคณิตศาสตร์โดยใช้เทคนิคการตรวจสอบยืนยันเชิงรูปนัย

บน Apple SoC A10 ขึ้นไป PKA รองรับกุญแจที่ผูกกับ OS ซึ่งเรียกได้อีกอย่างว่า Sealed Key Protection (SKP) กุญแจเหล่านี้ถูกสร้างขึ้นโดยใช้การรวมกันของ UID ของอุปกรณ์และแฮชของ sepOS ที่ใช้งานบนอุปกรณ์ดังกล่าว แฮชได้รับมาจาก Secure Enclave Boot ROM หรือจากตัวตรวจสอบการบูตของ Secure Enclave บน Apple SoC A13 ขึ้นไป กุญแจเหล่านี้ยังใช้เพื่อตรวจสอบยืนยันเวอร์ชั่น sepOS เมื่อส่งคำขอให้กับบางบริการของ Apple และยังใช้เพื่อปรับปรุงความปลอดภัยของข้อมูลที่มีการปกป้องด้วยรหัสด้วยเช่นกัน โดยจะช่วยป้องกันการเข้าถึงข้อมูลการป้อนหากมีการเปลี่ยนแปลงที่สำคัญไปยังระบบโดยไม่ได้รับอนุญาตจากผู้ใช้

พื้นที่จัดเก็บข้อมูลแบบถาวรที่ปลอดภัย

Secure Enclave มาพร้อมกับอุปกรณ์จัดเก็บข้อมูลแบบถาวรที่ปลอดภัยโดยเฉพาะ อุปกรณ์จัดเก็บข้อมูลแบบถาวรที่ปลอดภัยเชื่อมต่อกับ Secure Enclave โดยใช้บัส I2C เฉพาะเพื่อให้ Secure Enclave สามารถเข้าถึงได้เท่านั้น กุญแจการเข้ารหัสข้อมูลผู้ใช้ทั้งหมดมีรากฐานมาจาก Entropy ที่จัดเก็บอยู่ในอุปกรณ์จัดเก็บข้อมูลแบบถาวรของ Secure Enclave

ในอุปกรณ์ที่มี SoC A12, S4 ขึ้นไป Secure Enclave จะจับคู่กับส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยสำหรับพื้นที่จัดเก็บข้อมูล Entropy ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยถูกออกแบบมาพร้อมกับโค้ด ROM ที่เปลี่ยนไม่ได้ ตัวสร้างหมายเลขแบบสุ่มในระดับฮาร์ดแวร์ กุญแจการเข้ารหัสรายอุปกรณ์ กลไกการเข้ารหัสและการตรวจจับการดัดแปลงทางกายภาพ Secure Enclave และส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยสื่อสารกันโดยใช้โปรโตคอลที่เข้ารหัสและได้รับการตรวจสอบสิทธิ์ ซึ่งจะให้การเข้าถึงแบบพิเศษกับ Entropy

อุปกรณ์ที่วางจำหน่ายเป็นครั้งแรกในปี 2020 ขึ้นไปมาพร้อมกับส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยรุ่นที่ 2 ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยรุ่นที่ 2 จะเพิ่มตัวนับ lockbox ตัวนับ lockbox แต่ละตัวจะจัดเก็บ salt 128 บิต, ตัวตรวจสอบยืนยันรหัส 128 บิต, ตัวนับ 8 บิต และค่าความพยายามสูงสุด 8 บิต การเข้าถึงตัวนับ lockbox จะผ่านโปรโตคอลที่เข้ารหัสและได้รับการตรวจสอบสิทธิ์

ตัวนับ lockbox มี Entropy ที่จำเป็นในการปลดล็อคข้อมูลผู้ใช้ที่มีรหัสปกป้อง ในการเข้าถึงข้อมูลผู้ใช้ Secure Enclave ที่จับคู่กันอยู่จะต้องรับค่า Entropy ของรหัสที่ถูกต้องจากรหัสของผู้ใช้และ UID ของ Secure Enclave รหัสของผู้ใช้จะไม่สามารถเรียนรู้ได้โดยใช้ความพยายามในการปลดล็อคที่ส่งมาจากแหล่งอื่นนอกเหนือจาก Secure Enclave ที่จับคู่กันอยู่ ถ้าความพยายามในการป้อนรหัสเกิดขีดจำกัด (ตัวอย่างเช่น ความพยายาม 10 ครั้งบน iPhone) ข้อมูลที่ปกป้องด้วยรหัสจะถูกลบออกอย่างสมบูรณ์โดยส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัย

ในการสร้างตัวนับ lockbox นั้น Secure Enclave จะส่งค่า Entropy ของรหัสและค่าความพยายามสูงสุดให้กับส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัย ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยจะสร้างค่า salt โดยใช้ตัวสร้างหมายเลขแบบสุ่มของส่วนประกอบ จากนั้นส่วนประกอบจะรับค่าตัวตรวจสอบยืนยันรหัสและค่า Entropy lockbox จาก Entropy ของรหัสที่ให้มา กุญแจการเข้ารหัสที่ไม่ซ้ำกันของส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัย และค่า salt ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยจะเริ่มต้นการทำงานตัวนับ lockbox โดยเริ่มต้นนับจาก 0, ค่าความพยายามสูงสุดที่กำหนด, ค่าตัวตรวจสอบยืนยันรหัสที่ได้รับ และค่า salt จากนั้น ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยจะส่งคืนค่า Entropy lockbox ที่สร้างขึ้นไปยัง Secure Enclave

ในการดึงข้อมูลค่า Entropy lockbox จากตัวนับ lockbox ในภายหลัง Secure Enclave จะส่ง Entropy ของรหัสไปยังส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัย ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยจะเพิ่มตัวนับสำหรับ lockbox เป็นอันดับแรก ถ้าตัวนับที่เพิ่มขึ้นมีค่าความพยายามเกินค่าสูงสุด ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยจะลบตัวนับ lockbox โดยสมบูรณ์ ถ้ายังมีความพยายามไม่ถึงจำนวนสูงสุด ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยจะพยายามรับค่าตัวตรวจสอบยืนยันรหัสและค่า Entropy lockbox ด้วยอัลกอริทึมเดียวกันกับที่ใช้สร้างตัวนับ lockbox ถ้าค่าตัวตรวจสอบยืนยันรหัสที่ได้รับตรงกับค่าตัวตรวจสอบยืนยันรหัสที่จัดเก็บไว้ ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยจะส่งคืนค่า Entropy lockbox ไปยัง Secure Enclave แล้วรีเซ็ตตัวนับให้เป็น 0

กุญแจที่ใช้เพื่อเข้าถึงข้อมูลที่มีรหัสผ่านปกป้องจะมีรากฐานมาจาก Entropy ที่จัดเก็บอยู่ในตัวนับ lockbox โปรดดูที่ ภาพรวมการปกป้องข้อมูล สำหรับข้อมูลเพิ่มเติม

พื้นที่จัดเก็บข้อมูลแบบถาวรที่ปลอดภัยจะใช้กับบริการป้องกันการเล่นซ้ำทั้งหมดใน Secure Enclave บริการป้องกันการเล่นซ้ำบน Secure Enclave เป็นบริการที่ใช้เพิกถอนข้อมูลในกรณีที่มีการทำเครื่องหมายขอบเขตป้องกันการเล่นซ้ำ ซึ่งรวมถึง แต่ไม่จำกัดเพียง กรณีต่อไปนี้:

- การเปลี่ยนรหัส
- การเปิดใช้งานหรือปิดใช้งาน Face ID หรือ Touch ID
- การเพิ่มหรือลบใบหน้า Face ID หรือลายนิ้วมือ Touch ID
- การรีเซ็ต Face ID หรือ Touch ID
- การเพิ่มหรือการเอาบัตร Apple Pay ออก
- ลบข้อมูลเนื้อหาและการตั้งค่าทั้งหมด

บนสถาปัตยกรรมที่ไม่มีส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัย ระบบจะใช้ EEPROM (หน่วยความจำแบบอ่านอย่างเดียวที่เขียนโปรแกรมและลบข้อมูลแบบอิเล็กทรอนิกส์ได้) เพื่อให้บริการพื้นที่จัดเก็บข้อมูลที่ปลอดภัยสำหรับ Secure Enclave เช่นเดียวกับส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัย EEPROM จะแนบกับและเข้าถึงได้จาก Secure Enclave เท่านั้น แต่จะไม่มีคุณสมบัติด้านความปลอดภัยสำหรับฮาร์ดแวร์โดยเฉพาะ และไม่รับประกันการเข้าถึงแบบพิเศษไปยัง Entropy (นอกจากคุณลักษณะการแนบทางกายภาพ) และไม่มีฟังก์ชั่นตัวนับ lockbox

กลไกทางประสาทที่ปลอดภัย

บนอุปกรณ์ที่มี Face ID กลไกทางประสาทที่ปลอดภัยจะแปลงภาพ 2D และแผนที่ความลึกให้เป็นการแสดงเชิงคณิตศาสตร์ของใบหน้าผู้ใช้

บน A11 SoC จนถึง A13 SoC กลไกทางประสาทที่ปลอดภัยจะถูกรวมเข้ากับ Secure Enclave กลไกทางประสาทที่ปลอดภัยใช้การเข้าถึงหน่วยความจำโดยตรง (DMA) เพื่อประสิทธิภาพการทำงานสูง หน่วยการจัดการหน่วยความจำข้อมูลเข้า/ข้อมูลออก (IOMMU) ภายใต้ควบคุมของเคอร์เนล sepOS จะจำกัดการเข้าถึงโดยตรงไปยังพื้นที่หน่วยความจำที่อนุญาต

เริ่มต้นด้วย A14 และตระกูล M1 Neural Engine ที่ปลอดภัยจะถูกนำไปใช้เป็นโหมดปลอดภัยใน Neural Engine ของหน่วยประมวลผลแอปพลิเคชัน ตัวควบคุมความปลอดภัยของฮาร์ดแวร์โดยเฉพาะจะสลับระหว่างงานของหน่วยประมวลผลแอปพลิเคชันกับ Secure Enclave โดยจะรีเซ็ตสถานะของกลไกทางประสาทในการเปลี่ยนแต่ละครั้งเพื่อให้ข้อมูล Face ID ปลอดภัยอยู่เสมอ กลไกโดยเฉพาะจะปรับใช้การเข้ารหัสหน่วยความจำ การตรวจสอบสิทธิ์ และการควบคุมการเข้าถึง ในขณะเดียวกัน ก็ใช้กุญแจการเข้ารหัสแบบแยกต่างหากและช่วงหน่วยความจำเพื่อจำกัดกลไกทางประสาทที่ปลอดภัยให้อยู่ในพื้นที่หน่วยความจำที่อนุญาต

ตัวตรวจสอบพลังงานและนาฬิกา

ชิ้นส่วนอิเล็กทรอนิกส์ทุกชิ้นได้รับการออกแบบมาเพื่อทำงานภายในแรงดันไฟฟ้าและกรอบคลื่นความถี่ที่จำกัด เมื่อทำงานภายนอกกรอบนี้ ชิ้นส่วนอิเล็กทรอนิกส์สามารถทำงานผิดปกติได้ และตัวควบคุมความปลอดภัยอาจถูกบายพาส ในการช่วยทำให้มั่นใจว่าแรงดันไฟฟ้าและคลื่นความถี่จะคงอยู่ในช่วงที่ปลอดภัย Secure Enclave มีการออกแบบมาพร้อมกับวงจรการตรวจสอบ วงจรการตรวจสอบเหล่านี้ได้รับการออกแบบมาให้มีกรอบคลื่นการดำเนินการขนาดใหญ่กว่า Secure Enclave ที่เหลือ ถ้าตัวตรวจสอบตรวจพบจุดดำเนินการที่ไม่ถูกต้อง นาฬิกาใน Secure Enclave จะหยุดโดยอัตโนมัติและจะไม่เริ่มการทำงานใหม่จนกว่าจะรีเซ็ต SoC ครั้งต่อไป

เนื้อหาสรุปของคุณสมบัติ Secure Enclave

หมายเหตุ: ผลิตภัณฑ์ A12, A13, S4 และ S5 ที่เปิดตัวครั้งแรกในฤดูใบไม้ร่วงปี 2020 มีส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยรุ่นที่ 2 ในขณะที่ผลิตภัณฑ์รุ่นก่อนหน้าที่ใช้ SoC เหล่านี้จะมีส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยรุ่นที่ 1

SoC	กลไกการปกป้องหน่วยความจำ	พื้นที่จัดเก็บข้อมูลอย่างปลอดภัย	กลไก AES	PKA
A8	การเข้ารหัสและการตรวจสอบสิทธิ์	EEPROM	ยอมรับ	ไม่ยอมรับ
A9	การเข้ารหัสและการตรวจสอบสิทธิ์	EEPROM	การปกป้อง DPA	ยอมรับ
A10	การเข้ารหัสและการตรวจสอบสิทธิ์	EEPROM	การปกป้อง DPA และบิต Seed ที่ล็อคได้	กุญแจที่ผูกกับ OS
A11	การเข้ารหัส การตรวจสอบสิทธิ์ และการป้องกันการเล่นซ้ำ	EEPROM	การปกป้อง DPA และบิต Seed ที่ล็อคได้	กุญแจที่ผูกกับ OS
A12 (อุปกรณ์ Apple ที่วางจำหน่ายก่อนปี 2020)	การเข้ารหัส การตรวจสอบสิทธิ์ และการป้องกันการเล่นซ้ำ	ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยรุ่นที่ 1	การปกป้อง DPA และบิต Seed ที่ล็อคได้	กุญแจที่ผูกกับ OS
A12 (อุปกรณ์ Apple ที่วางจำหน่ายหลังปี 2020)	การเข้ารหัส การตรวจสอบสิทธิ์ และการป้องกันการเล่นซ้ำ	ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยรุ่นที่ 2	การปกป้อง DPA และบิต Seed ที่ล็อคได้	กุญแจที่ผูกกับ OS

SoC	กลไกการปกป้องหน่วยความจำ	พื้นที่จัดเก็บข้อมูลอย่างปลอดภัย	กลไก AES	PKA
A13 (อุปกรณ์ Apple ที่วางจำหน่ายก่อนปี 2020)	การเข้ารหัส การตรวจสอบสิทธิ์ และการป้องกันการเล่นซ้ำ	ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยรุ่นที่ 1	การปกป้อง DPA และบิต Seed ที่ล็อคได้	กุญแจที่ผูกกับ OS และตัวตรวจสอบการบูต
A13 (อุปกรณ์ Apple ที่วางจำหน่ายหลังปี 2020)	การเข้ารหัส การตรวจสอบสิทธิ์ และการป้องกันการเล่นซ้ำ	ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยรุ่นที่ 2	การปกป้อง DPA และบิต Seed ที่ล็อคได้	กุญแจที่ผูกกับ OS และตัวตรวจสอบการบูต
A14, A15	การเข้ารหัส การตรวจสอบสิทธิ์ และการป้องกันการเล่นซ้ำ	ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยรุ่นที่ 2	การปกป้อง DPA และบิต Seed ที่ล็อคได้	กุญแจที่ผูกกับ OS และตัวตรวจสอบการบูต
S3	การเข้ารหัสและการตรวจสอบสิทธิ์	EEPROM	การปกป้อง DPA และบิต Seed ที่ล็อคได้	ยอมรับ
S4	การเข้ารหัส การตรวจสอบสิทธิ์ และการป้องกันการเล่นซ้ำ	ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยรุ่นที่ 1	การปกป้อง DPA และบิต Seed ที่ล็อคได้	กุญแจที่ผูกกับ OS
S5 (อุปกรณ์ Apple ที่วางจำหน่ายก่อนปี 2020)	การเข้ารหัส การตรวจสอบสิทธิ์ และการป้องกันการเล่นซ้ำ	ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยรุ่นที่ 1	การปกป้อง DPA และบิต Seed ที่ล็อคได้	กุญแจที่ผูกกับ OS
S5 (อุปกรณ์ Apple ที่วางจำหน่ายหลังปี 2020)	การเข้ารหัส การตรวจสอบสิทธิ์ และการป้องกันการเล่นซ้ำ	ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยรุ่นที่ 2	การปกป้อง DPA และบิต Seed ที่ล็อคได้	กุญแจที่ผูกกับ OS
S6, S7	การเข้ารหัส การตรวจสอบสิทธิ์ และการป้องกันการเล่นซ้ำ	ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยรุ่นที่ 2	การปกป้อง DPA และบิต Seed ที่ล็อคได้	กุญแจที่ผูกกับ OS
T2	การเข้ารหัสและการตรวจสอบสิทธิ์	EEPROM	การปกป้อง DPA และบิต Seed ที่ล็อคได้	กุญแจที่ผูกกับ OS
ตระกูล M1	การเข้ารหัส การตรวจสอบสิทธิ์ และการป้องกันการเล่นซ้ำ	ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยรุ่นที่ 2	การปกป้อง DPA และบิต Seed ที่ล็อคได้	กุญแจที่ผูกกับ OS และตัวตรวจสอบการบูต

Face ID และ Touch ID

ความปลอดภัยของ Face ID และ Touch ID

รหัสและรหัสผ่านเป็นสิ่งสำคัญสำหรับความปลอดภัยของอุปกรณ์ Apple ในขณะเดียวกัน ผู้ใช้เองก็ต้องการการเข้าถึงอุปกรณ์ของตนเองที่สะดวกสบาย ซึ่งบ่อยครั้งมักจะมีจำนวนการเข้าถึงมากกว่าหนึ่งร้อยครั้งต่อวัน การตรวจสอบสิทธิ์แบบชีวมิติให้วิธีการเก็บรักษาความปลอดภัยของรหัสที่มีความปลอดภัยสูง หรือแม้กระทั่งทำให้รหัสหรือรหัสผ่านนั้นมีความปลอดภัยมากยิ่งขึ้นเนื่องจากไม่จำเป็นจะต้องป้อนรหัสหรือรหัสผ่านด้วยตัวเองบ่อยครั้ง ในขณะที่ให้ความสะดวกในการปลดล็อคอย่างรวดเร็วด้วยการกดนิ้วหรือการเหลือบมอง Face ID และ Touch ID ไม่ได้แทนที่รหัสหรือรหัสผ่าน แต่สามารถช่วยให้การเข้าถึงทำได้รวดเร็วและง่ายดายยิ่งขึ้นในหลายสถานการณ์

สถาปัตยกรรมความปลอดภัยด้านชีวมิติของ Apple จะใช้การแบ่งความรับผิดชอบออกจากกันอย่างเคร่งครัดระหว่างเซ็นเซอร์ชีวมิติและ Secure Enclave และการเชื่อมต่อที่ปลอดภัยระหว่างกัน เซ็นเซอร์จะบันทึกภาพชีวมิติและส่งภาพชีวมิตินั้นไปยัง Secure Enclave อย่างปลอดภัย ระหว่างการลงทะเบียน Secure Enclave จะประมวลผล เข้ารหัส และจัดเก็บข้อมูลแม่แบบของ Face ID และ Touch ID ที่เกี่ยวข้อง ระหว่างการจับคู่ Secure Enclave จะเปรียบเทียบข้อมูลขาเข้าจากเซ็นเซอร์ชีวมิติกับแม่แบบที่จัดเก็บไว้เพื่อพิจารณาว่าจะปลดล็อคอุปกรณ์หรือตอบสนองว่าการจับคู่นั้นถูกต้องหรือไม่ (สำหรับ Apple Pay, Face ID และ Touch ID ในแอป และการใช้งานอื่นๆ) สถาปัตยกรรมรองรับอุปกรณ์ที่มีทั้งเซ็นเซอร์และ Secure Enclave (ตัวอย่างเช่น iPhone, iPad และหลายๆ ระบบของ Mac) รวมถึงความสามารถในการแยกเซ็นเซอร์ออกเป็นอุปกรณ์ต่อพ่วงซึ่งจะถูกจับคู่กับ Secure Enclave ในภายหลังอย่างปลอดภัยใน Mac ที่ใช้ Apple Silicon

ความปลอดภัยของ Face ID

Face ID จะปลดล็อคอุปกรณ์ Apple ที่รองรับได้อย่างปลอดภัยด้วยการมองเพียงครู่เดียว Face ID ใช้การตรวจสอบสิทธิ์ที่ง่ายและปลอดภัยอันเกิดจากระบบกล้อง TrueDepth ซึ่งใช้เทคโนโลยีขั้นสูงที่สามารถสร้างแผนผังรูปทรงเรขาคณิตจากใบหน้าของผู้ใช้ได้อย่างแม่นยำ Face ID ใช้โครงข่ายประสาทเทียมในการระบุการตั้งใจมอง การจับคู่ และการป้องกันการสวมรอย ดังนั้นผู้ใช้จึงสามารถปลดล็อคโทรศัพท์ได้อย่างรวดเร็ว แม้สวมหน้ากากอนามัยไว้เมื่อใช้อุปกรณ์ที่รองรับ Face ID จะปรับไปใช้การเปลี่ยนแปลงของลักษณะโดยอัตโนมัติ และปกป้องความเป็นส่วนตัวและความปลอดภัยของข้อมูลทางชีวมิติของผู้ใช้อย่างรอบคอบ

Face ID ออกแบบมาเพื่อยืนยันการตั้งใจมองของผู้ใช้ มอบการตรวจสอบสิทธิ์ที่สมบูรณ์พร้อมอัตราการจับคู่ผิดต่ำ และจำกัดการสวมรอยทั้งทางดิจิตอลและทางกายภาพ

กล้อง TrueDepth ค้นหาใบหน้าของผู้ใช้โดยอัตโนมัติเมื่อผู้ใช้ปลุกอุปกรณ์ Apple ที่มีระบบทำงาน Face ID (โดยการยกเครื่องขึ้นหรือแตะหน้าจอ) รวมถึงเมื่ออุปกรณ์เหล่านั้นพยายามตรวจสอบสิทธิ์ของผู้ใช้เพื่อแสดงการแจ้งเตือนที่เข้ามา หรือเมื่อแอปที่รองรับขอให้มีการตรวจสอบสิทธิ์โดยใช้ Face ID เมื่อระบบตรวจพบใบหน้า Face ID จะยืนยันการตั้งใจมองและความตั้งใจปลดล็อคโดยตรวจจับว่าผู้ใช้ลืมตาและตั้งใจมองไปยังอุปกรณ์ของพวกเขาหรือไม่ สำหรับการช่วยการเข้าถึง การตรวจสอบการตั้งใจมองของ Face ID จะถูกปิดใช้งานเมื่อเปิดใช้งาน VoiceOver และสามารถปิดใช้งานแยกต่างหากได้หากจำเป็น จำเป็นต้องมีการตรวจจับการตั้งใจมองเสมอเมื่อใช้ Face ID ในขณะที่สวมหน้ากากอนามัย

หลังจากกล้อง TrueDepth ยืนยันใบหน้าที่ตั้งใจมองกล้องแล้ว กล้องจะฉายและอ่านจุดอินฟราเรดหลายพันจุดเพื่อสร้างแผนที่ความลึกของใบหน้าพร้อมกับภาพอินฟราเรด 2D ข้อมูลนี้ใช้เพื่อสร้างลำดับภาพ 2D และแผนที่ความลึก ซึ่งลงชื่อดิจิตอลแล้วส่งไปที่ Secure Enclave ในการต่อต้านการลอกเลียนแบบทางดิจิตอลและทางกายภาพ กล้อง TrueDepth จะสุ่มลำดับการจับภาพภาพ 2D และแผนที่ความลึก และแสดงรูปแบบสุ่มเฉพาะอุปกรณ์ ส่วนของกลไกทางประสาทที่ปลอดภัย ซึ่งปกป้องภายใน Secure Enclave จะแปลงข้อมูลนี้ให้อยู่ในการแสดงเชิงคณิตศาสตร์ แล้วเปรียบเทียบกับข้อมูลใบหน้าที่ลงทะเบียน ข้อมูลใบหน้าที่ลงทะเบียนนี้อยู่ในการแสดงเชิงคณิตศาสตร์ของใบหน้าผู้ใช้ที่จับภาพได้จากการแสดงท่าทางต่างๆ

ความปลอดภัยของ Touch ID

Touch ID คือระบบการจับเซ็นเซอร์ลายนิ้วมือที่ทำให้การเข้าถึงอุปกรณ์ Apple ที่รองรับอย่างปลอดภัยนั้นเร็วขึ้นและง่ายขึ้น เทคโนโลยีนี้อ่านข้อมูลลายนิ้วมือจากหลายๆ มุม และเรียนรู้ลายนิ้วมือของผู้ใช้เพิ่มเติมเมื่อเวลาผ่านไป โดยเซ็นเซอร์จะขยายแผนที่ลายนิ้วมือเมื่อมีโหนดที่ทับซ้อนกันเพิ่มเติมในการใช้งานแต่ละครั้ง

อุปกรณ์ Apple ที่มีเซ็นเซอร์ Touch ID สามารถปลดล็อคโดยใช้ลายนิ้วมือได้ Touch ID ไม่ได้ใช้แทนความจำเป็นในการใช้รหัสของอุปกรณ์หรือรหัสผ่านของผู้ใช้ ซึ่งยังต้องใช้หลังจากการเริ่มต้นทำงานของอุปกรณ์ เริ่มการทำงานเครื่องใหม่ หรือออกจากระบบ (บน Mac) ในบางแอป Touch ID ยังสามารถใช้แทนที่รหัสของอุปกรณ์หรือรหัสผ่านของผู้ใช้ได้อีกด้วย ตัวอย่างเช่น เพื่อปลดล็อคโน้ตที่มีรหัสผ่านปกป้องอยู่ในแอปโน้ต เพื่อปลดล็อคเว็บไซต์ที่มีพวงกุญแจปกป้องอยู่ และเพื่อปลดล็อครหัสผ่านของแอปที่รองรับ อย่างไรก็ตาม บางสถานการณ์จำเป็นต้องใช้รหัสของอุปกรณ์หรือรหัสผ่านของผู้ใช้เสมอ (ตัวอย่างเช่น เพื่อเปลี่ยนรหัสของอุปกรณ์หรือรหัสผ่านของผู้ใช้ที่มีอยู่แล้ว หรือเพื่อเอาการลงทะเบียนลายนิ้วมือที่มีอยู่ออกหรือสร้างการลงทะเบียนลายนิ้วมือใหม่)

เมื่อเซ็นเซอร์ลายนิ้วมือตรวจพบการสัมผัสของนิ้วมือ เซ็นเซอร์จะเปิดการทำงานแถวการจับภาพขั้นสูงเพื่อสแกนนิ้วมือและส่งการสแกนไปยัง Secure Enclave ช่องทางที่ใช้สำหรับทำให้การเชื่อมต่อนี้ปลอดภัยจะแตกต่างกัน ทั้งนี้ขึ้นอยู่กับว่าเซ็นเซอร์ Touch ID มีอยู่ในอุปกรณ์ที่มี Secure Enclave หรือมีอยู่ในอุปกรณ์ต่อพ่วงที่แยกต่างหาก

ในขณะที่การสแกนลายนิ้วมือถูกเปลี่ยนเป็นเวกเตอร์เพื่อการวิเคราะห์ การสแกนแบบแรสเตอร์จะถูกจัดเก็บไว้ชั่วคราวในหน่วยความจำที่เข้ารหัสภายใน Secure Enclave จากนั้นจะถูกลบทิ้ง การวิเคราะห์ใช้การเทียบผังมุมรอยเส้นใต้ผิวหนัง ซึ่งเป็นกระบวนการแบบยึดรายละเอียดหลักซึ่งทิ้ง “ข้อมูลรายละเอียดย่อยๆ ของนิ้วมือ” ที่จำเป็นต่อการสร้างลายนิ้วมือจริงของผู้ใช้ขึ้นมาใหม่ ในระหว่างการลงทะเบียน แผนผังผลลัพธ์ของโหนดจะถูกจัดเก็บในรูปแบบการเข้ารหัสซึ่งสามารถอ่านได้เฉพาะ Secure Enclave เท่านั้นในฐานะแม่แบบสำหรับเปรียบเทียบกับการจับคู่ในอนาคตที่ปราศจากข้อมูลประจำเครื่อง ข้อมูลนี้จะอยู่ในอุปกรณ์ตลอดเวลา และไม่ได้ถูกส่งไปที่ Apple หรือรวมอยู่ในข้อมูลสำรองของอุปกรณ์

ความปลอดภัยช่องทาง Touch ID ในตัวเครื่อง

การสื่อสารระหว่าง Secure Enclave และเซ็นเซอร์ Touch ID ในตัวเครื่องจะเกิดขึ้นบนบัสอินเทอร์เฟซอุปกรณ์ต่อพ่วงแบบอนุกรม หน่วยประมวลผลจะส่งต่อข้อมูลไปยัง Secure Enclave แต่ไม่สามารถอ่านข้อมูลได้ ข้อมูลมีการเข้ารหัสและตรวจสอบสิทธิ์ด้วยกุญแจเซสชั่นที่ติดต่อโดยใช้กุญแจที่แชร์ซึ่งกำหนดสิทธิ์ให้สำหรับเซ็นเซอร์ Touch ID แต่ละตัวและ Secure Enclave ที่สอดคล้องกันจากโรงงาน สำหรับเซ็นเซอร์ Touch ID ทุกชิ้น กุญแจที่แชร์จะมีความปลอดภัย เป็นแบบสุ่ม และมีความแตกต่างกัน การแลกเปลี่ยนกุญแจเซสชั่นจะใช้การห่อกุญแจ AES โดยทั้งสองฝั่งจะมอบกุญแจแบบสุ่มที่สร้างกุญแจเซสชั่นและใช้การเข้ารหัสการขนส่งที่ให้การตรวจสอบสิทธิ์และการรักษาความลับ (โดยใช้ AES-CCM)

Magic Keyboard ที่มี Touch ID

Magic Keyboard ที่มี Touch ID (และ Magic Keyboard ที่มี Touch ID และปุ่มตัวเลข) จะมอบเซ็นเซอร์ Touch ID ในแป้นพิมพ์ภายนอกซึ่งสามารถใช้ได้กับ Mac ที่ใช้ Apple Silicon ทุกรุ่น Magic Keyboard ที่มี Touch ID จะทำหน้าที่เป็นเซ็นเซอร์ชีวมิติ แต่จะไม่จัดเก็บแม่แบบชีวมิติ ไม่ดำเนินการจับคู่ทางชีวมิติ หรือบังคับใช้นโยบายความปลอดภัย (ตัวอย่างเช่น การป้อนรหัสผ่านหลังจากที่ไม่ได้ปลดล็อคอุปกรณ์เป็นเวลา 48 ชั่วโมง) เซ็นเซอร์ Touch ID ใน Magic Keyboard ที่มี Touch ID จะต้องจับคู่กับ Secure Enclave บน Mac อย่างปลอดภัยก่อนที่เซ็นเซอร์นั้นจะสามารถใช้งานได้ จากนั้น Secure Enclave จะดำเนินการการลงทะเบียนและจับคู่การทำงานแล้วบังคับใช้นโยบายความปลอดภัยในรูปแบบเดียวกันกับการจับคู่กับเซ็นเซอร์ Touch ID ในตัวเครื่อง Apple จะดำเนินการกระบวนการจับคู่ในโรงงานสำหรับ Magic Keyboard ที่มี Touch ID ซึ่งมาพร้อมกับ Mac การจับคู่ยังสามารถดำเนินการโดยผู้ใช้ได้อีกด้วย หากจำเป็น Magic Keyboard ที่มี Touch ID สามารถจับคู่อย่างปลอดภัยได้กับ Mac เพียงครั้งละหนึ่งเครื่องเท่านั้น แต่ Mac สามารถรักษาการจับคู่ที่ปลอดภัยกับแป้นพิมพ์ Magic Keyboard ที่มี Touch ID ได้สูงสุดถึงห้าตัว

Magic Keyboard ที่มี Touch ID และเซ็นเซอร์ Touch ID ในตัวเครื่องสามารถใช้งานร่วมกันได้ ถ้ามีการวางนิ้วที่ลงทะเบียนบนเซ็นเซอร์ Touch ID ในตัวของ Mac ลงบน Magic Keyboard ที่มี Touch ID แล้ว ระบบ Secure Enclave ใน Mac จะประมวลผลการจับคู่สำเร็จ และในทางกลับกัน

ในการรองรับการจับคู่และการสื่อสารระหว่าง Secure Enclave ของ Mac กับ Magic Keyboard ที่มี Touch ID แป้นพิมพ์จะมาพร้อมกับบล็อกตัวเร่งดำเนินการกุญแจสาธารณะ (PKA) ของฮาร์ดแวร์ซึ่งมอบการพิสูจน์ยืนยันและกุญแจด้านฮาร์ดแวร์ซึ่งสามารถดำเนินการการประมวลผลด้านการเข้ารหัสที่จำเป็นได้

การจับคู่ที่ปลอดภัย

ก่อนที่ Magic Keyboard ที่มี Touch ID สามารถใช้งานการทำงาน Touch ID ได้ แป้นพิมพ์จะต้องจับคู่อยู่กับ Mac อย่างปลอดภัยก่อน เมื่อต้องการจับคู่ Secure Enclave บน Mac และบล็อก PKA ใน Magic Keyboard ที่มี Touch ID จะแลกเปลี่ยนกุญแจสาธารณะซึ่งมีรากฐานอยู่ใน CA ของ Apple ที่เชื่อถือแล้ว และทั้งสองรายการก็จะใช้กุญแจการพิสูจน์ยืนยันที่ถือโดยฮาร์ดแวร์และ ECDH แบบชั่วคราวเพื่อพิสูจน์ยืนยันข้อมูลจำเพาะของตัวเอง บน Mac ข้อมูลจะได้รับการปกป้องโดย Secure Enclave ส่วนบน Magic Keyboard ที่มี Touch ID ข้อมูลนี้จะได้รับการปกป้องโดยบล็อก PKA หลังจากการจับคู่อย่างปลอดภัย ข้อมูล Touch ID ทั้งหมดที่สื่อสารระหว่าง Mac และ Magic Keyboard ที่มี Touch ID จะถูกเข้ารหัสโดย AES-GCM ซึ่งมีความยาวกุญแจ 256 บิต และด้วยกุญแจ ECDH ชั่วคราวโดยใช้เส้นโค้ง NIST P-256 ตามข้อมูลประจำตัวที่จัดเก็บไว้ (การกดแป้นพิมพ์ปกติจะแลกเปลี่ยนกันโดยใช้การรักษาความปลอดภัยแบบบลูทูธในลักษณะเดียวกับที่แป้นพิมพ์บลูทูธทำ)

ความตั้งใจที่ปลอดภัยในการจับคู่

ในการดำเนินการการทำงาน Touch ID บางรายการเป็นครั้งแรก เช่น การลงทะเบียนลายนิ้วมือใหม่ ผู้ใช้จะต้องยืนยันความตั้งใจของตนเองในการใช้ Magic Keyboard ที่มี Touch ID กับ Mac ความตั้งใจทางกายภาพสามารถยืนยันได้ด้วยการกดปุ่มเปิด/ปิด Mac สองครั้งเมื่อถูกแจ้งโดยอินเทอร์เฟซผู้ใช้ หรือยืนยันด้วยการจับคู่ลายนิ้วมือที่ลงทะเบียนบน Mac ไว้ก่อนหน้านี้ได้สำเร็จ โปรดดูที่ ความตั้งใจที่ปลอดภัยและการเชื่อมต่อกับ Secure Enclave สำหรับข้อมูลเพิ่มเติม

ธุรกรรม Apple Pay สามารถอนุญาตได้ด้วยการจับคู่ Touch ID หรือการป้อนรหัสผ่านผู้ใช้ของ macOS แล้วกดปุ่ม Touch ID สองครั้งบน Magic Keyboard ที่มี Touch ID วิธีการอย่างหลังทำให้ผู้ใช้สามารถยืนยันเจตนาทางกายภาพได้แม้ไม่มีการจับคู่ Touch ID

ความปลอดภัยของช่องทางของ Magic Keyboard ที่มี Touch ID

ในการช่วยให้ช่องทางการสื่อสารระหว่างเซ็นเซอร์ Touch ID ใน Magic Keyboard ที่มี Touch ID และ Secure Enclave บน Mac ที่จับคู่กันอยู่มีความปลอดภัย การสื่อสารจำเป็นต้องมีคุณสมบัติดังต่อไปนี้:

- การจับคู่ที่ปลอดภัยระหว่างบล็อก PKA ของ Magic Keyboard ที่มี Touch ID และ Secure Enclave ตามที่ได้ระบุไว้ข้างต้น
- ช่องทางที่ปลอดภัยระหว่างเซ็นเซอร์ Magic Keyboard ที่มี Touch ID และบล็อก PKA

ช่องทางที่ปลอดภัยระหว่างเซ็นเซอร์ Magic Keyboard ที่มี Touch ID และบล็อก PKA ของแป้นพิมพ์จะถูกสร้างขึ้นในโรงงานโดยใช้กุญแจเฉพาะซึ่งเซ็นเซอร์ของแป้นพิมพ์และบล็อค PKA ใช้ร่วมกัน (วิธีนี้เป็นเทคนิคเดียวกันกับที่ใช้ในการสร้างช่องทางที่ปลอดภัยระหว่าง Secure Enclave บน Mac และเซ็นเซอร์ในตัวเครื่อง สำหรับคอมพิวเตอร์ Mac ที่มี Touch ID ในตัวเครื่อง)

Face ID, Touch ID, รหัส และรหัสผ่าน

ในการใช้ Face ID หรือ Touch ID ผู้ใช้จะต้องตั้งค่าอุปกรณ์ให้ต้องใช้รหัสหรือรหัสผ่านในการปลดล็อค เมื่อ Face ID หรือ Touch ID ตรวจพบการจับคู่ที่ตรงกันสำเร็จ อุปกรณ์ของผู้ใช้จะปลดล็อคโดยไม่ต้องถามรหัสหรือรหัสผ่านของอุปกรณ์ ซึ่งทำให้การใช้รหัสหรือรหัสผ่านที่ยาวและซับซ้อนดูสมเหตุสมผลมากขึ้นเนื่องจากผู้ใช้ไม่จำเป็นต้องใส่รหัสเหล่านั้นบ่อยๆ Face ID และ Touch ID จะไม่แทนที่รหัสหรือรหัสผ่านของผู้ใช้ แต่ระบบทั้งสองนี้ทำให้เข้าถึงอุปกรณ์ได้โดยง่ายภายในขอบเขตและข้อจำกัดด้านเวลา การทำเช่นนี้เป็นสิ่งสำคัญเนื่องจากรหัสหรือรหัสผ่านที่มีความปลอดภัยสูงจะสร้างรากฐานสำหรับวิธีการที่อุปกรณ์ iPhone, iPad, Mac หรือ Apple Watch ของผู้ใช้ปกป้องข้อมูลของผู้ใช้คนนั้นด้วยการเข้ารหัส

เมื่อต้องใช้รหัสหรือรหัสผ่านของอุปกรณ์

ผู้ใช้สามารถใช้รหัสหรือรหัสผ่านของตนแทน Face ID หรือ Touch ID ได้ทุกเมื่อ แต่มีบางสถานการณ์ที่ไม่อนุญาตให้ใช้ข้อมูลทางชีวมิติ การดำเนินการต่อไปนี้ที่ต้องเน้นเรื่องความปลอดภัยต้องป้อนรหัสหรือรหัสผ่านเสมอ:

- การอัปเดตซอฟต์แวร์
- การลบข้อมูลอุปกรณ์
- การดูหรือเปลี่ยนการตั้งค่ารหัส
- การติดตั้งโปรไฟล์การกำหนดค่า
- การปลดล็อคบานหน้าต่างความปลอดภัยและความเป็นส่วนตัวในการตั้งค่าระบบบน Mac
- การปลดล็อคบานหน้าต่างผู้ใช้และกลุ่มในการตั้งค่าระบบบน Mac (หากเปิดใช้ FileVault อยู่)

ต้องใช้รหัสหรือรหัสผ่านหากอุปกรณ์อยู่ในสถานะอย่างหนึ่งอย่างใดดังต่อไปนี้:

- อุปกรณ์เพิ่งถูกเปิดหรือเพิ่งเริ่มการทำงานเครื่องใหม่
- ผู้ใช้ได้ออกจากระบบบัญชี Mac ของพวกเขา (หรือยังไม่ได้เข้าสู่ระบบ)
- ผู้ใช้ไม่ได้ปลดล็อคอุปกรณ์ของตนเป็นเวลานานกว่า 48 ชั่วโมง
- ผู้ใช้ไม่ได้ใช้รหัสหรือรหัสผ่านของตนในการปลดล็อคอุปกรณ์เป็นเวลา 156 ชั่วโมง (หกวันครึ่ง) และผู้ใช้ไม่ได้ใช้ข้อมูลทางชีวมิติในการปลดล็อคอุปกรณ์ของตนภายใน 4 ชั่วโมง
- อุปกรณ์ได้รับคำสั่งล็อคระยะไกล
- ผู้ใช้ออกจากการปิดเครื่อง/SOS ฉุกเฉินด้วยการกดปุ่มเพิ่มระดับเสียงหรือปุ่มลดระดับเสียงและปุ่มพัก/ปลุกค้างไว้พร้อมกันเป็นเวลา 2 วินาที แล้วกดปุ่มยกเลิก
- มีความพยายามในการจับคู่ข้อมูลทางชีวมิติไม่สำเร็จห้าครั้ง (แม้ว่าเพื่อการใช้งาน อุปกรณ์อาจเสนอการป้อนรหัสหรือรหัสผ่านแทนการใช้ข้อมูลทางชีวมิติหลังจากเกิดความล้มเหลวจำนวนน้อยครั้งกว่านี้)

เมื่อเปิดใช้งาน Face ID ในขณะที่สวมหน้ากากอนามัยบน iPhone คุณสมบัติจะใช้งานได้ในอีก 6.5 ชั่วโมงหลังจากผู้ใช้ดำเนินการอย่างใดอย่างหนึ่งต่อไปนี้:

- การพยายามจับคู่ Face ID ได้สำเร็จ (ขณะสวมหรือไม่สวมหน้ากากอนามัย)
- การตรวจสอบรหัสของอุปกรณ์
- การปลดล็อคอุปกรณ์ด้วย Apple Watch

การดำเนินการใดๆ เหล่านี้จะขยายระยะเวลาเพิ่มเติมอีก 6.5 ชั่วโมง

เมื่อเปิดใช้งาน Face ID หรือ Touch ID บน iPhone หรือ iPad แล้ว อุปกรณ์จะล็อคทันทีเมื่อกดปุ่มพัก/ปลุก และอุปกรณ์จะล็อคทุกครั้งที่เข้าสู่โหมดพักเครื่อง Face ID และ Touch ID ต้องใช้การจับคู่ที่สำเร็จ หรือใช้รหัสแทนทุกครั้งที่ปลุกเครื่อง

การใช้ Face ID จะทำให้ความน่าจะเป็นที่สุ่มบุคคลจากประชากรที่สามารถปลดล็อค iPhone หรือ iPad ของผู้ใช้มีน้อยกว่า 1 ใน 1,000,000 รวมถึงเมื่อ Face ID ในขณะที่สวมหน้ากากอนามัย สำหรับ iPhone, iPad, Mac รุ่นต่างๆ ของผู้ใช้ที่มี Touch ID และรุ่นที่มีการจับคู่กับ Magic Keyboard ความน่าจะเป็นจะน้อยกว่า 1 ใน 50,000 ความเป็นไปได้นี้จะสูงขึ้นเมื่อลงทะเบียนลายนิ้วมือ (สูงสุด 1 ใน 10,000 เมื่อมีลายนิ้วมือห้านิ้ว) หรือลักษณะใบหน้า (สูงสุด 1 ใน 500,000 เมื่อมีลักษณะใบหน้าสองลักษณะ) หลายรายการ เพื่อเป็นการป้องกันเพิ่มเติม ทั้ง Face ID และ Touch ID จะอนุญาตให้ทำการพยายามจับคู่ที่ไม่สำเร็จเพียงห้าครั้งเท่านั้นก่อนที่จะขอให้ใช้รหัสหรือรหัสผ่านเพื่อเข้าถึงอุปกรณ์หรือบัญชีของผู้ใช้ การใช้ Face ID จะทำให้ความน่าจะเป็นของการจับคู่ผิดสูงขึ้นในกรณีที่:

- เป็นฝาแฝดและพี่น้องที่หน้าตาเหมือนผู้ใช้
- เด็กอายุต่ำกว่า 13 ปี (เนื่องจากลักษณะใบหน้าที่สร้างความแตกต่างอาจยังไม่พัฒนาเต็มที่)

ความน่าจะเป็นจะเพิ่มขึ้นอีกในสองกรณีนี้ เมื่อใช้ Face ID ในขณะที่สวมหน้ากากอนามัย ถ้าผู้ใช้มีข้อกังวลเกี่ยวกับการจับคู่ผิด Apple ขอแนะนำการใช้รหัสเพื่อตรวจสอบสิทธิ์

ความปลอดภัยของการจับคู่ใบหน้า

การจับคู่ใบหน้าดำเนินการภายใน Secure Enclave โดยใช้โครงข่ายประสาทเทียมที่ได้รับการฝึกฝนมาเพื่อจุดประสงค์ดังกล่าวโดยเฉพาะ Apple ได้พัฒนาการจับคู่ใบหน้าโครงข่ายประสาทเทียมโดยใช้ภาพต่างๆ กว่าพันล้านภาพ รวมถึงอินฟราเรด (IR) และภาพความลึกที่เก็บรวบรวมในการศึกษาที่ดำเนินการภายใต้การยินยอมจากผู้เข้าร่วม จากนั้น Apple จึงทำงานร่วมกับผู้เข้าร่วมจากทั่วโลกเพื่อครอบคลุมกลุ่มผู้คนที่เป็นตัวแทนด้านต่างๆ ไม่ว่าจะเป็นเพศ อายุ เชื้อชาติ และปัจจัยอื่นๆ การศึกษาได้รับการเพิ่มเติมตามความจำเป็นในการมอบระดับความแม่นยำสูงสำหรับผู้ใช้ที่มีความหลากหลายแตกต่างกันไป Face ID ออกแบบมาเพื่อให้ใช้งานได้กับหมวก ผ้าพันคอ แว่นสายตา คอนแท็กเลนส์ และแว่นกันแดดหลายประเภท Face ID ยังรองรับการปลดล็อคในขณะที่สวมหน้ากากอนามัยสำหรับอุปกรณ์ iPhone ตั้งแต่ iPhone 12 และ iOS 15.4 ขึ้นไป นอกจากนี้ยังออกแบบมาเพื่อใช้งานในร่ม กลางแจ้ง และแม้แต่ในที่มืดสนิท โครงข่ายประสาทเทียมเพิ่มเติมที่ได้รับการฝึกฝนมาเพื่อตรวจพบและต่อต้านการลอกเลียนแบบจะป้องกันการพยายามปลดล็อคอุปกรณ์โดยใช้รูปภาพหรือหน้ากาก ข้อมูล Face ID รวมถึงการแสดงเชิงคณิตศาสตร์ของใบหน้าของผู้ใช้ถูกเข้ารหัสและสามารถใช้ได้เฉพาะกับ Secure Enclave ข้อมูลนี้จะอยู่ในอุปกรณ์ตลอดเวลา และไม่ได้ถูกส่งไปที่ Apple หรือรวมอยู่ในข้อมูลสำรองของอุปกรณ์ ข้อมูล Face ID ต่อไปนี้จะถูกบันทึกเข้ารหัสเฉพาะสำหรับใช้โดย Secure Enclave ในระหว่างการทำงานปกติ:

- การแสดงเชิงคณิตศาสตร์ของใบหน้าผู้ใช้จะถูกคำนวณในระหว่างการลงทะเบียน
- การแสดงเชิงคณิตศาสตร์ของใบหน้าผู้ใช้จะถูกคำนวณในระหว่างการพยายามปลดล็อคบางครั้งหากที่ Face ID ถือว่าข้อมูลเหล่านั้นเป็นประโยชน์ในการเพิ่มความแม่นยำในการจับคู่ในอนาคต

ระบบไม่ได้บันทึกภาพใบหน้าที่จับภาพได้ในระหว่างการทำงานปกติ แต่จะละทิ้งในทันทีแทนหลังจากการแสดงเชิงคณิตศาสตร์ได้รับการคำนวณสำหรับการลงทะเบียนหรือการเปรียบเทียบกับข้อมูล Face ID ที่ลงทะเบียนแล้ว

การปรับปรุงการจับคู่ Face ID

ในการปรับปรุงประสิทธิภาพการทำงานการจับคู่ให้ดียิ่งขึ้นและติดตามการเปลี่ยนแปลงตามธรรมชาติของใบหน้าและรูปลักษณ์ Face ID จะเพิ่มความแม่นยำของการแสดงเชิงคณิตศาสตร์ที่จัดเก็บไว้เมื่อเวลาผ่านไป เมื่อจับคู่สำเร็จ ในกรณีที่ข้อมูลมีคุณภาพเพียงพอ Face ID อาจนำการแสดงเชิงคณิตศาสตร์ที่คำนวณใหม่มาใช้อีกเป็นจำนวนครั้งหนึ่งๆ แล้วจึงละทิ้งข้อมูลนั้น ในทางตรงกันข้าม ถ้า Face ID จดจำใบหน้าไม่ได้ แต่คุณภาพการจับคู่สูงกว่าเกณฑ์ที่กำหนดและผู้ใช้ป้อนรหัสหลังจากการล้มเหลวนั้นทันที Face ID จะจับภาพอีกครั้งหนึ่งและนำการแสดงที่คำนวณทางคณิตศาสตร์ใหม่นี้ไปเสริมกับข้อมูล Face ID ที่ลงทะเบียนไว้ ข้อมูล Face ID ใหม่นี้จะถูกยกเลิกหากผู้ใช้หยุดการจับคู่กับข้อมูลดังกล่าวหรือหลังจากจำนวนการจับคู่ที่จำกัด ข้อมูลใหม่จะถูกยกเลิกเช่นกันเมื่อมีการเลือกตัวเลือกในการรีเซ็ต Face ID กระบวนการเสริมเหล่านี้ช่วยให้ Face ID ทันกับการเปลี่ยนแปลงอย่างมากของขนบนใบหน้าหรือการแต่งหน้าของผู้ใช้ และช่วยลดการให้ผ่านสำหรับผู้ที่ไม่ใช่ผู้ใช้จริง

การใช้งานสำหรับ Face ID และ Touch ID

การปลดล็อคอุปกรณ์หรือบัญชีผู้ใช้

เมื่ออุปกรณ์หรือบัญชีล็อค หากมีการปิดใช้ Face ID หรือ Touch ID กุญแจสำหรับคลาสการปกป้องข้อมูลระดับสูงสุดซึ่งอยู่ใน Secure Enclave จะถูกยกเลิก ไฟล์และรายการพวงกุญแจในคลาสนั้นจะไม่สามารถเข้าถึงได้จนกว่าผู้ใช้จะปลดล็อคอุปกรณ์หรือบัญชีโดยป้อนรหัสหรือรหัสผ่านของผู้ใช้

เมื่อเปิดใช้ Face ID หรือ Touch ID อยู่ กุญแจจะไม่ถูกยกเลิกเมื่ออุปกรณ์ล็อค แต่จะถูกห่อไว้กับกุญแจซึ่งมอบให้ระบบย่อยของ Face ID หรือ Touch ID ภายใน Secure Enclave เมื่อผู้ใช้พยายามปลดล็อคอุปกรณ์หรือบัญชี ถ้าอุปกรณ์ตรวจพบการจับคู่ที่สำเร็จ อุปกรณ์จะมอบกุญแจสำหรับแกะห่อกุญแจการปกป้องข้อมูล และจะปลดล็อคอุปกรณ์หรือบัญชี กระบวนการนี้จะให้การป้องกันเพิ่มเติมโดยต้องอาศัยการทำงานร่วมกันระหว่างการปกป้องข้อมูลและระบบย่อยของ Face ID หรือ Touch ID เพื่อปลดล็อคอุปกรณ์

เมื่ออุปกรณ์เริ่มการทำงานเครื่องใหม่ กุญแจที่จำเป็นสำหรับ Face ID หรือ Touch ID เพื่อใช้ในการปลดล็อคอุปกรณ์หรือบัญชีจะถูกยกเลิกโดย Secure Enclave หลังจากปฏิบัติตามเงื่อนไขใดๆ ที่ต้องป้อนรหัสหรือรหัสผ่าน

ทำให้การซื้อสินค้าปลอดภัยด้วย Apple Pay

ผู้ใช้ยังสามารถใช้ Face ID และ Touch ID กับ Apple Pay เพื่อทำให้การซื้อสินค้าในร้านค้า แอป และบนเว็บง่ายดายและปลอดภัยได้อีกด้วย:

- **การใช้ Face ID ในร้านค้า:** ในการอนุญาตการชำระเงินในร้านค้าด้วย Face ID ก่อนอื่นผู้ใช้ต้องยืนยันความตั้งใจชำระเงินโดยกดสองครั้งที่ปุ่มด้านข้าง การคลิกสองครั้งนี้จะบันทึกเจตนาของผู้ใช้โดยใช้คำสั่งนิ้วทางกายภาพที่เชื่อมโยงโดยตรงกับ Secure Enclave และต่อต้านการปลอมแปลงโดยกระบวนการที่เป็นอันตราย จากนั้นผู้ใช้ตรวจสอบสิทธิ์โดยใช้ Face ID ก่อนวางอุปกรณ์ใกล้กับเครื่องอ่านการชำระเงินแบบไร้การสัมผัส ผู้ใช้สามารถเลือกวิธีการชำระเงิน Apple Pay วิธีอื่นได้หลังจากการตรวจสอบสิทธิ์ด้วย Face ID ซึ่งจะต้องตรวจสอบสิทธิ์อีกครั้ง แต่ผู้ใช้ไม่ต้องกดสองครั้งที่ปุ่มด้านข้างอีกครั้ง
- **การใช้ Face ID ในแอปและบนเว็บ:** ในการชำระเงินภายในแอปและบนเว็บ ให้ผู้ใช้ยืนยันความตั้งใจของตนในการชำระเงินโดยกดสองครั้งที่ปุ่มด้านข้าง จากนั้นตรวจสอบสิทธิ์โดยใช้ Face ID เพื่ออนุญาตการชำระเงิน ถ้าธุรกรรมของ Apple Pay ไม่เสร็จสมบูรณ์ภายใน 60 วินาทีที่กดสองครั้งที่ปุ่มด้านข้าง ผู้ใช้ต้องยืนยันความตั้งใจในการชำระเงินอีกครั้งโดยกดสองครั้งที่ปุ่มด้านข้างอีกครั้ง
- **การใช้ Touch ID:** สำหรับ Touch ID ความตั้งใจในการชำระเงินจะยืนยันโดยใช้คำสั่งนิ้วในการเปิดใช้งานเซ็นเซอร์ Touch ID รวมกับการจับคู่ลายนิ้วมือของผู้ใช้ที่สำเร็จ

การใช้ API ที่ระบบให้มา

แอปของบริษัทอื่นสามารถใช้ API ที่ระบบจัดหาให้เพื่อขอให้ผู้ใช้ตรวจสอบสิทธิ์โดยใช้ Face ID หรือ Touch ID หรือรหัส หรือรหัสผ่านได้ และแอปที่รองรับ Touch ID จะรองรับ Face ID โดยอัตโนมัติโดยไม่มีการเปลี่ยนแปลงใดๆ เมื่อใช้ Face ID หรือ Touch ID แอปจะได้รับแจ้งเฉพาะว่าการตรวจสอบสิทธิ์สำเร็จหรือไม่ แอปจะไม่สามารถเข้าถึง Face ID, Touch ID หรือข้อมูลที่เชื่อมโยงกับผู้ใช้ที่ลงทะเบียนได้

การปกป้องรายการพวงกุญแจ

รายการพวงกุญแจยังได้รับการปกป้องด้วย Face ID หรือ Touch ID ได้อีกด้วย โดย Secure Enclave จะปล่อยข้อมูลเมื่อจับคู่สำเร็จหรือด้วยรหัสของอุปกรณ์หรือรหัสผ่านของบัญชีเท่านั้น นักพัฒนาแอปจะมี API เพื่อตรวจสอบยืนยันว่ามีการตั้งรหัสหรือรหัสผ่านโดยผู้ใช้หรือไม่ ก่อนที่จะกำหนดให้ใช้ Face ID หรือ Touch ID หรือรหัสหรือรหัสผ่านเพื่อปลดล็อครายการพวงกุญแจ นักพัฒนาแอปสามารถทำสิ่งใดๆ ต่อไปนี้ได้:

- กำหนดให้การทำงานของ API การตรวจสอบสิทธิ์ไม่กลับไปเรียกขอใช้รหัสผ่านของแอปหรือรหัสของอุปกรณ์ นักพัฒนาแอปสามารถค้นหาว่าผู้ใช้รายใดที่ลงทะเบียน โดยอนุญาตให้ใช้ Face ID หรือ Touch ID เป็นปัจจัยที่สองในแอปที่ให้ความสำคัญกับความปลอดภัยได้
- สร้างและใช้กุญแจการเข้ารหัสแบบเส้นโค้งรูปไข่ (ECC) ภายใน Secure Enclave ที่สามารถปกป้องได้ด้วย Face ID หรือ Touch ID การดำเนินการด้วยกุญแจเหล่านี้จะทำภายใน Secure Enclave เสมอหลังจาก Secure Enclave อนุญาตการใช้งาน

การซื้อสินค้าและการอนุญาตสินค้าที่ซื้อ

ผู้ใช้ยังสามารถกำหนดค่า Face ID หรือ Touch ID เพื่ออนุมัติการซื้อจาก iTunes Store, App Store, Apple Books และอื่นๆ ได้ ดังนั้นผู้ใช้จึงไม่ต้องป้อนรหัสผ่าน Apple ID เมื่อซื้อสินค้า Secure Enclave จะตรวจสอบยืนยันว่ามีการตรวจสอบสิทธิ์แบบชีวมิติเกิดขึ้น จากนั้นจะปล่อยกุญแจ ECC ที่ใช้เพื่อลงชื่อคำขอร้านค้า

ความตั้งใจที่ปลอดภัยและการเชื่อมต่อกับ Secure Enclave

ความตั้งใจที่ปลอดภัยจะมอบวิธีสำหรับยืนยันความตั้งใจของผู้ใช้โดยปราศจากการโต้ตอบกับระบบปฏิบัติการหรือหน่วยประมวลผลแอปพลิเคชัน การเชื่อมต่อคือการเชื่อมโยงทางกายภาพจากปุ่มกายภาพไปยัง Secure Enclave ซึ่งมีให้ใช้งานในอุปกรณ์ต่อไปนี้:

- iPhone X ขึ้นไป
- Apple Watch Series 1 ขึ้นไป
- iPad Pro (ทุกรุ่น)
- iPad Air (2020)
- คอมพิวเตอร์ Mac ที่ใช้ Apple Silicon

เมื่อใช้การเชื่อมโยงนี้ ผู้ใช้สามารถยืนยันความตั้งใจในการดำเนินการการทำงานให้เสร็จสมบูรณ์ได้ด้วยวิธีที่ได้รับการออกแบบมาให้แม้แต่ซอฟแวร์ที่ทำงานโดยสิทธิ์รากแบบพิเศษหรือทำงานในเคอร์เนลไม่สามารถเลียนแบบได้

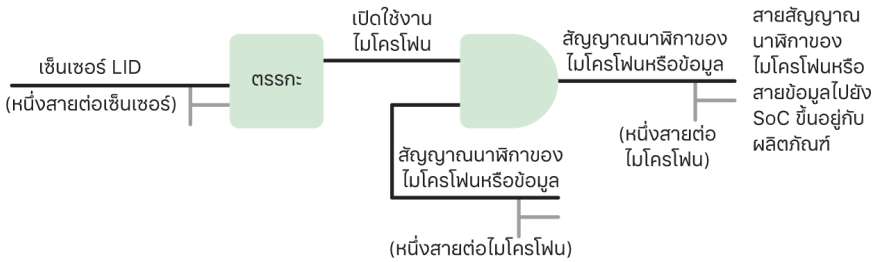
คุณสมบัตินี้จะถูกใช้เพื่อยืนยันความตั้งใจในระหว่างธุรกรรม Apple Pay และเมื่อระบบดำเนินการจับคู่ Magic Keyboard ที่มี Touch ID กับ Mac ที่ใช้ Apple Silicon ให้เสร็จสมบูรณ์ กดสองครั้งบนปุ่มที่เหมาะสม (สำหรับ Face ID) หรือการสแกนลายนิ้วมือ (สำหรับ Touch ID) เมื่อได้รับแจ้งจากอินเทอร์เฟซผู้ใช้ซึ่งส่งสัญญาณเพื่อยืนยันเจตนาของผู้ใช้ โปรดดูที่ ทำให้การซื้อสินค้าปลอดภัยด้วย Apple Pay สำหรับข้อมูลเพิ่มเติม กลไกแบบเดียวกันซึ่งอิงจากเฟิร์มแวร์ Secure Enclave และ T2 จะรองรับบน MacBook รุ่นที่มีชิป Apple T2 Security และไม่มี Touch Bar

การเลิกเชื่อมต่อไมโครโฟนฮาร์ดแวร์

โน้ตบุ๊ก Mac ที่ใช้ Apple Silicon และโน้ตบุ๊ก Mac ที่ใช้ Intel ที่มีชิป Apple T2 Security ทั้งหมดมีการเลิกเชื่อมต่อฮาร์ดแวร์ที่ปิดใช้งานไมโครโฟนเมื่อใดก็ตามที่ฝาบนปิดอยู่ บนโน้ตบุ๊ก MacBook Pro รุ่น 13 นิ้ว และ MacBook Air ทุกเครื่องที่มีชิป T2, โน้ตบุ๊ก MacBook ทุกเครื่องที่มีชิป T2 ตั้งแต่ปี 2019 ขึ้นไป และโน้ตบุ๊ก Mac ที่ใช้ Apple Silicon การเลิกเชื่อมต่อจะใช้ในฮาร์ดแวร์เท่านั้น การเลิกเชื่อมต่อนี้ได้รับการออกแบบมาเพื่อป้องกันไม่ให้ซอฟต์แวร์ใดๆ แม้แต่ซอฟต์แวร์ที่มีรากหรือเคอร์เนลแบบพิเศษใน macOS และแม้แต่ซอฟต์แวร์บนชิป T2 หรือเฟิร์มแวร์อื่นเชื่อมต่อกับไมโครโฟนเมื่อฝาบนปิดอยู่ (กล้องจะไม่เลิกเชื่อมต่อในฮาร์ดแวร์เนื่องจากช่องมุมมองของกล้องจะถูกขวางกั้นโดยสมบูรณ์เมื่อฝาบนปิด)

iPad รุ่นที่เริ่มต้นในปี 2020 จะมีการเลิกเชื่อมต่อไมโครโฟนของฮาร์ดแวร์ด้วย เมื่อใส่เคสที่ตรงตามมาตรฐาน MFi (รวมถึงเคสที่ขายโดย Apple) กับ iPad และปิดเคสอยู่ ไมโครโฟนจะเลิกเชื่อมต่อในฮาร์ดแวร์ วิธีนี้ได้รับการออกแบบมาเพื่อป้องกันไม่ให้ซอฟต์แวร์ใดๆ สามารถใช้งานข้อมูลเสียงไมโครโฟนได้แม้ว่าจะมีสิทธิ์รากหรือเคอร์เนลแบบพิเศษใน iPadOS หรือเฟิร์มแวร์บนอุปกรณ์รุ่นใดก็ตาม

การปกป้องในส่วนนี้จะใช้โดยตรงกับตรรกะฮาร์ดแวร์ตามแผนภาพวงจรต่อไปนี้:



ในแต่ละผลิตภัณฑ์ที่มีการตัดไมโครโฟนแบบฮาร์ดแวร์ เซ็นเซอร์การตรวจจับฝาอย่างน้อยหนึ่งตัวจะตรวจจับการปิดฝาหรือเคสทางกายภาพโดยใช้คุณสมบัติทางกายภาพบางประการ (ตัวอย่างเช่น เซ็นเซอร์เอฟเฟ็กต์ฮอลล์หรือเซ็นเซอร์มุมบานพับ) ของการโต้ตอบ สำหรับเซ็นเซอร์ที่จำเป็นต้องมีการปรับเทียบ พารามิเตอร์จะถูกตั้งค่าในระหว่างการผลิตอุปกรณ์และกระบวนการปรับเทียบจะรวมถึงการป้องกันไม่ให้ฮาร์ดแวร์สามารถผันกลับได้เมื่อมีการเปลี่ยนแปลงพารามิเตอร์ที่มีความอ่อนไหวบนเซ็นเซอร์ในภายหลัง เซ็นเซอร์เหล่านี้จะปล่อยสัญญาณฮาร์ดแวร์ตรงที่จะผ่านไปยังชุดตรรกะฮาร์ดแวร์ที่ไม่สามารถตั้งโปรแกรมใหม่ได้ ตรรกะนี้จะให้การป้องกันการสะท้อนสัญญาณ ฮิสเทอรีซิส และ/หรือการหน่วงสูงถึง 500 ms ก่อนจะปิดใช้งานไมโครโฟน ทั้งนี้ขึ้นอยู่กับผลิตภัณฑ์ สัญญาณนี้สามารถใช้ได้โดยการปิดใช้งานสายการส่งต่อข้อมูลระหว่างไมโครโฟนและชิปบนระบบ (SoC) หรือโดยการปิดใช้งานหนึ่งในสายข้อมูลเข้าไปยังโมดูลไมโครโฟนซึ่งช่วยให้โมดูลเปิดใช้งานได้ ตัวอย่างเช่น สายนาฬิกาหรือการควบคุมที่มีประสิทธิภาพที่คล้ายคลึงกัน

บัตรโดยสารด่วนที่มีพลังงานสำรอง

ถ้า iOS ไม่ได้ทำงานอยู่เนื่องจาก iPhone จำเป็นต้องชาร์จ อุปกรณ์ของคุณยังอาจมีพลังงานเหลืออยู่ในแบตเตอรี่ซึ่งเพียงพอสำหรับการทำธุรกรรมบัตรโดยสารด่วนได้ อุปกรณ์ iPhone ที่รองรับจะรองรับคุณสมบัตินี้โดยอัตโนมัติกับบัตรต่อไปนี้:

- การชำระเงินหรือบัตรโดยสารที่ถูกกำหนดให้เป็นบัตรโดยสารด่วน
- บัตรนักเรียนที่เปิดใช้โหมดเร่งด่วนอยู่
- กุญแจรถที่เปิดใช้โหมดเร่งด่วนอยู่
- กุญแจบ้านที่เปิดโหมดเร่งด่วนไว้
- บัตรรับรองหรือบัตรสำหรับองค์กรที่เปิดใช้โหมดเร่งด่วน

การกดปุ่มด้านข้าง (หรือบน iPhone SE รุ่นที่ 2, ปุ่มโฮม) จะแสดงไอคอนแบตเตอรี่ต่ำ พร้อมด้วยข้อความที่บ่งชี้ว่าสามารถใช้บัตรโดยสารด่วนได้ ตัวควบคุม NFC จะดำเนินธุรกรรมบัตรโดยสารด่วนภายใต้เงื่อนไขเดียวกับตอนที่ iOS ทำงานอยู่ เว้นแต่ว่าจะระบุธุรกรรมโดยใช้การแจ้งเตือนด้วยการสั่นเพียงอย่างเดียว (ไม่มีการแจ้งเตือนที่มองเห็นได้แสดงให้เห็น) บน iPhone SE รุ่นที่ 2 ธุรกรรมที่สำเร็จแล้วอาจใช้เวลาสองสามวินาทีในการแสดงขึ้นบนหน้าจอ คุณสมบัตินี้จะไม่สามารถใช้ได้หากมีการปิดเครื่องโดยผู้ใช้ตามปกติ

ความปลอดภัยของระบบ

ภาพรวมความปลอดภัยของระบบ

ด้วยความสามารถเฉพาะของฮาร์ดแวร์ของ Apple ความปลอดภัยของระบบจะทำหน้าที่ควบคุมการเข้าถึงทรัพยากรระบบในอุปกรณ์ Apple โดยไม่กระทบต่อการใช้งาน ความปลอดภัยของระบบครอบคลุมกระบวนการเริ่มต้นระบบ รายการอัปเดตซอฟต์แวร์ และการปกป้องทรัพยากรระบบของคอมพิวเตอร์ เช่น CPU, หน่วยความจำ, ดิสก์, โปรแกรมซอฟต์แวร์ และข้อมูลที่จัดเก็บอยู่

ระบบปฏิบัติการเวอร์ชั่นล่าสุดของ Apple ถือว่าปลอดภัยที่สุด ส่วนสำคัญของความปลอดภัยของ Apple คือ **การบูตที่ปลอดภัย** ซึ่งจะปกป้องระบบจากการติดมัลแวร์ในขณะบูต การบูตที่ปลอดภัยจะเริ่มต้นในฮาร์ดแวร์และสร้างลำดับการตรวจสอบความน่าเชื่อถือผ่านซอฟต์แวร์ ซึ่งขั้นตอนต่างๆ ได้รับการออกแบบมาเพื่อให้แน่ใจว่าแต่ละขั้นจะเป็นการตรวจสอบว่าลำดับต่อไปจะทำงานอย่างเหมาะสมก่อนที่จะส่งมอบการควบคุม โมเดลความปลอดภัยนี้ไม่เพียงแต่จะรองรับการบูตเริ่มต้นของอุปกรณ์ Apple แต่ยังรองรับโหมดต่างๆ สำหรับการกู้คืนและการอัปเดตที่ตรงเวลาบนอุปกรณ์ Apple อีกด้วย ส่วนประกอบย่อยอย่างชิป T2 และ Secure Enclave ก็ดำเนินการบูตอย่างปลอดภัยของตัวเองเช่นเดียวกัน ทั้งนี้เพื่อช่วยให้แน่ใจว่าส่วนประกอบย่อยเหล่านั้นจะบูตเฉพาะโค้ดที่ใช้งานได้จาก Apple เท่านั้น ระบบการอัปเดตสามารถป้องกันได้แม้กระทั่งการโจมตีแบบดาวน์เกรด ทั้งนี้เพื่อให้อุปกรณ์ไม่สามารถย้อนกลับไปเป็นระบบปฏิบัติการเวอร์ชั่นเก่าได้ (ผู้โจมตีจะทราบวิธีการโจมตี) ซึ่งถือเป็นวิธีหนึ่งในการขโมยข้อมูลของผู้ใช้

อุปกรณ์ Apple ยังมีระบบป้องกันการบูตและรันไทม์เพื่อให้อุปกรณ์ยังคงความสมบูรณ์ในระหว่างการทำงานอย่างต่อเนื่อง Silicon ที่ Apple ออกแบบบน iPhone, iPad, Apple Watch, Apple TV, HomePod และ Mac ที่ใช้ Apple Silicon จะมีสถาปัตยกรรมแบบเดียวกันในการปกป้องความสมบูรณ์ของระบบปฏิบัติการ นอกจากนี้ macOS ยังมีชุดความสามารถด้านการปกป้องที่เพิ่มขึ้นและกำหนดค่าได้เพื่อรองรับรุ่นคอมพิวเตอร์ที่แตกต่างกัน รวมถึงความสามารถต่างๆ ที่รองรับบนแพลตฟอร์มฮาร์ดแวร์ Mac ทุกรุ่นอีกด้วย

การบูตที่ปลอดภัย

กระบวนการบูตสำหรับอุปกรณ์ iOS และ iPadOS

ขั้นตอนแต่ละขั้นตอนของกระบวนการเริ่มต้นทำงานประกอบด้วยส่วนประกอบที่ Apple ลงชื่อรับรองแบบเข้ารหัสเพื่อให้สามารถตรวจสอบความสมบูรณ์ได้ ซึ่งจะทำให้การบูตดำเนินการหลังจากที่ตรวจสอบยืนยันลำดับความน่าเชื่อถือแล้วเท่านั้น ส่วนประกอบเหล่านี้รวมถึงตัวโหลดเริ่มต้นระบบ เคอร์เนล ส่วนขยายเคอร์เนล และเฟิร์มแวร์เบสแบนด์เซลลูลาร์ ลำดับการบูตอย่างปลอดภัยนี้ออกแบบมาเพื่อตรวจสอบยืนยันว่าระดับต่ำที่สุดของซอฟต์แวร์จะไม่ถูกรบกวน

เมื่อเปิดอุปกรณ์ iOS หรือ iPadOS หน่วยประมวลผลแอปพลิเคชันจะเรียกใช้โค้ดจากหน่วยความจำแบบอ่านอย่างเดียวซึ่งเรียกว่า Boot ROM ทันที โค้ดที่เปลี่ยนไม่ได้นี้ซึ่งเป็นที่รู้จักกันว่าคือ**รากของความเชื่อถือฮาร์ดแวร์** จะมีการระบุระหว่างขั้นตอนการผลิตชิป และจะมีการกำหนดความเชื่อถือโดยนัย โค้ด Boot ROM ประกอบด้วยกุญแจสาธารณะของผู้ให้บริการออกใบรับรอง (CA) Apple Root ที่ใช้เพื่อตรวจสอบยืนยันว่าตัวโหลดเริ่มต้นระบบของ iBoot ลงชื่อโดย Apple แล้วก่อนอนุญาตให้โหลด นี่เป็นขั้นตอนแรกในลำดับการตรวจสอบความน่าเชื่อถือซึ่งขั้นตอนแต่ละขั้นเป็นการตรวจสอบว่าลำดับต่อไปมีการลงชื่อโดย Apple เมื่อ iBoot ทำงานเสร็จแล้วจะตรวจสอบยืนยันและใช้งานเคอร์เนลของ iOS หรือ iPadOS สำหรับอุปกรณ์ที่มีหน่วยประมวลผล A9 หรือซีรีส์ A รุ่นก่อนหน้าจะมีการโหลดและตรวจสอบขั้นตอน Low Level Bootloader (LLB) เพิ่มเติมโดย Boot ROM และเมื่อเสร็จแล้วจะโหลดและตรวจสอบยืนยัน iBoot

การโหลดหรือการตรวจสอบยืนยันสถานะดังต่อไปนี้ที่ไม่สำเร็จจะได้รับการจัดการแตกต่างกันไปขึ้นอยู่กับฮาร์ดแวร์:

- **Boot ROM ไม่สามารถโหลด LLB (อุปกรณ์รุ่นที่เก่ากว่า) ได้:** โหมดอัปเกรดเฟิร์มแวร์อุปกรณ์ (DFU)
- **LLB หรือ iBoot:** โหมดการกู้คืน

ในกรณีใดกรณีหนึ่งนี้ อุปกรณ์จะต้องเชื่อมต่อกับ Finder (ใน macOS 10.15 ขึ้นไป) หรือ iTunes (macOS 10.14 หรือก่อนหน้า) ผ่านทาง USB และกู้คืนกลับเป็นการตั้งค่าเริ่มต้นจากโรงงาน

Secure Enclave จะใช้ Boot Progress Register (BPR) ในการจำกัดการเข้าถึงข้อมูลผู้ใช้ในโหมดต่างๆ และจะได้รับการอัปเดตก่อนที่จะเข้าสู่โหมดดังต่อไปนี้:

- **โหมด DFU:** ตั้งค่าด้วย Boot ROM บนอุปกรณ์ที่มี SoC ของ Apple เวอร์ชั่น A12 ขึ้นไป
- **โหมดการกู้คืน:** ตั้งค่าด้วย iBoot บนอุปกรณ์ที่มี SoC ของ Apple เวอร์ชั่น A10, S2 ขึ้นไป

ในอุปกรณ์ที่มีเครือข่ายเซลลูลาร์ ระบบย่อยเบสแบนด์เซลลูลาร์ยังดำเนินการบูตแบบปลอดภัยเพิ่มเติมด้วยซอฟต์แวร์ที่ลงชื่อและกุญแจที่มีการตรวจสอบยืนยันโดยหน่วยประมวลผลของเบสแบนด์ที่คล้ายคลึงกันด้วย

นอกจากนี้ Secure Enclave ยังดำเนินการการบูตที่ปลอดภัยเพื่อตรวจสอบให้แน่ใจว่าซอฟต์แวร์ (sepOS) ได้รับการตรวจสอบยืนยันและลงชื่อโดย Apple แล้ว

การใช้ iBoot ที่ปลอดภัยสำหรับหน่วยความจำ

ใน iOS 14 และ iPadOS 14 นั้น Apple ได้แก้ไข C compiler toolchain ที่ใช้สำหรับสร้างตัวโหลดเริ่มต้นระบบของ iBoot เพื่อปรับปรุงความปลอดภัย โดย toolchain จะใช้รหัสที่ได้รับการออกแบบมาเพื่อป้องกันปัญหาเกี่ยวกับหน่วยความจำและปัญหาความปลอดภัยประเภทต่างๆ ที่เกิดขึ้นโดยทั่วไปในโปรแกรม C ตัวอย่างเช่น วิธีนี้จะช่วยป้องกันช่องโหว่ส่วนใหญ่ในคลาสดังต่อไปนี้:

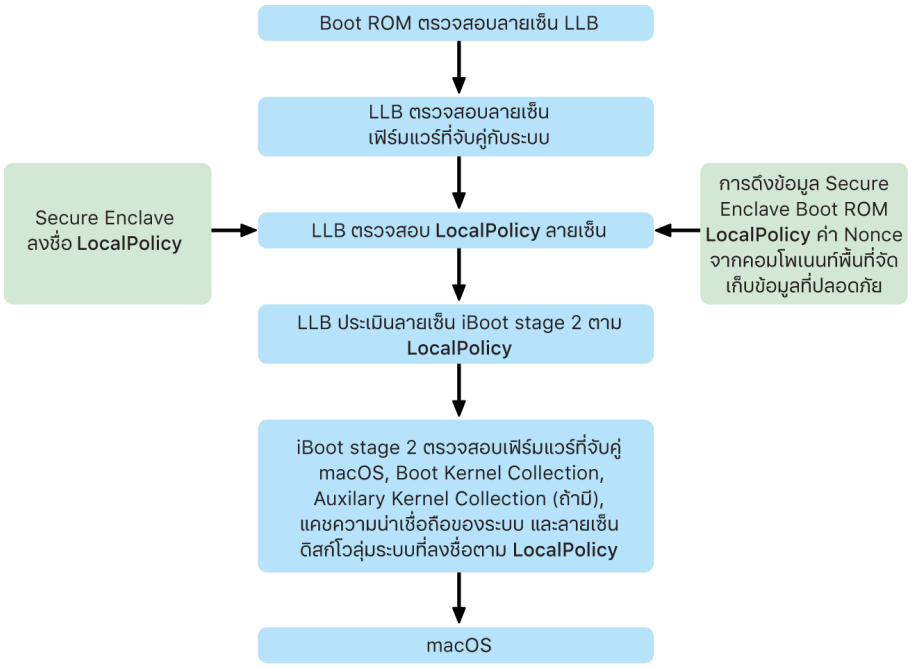
- Buffer overflow โดยตรวจสอบให้แน่ใจว่าตัวชี้ทั้งหมดมีข้อมูลขอบเขตที่ได้รับการตรวจสอบยืนยันแล้วเมื่อมีการเข้าถึงหน่วยความจำ
- Heap exploitation โดยการแยกข้อมูลอีปออกจากเมตาดาต้าและการตรวจจับเงื่อนไขข้อผิดพลาดอย่างแม่นยำ เช่น ข้อผิดพลาด double free
- Type confusion โดยการรับรองว่าตัวชี้ทั้งหมดมีข้อมูลรันไทม์ที่ได้รับการตรวจสอบยืนยันแล้วระหว่างดำเนินการคาสต์ตัวชี้
- Type confusion ที่เกิดจากข้อผิดพลาด use after free โดยแยกการแจกจ่ายหน่วยความจำแบบไดนามิกทั้งหมดตามประเภทแบบคงที่

เทคโนโลยีนี้มีให้ใช้งานบน iPhone ที่มี Apple A13 Bionic ขึ้นไป และ iPad ที่มีชิป A14 Bionic

คอมพิวเตอร์ Mac ที่ใช้ Apple Silicon

กระบวนการบูตสำหรับ Mac ที่ใช้ Apple Silicon

เมื่อเปิด Mac ที่ใช้ Apple Silicon อุปกรณ์จะดำเนินการกระบวนการบูตที่คล้ายกันอย่างมากกับกระบวนการบูตของ iPhone และ iPad



ชิปจะเรียกใช้โค้ดจาก Boot ROM ในขั้นตอนแรกของลำดับการตรวจสอบความน่าเชื่อถือ การบูตอย่างปลอดภัยของ macOS บน Mac ที่ใช้ Apple Silicon ไม่ได้ตรวจสอบยืนยันเพียงโค้ดระบบปฏิบัติการเท่านั้น แต่ยังรวมถึงนโยบายความปลอดภัยและแม้แต่ kext (รองรับ แต่ไม่แนะนำ) ที่กำหนดค่าโดยผู้ใช้ที่ได้รับอนุญาตอีกด้วย

เมื่อเปิดใช้ LLB (ซึ่งย่อมาจาก Low Level Bootstrap) ระบบจะตรวจสอบลายเซ็นและโหลดเฟิร์มแวร์ที่จับคู่กับระบบสำหรับคอร์ SoC ภายใน เช่น พื้นที่จัดเก็บข้อมูล จอภาพ การจัดการระบบ และตัวควบคุม Thunderbolt LLB ยังทำหน้าที่ในการโหลด LocalPolicy อีกด้วย ซึ่งเป็นไฟล์ที่ลงชื่อโดยหน่วยประมวลผล Secure Enclave ไฟล์ LocalPolicy จะอธิบายการกำหนดค่าที่ผู้ใช้เลือกไว้สำหรับการบูตระบบและนโยบายความปลอดภัยของรันไทม์ LocalPolicy มีรูปแบบโครงสร้างข้อมูลเหมือนกับวัตถุการบูตอื่นๆ ทั้งหมด แต่ LocalPolicy จะถูกลงชื่อภายในเครื่องโดยกุญแจส่วนตัวซึ่งมีให้เฉพาะภายใน Secure Enclave ของคอมพิวเตอร์บางเครื่องแทนการลงชื่อโดยเซิร์ฟเวอร์ส่วนกลางของ Apple (เช่น รายการอัปเดตซอฟต์แวร์)

LLB จะต้องค้นดู nonce จาก Secure Enclave ในส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัย เพื่อช่วยป้องกันการเล่นซ้ำของ LocalPolicy ก่อนหน้า ในการทำเช่นนี้ LLB จะใช้ Secure Enclave Boot ROM และตรวจสอบให้แน่ใจว่า Nonce ใน LocalPolicy ตรงกับ Nonce ในส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัย การทำเช่นนี้จะช่วยป้องกันไม่ให้ LocalPolicy เดิมที่อาจได้รับการกำหนดค่าสำหรับความปลอดภัยต่ำถูกปรับใช้กับระบบอีกครั้งหลังจากที่อัปเกรดความปลอดภัย ผลลัพธ์คือ การบูตอย่างปลอดภัยบน Mac ที่ใช้ Apple Silicon ไม่เพียงจะช่วยป้องกันการย้อนกลับของเวอร์ชั่นระบบปฏิบัติการ แต่ยังป้องกันการดาวน์เกรดนโยบายความปลอดภัยอีกด้วย

ไฟล์ LocalPolicy จะบันทึกว่าระบบปฏิบัติการได้รับการกำหนดค่าความปลอดภัยแบบเต็ม ความปลอดภัยลดลง หรือความปลอดภัยที่อนุญาต

- **ความปลอดภัยแบบเต็ม:** ระบบจะทำงานเหมือนกับ iOS และ iPadOS และอนุญาตการบูตซอฟต์แวร์ที่มีให้ใช้ล่าสุดในขณะที่มีการติดตั้งเท่านั้น
- **ความปลอดภัยลดลง:** LLB ถูกสั่งการให้เชื่อถือลายเซ็น “สากล” ที่รวมเข้ากับระบบปฏิบัติการ ซึ่งอนุญาตให้ระบบเรียกใช้ macOS เวอร์ชั่นเก่ากว่าได้ เนื่องจาก macOS เวอร์ชั่นเก่ากว่าจะมีช่องโหว่ที่หลีกเลี่ยงไม่ได้ โหมดความปลอดภัยนี้จึงได้รับการอธิบายว่าเป็น**ความปลอดภัยแบบลดลง** นโยบายระดับนี้ยังเป็นระดับที่จำเป็นในการรองรับการบูตส่วนขยายเคอร์เนล (kext) อีกด้วย
- **ความปลอดภัยที่อนุญาต:** ความปลอดภัยนี้จะทำงานเหมือนความปลอดภัยแบบลดลง ซึ่งจะใช้การตรวจสอบยืนยันลายเซ็นสากลสำหรับ iBoot และอื่นๆ รวมถึงยังบอก iBoot ว่าควรยอมรับวัตถุการบูตบางรายการที่ลงชื่อโดย Secure Enclave ด้วยกุญแจเดียวกันกับที่ลงชื่อ LocalPolicy นโยบายระดับนี้จะรองรับผู้ใช้ที่กำลังสร้าง ลงชื่อ และบูตเคอร์เนล XNU แบบกำหนดเองของตัวเอง

ถ้า LocalPolicy ระบุกับ LLB ว่าระบบปฏิบัติการที่เลือกทำงานในโหมดความปลอดภัยแบบเต็ม LLB จะประเมินลายเซ็นที่ได้รับการปรับให้เป็นส่วนตัวสำหรับ iBoot ถ้าระบบปฏิบัติการทำงานในโหมดความปลอดภัยลดลงหรือความปลอดภัยที่อนุญาต ระบบจะประเมินลายเซ็นสากล ข้อผิดพลาดเกี่ยวกับการตรวจสอบยืนยันลายเซ็นจะทำให้ระบบบูตไปยัง recoveryOS เพื่อให้ตัวเลือกการซ่อมแซม

หลังจาก LLB ส่งต่อไปยัง iBoot ระบบจะโหลดเฟิร์มแวร์ที่จับคู่กับ macOS เช่น เฟิร์มแวร์สำหรับ Neural Engine ที่ปลอดภัย, Always On Processor และเฟิร์มแวร์อื่นๆ นอกจากนี้ iBoot ยังดูข้อมูลเกี่ยวกับ LocalPolicy ที่ส่งมาจาก LLB อีกด้วย ถ้า LocalPolicy ระบุว่าควรมีคอลเลกชั่นเคอร์เนลเสริม (AuxKC) แล้ว iBoot จะค้นหา AuxKC บนระบบไฟล์ ตรวจสอบยืนยันว่าลงชื่อโดย Secure Enclave ด้วยกุญแจเดียวกันกับ LocalPolicy จากนั้นตรวจสอบยืนยันว่าแฮชตรงกันกับแฮชที่จัดเก็บอยู่ใน LocalPolicy ถ้า AuxKC ได้รับการตรวจสอบยืนยันแล้ว iBoot จะวาง AuxKC อยู่ในหน่วยความจำที่มีคอลเลกชั่นเคอร์เนลบูตก่อนที่จะล็อคพื้นที่หน่วยความจำแบบเต็มโดยครอบคลุมคอลเลกชั่นเคอร์เนลบูตและ AuxKC ด้วยการปกป้องความสมบูรณ์ของหน่วยประมวลผลร่วมของระบบ (SCIP) ถ้านโยบายระบุว่าควรมี AuxKC แต่หาไม่พบ ระบบจะดำเนินการบูตเข้าสู่ macOS ต่อไปโดยไม่มี AuxKC นอกจากนี้ iBoot ยังทำหน้าที่ตรวจสอบยืนยันแฮชรากสำหรับดิสก์โวลุ่มระบบที่ลงชื่อ (SSV) อีกด้วย ทั้งนี้เพื่อตรวจสอบให้แน่ใจว่าระบบไฟล์ที่จะต่อเชื่อมเคอร์เนลมีการตรวจสอบยืนยันความสมบูรณ์อย่างเต็มรูปแบบ

โหมดการบูตสำหรับ Mac ที่ใช้ Apple Silicon

Mac ที่ใช้ Apple Silicon มีโหมดการบูตดังที่อธิบายด้านล่าง

โหมด	ปุ่มผสม	คำอธิบาย
macOS	จากสถานะปิดเครื่อง ให้กดปุ่มเปิด/ปิด แล้ว**ปล่อย**	1. Boot ROM ส่งต่อไปยัง LLB 2. LLB โหลดเฟิร์มแวร์ที่จับคู่กับระบบและ LocalPolicy สำหรับ macOS ที่เลือก 3. LLB ล็อคตัวบ่งชี้ใน Boot Progress Register (BPR) ว่ากำลังบูตเข้าสู่ macOS และส่งต่อไปยัง iBoot 4. iBoot โหลดเฟิร์มแวร์ที่จับคู่กับ macOS การแคชความเชื่อถือแบบคงที่ โครงสร้างอุปกรณ์ และคอลเลกชั่นเคอร์เนลบูต 5. ถ้า LocalPolicy อนุญาต iBoot จะโหลดคอลเลกชั่นเคอร์เนลเสริม (AuxKC) ของ kext บริษัทอื่น 6. ถ้า LocalPolicy ไม่ได้ปิดใช้งาน iBoot จะตรวจสอบยืนยันแฮชลายเซ็นรากสำหรับดิสก์โวลุ่มระบบที่ลงชื่อ (SSV)
การจับคู่ recoveryOS	จากสถานะปิดเครื่อง ให้กดปุ่มเปิด/ปิด**ค้าง**ไว้	1. Boot ROM ส่งต่อไปยัง LLB 2. LLB โหลดเฟิร์มแวร์ที่จับคู่กับระบบและ LocalPolicy สำหรับ recoveryOS 3. LLB ล็อคตัวบ่งชี้ใน Boot Progress Register ว่ากำลังบูตเข้าสู่ recoveryOS ที่จับคู่แล้ว และส่งต่อไปยัง iBoot สำหรับ recoveryOS ที่จับคู่แล้ว 4. iBoot โหลดเฟิร์มแวร์ที่จับคู่กับ macOS การแคชความเชื่อถือโครงสร้างอุปกรณ์ และคอลเลกชั่นเคอร์เนลบูต 5. ถ้าการบูต recoveryOS ที่จับคู่แล้วล้มเหลว จะมีการพยายามบูตเข้าสู่ recoveryOS สำรอง **หมายเหตุ:** ไม่อนุญาตให้ดาวน์เกรดความปลอดภัยสำหรับ LocalPolicy ของ recoveryOS ที่จับคู่แล้ว
recoveryOS แบบสำรอง	จากสถานะปิดเครื่อง ให้**กดปุ่มเปิด/ปิดสองครั้งแล้วค้างไว้**	1. Boot ROM ส่งต่อไปยัง LLB 2. LLB โหลดเฟิร์มแวร์ที่จับคู่กับระบบและ LocalPolicy สำหรับ recoveryOS 3. LLB ล็อคตัวบ่งชี้ใน Boot Progress Register ว่ากำลังบูตเข้าสู่ recoveryOS ที่จับคู่แล้ว และส่งต่อไปยัง iBoot สำหรับ recoveryOS 4. iBoot โหลดเฟิร์มแวร์ที่จับคู่กับ macOS การแคชความเชื่อถือโครงสร้างอุปกรณ์ และคอลเลกชั่นเคอร์เนลบูต **หมายเหตุ:** ไม่อนุญาตให้ดาวน์เกรดความปลอดภัยสำหรับ LocalPolicy ของ recoveryOS ที่จับคู่แล้ว
เซฟโหมด	บูตไปยัง recoveryOS ดังกล่าวข้างต้น จากนั้นกด **Shift** ค้างไว้ขณะเลือกดิสก์โวลุ่มเริ่มต้นระบบ	1. บูตไปยัง recoveryOS ดังกล่าวข้างต้น 2. การกดปุ่ม Shift ค้างไว้ในขณะเลือกดิสก์โวลุ่มจะทำให้แอป BootPicker อนุมัติ macOS สำหรับการบูตตามปกติ และยังตั้งค่าตัวแปร `nvram` ที่จะบอก iBoot ไม่ให้โหลด AuxKC ในการบูตครั้งถัดไปด้วย 3. ระบบจะรีบูตและบูตไปยังดิสก์โวลุ่มเป้าหมาย แต่ iBoot จะไม่โหลด AuxKC

ข้อจำกัดสำหรับ recoveryOS ที่จับคู่แล้ว

สำหรับ macOS 12.0.1 ขึ้นไป ทุกการติดตั้ง macOS ใหม่จะมีการติดตั้ง recoveryOS เวอร์ชั่นที่จับคู่แล้วในกลุ่มดิสก์โวลุ่ม APFS ที่เกี่ยวข้องด้วย ผู้ใช้คอมพิวเตอร์ Mac ที่ใช้ Intel จะคุ้นเคยกับการออกแบบนี้แต่สำหรับผู้ใช้คอมพิวเตอร์ Mac ที่มี Apple Silicon จะมีการรับประกันความปลอดภัยและความเข้ากันได้เพิ่มเติม เนื่องจากตอนนี้การติดตั้ง macOS ทุกครั้งมี recoveryOS ที่จับคู่แล้วโดยเฉพาะ ซึ่งช่วยให้มั่นใจว่ามีเพียง recoveryOS จับคู่เฉพาะเท่านั้นที่สามารถดำเนินการดาวน์เกรดความปลอดภัยได้ ซึ่งช่วยปกป้องการติดตั้ง macOS เวอร์ชั่นที่ใหม่กว่าจากการแทรกแซงที่เริ่มต้นจาก macOS เวอร์ชั่นเก่า และในทางกลับกัน

ข้อจำกัดในการจับคู่มีดังนี้:

- การติดตั้ง macOS 11 ทั้งหมดจะจับคู่กับ recoveryOS ถ้าเลือกให้การติดตั้ง macOS 11 บูตเป็นค่าเริ่มต้น recoveryOS จะทำการบูตโดยการกดปุ่มเปิด/ปิดค้างไว้ในขณะที่บูตบน Mac ที่มี Apple Silicon recoveryOS สามารถดาวน์เกรดการตั้งค่าความปลอดภัยของการติดตั้ง macOS 11 ใดๆ ได้ แต่ไม่สามารถดาวน์เกรดการตั้งค่าความปลอดภัยของการติดตั้ง macOS 12.0.1 ได้
- ถ้าเลือกการติดตั้ง macOS 12.0.1 ขึ้นไปให้บูตเป็นค่าเริ่มต้น recoveryOS ที่จับคู่แล้วจะทำการบูตโดยการกดปุ่มเปิด/ปิดค้างไว้เมื่อ Mac เริ่มทำงาน recoveryOS ที่จับคู่แล้วสามารถดาวน์เกรดการตั้งค่าความปลอดภัยสำหรับการติดตั้ง macOS ที่จับคู่แล้วได้ แต่ไม่สามารถดาวน์เกรดการตั้งค่าความปลอดภัยสำหรับการติดตั้ง macOS อื่นๆ

ในการบูตเข้าสู่ recoveryOS ที่จับคู่แล้วสำหรับการติดตั้ง macOS ใดๆ การติดตั้งนั้นจะต้องถูกเลือกเป็นค่าเริ่มต้น ซึ่งทำได้โดยใช้ดิสก์เริ่มต้นระบบในการตั้งค่าระบบหรือโดยการเริ่ม recoveryOS ใดๆ และกดปุ่ม Option ค้างไว้ขณะเลือกดิสก์โวลุ่ม

หมายเหตุ: recoveryOS สำรอง ไม่สามารถดาวน์เกรดการตั้งค่าความปลอดภัยสำหรับการติดตั้ง macOS ใดๆ ได้

การควบคุมนโยบายความปลอดภัยดิสก์เริ่มต้นระบบสำหรับ Mac ที่ใช้ Apple Silicon

ภาพรวม

นโยบายความปลอดภัยบน Mac ที่ใช้ Apple Silicon จะมีให้กับระบบปฏิบัติการที่ติดตั้งแต่ละระบบ ซึ่งแตกต่างจากนโยบายความปลอดภัยบน Mac ที่ใช้ Intel สิ่งนี้หมายความว่าอินสแตนซ์ macOS ที่ติดตั้งอยู่หลายรายการซึ่งมีเวอร์ชั่นและนโยบายความปลอดภัยที่แตกต่างกันจะมีการรองรับบน Mac เครื่องเดียวกัน ด้วยเหตุนี้จึงมีการเพิ่ม **ตัวเลือกระบบปฏิบัติการ**ในยูทิลิตี้ความปลอดภัยของการเริ่มต้นระบบ

บน Mac ที่ใช้ Apple Silicon ยูทิลิตี้ความปลอดภัยของระบบจะระบุสถานะความปลอดภัยโดยรวมของ macOS ที่ผู้ใช้กำหนดค่า เช่น การบูตของ kext หรือการกำหนดค่าของการปกป้องความสมบูรณ์ของระบบ (SIP) ถ้าการเปลี่ยนการตั้งค่าความปลอดภัยจะลดความปลอดภัยลงอย่างมากหรือทำให้ระบบถูกโจมตีได้ง่ายขึ้น ผู้ใช้ต้องเข้าสู่ recoveryOS โดยกดปุ่มเปิด/ปิดค้างไว้ (เพื่อไม่ให้มัลแวร์ทริกเกอร์สัญญาณ และมีเพียงมนุษย์ที่เข้าถึงทางกายภาพเท่านั้นที่จะสามารถทำได้) เพื่อดำเนินการเปลี่ยนแปลง ด้วยเหตุนี้ Mac ที่ใช้ Apple Silicon จึงไม่ใช้ (หรือไม่รองรับ) รหัสผ่านเฟิร์มแวร์ด้วยเช่นกัน การเปลี่ยนแปลงที่สำคัญทั้งหมดมีการปกป้องด้วยการอนุญาตของผู้ใช้อยู่แล้ว โปรดดูที่ การปกป้องความสมบูรณ์ของระบบ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ SIP

ความปลอดภัยแบบเต็มและความปลอดภัยลดลงสามารถตั้งค่าได้โดยใช้ยูทิลิตี้ความปลอดภัยของการเริ่มต้นระบบจาก recoveryOS แต่ความปลอดภัยที่อนุญาตสามารถเข้าถึงได้เฉพาะจากเครื่องมือบรรทัดคำสั่งสำหรับผู้ใช้ที่ยอมรับความเสี่ยงในการทำให้ Mac ของตนเองมีความปลอดภัยลดลงเป็นอย่างมาก

นโยบายความปลอดภัยแบบเต็ม

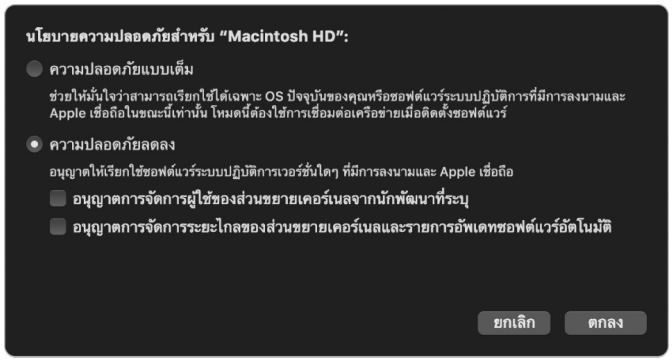
ความปลอดภัยแบบเต็มเป็นค่าเริ่มต้นและทำงานเหมือนกับ iOS และ iPadOS เมื่อดาวน์โหลดและเตรียมการติดตั้งซอฟต์แวร์ แทนที่จะใช้ลายเซ็นสากลที่มาพร้อมกับซอฟต์แวร์ macOS จะสื่อสารกับเซิร์ฟเวอร์การลงชื่อของ Apple เดียวกับที่ใช้สำหรับ iOS และ iPadOS และขอลายเซ็นใหม่ “โดยเฉพาะ” ลายเซ็นจะได้รับการพิจารณาว่าเป็นแบบสำหรับคุณโดยเฉพาะเมื่อรวม Exclusive Chip Identification (ECID) ซึ่งเป็น ID เฉพาะสำหรับ Apple CPU ในกรณีนี้ เป็นส่วนหนึ่งของคำขอลงชื่อ ลายเซ็นที่ได้รับจากเซิร์ฟเวอร์การลงชื่อนั้นจะไม่ซ้ำใครและสามารถใช้งานได้โดย Apple CPU เฉพาะเท่านั้น เมื่อนโยบายด้านความปลอดภัยแบบเต็มมีผลบังคับใช้ Boot ROM และ LLB จะช่วยทำให้มั่นใจว่าลายเซ็นที่ให้มานั้นไม่ได้เพียงแค่ลงชื่อโดย Apple แต่ลงชื่อสำหรับ Mac เครื่องนี้โดยเฉพาะ แล้วผูก macOS เวอร์ชั่นนั้นกับ Mac เครื่องดังกล่าว

การใช้เซิร์ฟเวอร์การลงชื่อทางออนไลน์ยังให้การป้องกันการโจมตีแบบย้อนกลับได้ดีกว่าการใช้ลายเซ็นสากลทั่วไปอีกด้วย ในระบบการลงชื่อแบบสากล epoch ด้านความปลอดภัยสามารถดำเนินการได้หลายครั้ง แต่ระบบที่ไม่เคยเห็นเฟิร์มแวร์รุ่นล่าสุดจะไม่รู้จักสิ่งนี้ ตัวอย่างเช่น คอมพิวเตอร์ที่เชื่อว่าอยู่ใน epoch ด้านความปลอดภัย 1 จะยอมรับซอฟต์แวร์จาก epoch ด้านความปลอดภัย 2 แม้ว่า epoch ด้านความปลอดภัยที่แท้จริงในปัจจุบันคือ 5 ด้วยระบบการลงชื่อทางออนไลน์ในประเภทของ Apple Silicon เซิร์ฟเวอร์การลงชื่อสามารถปฏิเสธการสร้างลายเซ็นสำหรับซอฟต์แวร์ซึ่งจะมีอยู่ในทุกอย่างยกเว้น epoch ด้านความปลอดภัยล่าสุด

นอกจากนี้ ถ้าผู้โจมตีค้นพบช่องโหว่หลังจากเปลี่ยนแปลง epoch ด้านความปลอดภัยแล้ว ผู้โจมตีรายนั้นจะไม่สามารถรับซอฟต์แวร์ที่มีช่องโหว่จาก epoch ก่อนหน้านี้ออกจากระบบ A และนำไปปรับใช้กับระบบ B เพื่อโจมตีได้ ข้อเท็จจริงที่ว่าซอฟต์แวร์ที่มีช่องโหว่จาก epoch เก่าถูกปรับให้เข้ากับระบบ A นั้นจะช่วยทำให้ซอฟต์แวร์ไม่สามารถถ่ายโอนได้และถูกนำมาใช้เพื่อโจมตีระบบ B กลไกเหล่านี้ทั้งหมดจะทำงานร่วมกันเพื่อให้การรับประกันที่หนักแน่นมากยิ่งขึ้นว่าผู้โจมตีจะไม่สามารถวางซอฟต์แวร์ที่มีช่องโหว่ลงบนคอมพิวเตอร์อย่างจงใจเพื่อหลีกเลี่ยงการปกป้องที่ซอฟต์แวร์เวอร์ชั่นล่าสุดมอบให้ได้ แต่ผู้ใช้ที่ครอบครองชื่อผู้ใช้และรหัสผ่านของผู้ดูแลระบบสำหรับ Mac เครื่องนั้นจะสามารถเลือกนโยบายด้านความปลอดภัยที่ใช้งานได้ดีที่สุดสำหรับกรณีการใช้งานของพวกเขาได้เสมอ

นโยบายความปลอดภัยลดลง

การทำงานของนโยบายความปลอดภัยแบบลดลงจะคล้ายกับนโยบายความปลอดภัยปานกลางบน Mac ที่ใช้ Intel ที่มีชิป T2 ซึ่งผู้จำหน่าย (ในกรณีนี้คือ Apple) จะสร้างลายเซ็นดิจิตอลสำหรับโค้ดเพื่อยืนยันว่ามาจากผู้จำหน่าย การออกแบบนี้จะช่วยป้องกันไม่ให้ผู้โจมตีป้อนโค้ดที่ไม่ได้ลงชื่อได้ Apple เรียกลายเซ็นนี้ว่าเป็นลายเซ็น “สากล” เนื่องจากสามารถใช้บน Mac ได้ทุกเครื่องโดยไม่จำกัดจำนวนครั้ง สำหรับ Mac ที่มีชุดนโยบายความปลอดภัยแบบลดลง ความปลอดภัยลดลงไม่ได้ให้การปกป้องจากการโจมตีแบบย้อนกลับด้วยตัวเอง (แม้ว่าการเปลี่ยนแปลงระบบปฏิบัติการโดยไม่ได้รับอนุญาตอาจส่งผลให้ข้อมูลผู้ใช้ถูกทำให้ไม่สามารถเข้าถึงได้ โปรดดูที่ ส่วนขยายเคอร์เนลใน Mac ที่ใช้ Apple Silicon สำหรับข้อมูลเพิ่มเติม



นอกจากจะทำให้ผู้ใช้สามารถเรียกใช้ macOS เวอร์ชั่นเก่ากว่าได้แล้ว ความปลอดภัยแบบลดลงยังต้องใช้สำหรับการทำงานอื่นที่อาจทำให้ความปลอดภัยของระบบของผู้ใช้มีความเสี่ยงอีกด้วย เช่น การใช้ส่วนขยายเคอร์เนลของบริษัทอื่น (kext) kext มีสิทธิ์เท่าเทียมกันกับเคอร์เนล ช่องว่างใดๆ ใน kext ของบริษัทอื่นจึงสามารถนำไปสู่การโจมตีระบบปฏิบัติการแบบเต็มได้ นี่จึงเป็นเหตุผลที่มีการแนะนำนักพัฒนาเป็นอย่างยิ่งให้ใช้ส่วนขยายระบบก่อนที่จะเอาการรองรับ kext ออกจาก macOS สำหรับ Mac ที่ใช้ Apple Silicon ในอนาคต แม้ว่าจะเปิดใช้งาน kext ของบริษัทอื่น ระบบจะไม่สามารถโหลด kext ลงในเคอร์เนลตามคำร้องขอได้ แต่ kext เหล่านั้นจะถูกผสานเข้ากับคอลเลกชั่นเคอร์เนลเสริม (AuxKC) ซึ่งจะมีแฮชที่จัดเก็บอยู่ใน LocalPolicy ดังนั้นจึงต้องมีการรีบูต โปรดดูที่ ส่วนขยายเคอร์เนลใน macOS สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการสร้าง AuxKC

นโยบายความปลอดภัยที่อนุญาต

ความปลอดภัยที่อนุญาตเป็นความปลอดภัยสำหรับผู้ใช้ที่ยอมรับความเสี่ยงในการทำให้ Mac ของตนเองอยู่ในสถานะที่ไม่ปลอดภัยเป็นอย่างมาก โหมดนี้จะแตกต่างจากโหมดไม่มีความปลอดภัยบน Mac ที่ใช้ Intel ที่มีชิป T2 ด้วยความปลอดภัยที่อนุญาต การตรวจสอบยืนยันลายเซ็นยังคงดำเนินการพร้อมกับลำดับการบูตอย่างปลอดภัยทั้งหมด ยกเว้นการตั้งค่านโยบายเป็นความปลอดภัยที่อนุญาตเป็นการส่งสัญญาณให้กับ iBoot ว่าควรยอมรับวัตถุการบูตที่ลงชื่อ Secure Enclave ภายในเครื่อง เช่น คอลเลกชั่นเคอร์เนลบูตที่สร้างโดยผู้ใช้ที่สร้างขึ้นจากเคอร์เนล XNU แบบกำหนดเอง ด้วยวิธีนี้ ความปลอดภัยที่อนุญาตยังมีความสามารถในการเรียกใช้เคอร์เนล “ระบบปฏิบัติการที่ไม่ได้รับการเชื่อถือเต็มรูปแบบ” ตามอำเภอใจได้อีกด้วย เมื่อคอลเลกชั่นเคอร์เนลบูตหรือระบบปฏิบัติการที่ไม่ได้รับการเชื่อถือเต็มรูปแบบโหลดขึ้นบนระบบ กุญแจการถอดรหัสบางรายการอาจใช้งานไม่ได้ วิธีนี้ได้รับการออกแบบมาเพื่อป้องกันไม่ให้ระบบปฏิบัติการที่ไม่ได้รับการเชื่อถือเต็มรูปแบบเข้าถึงข้อมูลจากระบบปฏิบัติการที่เชื่อถือแล้วได้

สิ่งสำคัญ: Apple ไม่มีหรือไม่รองรับเคอร์เนล XNU แบบกำหนดเอง

ความแตกต่างอีกอย่างระหว่างความปลอดภัยแบบอนุญาตกับไม่มีความปลอดภัยบน Mac ที่ใช้ Intel ที่มีชิป T2: ความปลอดภัยที่อนุญาตเป็นข้อกำหนดเบื้องต้นสำหรับการดาวน์เกรดความปลอดภัยบางรายการที่ในอดีตสามารถควบคุมได้อย่างอิสระ โดยเฉพาะอย่างยิ่งในกรณีที่ต้องการปิดใช้งานการปกป้องความสมบูรณ์ของระบบ (SIP) บน Mac ที่ใช้ Apple Silicon ผู้ใช้จะต้องรับทราบว่าตนกำลังนำระบบเข้าสู่ความปลอดภัยแบบอนุญาต ต้องทำเช่นนี้เนื่องจากการปิดใช้งาน SIP จะทำให้ระบบเข้าสู่สถานะที่ทำให้เคอร์เนลถูกโจมตีได้ง่ายมากยิ่งขึ้นอยู่เสมอ โดยเฉพาะการปิดใช้งาน SIP บน Mac ที่ใช้ Apple Silicon จะปิดใช้งานการบังคับใช้ลายเซ็น kext ในระหว่างช่วงเวลาการสร้าง AuxKC ซึ่งทำให้สามารถโหลด kext ตามอำเภอใจใดๆ ไปยังหน่วยความจำเคอร์เนลได้ การปรับปรุง SIP อีกรายการที่มีการดำเนินการบน Mac ที่ใช้ Apple Silicon คือมีการย้ายการจัดเก็บนโยบายออกจาก NVRAM และย้ายไปยัง LocalPolicy ดังนั้นในตอนนี้ การปิดใช้งาน SIP ต้องใช้การตรวจสอบสิทธิ์โดยผู้ใช้ที่มีสิทธิ์เข้าถึงกุญแจที่ลงชื่อ LocalPolicy จาก recoveryOS (เข้าถึงได้โดยกดปุ่มเปิด/ปิดค้างไว้) ซึ่งทำให้ผู้โจมตีเฉพาะซอฟต์แวร์หรือผู้โจมตีทางกายภาพสามารถปิดใช้งาน SIP ได้ยากมากขึ้น

คุณไม่สามารถดาวน์เกรดความปลอดภัยที่อนุญาตจากแอปยูทิลิตี้ความปลอดภัยของการเริ่มต้นระบบได้ ผู้ใช้จะดาวน์เกรดได้ก็ต่อเมื่อเรียกใช้เครื่องมือบรรทัดคำสั่งจากเทอร์มินัลใน recoveryOS เช่น `csrutil` (เพื่อปิดใช้งาน SIP) หลังจากที่ผู้ใช้ดาวน์เกรดแล้ว ข้อเท็จจริงที่สิ่งนี้ได้เกิดขึ้นจะแสดงให้เห็นในยูทิลิตี้ความปลอดภัยของการเริ่มต้นระบบ และด้วยเหตุนี้ ผู้ใช้จึงสามารถตั้งค่าความปลอดภัยเป็นโหมดที่ปลอดภัยยิ่งขึ้นได้อย่างง่ายดาย

หมายเหตุ: Mac ที่ใช้ Apple Silicon ไม่ต้องใช้หรือไม่รองรับนโยบายการบูตสื่อเนื่องจากในความเป็นจริงนั้น การบูตทั้งหมดเกิดขึ้นภายในเครื่อง ถ้าผู้ใช้เลือกที่จะบูตจากสื่อภายนอก เวอร์ชั่นระบบปฏิบัติการนั้นจะต้องมีการปรับให้เป็นส่วนตัวก่อนโดยใช้การรีบูตที่ตรวจสอบสิทธิ์แล้วจาก recoveryOS การรีบูตนี้จะสร้างไฟล์ LocalPolicy บนไดรฟ์ภายในที่จะใช้ดำเนินการบูตที่เชื่อถือจากระบบปฏิบัติการที่จัดเก็บอยู่ในสื่อภายนอก นี่หมายความว่าการกำหนดค่าการบูตจากสื่อภายนอกจะเปิดใช้งานอยู่เสมออย่างชัดเจนโดยขึ้นอยู่กับระบบปฏิบัติการแต่ละระบบ และต้องใช้การอนุญาตของผู้ใช้อยู่แล้ว จึงไม่จำเป็นต้องกำหนดค่าความปลอดภัยเพิ่มเติม

การสร้างและการจัดการกุญแจที่ลงชื่อ LocalPolicy

การสร้าง

เมื่อมีการติดตั้ง macOS เป็นครั้งแรกในโรงงาน หรือเมื่อมีการดำเนินการลบข้อมูลแล้วติดตั้งใหม่แบบเชื่อมต่อนั้น Mac จะเรียกใช้โค้ดจากดิสก์ RAM การกู้คืนแบบชั่วคราวเพื่อกำหนดค่าเริ่มต้นของสถานะเริ่มต้น ในระหว่างกระบวนการนี้ สภาพแวดล้อมการกู้คืนจะสร้างกุญแจสาธารณะและกุญแจส่วนตัวคู่ใหม่ซึ่งจะถูกจัดเก็บใน Secure Enclave กุญแจส่วนตัวเรียกว่า **Owner Identity Key (OIK)** ถ้ามี OIK ใดๆ อยู่ก่อนแล้ว กุญแจจะถูกทำลายในกระบวนการนี้ สภาพแวดล้อมการกู้คืนยังกำหนดค่าเริ่มต้นของกุญแจที่ใช้ในการล็อคการเข้าใช้เครื่องอีกด้วย ซึ่งเรียกว่า **User Identity Key (UIK)** ส่วนหนึ่งของกระบวนการดังกล่าวที่เกิดขึ้นเฉพาะกับ Mac ที่ใช้ Apple Silicon คือเมื่อมีการร้องขอการรับรอง UIK เพื่อการล็อคการเข้าใช้เครื่อง ชุดของข้อจำกัดที่ร้องขอที่จะบังคับใช้เมื่อถึงเวลาตรวจสอบความถูกต้องบน LocalPolicy จะถูกรวมไปด้วย ถ้าอุปกรณ์ไม่สามารถรับรอง UIK สำหรับการล็อคการเข้าใช้เครื่องได้ (ตัวอย่างเช่น เนื่องจากอุปกรณ์ผูกอยู่กับบัญชี "ค้นหา Mac ของฉัน" และถูกแจ้งเป็นอุปกรณ์สูญหาย) อุปกรณ์จะไม่สามารถดำเนินการต่อเพื่อสร้างนโยบายภายในเครื่องได้ ถ้าอุปกรณ์ได้รับการออกใบรับรอง **User identity Certificate (ucrt)** ใบรับรอง ucrt นั้นจะมีข้อจำกัดนโยบายที่กำหนดโดยเซิร์ฟเวอร์และข้อจำกัดนโยบายที่ผู้ใช้ร้องขอในส่วนขยาย X.509 v3

เมื่อดึงข้อมูลการล็อคการเปิดใช้งาน/`ucrt` สำเร็จแล้ว ข้อมูลจะถูกเก็บไว้ในฐานข้อมูลทางฝั่งเซิร์ฟเวอร์และส่งคืนไปยังอุปกรณ์ด้วย เมื่ออุปกรณ์มี ucrt คำขอการรับรองสำหรับกุญแจสาธารณะที่สัมพันธ์กับ OIK จะถูกส่งไปที่เซิร์ฟเวอร์ **Basic Attestation Authority (BAA)** BAA จะตรวจสอบยืนยันคำขอการรับรอง OIK โดยใช้กุญแจสาธารณะจาก ucrt ที่จัดเก็บอยู่ในฐานข้อมูลที่ BAA เข้าถึงได้ ถ้า BAA สามารถตรวจสอบยืนยันการรับรองได้ เซิร์ฟเวอร์จะรับรองกุญแจสาธารณะ แล้วส่งคืน **Owner Identity Certificate (OIC)** ที่ลงชื่อโดย BAA และมีข้อจำกัดที่จัดเก็บใน ucrt OIC จะถูกส่งกลับไปยัง Secure Enclave หลังจากนั้น เมื่อใดก็ตามที่ Secure Enclave ลงชื่อ LocalPolicy ใหม่ ก็จะแนบ OIC ไปกับ Image4 ด้วย LLB มีความเชื่อถือแบบในตัวในใบรับรองราก BAA ซึ่งทำให้ระบบเชื่อถือ OIC ซึ่งส่งผลให้ระบบเชื่อถือลายเซ็น LocalPolicy โดยรวม

ข้อจำกัด RemotePolicy

ไฟล์ Image4 ทั้งหมด ไม่ใช่แค่นโยบายภายในเครื่อง มีข้อจำกัดในการประเมินรายการ Image4 ข้อจำกัดเหล่านี้มีการเข้ารหัสโดยใช้ข้อมูลจำเพาะวัตถุพิเศษ (OID) ในใบรับรองปลายทาง คลังการตรวจสอบยืนยัน Image4 จะค้นหา OID ของข้อจำกัดใบรับรองแบบพิเศษจากใบรับรองในระหว่างการประเมินลายเซ็น แล้วประเมินข้อจำกัดในเชิงกลไกที่ระบุในนั้น ข้อจำกัดมีรูปแบบดังต่อไปนี้:

- ต้องมี X
- ต้องไม่มี X
- X ต้องมีค่าเฉพาะ

ตัวอย่างเช่น สำหรับลายเซ็น “โดยเฉพาะ” ข้อจำกัดใบรับรองจะประกอบด้วย “ต้องมี ECID” และ สำหรับลายเซ็น “สากล” จะต้องประกอบด้วย “ต้องไม่มี ECID” ข้อจำกัดเหล่านี้ได้รับการออกแบบมาเพื่อให้แน่ใจว่าไฟล์ Image4 ทั้งหมดที่ลงชื่อโดยกุญแจที่กำหนดต้องปฏิบัติตามข้อกำหนดบางประการเพื่อหลีกเลี่ยงการสร้างรายการ Image4 ที่ลงชื่อที่มีข้อผิดพลาด

ในบริบทของ LocalPolicy แต่ละไฟล์ ข้อจำกัดใบรับรอง Image4 เหล่านี้จะเรียกว่า **RemotePolicy** RemotePolicy อื่นอาจมีอยู่สำหรับ LocalPolicy ของสภาพแวดล้อมการบูตอื่น RemotePolicy ถูกใช้เพื่อจำกัด LocalPolicy ของ recoveryOS ดังนั้นเมื่อมีการบูต recoveryOS ระบบจะทำงานเหมือนกับการบูตด้วยความปลอดภัยแบบเต็มเท่านั้น การทำเช่นนี้จะเพิ่มความเชื่อถือในความสมบูรณ์ของสภาพแวดล้อมการบูต recoveryOS ซึ่งเป็นที่ที่เปลี่ยนแปลงนโยบายได้ RemotePolicy จะจำกัด LocalPolicy ให้ประกอบด้วย ECID ของ Mac ที่ LocalPolicy ถูกสร้างขึ้น และแฮช Nonce ของนโยบายระยะไกล (`rpnh`) เฉพาะที่จัดเก็บอยู่ในส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยบน Mac `rpnh` และ RemotePolicy จะเปลี่ยนแปลงเฉพาะเมื่อมีการทำงานสำหรับ “ค้นหา Mac ของฉัน” และการล็อคการเข้าใช้เครื่อง เช่น การลงทะเบียน การเลิกลงทะเบียน การล็อคระยะไกล และการลบล้างจากทางไกล ข้อจำกัดของนโยบายระยะไกลจะมีการกำหนดและระบุเมื่อมีการรับรอง User Identity Key (UIK) และจะมีการลงชื่อเข้า User identity Certificate (ucrt) ที่ออกให้ ข้อจำกัดบางรายการของนโยบายระยะไกล เช่น ECID, ChipID และ BoardID จะถูกกำหนดโดยเซิร์ฟเวอร์ วิธีนี้ได้รับการออกแบบมาเพื่อป้องกันอุปกรณ์ไม่ให้ลงชื่อไฟล์ LocalPolicy สำหรับอุปกรณ์เครื่องอื่น ข้อจำกัดอื่นๆ ของนโยบายระยะไกลอาจระบุโดยอุปกรณ์เพื่อช่วยป้องกันการดาวน์เกรดความปลอดภัยของ Local Policy โดยไม่ดำเนินการทั้งการตรวจสอบสิทธิ์ภายในเครื่องที่จำเป็นต่อการเข้าถึง OIK ปัจจุบันและการตรวจสอบสิทธิ์ระยะไกลของบัญชีที่มีการล็อคการเข้าใช้อุปกรณ์

เนื้อหาของไฟล์ LocalPolicy สำหรับ Mac ที่ใช้ Apple Silicon

LocalPolicy คือไฟล์ Image4 ที่ลงชื่อด้วย Secure Enclave Image4 อยู่ในรูปแบบโครงสร้างข้อมูลที่เข้ารหัส ASN.1 (Abstract Syntax Notation One) DER ซึ่งใช้สำหรับอธิบายข้อมูลเกี่ยวกับวัตถุลำดับการบูตอย่างปลอดภัยบนแพลตฟอร์ม Apple ในโมเดลการบูตอย่างปลอดภัยที่ใช้ Image4 ระบบจะขอนโยบายความปลอดภัยเมื่อเริ่มการติดตั้งซอฟต์แวร์โดยคำขอการลงชื่อไปยังเซิร์ฟเวอร์การลงชื่อส่วนกลางของ Apple ถ้านโยบายเป็นที่ยอมรับ เซิร์ฟเวอร์การลงชื่อจะส่งกลับไฟล์ Image4 ที่ลงชื่อ ซึ่งประกอบด้วยรหัสอักขระสี่ตัว (4CC) ที่หลากหลาย โดยไฟล์ Image4 ที่ลงชื่อและ 4CC เหล่านี้จะได้รับการประเมินเมื่อเริ่มต้นระบบโดยซอฟต์แวร์ เช่น Boot ROM หรือ LLB

การส่งต่อความเป็นเจ้าของระหว่างระบบปฏิบัติการต่างๆ

การเข้าถึง Owner Identity Key (OIK) เรียกว่า "ความเป็นเจ้าของ" ความเป็นเจ้าของเป็นสิ่งจำเป็นที่ทำให้ผู้ใช้สามารถลงชื่อ LocalPolicy อีกครั้งหลังจากเปลี่ยนแปลงนโยบายหรือซอฟต์แวร์ได้ OIK ได้รับการปกป้องด้วยลำดับชั้นกุญแจเดียวกันกับที่อธิบายใน Sealed Key Protection (SKP) โดยที่ OIK ได้รับการปกป้องด้วยกุญแจการเข้ารหัสกุญแจ (KEK) แบบเดียวกันกับกุญแจการเข้ารหัสดิสก์โวลุ่ม (VEK) ซึ่งหมายความว่าโดยปกติแล้วกุญแจจะได้รับการปกป้องจากทั้งรหัสผ่านของผู้ใช้และการวัดของระบบปฏิบัติการและนโยบาย ระบบปฏิบัติการทั้งหมดบน Mac มี OIK เพียงรายการเดียวเท่านั้น ดังนั้น เมื่อติดตั้งระบบปฏิบัติการที่สอง ผู้ใช้บนระบบปฏิบัติการแรกจะต้องให้การยินยอมอย่างชัดแจ้งเพื่อส่งต่อความเป็นเจ้าของให้กับผู้ใช้บนระบบปฏิบัติการที่สอง อย่างไรก็ตาม ยังไม่มีผู้ใช้สำหรับระบบปฏิบัติการที่สองเมื่อตัวติดตั้งทำงานจากระบบปฏิบัติการแรก โดยปกติแล้ว ผู้ใช้ในระบบปฏิบัติการจะไม่ถูกสร้างขึ้นจนกว่าจะมีการบูตระบบปฏิบัติการและผู้ช่วยตั้งค่าทำงานอยู่ การทำงานใหม่สองรายการที่ต้องใช้เมื่อติดตั้งระบบปฏิบัติการที่สองบน Mac ที่ใช้ Apple Silicon:

- การสร้าง LocalPolicy สำหรับระบบปฏิบัติการที่สอง
- การเตรียม "ติดตั้งผู้ใช้" เพื่อส่งต่อความเป็นเจ้าของ

เมื่อเรียกใช้ผู้ช่วยติดตั้งและกำหนดเป้าหมายการติดตั้งสำหรับดิสก์โวลุ่มที่สองที่ว่างเปล่า การแจ้งจะถามผู้ใช้ว่าต้องการคัดลอกผู้ใช้จากดิสก์โวลุ่มปัจจุบันไปเป็นผู้ใช้คนแรกของดิสก์โวลุ่มที่สองหรือไม่ ถ้าผู้ใช้ตอบตกลง "ติดตั้งผู้ใช้" ที่ถูกสร้างขึ้น แท้จริงแล้วจะเป็น KEK ซึ่งมาจากรหัสผ่านของผู้ใช้ที่เลือกอยู่และกุญแจฮาร์ดแวร์ ซึ่งต่อมาจะถูกใช้เพื่อเข้ารหัส OIK ขณะที่ถูกส่งไปยังระบบปฏิบัติการที่สอง จากนั้นจากภายในผู้ช่วยติดตั้งของระบบปฏิบัติการที่สอง กุญแจจะร้องขอรหัสผ่านของผู้ใช้คนนั้น เพื่อให้สามารถเข้าถึง OIK ใน Secure Enclave สำหรับระบบปฏิบัติการใหม่ได้ ถ้าผู้ใช้เลือกที่จะไม่คัดลอกผู้ใช้ ติดตั้งผู้ใช้จะยังคงถูกสร้างในลักษณะเดียวกัน แต่จะมีการใช้รหัสผ่านที่ว่างเปล่าแทนรหัสผ่านของผู้ใช้ วิธีการที่สองนี้จะเกิดขึ้นในสถานการณ์การจัดการระบบบางสถานการณ์ อย่างไรก็ตาม ผู้ใช้ที่ต้องการติดตั้งในหลายดิสก์โวลุ่มและต้องการดำเนินการส่งต่อความเป็นเจ้าของด้วยวิธีการที่ปลอดภัยที่สุดควรเลือกที่จะคัดลอกผู้ใช้จากระบบปฏิบัติการแรกไปยังระบบปฏิบัติการที่สองเสมอ

LocalPolicy บน Mac ที่ใช้ Apple Silicon

สำหรับ Mac ที่ใช้ Apple Silicon การควบคุมนโยบายความปลอดภัยภายในเครื่องได้ถูกมอบหมายไปยังแอปพลิเคชันที่ทำงานใน Secure Enclave ซอฟต์แวร์นี้สามารถใช้เอกสารสิทธิ์ของผู้ใช้และโหมดการบูตของ CPU หลักเพื่อกำหนดคนที่จะสามารถเปลี่ยนนโยบายความปลอดภัยและเปลี่ยนจากสภาพแวดล้อมการบูตแบบใดได้ กระบวนการนี้จะช่วยป้องกันไม่ให้ซอฟต์แวร์ที่ประสงค์ร้ายใช้การควบคุมนโยบายความปลอดภัยกับผู้ใช้โดยดาวน์เกรดการควบคุมเพื่อเพิ่มสิทธิ์มากขึ้นได้

คุณสมบัติรายการ LocalPolicy

ไฟล์ LocalPolicy ประกอบด้วย 4CC ในเชิงสถาปัตยกรรมบางรายการที่พบได้ในไฟล์ Image4 ส่วนใหญ่ทั้งหมด เช่น ID บอร์ดหรือโมเดล (BORD), การบ่งชี้ชิปของ Apple โดยเฉพาะ (CHIP) หรือ Exclusive Chip Identification (ECID) แต่ 4CC ที่อยู่ด้านล่างมุ่งเน้นเฉพาะนโยบายความปลอดภัยที่ผู้ใช้สามารถกำหนดค่าได้

หมายเหตุ: Apple ใช้คำว่า **Paired One True recoveryOS (1TR)** เพื่อระบุการบูตเข้าสู่ recoveryOS ที่จับคู่แล้วโดยใช้ปุ่มเปิด/ปิดทางกายภาพแบบกดครั้งเดียวค้างไว้ ซึ่งแตกต่างจากการบูต recoveryOS ปกติซึ่งเกิดขึ้นโดยใช้ NVRAM หรือการกดสองครั้งค้างไว้ หรืออาจเกิดขึ้นเมื่อเกิดข้อผิดพลาดในการเริ่มต้นระบบ การกดปุ่มทางกายภาพบางลักษณะจะช่วยเพิ่มความมั่นใจว่าสภาพแวดล้อมการบูตไม่สามารถเข้าถึงได้โดยผู้โจมตีเฉพาะซอฟต์แวร์ที่บุกเข้ามาใน macOS

แฮช Nonce ของ LocalPolicy (lpnh)

- **ประเภท:** OctetString (48)
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR, recoveryOS, macOS
- **คำอธิบาย:** `lpnh` ใช้สำหรับป้องกันการเล่นซ้ำของ LocalPolicy นี่คือแฮช SHA384 ของ LocalPolicy Nonce (LPN) ซึ่งจัดเก็บอยู่ในส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัย และสามารถเข้าถึงได้โดยใช้ Secure Enclave Boot ROM หรือ Secure Enclave หน่วยประมวลผลแอปพลิเคชันไม่สามารถมองเห็น Nonce แบบดิบ มีเพียง sepOS เท่านั้นที่มองเห็นได้ ผู้โจมตีที่ต้องการโน้มน้าว LLB ว่า LocalPolicy ที่ผู้โจมตีบันทึกไว้ก่อนหน้านี้ถูกต้องจะต้องวางค่าลงในส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัย ซึ่งจะแฮชเป็นค่า `lpnh` เดียวกันที่พบใน LocalPolicy ที่ต้องการเล่นซ้ำ โดยปกติแล้วจะมี LPN เพียงรายการเดียวที่ถูกต้องบนระบบ ยกเว้นในระหว่างการอัปเดตซอฟต์แวร์ ซึ่งจะมี LPN สองรายการที่มีความถูกต้องพร้อมกันเพื่อให้มีโอกาสในการกลับไปยังการบูตซอฟต์แวร์เดิมในกรณีที่เกิดข้อผิดพลาดในการอัปเดต เมื่อ LocalPolicy สำหรับระบบปฏิบัติการใดๆ มีการเปลี่ยนแปลง นโยบายทั้งหมดจะถูกลงชื่อใหม่ด้วยค่า **lpnh** ใหม่ที่สอดคล้องกับ LPN ใหม่ที่พบในส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัย การเปลี่ยนแปลงนี้เกิดขึ้นเมื่อผู้ใช้เปลี่ยนการตั้งค่าความปลอดภัยหรือสร้างระบบปฏิบัติการใหม่ที่มี LocalPolicy สำหรับแต่ละระบบ

แฮช Nonce ของนโยบายระยะไกล (rpnh)

- **ประเภท:** OctetString (48)
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR, recoveryOS, macOS
- **คำอธิบาย:** `rpnh` นี้จะทำงานเหมือนกับ `lpnh` แต่จะได้รับการอัปเดตเฉพาะเมื่อนโยบายระยะไกลได้รับการอัปเดต เช่น เมื่อเปลี่ยนสถานะของการลงทะเบียน “ค้นหาของฉัน” การเปลี่ยนแปลงนี้เกิดขึ้นเมื่อผู้ใช้เปลี่ยนสถานะ “ค้นหาของฉัน” บน Mac ของตน

แฮช Nonce ของ recoveryOS (ronh)

- **ประเภท:** OctetString (48)
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR, recoveryOS, macOS
- **คำอธิบาย:** `ronh` ทำงานในลักษณะเดียวกับ lpnh แต่พบได้เฉพาะใน LocalPolicy สำหรับระบบ recoveryOS เท่านั้น จะมีการอัปเดตเมื่อมีการอัปเดตระบบ recoveryOS เช่น การอัปเดตซอฟต์แวร์ Nonce ที่แยกจาก `lpnh` และ `rpnh` จะถูกใช้เพื่อที่ว่าเมื่ออุปกรณ์ถูกบังคับปิดใช้งานโดย “ค้นหาของฉัน” แล้ว ระบบปฏิบัติการที่มีอยู่จะสามารถปิดใช้งานได้ (โดยเอา LPN และ RPN ออกจากส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัย) ในขณะที่ยังคงปล่อยให้ recoveryOS ระบบบูตได้ ด้วยวิธีนี้ ระบบปฏิบัติการจะสามารถเปิดใช้งานอีกครั้งได้เมื่อเจ้าของระบบพิสูจน์สิทธิ์ในการควบคุมระบบโดยใส่รหัสผ่าน iCloud ของตนที่ใช้กับบัญชี “ค้นหาของฉัน” การเปลี่ยนแปลงนี้เกิดขึ้นเมื่อผู้ใช้อัปเดตระบบ recoveryOS หรือสร้างระบบปฏิบัติการใหม่

แฮชรายการ Image4 ในขั้นตอนถัดไป (nsih)

- **ประเภท:** OctetString (48)
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR, recoveryOS, macOS
- **คำอธิบาย:** ช่อง **nsih** แสดงถึงแฮช SHA384 ของโครงสร้างข้อมูลรายการ Image4 ซึ่งอธิบาย macOS ที่บูต รายการ Image4 ใน macOS ประกอบด้วยการวัดวัตถุการบูตทั้งหมด เช่น iBoot, การแคชความเชื่อถือแบบคงที่, โครงสร้างอุปกรณ์, คอลเลกชั่นเคอร์เนลบูต และแฮชรากดิสก์โวลุ่มสำหรับดิสก์โวลุ่มระบบที่ลงชื่อ (SSV) เมื่อ LLB ถูกสั่งการให้บูต macOS ที่กำหนด LLB วิธีนี้ได้รับการออกแบบมาเพื่อให้แน่ใจว่ารายการ Image4 ใน macOS ที่แนบกับ iBoot ตรงกับที่บันทึกไว้ในช่อง `nsih` ของ LocalPolicy วิธีนี้ `nsih` จะบันทึกเจตนาของผู้ใช้เกี่ยวกับระบบปฏิบัติการที่ผู้ใช้ได้สร้าง LocalPolicy ไว้ ผู้ใช้จะเปลี่ยนค่า `nsih` โดยนัยเมื่อดำเนินการอัปเดตซอฟต์แวร์

แฮชนโยบาย (auxp) คอลเลกชั่นเคอร์เนลเสริม (AuxKC)

- **ประเภท:** OctetString (48)
- **สภาพแวดล้อมที่ผันแปรได้:** macOS
- **คำอธิบาย:** `auxp` คือแฮช SHA384 ของนโยบายรายการ kext ที่ผู้ใช้อนุญาต (UAKL) สิ่งนี้จะใช้ในระหว่างการสร้าง AuxKC เพื่อช่วยให้แน่ใจว่ามีเพียง kext ที่ผู้ใช้อนุญาตรวมอยู่ใน AuxKC เท่านั้น `smb2` เป็นข้อกำหนดเบื้องต้นสำหรับตั้งค่าช่องนี้ ผู้ใช้จะเป็นผู้เปลี่ยนค่า `auxp` โดยนัยเมื่อเปลี่ยน UAKL ด้วยการอนุญาต kext จากบานหน้าต่างความปลอดภัยและความเป็นส่วนตัวในการตั้งค่าระบบ

แฮชรายการ Image4 (auxi) คอลเลกชั่นเคอร์เนลเสริม (AuxKC)

- **ประเภท:** OctetString (48)
- **สภาพแวดล้อมที่ผันแปรได้:** macOS
- **คำอธิบาย:** หลังจากที่ระบบตรวจสอบยืนยันว่าแฮช UAKL ตรงกับแฮชที่พบในช่อง `auxp` ของ LocalPolicy ระบบจะขอให้ AuxKC ลงชื่อโดยแอปพลิเคชันหน่วยประมวลผล Secure Enclave ที่รับผิดชอบในการลงชื่อ LocalPolicy จากนั้นแฮช SHA384 ของลายเซ็นรายการ Image4 ของ AuxKC จะถูกวางลงใน LocalPolicy เพื่อหลีกเลี่ยงโอกาสในการผสมและจับคู่ AuxKC ที่ลงชื่อไว้ก่อนหน้านี้กับระบบปฏิบัติการเมื่อมีการบูต ถ้า iBoot พบช่อง `auxi` ใน LocalPolicy แล้ว iBoot จะพยายามโหลด AuxKC จากพื้นที่จัดเก็บข้อมูลแล้วตรวจสอบความถูกต้องของลายเซ็น iBoot ยังตรวจสอบยืนยันแฮชของรายการ Image4 ที่แนบมากับ AuxKC ว่าตรงกับค่าที่พบในช่อง `auxi` หรือไม่อีกด้วย ถ้า AuxKC โหลดไม่สำเร็จด้วยเหตุผลใดก็ตาม ระบบจะดำเนินการบูตต่อไปโดยไม่มีวัตถุการบูตนี้และ (ดังนั้น) ไม่มี kext ของบริษัทอื่นถูกโหลด ช่อง `auxp` เป็นข้อกำหนดเบื้องต้นสำหรับการตั้งค่าช่อง auxi ใน LocalPolicy ผู้ใช้จะเป็นผู้เปลี่ยนค่า `auxi` โดยนัยเมื่อเปลี่ยน UAKL ด้วยการอนุญาต kext จากบานหน้าต่างความปลอดภัยและความเป็นส่วนตัวในการตั้งค่าระบบ

แฮชคำขอ (auxr) คอลเลกชั่นเคอร์เนลเสริม (AuxKC)

- **ประเภท:** OctetString (48)
- **สภาพแวดล้อมที่ผันแปรได้:** macOS
- **คำอธิบาย:** `auxr` คือแฮช SHA384 ของคำขอ AuxKC ซึ่งระบุชุดที่ตรงกันของ kext ที่มีอยู่ใน AuxKC โดยคำขอ AuxKC อาจเป็นชุดย่อยของ UAKL เนื่องจาก kext สามารถแยกออกจาก AuxKC ได้แม้ว่าจะได้รับอนุญาตจากผู้ใช้ก็ตาม หากทราบว่าใช้สำหรับการโจมตี นอกจากนี้ kext บางรายการซึ่งสามารถใช้เพื่อทำลายขอบเขตเคอร์เนลของผู้ใช้อาจนำไปสู่ฟังก์ชั่นการทำงานที่ลดลง เช่น ไม่สามารถใช้ Apple Pay หรือเล่นเนื้อหา 4K และ HDR ได้ ผู้ใช้ที่ต้องการให้มีความสามารถเหล่านี้จะเลือกใช้การรวม AuxKC ที่มีข้อจำกัดเพิ่มเติม ช่อง `auxp` เป็นข้อกำหนดเบื้องต้นสำหรับการตั้งค่าช่อง `auxr` ใน LocalPolicy ผู้ใช้จะเป็นผู้เปลี่ยนค่า `auxr` โดยนัยเมื่อสร้าง AuxKC ใหม่จากบานหน้าต่างความปลอดภัยและความเป็นส่วนตัวในการตั้งค่าระบบ

แฮชรายการ Image4 CustomOS (coih)

- **ประเภท:** OctetString (48)
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR
- **คำอธิบาย:** `coih` คือแฮช SHA384 ของรายการ Image4 CustomOS เพย์โหลดสำหรับรายการนั้นจะถูกใช้โดย iBoot (แทนที่จะเป็นเคอร์เนล XNU) ในการถ่ายโอนการควบคุม ผู้ใช้จะเป็นผู้เปลี่ยนค่า `coih` โดยนัยเมื่อใช้เครื่องมือบรรทัดสั่ง `kmutil configure-boot` ใน 1TR

UUID ของกลุ่มดิสก์โวลุ่ม APFS (vuid)

- **ประเภท:** OctetString (16)
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR, recoveryOS, macOS
- **คำอธิบาย:** `vuid` ระบุว่ากลุ่มดิสก์โวลุ่มที่เคอร์เนลควรใช้เป็นราก ช่องนี้แสดงข้อมูลพื้นฐานและไม่ได้ใช้เพื่อจำกัดด้านความปลอดภัย `vuid` นี้ตั้งค่าโดยผู้ใช้โดยนัยเมื่อสร้างการติดตั้งระบบปฏิบัติการใหม่

UUID กลุ่ม (kuid) กุญแจการเข้ารหัสกุญแจ (KEK)

- **ประเภท:** OctetString (16)
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR, recoveryOS, macOS
- **คำอธิบาย:** `kuid` ระบุดิสก์โวลุ่มที่บูต โดยทั่วไปกุญแจการเข้ารหัสกุญแจจะถูกใช้สำหรับการปกป้องข้อมูล สำหรับ LocalPolicy นั้นจะใช้เพื่อปกป้องกุญแจการลงชื่อ LocalPolicy `kuid` ตั้งค่าโดยผู้ใช้โดยนัยเมื่อสร้างการติดตั้งระบบปฏิบัติการใหม่

การวัดนโยบายการบูตที่เชื่อถือของ recoveryOS ที่จับคู่ (prot)

- **ประเภท:** OctetString (48)
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR, recoveryOS, macOS
- **คำอธิบาย:** การวัดนโยบายการบูตที่เชื่อถือของ recoveryOS ที่จับคู่ (TBPM) คือการคำนวณแฮช SHA384 แบบทำซ้ำชนิดพิเศษผ่านรายการ Image4 ของ LocalPolicy แต่ไม่รวมถึง Nonce เพื่อมอบการวัดที่สอดคล้องกันเมื่อเวลาผ่านไป (เนื่องจาก Nonce แบบ `lpnh` จะได้รับการอัปเดตบ่อยครั้ง) ช่อง `prot` ที่พบอยู่ใน LocalPolicy แต่ละรายการสำหรับ macOS เท่านั้น จะมอบการจับคู่เพื่อระบุ LocalPolicy สำหรับ recoveryOS ซึ่งจะสอดคล้องกับ LocalPolicy สำหรับ macOS

นโยบายภายในเครื่อง recoveryOS ที่ลงชื่อด้วยแฮช Secure Enclave (hrlp)

- **ประเภท:** บูลีน
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR, recoveryOS, macOS
- **คำอธิบาย:** `hrlp` ระบุว่าค่า `prot` (ด้านบน) คือการวัดของ recoveryOS LocalPolicy ที่ลงชื่อด้วย Secure Enclave หรือไม่ ถ้าไม่ใช่ แสดงว่า LocalPolicy สำหรับ recoveryOS มีการลงชื่อโดยเซิร์ฟเวอร์การลงชื่อทางออนไลน์ของ Apple ซึ่งเป็นเซิร์ฟเวอร์ที่ลงชื่อสิ่งต่างๆ เช่นไฟล์ Image4 ของ macOS

Local Operating System Version (love)

- **ประเภท:** บูลีน
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR, recoveryOS, macOS
- **คำอธิบาย:** `love` บ่งชี้เวอร์ชั่น OS ที่ LocalPolicy ถูกสร้างขึ้นเพื่อตอบรับเวอร์ชั่น OS นั้น เวอร์ชั่นนี้ได้มาจากรายการสถานะถัดไประหว่างการสร้าง LocalPolicy และใช้เพื่อบังคับใช้ข้อจำกัดในการจับคู่ recoveryOS

การบูตหลายรายการอย่างปลอดภัย (smb0)

- **ประเภท:** บูลีน
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR, recoveryOS
- **คำอธิบาย:** ถ้า `smb0` มีอยู่และเป็นจริง LLB จะอนุญาตให้รายการ Image4 ในขั้นตอนถัดไปได้รับการลงชื่อสากลแทนที่จะต้องใช้ลายเซ็นที่ปรับให้เป็นส่วนตัว ผู้ใช้สามารถเปลี่ยนแปลงช่องนี้ได้โดยใช้ยูทิลิตี้ความปลอดภัยของการเริ่มต้นระบบหรือ `bputil` เพื่อดาวน์เกรดเป็นความปลอดภัยแบบลดลง

การบูตหลายรายการอย่างปลอดภัย (smb1)

- **ประเภท:** บูลีน
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR
- **คำอธิบาย:** ถ้า `smb1` มีอยู่และเป็นจริง iBoot จะอนุญาตให้วัตถุ เช่น คอลเลกชั่นเคอร์เนลแบบกำหนดเองลงชื่อด้วย Secure Enclave โดยใช้กุญแจเดียวกันกับ LocalPolicy การมีอยู่ของ `smb0` เป็นข้อกำหนดเบื้องต้นสำหรับการมีอยู่ของ `smb1` ผู้ใช้สามารถเปลี่ยนแปลงช่องนี้ได้โดยใช้เครื่องมือบรรทัดคำสั่ง เช่น `csrutil` หรือ `bputil` เพื่อดาวน์เกรดเป็นความปลอดภัยที่อนุญาต

การบูตหลายรายการอย่างปลอดภัย (smb2)

- **ประเภท:** บูลีน
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR
- **คำอธิบาย:** ถ้า `smb2` มีอยู่และเป็นจริง iBoot จะอนุญาตให้คอลเลกชั่นเคอร์เนลเสริมลงชื่อด้วย Secure Enclave โดยใช้กุญแจเดียวกันกับ LocalPolicy การมีอยู่ของ `smb0` เป็นข้อกำหนดเบื้องต้นสำหรับการมีอยู่ของ `smb2` ผู้ใช้สามารถเปลี่ยนแปลงช่องนี้ได้โดยใช้ยูทิลิตี้ความปลอดภัยของการเริ่มต้นระบบหรือ `bputil` เพื่อดาวน์เกรดเป็นความปลอดภัยลดลงและเปิดใช้งาน kext ของบริษัทอื่น

การบูตหลายรายการอย่างปลอดภัย (smb3)

- **ประเภท:** บูลีน
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR
- **คำอธิบาย:** ถ้า `smb3` มีอยู่และเป็นจริง แสดงว่าผู้ใช้ที่อยู่ที่อุปกรณ์ได้เลือกที่จะควบคุมการจัดการอุปกรณ์เคลื่อนที่ (MDM) ของระบบของตนเองไว้ การมีอยู่ของช่องนี้ช่วยให้แอปพลิเคชันหน่วยประมวลผล Secure Enclave ที่ควบคุม LocalPolicy ยอมรับการตรวจสอบสิทธิ์ MDM แทนการใช้การตรวจสอบสิทธิ์ผู้ใช้ภายในเครื่อง ผู้ใช้สามารถเปลี่ยนแปลงช่องนี้ได้โดยใช้ยูทิลิตี้ความปลอดภัยของการเริ่มต้นระบบหรือ `bputil` เพื่อเปิดใช้งานการควบคุมที่ได้รับการจัดการผ่าน kext ของบริษัทอื่นและรายการอัปเดตซอฟต์แวร์ (ใน macOS 11.2 ขึ้นไป MDM ยังสามารถเริ่มต้นการอัปเดตเป็น macOS เวอร์ชั่นล่าสุดได้หากโหมดความปลอดภัยในขณะนั้นเป็นความปลอดภัยแบบเต็ม)

การบูตหลายรายการอย่างปลอดภัย (smb4)

- **ประเภท:** บูลีน
- **สภาพแวดล้อมที่ผันแปรได้:** macOS
- **คำอธิบาย:** ถ้ามี `smb4` และเป็นจริง แสดงว่าอุปกรณ์ได้เลือกใช้การควบคุม MDM ของระบบปฏิบัติการโดยใช้ Apple School Manager, Apple Business Manager หรือ Apple Business Essentials การมีอยู่ของช่องนี้ช่วยให้แอปพลิเคชัน Secure Enclave ที่ควบคุม LocalPolicy ยอมรับการตรวจสอบสิทธิ์ MDM แทนการใช้การตรวจสอบสิทธิ์ผู้ใช้ภายในเครื่อง ช่องนี้จะมีการเปลี่ยนแปลงโดยโซลูชั่น MDM เมื่อตรวจพบว่าหมายเลขประจำเครื่องของอุปกรณ์แสดงในบริการใดๆ จากทั้งสามบริการนี้

การปกป้องความสมบูรณ์ของระบบ (sip0)

- **ประเภท:** จำนวนเต็มที่ไม่ได้ลงชื่อ 64 บิต
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR
- **คำอธิบาย:** `sip0` มีบิตนโยบายการปกป้องความสมบูรณ์ของระบบ (SIP) ที่มีอยู่ซึ่งเคยจัดเก็บไว้ใน NVRAM ก่อนหน้านี้ บิตนโยบาย SIP ใหม่จะถูกเพิ่มที่นี่ (แทนการใช้ช่อง LocalPolicy ตามด้านล่าง) หากใช้เฉพาะใน macOS และไม่ได้ใช้โดย LLB ผู้ใช้สามารถเปลี่ยนแปลงช่องนี้ได้โดยใช้ `csrutil` จาก 1TR เพื่อปิดใช้งาน SIP และดาวน์เกรดเป็นความปลอดภัยที่อนุญาต

การปกป้องความสมบูรณ์ของระบบ (sip1)

- **ประเภท:** บูลีน
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR
- **คำอธิบาย:** ถ้า `sip1` มีอยู่และเป็นจริง iBoot จะอนุญาตข้อผิดพลาดในการตรวจสอบยืนยันแฮชรากดิสก์โวลุ่ม SSV ผู้ใช้สามารถเปลี่ยนแปลงช่องนี้ได้โดยใช้ `csrutil` หรือ `bputil` จาก 1TR

การปกป้องความสมบูรณ์ของระบบ (sip2)

- **ประเภท:** บูลีน
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR
- **คำอธิบาย:** ถ้า sip2 มีอยู่และเป็นจริง iBoot จะไม่ล็อคการลงทะเบียนฮาร์ดแวร์ **ภูมิภาคข้อความกำหนดค่าแบบอ่านได้อย่างเดียว (CTRR)** ซึ่งทำเครื่องหมายให้หน่วยความจำเคอร์เนลเป็นหน่วยความจำที่ไม่สามารถเขียนได้ ผู้ใช้สามารถเปลี่ยนแปลงช่องนี้ได้โดยใช้ `csrutil` หรือ `bputil` จาก 1TR

การปกป้องความสมบูรณ์ของระบบ (sip3)

- **ประเภท:** บูลีน
- **สภาพแวดล้อมที่ผันแปรได้:** 1TR
- **คำอธิบาย:** ถ้า `sip3` มีอยู่และเป็นจริง iBoot จะไม่บังคับใช้รายการอนุญาตที่มีในตัวสำหรับตัวแปร boot-args ของตัวแปร NVRAM ซึ่งจะฟิลเตอร์ตัวเลือกที่ส่งผ่านไปยังเคอร์เนล ผู้ใช้สามารถเปลี่ยนแปลงช่องนี้ได้โดยใช้ `csrutil` หรือ `bputil` จาก 1TR

ใบรับรองและ RemotePolicy

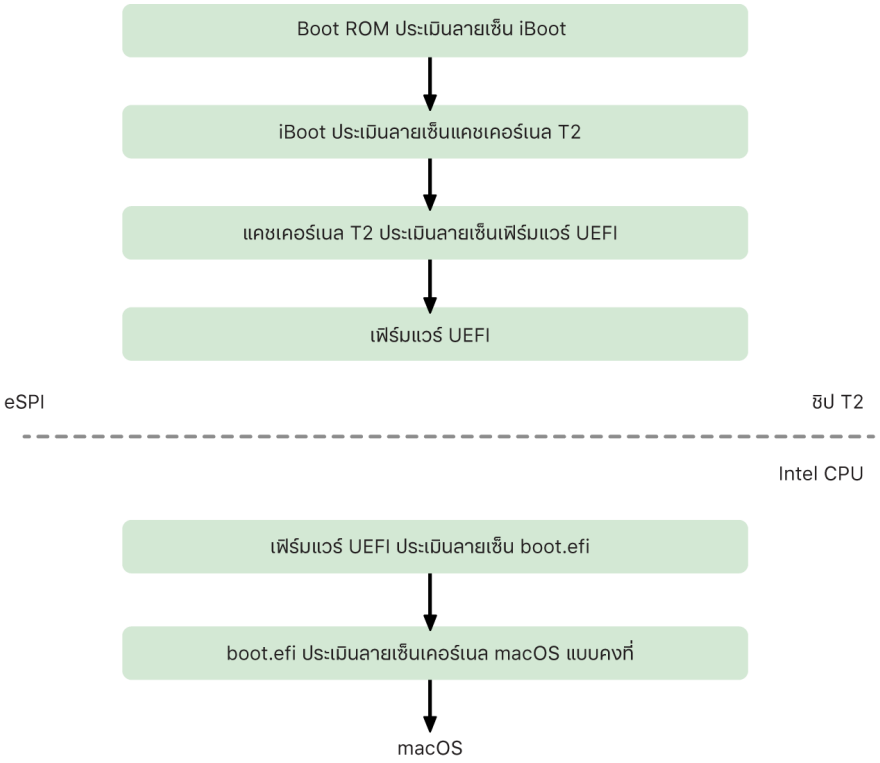
ตามที่ได้อธิบายในการสร้างและการจัดการกุญแจที่ลงชื่อ LocalPolicy นั้น Image4 ของ LocalPolicy ยังมี Owner Identity Certificate (OIC) และ RemotePolicy ที่ฝังอยู่อีกด้วย

คอมพิวเตอร์ Mac ที่ใช้ Intel

กระบวนการบูตสำหรับ Mac ที่ใช้ Intel

Mac ที่ใช้ Intel ที่มีชิป Apple T2 Security

เมื่อเปิดคอมพิวเตอร์ Mac ที่ใช้ Intel ที่มีชิป Apple T2 Security ชิปจะดำเนินการบูตอย่างปลอดภัยจาก Boot ROM ของชิปในลักษณะเดียวกันกับ iPhone, iPad และ Mac ที่ใช้ Apple Silicon ขั้นตอนนี้จะตรวจสอบยืนยันตัวโหลดเริ่มต้นระบบ iBoot และเป็นขั้นตอนแรกในลำดับการตรวจสอบความน่าเชื่อถือ โดย iBoot จะตรวจสอบเคอร์เนลและโค้ดส่วนขยายเคอร์เนลบนชิป T2 ซึ่งหลังจากนั้นจะตรวจสอบเฟิร์มแวร์ UEFI ของ Intel เฟิร์มแวร์ UEFI และลายเซ็นที่เกี่ยวข้องจะสามารถใช้กับชิป T2 ได้แค่ในตอนแรกเท่านั้น



หลังจากการตรวจสอบยืนยัน ภาพดิสก์เฟิร์มแวร์ UEFI จะถูกเทียบผังไปยังส่วนหนึ่งของหน่วยความจำชิป T2 หน่วยความจำนี้สามารถใช้งานได้กับ Intel CPU ผ่าน enhanced Serial Peripheral Interface (eSPI) เมื่อ Intel CPU ดังกล่าวบูตเป็นครั้งแรก จะดึงข้อมูลเฟิร์มแวร์ UEFI ผ่าน eSPI จากสำเนาที่มีการตรวจสอบความสมบูรณ์และเทียบผังหน่วยความจำของเฟิร์มแวร์ซึ่งอยู่บนชิป T2

การประเมินลำดับการตรวจสอบความน่าเชื่อถือจะดำเนินการต่อบน Intel CPU โดยเฟิร์มแวร์ UEFI จะประเมินลายเซ็นของ boot.efi ซึ่งเป็นตัวโหลดเริ่มต้นระบบของ macOS ลายเซ็นการบูตอย่างปลอดภัยของ macOS สำหรับ Intel จะถูกจัดเก็บในรูปแบบ Image4 เดียวกันกับที่ใช้สำหรับการบูตอย่างปลอดภัยของ iOS, iPadOS และชิป T2 และโค้ดที่แยกวิเคราะห์ไฟล์ Image4 เป็นโค้ดเดียวกันที่เข้มงวดขึ้นจากการใช้งานการบูตอย่างปลอดภัยสำหรับ iOS และ iPadOS ปัจจุบัน Boot.efi จะตรวจสอบยืนยันลายเซ็นของไฟล์ที่เรียกว่า immutablekernel เมื่อการบูตอย่างปลอดภัยเปิดใช้งานอยู่ ไฟล์ immutablekernel จะแสดงถึงชุดส่วนขยายเคอร์เนลของ Apple ที่สมบูรณ์ที่ต้องใช้ในการบูต macOS นโยบายการบูตอย่างปลอดภัยจะสิ้นสุดลงเมื่อส่งต่อไปยัง immutablekernel และหลังจากนั้นนโยบายด้านความปลอดภัยของ macOS (เช่น การปกป้องความสมบูรณ์ของระบบ และส่วนขยายเคอร์เนลที่มีการลงชื่อ) จะมีผล

ถ้ามีข้อผิดพลาดหรือความล้มเหลวใดๆ ในกระบวนการนี้ Mac จะเข้าสู่โหมดการกู้คืน โหมดการกู้คืนชิป Apple T2 Security หรือโหมดอัปเกรดเฟิร์มแวร์อุปกรณ์ (DFU) ของชิป Apple T2 Security

Microsoft Windows บน Mac ที่ใช้ Intel ที่มีชิป T2

ตามค่าเริ่มต้น Mac ที่ใช้ Intel ที่รองรับการบูตอย่างปลอดภัยจะเชื่อถือเนื้อหาที่ลงชื่อโดย Apple เท่านั้น อย่างไรก็ตาม ในการปรับปรุงความปลอดภัยของการติดตั้ง Boot Camp บริษัท Apple ยังรองรับการบูตอย่างปลอดภัยสำหรับ Windows อีกด้วย เฟิร์มแวร์ Unified Extensible Firmware Interface (UEFi) มีสำเนาของใบรับรอง Microsoft Windows Production CA 2011 ที่ใช้ตรวจสอบสิทธิ์ Bootloader ของ Microsoft

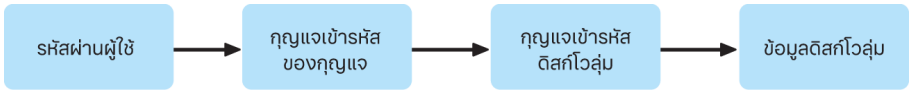
หมายเหตุ: ในปัจจุบัน ไม่มีความเชื่อถือให้สำหรับ Microsoft Corporation UEFI CA 2011 ที่จะอนุญาตให้ตรวจสอบยืนยันโค้ดที่ลงชื่อโดยคู่ค้าของ Microsoft UEFI CA นี้มักนำมาใช้ในการตรวจสอบยืนยันความถูกต้องของตัวโหลดเริ่มต้นระบบสำหรับระบบปฏิบัติการอื่นๆ เช่น ระบบปฏิบัติการต่างๆ ของ Linux

การรองรับการบูต Windows อย่างปลอดภัยไม่ได้เปิดใช้งานตามค่าเริ่มต้น แต่จะถูกเปิดใช้งานโดยใช้ผู้ช่วย Boot Camp (BCA) เมื่อผู้ใช้เรียกใช้ BCA จะมีการกำหนดค่า macOS อีกครั้งเพื่อให้เชื่อถือรหัสที่ลงชื่อของบริษัทแรกจาก Microsoft ในระหว่างการบูต หลังจาก BCA ดำเนินการเสร็จสิ้นแล้ว ถ้า macOS ส่งผ่านการประเมินความน่าเชื่อถือของบริษัทแรกจาก Apple ในระหว่างการบูตอย่างปลอดภัย เฟิร์มแวร์ UEFI จะพยายามประเมินความน่าเชื่อถือของวัตถุตามการจัดรูปแบบการบูตอย่างปลอดภัยสำหรับ UEFI ถ้าดำเนินการประเมินความน่าเชื่อถือได้สำเร็จ Mac จะดำเนินการต่อและบูต Windows ถ้าดำเนินการไม่สำเร็จ Mac จะเข้าสู่ recoveryOS และแจ้งผู้ใช้ว่าประเมินความน่าเชื่อถือไม่สำเร็จ

คอมพิวเตอร์ Mac ที่ใช้ Intel ที่ไม่มีชิป T2

Mac ที่ใช้ Intel ที่ไม่มีชิป T2 จะไม่รองรับการบูตอย่างปลอดภัย ดังนั้นเฟิร์มแวร์ Unified Extensible Firmware Interface (UEFi) จะโหลดตัวบูต macOS (boot.efi) จากระบบไฟล์โดยไม่มีการตรวจสอบยืนยัน และตัวบูตจะโหลดเคอร์เนล (prelinkedkernel) จากระบบไฟล์โดยไม่มีการตรวจสอบยืนยัน ในการปกป้องความสมบูรณ์ของลำดับการบูต ผู้ใช้ควรเปิดใช้งานกลไกความปลอดภัยต่อไปนี้ทั้งหมด:

- **การปกป้องความสมบูรณ์ของระบบ (SIP):** การตั้งค่านี้จะเปิดใช้งานตามค่าเริ่มต้น โดยจะปกป้องตัวบูตและเคอร์เนลจากการเขียนที่เป็นอันตรายจากภายใน macOS ที่ใช้งานอยู่
- **FileVault:** สามารถเปิดใช้งานการตั้งค่านี้ได้สองวิธี: โดยผู้ใช้หรือโดยผู้ดูแลของการจัดการอุปกรณ์เคลื่อนที่ (MDM) การตั้งค่านี้จะป้องกันผู้โจมตีที่ใช้วิธีทางกายภาพโดยใช้โหมดดิสก์เป้าหมายในการเขียนทับตัวบูต
- **รหัสผ่านเฟิร์มแวร์:** สามารถเปิดใช้งานการตั้งค่านี้ได้สองวิธี: โดยผู้ใช้หรือโดยผู้ดูแลของ MDM การตั้งค่านี้จะช่วยป้องกันไม่ให้ผู้โจมตีที่ใช้วิธีทางกายภาพเปิดทำงานโหมดบูตอื่นๆ เช่น recoveryOS, โหมดผู้ใช้รายเดียว หรือโหมดดิสก์เป้าหมาย ซึ่งอาจทำให้ตัวบูตถูกเขียนทับได้ และยังช่วยป้องกันไม่ให้มีการบูตจากสื่ออื่น ซึ่งผู้โจมตีสามารถเรียกใช้รหัสเพื่อเขียนทับตัวบูตได้



โหมดการบูตของ Mac ที่ใช้ Intel ที่มีชิป Apple T2 Security

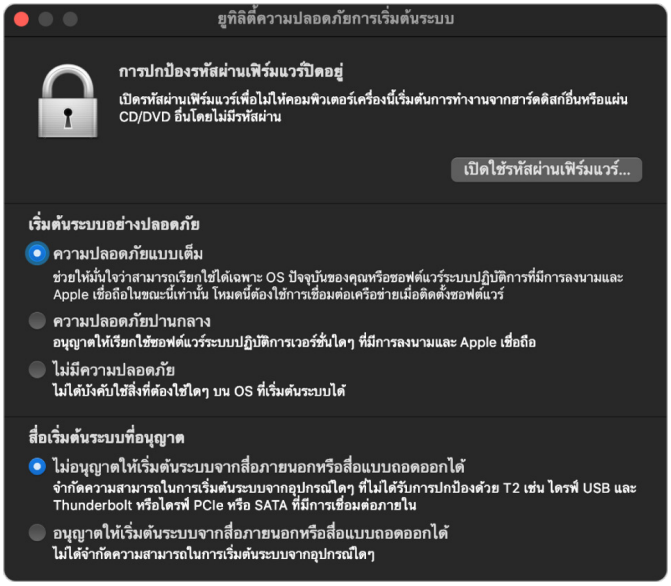
Mac ที่ใช้ Intel ที่มีชิป Apple T2 Security มีโหมดการบูตหลากหลายโหมดที่สามารถใช้ได้ในระหว่างการบูตโดยการกดชุดคำสั่งแป้นพิมพ์ที่เฟิร์มแวร์หรือตัวบูต UEFI รู้จัก โหมดบูตบางโหมด เช่น โหมดผู้ใช้รายเดียว จะใช้ไม่ได้จนกว่าจะเปลี่ยนนโยบายความปลอดภัยเป็น ไม่มีความปลอดภัย ในยูทิลิตี้ความปลอดภัยของการเริ่มต้นระบบ

โหมด	ปุ่มผสม	คำอธิบาย
การบูต macOS	ไม่มี	เฟิร์มแวร์ UEFI จะส่งต่อไปยังตัวบูต macOS (แอปพลิเคชัน UEFI) ซึ่งส่งต่อไปยังเคอร์เนลของ macOS เมื่อบูตแบบมาตรฐานบน Mac ที่เปิดใช้งาน FileVault อยู่ ตัวบูต macOS จะแสดงอินเทอร์เฟซหน้าต่างเข้าสู่ระบบ ซึ่งจะใช้รหัสผ่านเพื่อถอดรหัสพื้นที่จัดเก็บข้อมูล
ตัวจัดการการเริ่มต้นทำงาน	Option (⌥)	เฟิร์มแวร์ UEFI จะเปิดใช้แอปพลิเคชัน UEFI ในตัวที่แสดงอินเทอร์เฟซการเลือกอุปกรณ์สำหรับการบูตให้กับผู้ใช้
โหมดดิสก์เป้าหมาย (TDM)	T	เฟิร์มแวร์ UEFI เปิดใช้แอปพลิเคชัน UEFI ในตัวที่แสดงอุปกรณ์จัดเก็บข้อมูลภายในเป็นอุปกรณ์จัดเก็บข้อมูลแบบดิบที่ทำงานบนบล็อกผ่าน FireWire, Thunderbolt, USB หรือการรวมกันแบบต่างๆ ของสามพอร์ตนี้ (ขึ้นอยู่กับรุ่นของ Mac)
โหมดผู้ใช้รายเดียว	Command (⌘)-S	เคอร์เนลของ macOS ส่งผ่านธง –s ในเวคเตอร์อาร์กิวเมนต์ของ launchd จากนั้น launchd จะสร้างเชลล์ผู้ใช้รายเดียวใน tty ของแอปจอคอนโซล **หมายเหตุ:** ถ้าผู้ใช้ออกจากเชลล์ macOS จะบูตต่อเนื่องไปยังหน้าต่างเข้าสู่ระบบ
recoveryOS	Command (⌘)-R	เฟิร์มแวร์ UEFI จะโหลด macOS ขั้นต่ำจากไฟล์ภาพดิสก์ (.dmg) ที่ลงชื่อบนอุปกรณ์จัดเก็บข้อมูลภายใน
RecoveryOS ทางอินเทอร์เน็ต	Option (⌥)-Command (⌘)-R	ภาพดิสก์ที่ลงชื่อจะถูกดาวน์โหลดจากอินเทอร์เน็ตโดยใช้ HTTP
การวินิจฉัย	D	เฟิร์มแวร์ UEFI จะโหลดสภาพแวดล้อมการวินิจฉัย UEFI ขั้นต่ำจากไฟล์ภาพดิสก์ที่ลงชื่อบนอุปกรณ์จัดเก็บข้อมูลภายใน
การวินิจฉัยทางอินเทอร์เน็ต	Option (⌥)-D	ภาพดิสก์ที่ลงชื่อจะถูกดาวน์โหลดจากอินเทอร์เน็ตโดยใช้ HTTP
การบูต Windows	ไม่มี	ถ้า Windows ได้รับการติดตั้งโดยใช้ Boot Camp เฟิร์มแวร์ UEFI จะส่งต่อไปยังตัวบูต Windows ซึ่งส่งต่อไปยังเคอร์เนลของ Windows

ยูทิลิตี้ความปลอดภัยของการเริ่มต้นระบบบน Mac ที่มีชิป Apple T2 Security

ภาพรวม

บน Mac ที่ใช้ Intel ที่มีชิป Apple T2 Security ยูทิลิตี้ความปลอดภัยของการเริ่มต้นระบบจะจัดการกับการตั้งค่านโยบายด้านความปลอดภัยหลายรายการ ยูทิลิตี้สามารถเข้าถึงได้โดยการบูตไปยัง recoveryOS แล้วเลือกยูทิลิตี้ความปลอดภัยของการเริ่มต้นระบบจากเมนูยูทิลิตี้ และยูทิลิตี้จะปกป้องการตั้งค่าความปลอดภัยที่รองรับจากจากการควบคุมโดยง่ายจากผู้โจมตี



การเปลี่ยนแปลงนโยบายที่สำคัญต้องใช้การตรวจสอบสิทธิ์แม้จะอยู่ในโหมดการกู้คืน เมื่อเปิดยูทิลิตี้ความปลอดภัยของการเริ่มต้นระบบเป็นครั้งแรก ระบบจะแจ้งให้ผู้ใช้ป้อนรหัสผ่านผู้ดูแลระบบจากการติดตั้ง macOS หลักที่เชื่อมโยงกับ recoveryOS ที่บูตอยู่ในปัจจุบัน แต่ถ้าไม่มีผู้ดูแลระบบ จะต้องสร้างผู้ดูแลขึ้นมาหนึ่งรายก่อนจึงจะสามารถเปลี่ยนแปลงนโยบายได้ ชิป T2 กำหนดให้คอมพิวเตอร์ Mac ต้องบูตเข้าสู่ recoveryOS และต้องมีการตรวจสอบสิทธิ์ด้วยข้อมูลประจำตัวที่ได้รับการสนับสนุนจาก Secure Enclave ก่อนจึงจะสามารถทำการเปลี่ยนแปลงนโยบายดังกล่าวได้ การเปลี่ยนแปลงนโยบายด้านความปลอดภัยมีข้อกำหนดโดยนัยสองข้อ recoveryOS จะต้อง:

- บูตจากอุปกรณ์จัดเก็บข้อมูลที่เชื่อมต่อโดยตรงกับชิป T2 เนื่องจากพาร์ติชั่นบนอุปกรณ์เครื่องอื่นๆ ไม่มีเอกสารสิทธิ์ที่รองรับ Secure Enclave ซึ่งผูกกับอุปกรณ์จัดเก็บข้อมูลภายใน
- อยู่บนดิสก์โวลุ่มที่ใช้ APFS เนื่องจากมีการรองรับเฉพาะการจัดเก็บเอกสารสิทธิ์ของการตรวจสอบสิทธิ์ในการกู้คืนที่ส่งไปยัง Secure Enclave บนดิสก์โวลุ่ม APFS “พรีบูต” ของไดรฟ์ ดิสก์โวลุ่มที่จัดรูปแบบ HFS Plus จะไม่สามารถใช้การบูตอย่างปลอดภัยได้

นโยบายนี้จะแสดงเฉพาะในยูทิลิตี้ความปลอดภัยของการเริ่มต้นระบบบน Mac ที่ใช้ Intel ที่มีชิป T2 แม้ว่ากรณีการใช้งานส่วนใหญ่ไม่ควรต้องเปลี่ยนแปลงนโยบายการบูตอย่างปลอดภัย แต่ในท้ายที่สุดผู้ใช้ก็จะสามารถควบคุมการตั้งค่าอุปกรณ์ของตนเองได้ และอาจเลือกที่จะปิดใช้งานหรือดาวน์เกรดฟังก์ชั่นการทำงานของการบูตอย่างปลอดภัยบน Mac ตามความต้องการของตนเอง

การเปลี่ยนแปลงนโยบายการบูตอย่างปลอดภัยที่ดำเนินการจากภายในแอปนี้จะปรับใช้เฉพาะกับการประเมินลำดับการตรวจสอบความน่าเชื่อถือที่มีการตรวจสอบยืนยันบนหน่วยประมวลผล Intel ตัวเลือก “การบูตชิป T2 อย่างปลอดภัย” จะมีผลเสมอ

นโยบายการบูตอย่างปลอดภัยสามารถกำหนดค่าเป็นการตั้งค่าอย่างใดอย่างหนึ่งจากสามการตั้งค่าเหล่านี้ได้: ความปลอดภัยแบบเต็ม ความปลอดภัยแบบปานกลาง และไม่มีความปลอดภัย ไม่มีความปลอดภัยใดที่ปิดใช้งานการประเมินการบูตอย่างปลอดภัยบนหน่วยประมวลผล Intel ได้อย่างสมบูรณ์และอนุญาตให้ผู้ใช้สามารถบูตทุกสิ่งที่พวกเขาต้องการได้

นโยบายการบูตด้วยความปลอดภัยแบบเต็ม

ความปลอดภัยแบบเต็มเป็นนโยบายการบูตเริ่มต้นและทำงานคล้ายกับ iOS และ iPadOS หรือความปลอดภัยแบบเต็มบน Mac ที่ใช้ Apple Silicon เมื่อซอฟต์แวร์ดาวน์โหลดเสร็จและพร้อมติดตั้ง ซอฟต์แวร์จะถูกปรับให้เป็นส่วนตัวด้วยลายเซ็นที่มี Exclusive Chip Identification (ECID) ซึ่งเป็น ID เฉพาะสำหรับชิป T2 ในกรณีนี้ เป็นส่วนหนึ่งของคำขอลงชื่อ ลายเซ็นที่ได้รับจากเซิร์ฟเวอร์การลงชื่อนั้นจะไม่ซ้ำใครและสามารถใช้งานได้โดยชิป T2 เฉพาะเท่านั้น เฟิร์มแวร์ Unified Extensible Firmware Interface (UEFi) ได้รับการออกแบบมาเพื่อให้แน่ใจว่าเมื่อนโยบายความปลอดภัยเต็มรูปแบบมีผลบังคับใช้ ลายเซ็นที่กำหนดไม่ได้เป็นเพียงการเซ็นโดย Apple เท่านั้น แต่เป็นการเซ็นสำหรับ Mac เครื่องนี้โดยเฉพาะ โดยจะเชื่อมโยง macOS เวอร์ชั่นนั้นกับ Mac เครื่องนั้น กระบวนการนี้จะช่วยป้องกันการโจมตีแบบย้อนกลับดังที่ได้อธิบายไว้สำหรับความปลอดภัยแบบเต็มบน Mac ที่ใช้ Apple Silicon

นโยบายการบูตด้วยความปลอดภัยปานกลาง

นโยบายการบูตด้วยความปลอดภัยปานกลางค่อนข้างเหมือนกับการบูต UEFI อย่างปลอดภัยแบบดั้งเดิม ซึ่งผู้จำหน่าย (ในกรณีนี้คือ Apple) จะสร้างลายเซ็นดิจิตอลสำหรับโค้ดเพื่อยืนยันว่ามาจากผู้จำหน่าย ด้วยวิธีนี้ ผู้โจมตีจะไม่สามารถใส่โค้ดที่ไม่ได้ลงชื่อได้ เราเรียกลายเซ็นนี้ว่าเป็นลายเซ็น "สากล" เนื่องจากสามารถใช้บน Mac ได้ทุกเครื่องโดยไม่จำกัดจำนวนครั้ง สำหรับ Mac ที่มีชุดนโยบายความปลอดภัยปานกลาง iOS, iPadOS และชิป T2 เองไม่รองรับลายเซ็นสากล การตั้งค่านี้จะไม่พยายามป้องกันการโจมตีแบบย้อนกลับ

นโยบายการบูตสื่อ

นโยบายการบูตสื่อจะมีเฉพาะบน Mac ที่ใช้ Intel ที่มีชิป T2 เท่านั้นและเป็นอิสระจากนโยบายการบูตอย่างปลอดภัย ดังนั้นแม้ว่าผู้ใช้จะปิดใช้งานการบูตอย่างปลอดภัย แต่การดำเนินการนี้จะไม่เปลี่ยนลักษณะการทำงานตามค่าเริ่มต้นที่ป้องกันไม่ให้สิ่งอื่นใดบูต Mac ได้นอกเหนือจากอุปกรณ์จัดเก็บข้อมูลที่เชื่อมต่อโดยตรงกับชิป T2 (นโยบายการบูตสื่อไม่จำเป็นบน Mac ที่ใช้ Apple Silicon สำหรับข้อมูลเพิ่มเติม โปรดดูการควบคุมนโยบายความปลอดภัยดิสก์เริ่มต้นระบบ)

การปกป้องด้วยรหัสผ่านเฟิร์มแวร์ใน Mac ที่ใช้ Intel

macOS บนคอมพิวเตอร์ Mac ที่ใช้ Intel ที่มีชิป Apple T2 Security รองรับการใช้รหัสผ่านเฟิร์มแวร์เพื่อช่วยป้องกันการแก้ไขการตั้งค่าเฟิร์มแวร์โดยไม่ตั้งใจบน Mac ที่ระบุเฉพาะ รหัสผ่านเฟิร์มแวร์ได้รับการออกแบบมาเพื่อป้องกันไม่ให้มีการเลือกโหมดบูตอื่นๆ เช่น การบูตไปยัง recoveryOS หรือโหมดผู้ใช้รายเดียว การบูตจากดิสก์โวลุ่มที่ไม่ได้รับอนุญาต หรือการบูตไปยังโหมดดิสก์เป้าหมาย

หมายเหตุ: รหัสผ่านเฟิร์มแวร์ไม่ใช่สิ่งจำเป็นบน Mac ที่ใช้ Apple Silicon เนื่องจากฟังก์ชั่นการทำงานของเฟิร์มแวร์ที่สำคัญที่มีการจำกัดนั้นได้ถูกย้ายไปยัง recoveryOS แล้ว และ (เมื่อเปิดใช้งาน FileVault) recoveryOS จะใช้การตรวจสอบสิทธิ์ของผู้ใช้ก่อนจะสามารถเข้าถึงฟังก์ชั่นการทำงานที่สำคัญได้

โหมดที่เป็นพื้นฐานที่สุดของรหัสผ่านเฟิร์มแวร์สามารถเข้าถึงได้จากยูทิลิตี้รหัสผ่านเฟิร์มแวร์ของ recoveryOS บน Mac ที่ใช้ Intel ที่**ไม่มี**ชิป T2 และจากยูทิลิตี้ความปลอดภัยของการเริ่มต้นระบบบน Mac ที่ใช้ Intel ที่**มี**ชิป T2 ตัวเลือกขั้นสูง (เช่น ความสามารถในการแจ้งขอรหัสผ่านในการบูตทุกครั้ง) มีให้เลือกจากเครื่องมือบรรทัดคำสั่ง `firmwarepasswd` ใน macOS

การตั้งรหัสผ่านเฟิร์มแวร์ถือเป็นสิ่งสำคัญอย่างยิ่งในการลดความเสี่ยงของการโจมตีบนคอมพิวเตอร์ Mac ที่ใช้ Intel ซึ่งไม่มีชิป T2 จากผู้โจมตีทางกายภาพ รหัสผ่านเฟิร์มแวร์สามารถช่วยป้องกันผู้โจมตีไม่ให้บูตไปยัง recoveryOS ซึ่งสามารถปิดใช้งานการปกป้องความสมบูรณ์ของระบบ (SIP) ได้ และด้วยการจำกัดการบูตสื่ออื่น ผู้โจมตีจะไม่สามารถเรียกใช้โค้ดที่มีสิทธิ์พิเศษจากระบบปฏิบัติการอื่นเพื่อโจมตีเฟิร์มแวร์อุปกรณ์ต่อพ่วงได้

กลไกการรีเซ็ตรหัสผ่านเฟิร์มแวร์มีให้เพื่อช่วยผู้ใช้ที่ลืมรหัสผ่านของตัวเอง ให้ผู้ใช้กดชุดคำสั่งแป้นพิมพ์เมื่อเริ่มต้นระบบ แล้วจะมีสตริงเฉพาะรุ่นแสดงขึ้นมาเพื่อให้นำไปให้กับ AppleCare AppleCare จะลงชื่อแบบดิจิตอลบนแหล่งข้อมูลที่ได้รับการตรวจสอบลายเซ็นโดยตัวระบุแหล่งทรัพยากรสากล (URI) ถ้าลายเซ็นดังกล่าวผ่านการตรวจสอบความถูกต้อง และเนื้อหานั้นมีไว้สำหรับ Mac ที่ระบุเฉพาะ เฟิร์มแวร์ UEFI จะเอารหัสผ่านเฟิร์มแวร์ออก

สำหรับผู้ใช้ที่ไม่ต้องการให้ผู้อื่นนอกจากตัวเองเอารหัสผ่านเฟิร์มแวร์ของตนออกโดยใช้ซอฟต์แวร์ ตัวเลือก `–disable–reset–capability` จึงถูกเพิ่มไปยังเครื่องมือบรรทัดคำสั่ง `firmwarepasswd` ใน macOS 10.15 ก่อนการตั้งค่าตัวเลือกนี้ ผู้ใช้จะต้องรับทราบว่าหากลืมรหัสผ่านและต้องการเอาออก ผู้ใช้จะต้องรับผิดชอบค่าใช้จ่ายในการเปลี่ยนลอจิกบอร์ดที่จำเป็นเพื่อให้บรรลุเป้าหมายนี้ องค์กรที่ต้องการปกป้องคอมพิวเตอร์ Mac ของตนจากผู้โจมตีภายนอกและจากพนักงานจะต้องตั้งรหัสผ่านเฟิร์มแวร์บนระบบที่เป็นขององค์กร กระบวนการนี้สามารถดำเนินการบนอุปกรณ์ได้ตามวิธีใดๆ ดังต่อไปนี้:

- เมื่อเตรียมใช้งานโดยใช้เครื่องมือบรรทัดคำสั่ง `firmwarepasswd` ด้วยตัวเอง
- ด้วยเครื่องมือการจัดการของบริษัทอื่นที่ใช้เครื่องมือบรรทัดคำสั่ง `firmwarepasswd`
- การใช้การจัดการอุปกรณ์เคลื่อนที่ (MDM)

recoveryOS และสภาพแวดล้อมการวินิจฉัยสำหรับ Mac ที่ใช้ Intel

recoveryOS

recoveryOS ถูกแยกออกจาก macOS หลักอย่างสมบูรณ์ และเนื้อหาทั้งหมดจะถูกจัดเก็บไว้ในไฟล์ภาพดิสก์ที่ชื่อ BaseSystem.dmg และยังมี BaseSystem.chunklist ที่เกี่ยวข้องซึ่งใช้ในการตรวจสอบยืนยันความสมบูรณ์ของ BaseSystem.dmg อีกด้วย chunklist คือชุดแฮชสำหรับชิ้นส่วนขนาด 10 MB ของ BaseSystem.dmg เฟิร์มแวร์ Unified Extensible Firmware Interface (UEFi) จะประเมินลายเซ็นของไฟล์ chunklist จากนั้นประเมินแฮชทีละรายการจาก BaseSystem.dmg วิธีนี้จะช่วยให้มั่นใจว่าลายเซ็นจะตรงกับเนื้อหาลงชื่อซึ่งมีอยู่ใน chunklist ถ้าแฮชใดๆ เหล่านี้ไม่ตรงกัน การบูตจาก recoveryOS ในเครื่องจะถูกยกเลิก และเฟิร์มแวร์ UEFI จะพยายามบูตจาก recoveryOS ทางอินเทอร์เน็ตแทน

ถ้าการตรวจสอบยืนยันดำเนินการสำเร็จแล้ว เฟิร์มแวร์ UEFI จะต่อเชื่อม BaseSystem.dmg เป็นดิสก์ RAM และเปิดใช้ไฟล์ boot.efi ที่อยู่ในนั้น ไม่จำเป็นต้องให้เฟิร์มแวร์ UEFI ดำเนินการตรวจสอบเฉพาะสำหรับ boot.efi หรือไม่ต้องให้ boot.efi ดำเนินการตรวจสอบเคอร์เนล เนื่องจากเนื้อหาแบบสมบูรณ์ของระบบปฏิบัติการ (ซึ่งมีองค์ประกอบเหล่านี้เป็นเพียงส่วนย่อย) ได้รับการตรวจสอบความสมบูรณ์เรียบร้อยแล้ว

การวินิจฉัยของ Apple

ขั้นตอนสำหรับการบูตสภาพแวดล้อมการวินิจฉัยในเครื่องจะเหมือนกับการเปิดทำงาน recoveryOS เกือบทั้งหมด ไฟล์ AppleDiagnostics.dmg และ AppleDiagnostics.chunklist จะถูกนำมาใช้แยกจากกัน แต่จะได้รับการตรวจสอบยืนยันในลักษณะเดียวกับไฟล์ BaseSystem แทนที่จะเปิดใช้ boot.efi เฟิร์มแวร์ UEFI จะเปิดใช้ไฟล์ภายในภาพดิสก์ (ไฟล์ .dmg) ที่ชื่อ diags.efi ซึ่งมีหน้าที่เรียกใช้ไดรเวอร์ UEFI อื่นๆ ที่สามารถเป็นสื่อกลางและตรวจสอบหาข้อผิดพลาดในฮาร์ดแวร์ได้

recoveryOS และสภาพแวดล้อมการวินิจฉัยทางอินเทอร์เน็ต

ถ้าเกิดข้อผิดพลาดขึ้นในการเปิดทำงานของการกู้คืนในเครื่องหรือสภาพแวดล้อมการวินิจฉัย เฟิร์มแวร์ UEFI จะพยายามดาวน์โหลดภาพดิสก์จากอินเทอร์เน็ตแทน (ผู้ใช้ยังสามารถร้องขอให้ดึงข้อมูลภาพดิสก์จากอินเทอร์เน็ตโดยเฉพาะได้โดยใช้ลำดับปุ่มแบบพิเศษที่กดค้างไว้ในขณะที่บูต) การตรวจสอบความถูกต้องของความสมบูรณ์ของภาพดิสก์และ chunklist ที่ดาวน์โหลดจากเซิร์ฟเวอร์การกู้คืน OS จะดำเนินการในลักษณะเดียวกับภาพดิสก์ที่ดึงข้อมูลมาจากอุปกรณ์จัดเก็บข้อมูล

แม้ว่าจะเชื่อมต่อกับเซิร์ฟเวอร์การกู้คืน OS โดยใช้ HTTP แต่เนื้อหาที่ดาวน์โหลดทั้งหมดจะยังคงถูกตรวจสอบความสมบูรณ์ตามที่อธิบายไว้ก่อนหน้านี้ และด้วยเหตุนั้นจึงได้รับการปกป้องจากการถูกจัดการโดยผู้โจมตีที่มีการควบคุมเครือข่าย ในกรณีที่ชิ้นส่วนแต่ละชิ้นไม่ผ่านการตรวจสอบยืนยันความสมบูรณ์ ชิ้นส่วนนั้นจะได้รับการร้องขออีกครั้งจากเซิร์ฟเวอร์การกู้คืน OS เป็นจำนวน 11 ครั้งก่อนที่จะยกเลิกและแสดงข้อผิดพลาด

เมื่อเพิ่มโหมดการกู้คืนทางอินเทอร์เน็ตและโหมดการวินิจฉัยลงในคอมพิวเตอร์ Mac ในปี 2011 มีการตัดสินใจว่าวิธีที่น่าจะดีกว่าคือการใช้การส่งต่อข้อมูล HTTP ที่ง่ายขึ้นและการจัดการการตรวจสอบสิทธิ์เนื้อหาโดยใช้กลไก chunklist แทนการใช้ฟังก์ชั่นการทำงาน HTTPS ที่ซับซ้อนกว่าในเฟิร์มแวร์ UEFI และส่งผลให้เพิ่มพื้นหน้าของการโจมตีของเฟิร์มแวร์

ความปลอดภัยของดิสก์โวลุ่มระบบที่ลงชื่อใน iOS, iPadOS และ macOS

Apple ได้เปิดตัวดิสก์โวลุ่มระบบแบบอ่านอย่างเดียว ซึ่งเป็นดิสก์โวลุ่มแยกเฉพาะสำหรับเนื้อหาระบบสำหรับ macOS 10.15 และมีการเพิ่มการป้องกันการเข้ารหัสที่รัดกุมให้กับเนื้อหาระบบด้วย **ดิสก์โวลุ่มระบบที่ลงชื่อ (SSV)** สำหรับ macOS 11 ขึ้นไป SSV มีกลไกเคอร์เนลที่ตรวจสอบยืนยันความสมบูรณ์ของเนื้อหาระบบในรันไทม์ และปฏิเสธข้อมูลใดๆ เช่น รหัสและไม่ใช่รหัส โดยไม่ต้องมีลายเซ็นการเข้ารหัสที่ถูกต้องจาก Apple ตั้งแต่ iOS 15 และ iPadOS 15 เป็นต้นไป ดิสก์โวลุ่มระบบบนอุปกรณ์ iOS และ iPadOS ยังได้รับการป้องกันด้วยการเข้ารหัสของดิสก์โวลุ่มระบบที่ลงชื่อ

SSV นอกจากจะช่วยป้องกันการดัดแปลงซอฟต์แวร์ใดๆ ของ Apple ที่เป็นส่วนหนึ่งของระบบปฏิบัติการแล้ว ยังทำให้การอัปเดตซอฟต์แวร์ macOS มีความเสถียรและปลอดภัยมากขึ้นอีกด้วย และเนื่องจาก SSV ใช้สแนปช็อต APFS (Apple File System) ถ้ามีการอัปเดตที่ไม่สามารถดำเนินการได้ เวอร์ชั่นเก่าของระบบจะถูกกู้คืนโดยไม่มีการติดตั้งอีกครั้ง

ตั้งแต่มีการเปิดตัว APFS ได้มอบความสมบูรณ์ให้กับเมตาดาต้าของระบบไฟล์โดยใช้เช็คซัมที่ไม่เข้ารหัสบนอุปกรณ์จัดเก็บข้อมูลภายใน SSV เพิ่มความปลอดภัยให้กลไกความสมบูรณ์โดยเพิ่มแฮชการเข้ารหัส ซึ่งจะขยายกลไกเพื่อรวมทุกไบต์ของข้อมูลไฟล์ ข้อมูลจากอุปกรณ์จัดเก็บข้อมูลภายใน (รวมถึงเมตาดาต้าของระบบไฟล์) จะถูกแฮชแบบเข้ารหัสในเส้นทางการอ่าน และเปรียบเทียบแฮชกับค่าที่คาดไว้ในเมตาดาต้าของระบบไฟล์ ในกรณีที่ไม่ตรงกัน ระบบจะอนุมานว่าข้อมูลถูกดัดแปลง และจะไม่ส่งกลับไปยังซอฟต์แวร์ที่ขอ

แฮช SHA256 ของ SSV แต่ละรายการถูกจัดเก็บไว้ในโครงสร้างเมตาดาต้าของระบบไฟล์หลักซึ่งมีการแฮชเอง และเนื่องจากแต่ละโหนดของโครงสร้างจะตรวจสอบยืนยันความสมบูรณ์ของแฮชของโหนดลูกซ้ำๆ ซึ่งคล้ายกับโครงสร้างแฮชไบนารี (Merkle) ค่าแฮชของโหนดราก หรือที่เรียกว่า**ตราประทับ** จะครอบคลุมทุกไบต์ของข้อมูลใน SSV ซึ่งหมายความว่าลายเซ็นการเข้ารหัสจะครอบคลุมดิสก์โวลุ่มระบบทั้งดิสก์

ระหว่างการติดตั้งและอัปเดต macOS ตราประทับจะถูกคำนวณใหม่จากระบบไฟล์ในอุปกรณ์ และการคำนวณนั้นจะถูกตรวจสอบเทียบกับการคำนวณที่ Apple ลงชื่อไว้ บน Mac ที่ใช้ Apple Silicon ตัวโหลดเริ่มต้นระบบจะตรวจสอบยืนยันตราประทับก่อนถ่ายโอนการควบคุมไปยังเคอร์เนล บน Mac ที่ใช้ Intel ที่มีชิป Apple T2 Security ตัวโหลดเริ่มต้นระบบจะส่งต่อการวัดและลายเซ็นไปยังเคอร์เนล จากนั้นจะตรวจสอบยืนยันตราประทับโดยตรงก่อนต่อเชื่อมกับระบบไฟล์ราก ในกรณีใดกรณีหนึ่งต่อไปนี้ หากดำเนินการตรวจสอบยืนยันไม่สำเร็จ กระบวนการเริ่มต้นระบบจะหยุด และผู้ใช้จะได้รับการแจ้งให้ติดตั้ง macOS อีกครั้ง ขั้นตอนนี้จะดำเนินการซ้ำทุกครั้งที่มีการบูต ยกเว้นว่าผู้ใช้ได้เลือกที่จะเข้าสู่โหมดความปลอดภัยต่ำและได้เลือกที่จะปิดใช้งานดิสก์โวลุ่มระบบที่ลงชื่อไว้แยกต่างหาก

ในระหว่างการอัปเดตซอฟต์แวร์ iOS และ iPadOS ดิสก์โวลุ่มของระบบจะถูกจัดเตรียมและคำนวณใหม่ในลักษณะเดียวกัน Bootloader ของ iOS และ iPadOS จะตรวจสอบยืนยันว่าตราประทับไม่เสียหายและตรงกับค่าที่ลงชื่อไว้โดย Apple ก่อนที่จะอนุญาตให้อุปกรณ์เริ่มใช้งานเคอร์เนลได้ ไม่ตรงกันเมื่อบูตแจ้งให้ผู้ใช้อัปเดตซอฟต์แวร์ระบบบนอุปกรณ์ ผู้ใช้ไม่ได้รับอนุญาตให้ปิดใช้งานการป้องกันดิสก์โวลุ่มระบบที่ลงชื่อบน iOS และ iPadOS

SSV และการลงชื่อรหัส

การลงชื่อรหัสยังคงมีอยู่และบังคับใช้โดยเคอร์เนล ดิสก์โวลุ่มระบบที่ลงชื่อจะให้การปกป้องเมื่อมีการอ่านไบต์จากอุปกรณ์จัดเก็บข้อมูลภายนอก ในทางกลับกัน การลงชื่อโค้ดจะให้การปกป้องเมื่อวัตถุ Mach ได้รับการเทียบผังหน่วยความจำเป็นสามารถเรียกใช้ได้ ทั้ง SSV และการลงชื่อรหัสจะปกป้องรหัสที่ปฏิบัติงานได้บนเส้นทางการอ่านและปฏิบัติการทั้งหมด

SSV และ FileVault

ใน macOS 11 การปกป้องในเครื่องที่เทียบเท่ากันสำหรับเนื้อหาระบบจะมาจาก SSV ดังนั้นดิสก์โวลุ่มระบบไม่จำเป็นต้องเข้ารหัสอีกต่อไป การแก้ไขใดๆ ที่ดำเนินการไปยังระบบไฟล์ขณะพักอยู่จะตรวจพบโดยระบบไฟล์เมื่อมีการอ่าน ถ้าผู้ใช้ได้เปิดใช้งาน FileVault ไว้ เนื้อหาของผู้ใช้บนดิสก์โวลุ่มข้อมูลจะยังคงเข้ารหัสอยู่ด้วยความลับที่ผู้ใช้กำหนด

ถ้าผู้ใช้เลือกที่จะปิดใช้งาน SSV ระบบที่พักอยู่จะมีช่องโหว่ให้ดัดแปลง และการดัดแปลงนี้อาจช่วยให้ผู้โจมตีดึงข้อมูลผู้ใช้ที่เข้ารหัสเมื่อมีการเริ่มต้นระบบในครั้งถัดไปได้ ดังนั้น ระบบจะไม่อนุญาตให้ผู้ใช้ปิดใช้งาน SSV หากเปิดใช้งาน FileVault อยู่ การปกป้องขณะพักอยู่ต้องเปิดใช้งานหรือปิดใช้งานอยู่สำหรับดิสก์โวลุ่มทั้งสองดิสก์ด้วยการทำงานที่สอดคล้องกัน

ใน macOS 10.15 หรือก่อนหน้า FileVault ปกป้องซอฟต์แวร์ของระบบปฏิบัติการขณะที่ซอฟต์แวร์พักอยู่โดยการเข้ารหัสเนื้อหาของผู้ใช้และระบบด้วยกุญแจที่ปกป้องโดยความลับที่ผู้ใช้กำหนด การทำงานนี้จะป้องกันผู้โจมตีที่เข้าถึงอุปกรณ์ทางกายภาพได้ไม่ให้สามารถเข้าถึงหรือแก้ไขระบบไฟล์ที่มีซอฟต์แวร์ระบบได้อย่างมีประสิทธิภาพ

SSV และ Mac ที่มีชิป Apple T2 Security

บน Mac ที่มีชิป Apple T2 Security เฉพาะ macOS เองเท่านั้นที่ได้รับการปกป้องจาก SSV ซอฟต์แวร์ที่ทำงานบนชิป T2 และตรวจสอบยืนยัน macOS ได้รับการปกป้องโดยการบูตอย่างปลอดภัย

รายการอัปเดตซอฟต์แวร์ที่ปลอดภัย

ความปลอดภัยคือกระบวนการ การบูตระบบปฏิบัติการเวอร์ชั่นที่ติดตั้งจากโรงงานได้อย่างสม่ำเสมอนั้นไม่เพียงพอ ระบบยังต้องมีกลไกที่สามารถรับรายการอัปเดตความปลอดภัยล่าสุดได้อย่างรวดเร็วและปลอดภัยอีกด้วย Apple ออกรายการอัปเดตซอฟต์แวร์เพื่อแก้ไขข้อกังวลเรื่องความปลอดภัยที่เกิดขึ้นอยู่เสมอ ผู้ใช้อุปกรณ์ iOS และ iPadOS จะรับการแจ้งเตือนรายการอัปเดตบนอุปกรณ์ ผู้ใช้ Mac จะพบรายการอัปเดตที่มีให้ใช้งานในการตั้งค่าระบบ รายการอัปเดตจะมีการส่งแบบไร้สาย เพื่อให้รับการแก้ไขความปลอดภัยล่าสุดได้อย่างรวดเร็ว

กระบวนการอัปเดต

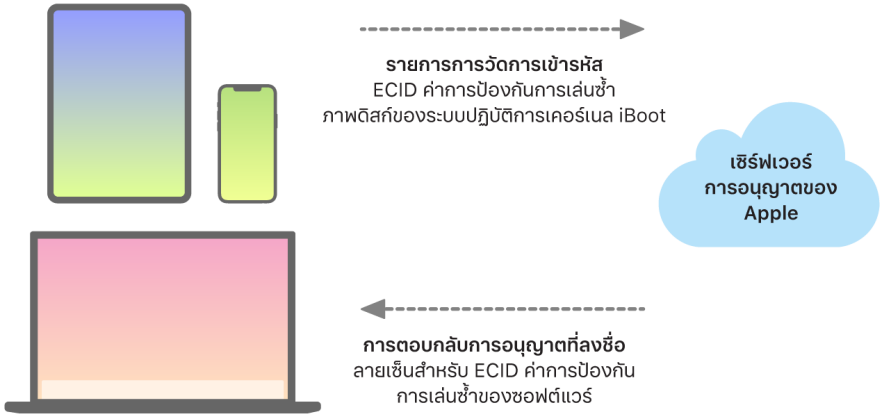
กระบวนการอัปเดตจะใช้รากของความเชื่อถือด้านฮาร์ดแวร์เดียวกันกับที่การบูตอย่างปลอดภัยใช้ ซึ่งออกแบบมาเพื่อติดตั้งเฉพาะโค้ดที่ Apple ลงชื่อเท่านั้น กระบวนการอัปเดตยังใช้การอนุญาตซอฟต์แวร์ระบบเพื่อตรวจสอบให้แน่ใจด้วยว่ามีเพียงสำเนาของเวอร์ชั่นระบบปฏิบัติการที่ลงชื่อโดย Apple เท่านั้นที่จะสามารถติดตั้งบนอุปกรณ์ iOS และ iPadOS หรือบนคอมพิวเตอร์ Mac ได้ โดยที่มีการตั้งค่าความปลอดภัยแบบเต็มถูกกำหนดค่าเป็นนโยบายการบูตอย่างปลอดภัยในยูทิลิตี้ความปลอดภัยของการเริ่มต้นระบบ กระบวนการที่ปลอดภัยเหล่านี้ช่วยให้ Apple หยุดลงชื่อระบบปฏิบัติการเวอร์ชั่นเก่ากว่าที่มีช่องโหว่ที่รู้จักและช่วยป้องกันการโจมตีแบบดาวน์เกรดได้

เพื่อความปลอดภัยมากยิ่งขึ้นในการอัปเดตซอฟต์แวร์ เมื่อเสียบอุปกรณ์ที่จะอัปเกรดเข้ากับ Mac ระบบจะดาวน์โหลดและติดตั้งสำเนาแบบเต็มของ iOS หรือ iPadOS แต่สำหรับการอัปเดตซอฟต์แวร์ผ่านทางอากาศ (OTA) **จะดาวน์โหลดเฉพาะองค์ประกอบที่จำเป็นต่อการอัปเดตให้สมบูรณ์เท่านั้น** ซึ่งจะช่วยปรับปรุงประสิทธิภาพเครือข่ายโดยไม่ดาวน์โหลดระบบปฏิบัติการทั้งระบบ นอกจากนี้ รายการอัปเดตซอฟต์แวร์ยังสามารถจัดเก็บเป็นแคชบน Mac ที่ใช้ macOS 10.13 ขึ้นไปที่เปิดใช้การแคชเนื้อหาได้อีกด้วย ดังนั้นอุปกรณ์ iOS และ iPadOS จึงไม่จำเป็นต้องดาวน์โหลดรายการอัปเดตที่จำเป็นผ่านทางอินเทอร์เน็ตอีกครั้ง (แต่ยังคงต้องติดต่อเซิร์ฟเวอร์ของ Apple เพื่อดำเนินการกระบวนการอัปเดตให้เสร็จสมบูรณ์)

กระบวนการอัปเดตที่ปรับให้เป็นส่วนตัว

ในระหว่างที่อัปเกรดและอัปเดตนั้น จะมีการเชื่อมต่อกับเซิร์ฟเวอร์รับรองความถูกต้องในการติดตั้งของ Apple ซึ่งประกอบด้วยรายการหน่วยที่เข้ารหัสสำหรับส่วนของชุดรวมการติดตั้งแต่ละส่วนที่ต้องติดตั้ง (ตัวอย่างเช่น iBoot, เคอร์เนล และภาพดิสก์ระบบปฏิบัติการ) ค่าป้องกันการเล่นซ้ำแบบสุ่ม (Nonce) และ Exclusive Chip Identification (ECID) เฉพาะของอุปกรณ์

เซิร์ฟเวอร์การอนุญาตจะตรวจสอบรายการหน่วยที่นำเสนอเทียบกับเวอร์ชั่นที่ได้รับอนุญาตให้ติดตั้ง และถ้าพบรายการที่ตรงกัน จะเพิ่ม ECID ไปที่หน่วยและลงชื่อในผลการตรวจสอบ เซิร์ฟเวอร์จะส่งชุดของข้อมูลที่ลงชื่อที่สมบูรณ์ไปยังอุปกรณ์เป็นส่วนหนึ่งของกระบวนการอัปเกรด การเพิ่ม ECID เป็นการ “ปรับเฉพาะเครื่อง” สำหรับการรับรองความถูกต้องของอุปกรณ์ที่ร้องขอ ด้วยการตรวจสอบความถูกต้องและลงชื่อเฉพาะหน่วยที่ทราบชื่อ เซิร์ฟเวอร์จะช่วยให้การรับรองว่าการอัปเดตเกิดขึ้นตามที่ Apple กำหนดอย่างไม่ผิดเพี้ยน



การประเมินลำดับการตรวจสอบความน่าเชื่อถือในการบูตจะตรวจสอบยืนยันว่าลายเซ็นมาจาก Apple และหน่วยของรายการที่โหลดจากอุปกรณ์จัดเก็บข้อมูลพร้อมกับ ECID ของอุปกรณ์นั้นตรงกับข้อมูลที่รับรองด้วยลายเซ็นนั้น ขั้นตอนเหล่านี้ได้รับการออกแบบมาเพื่อให้แน่ใจว่าบนอุปกรณ์ที่รองรับการปรับให้เป็นส่วนตัว การอนุญาตจะเป็นไปสำหรับอุปกรณ์ที่เจาะจงและระบบปฏิบัติการที่เก่ากว่าหรือเวอร์ชั่นเฟิร์มแวร์จากอุปกรณ์เครื่องหนึ่งจะไม่สามารถคัดลอกไปยังอุปกรณ์เครื่องอื่นได้ Nonce ช่วยป้องกันไม่ให้ผู้โจมตีบันทึกการตอบสนองของเซิร์ฟเวอร์และใช้เพื่อแทรกแซงอุปกรณ์หรือแก้ไขซอฟต์แวร์ระบบ

กระบวนการปรับให้เป็นส่วนตัวเป็นเหตุผลที่ต้องใช้การเชื่อมต่อเครือข่ายไปที่ Apple เสมอในการอัปเดตอุปกรณ์ใดก็ตามที่ใช้ Silicon ที่ Apple ออกแบบ ซึ่งรวมถึง Mac ที่ใช้ Intel ที่มีชิป Apple T2 Security

สุดท้ายแล้ว ดิสก์โวลุ่มข้อมูลของผู้ใช้จะไม่ถูกต่อเชื่อมในระหว่างการอัปเดตซอฟต์แวร์ เพื่อช่วยป้องกันไม่ให้มีการอ่านหรือเขียนดิสก์โวลุ่มนั้นในระหว่างการอัปเดต

บนอุปกรณ์ที่มี Secure Enclave ฮาร์ดแวร์นั้นจะใช้การอนุญาตซอฟต์แวร์ระบบในลักษณะที่คล้ายกันเพื่อตรวจสอบถึงความสมบูรณ์ของซอฟต์แวร์และได้รับการออกแบบมาเพื่อป้องกันการติดตั้งเวอร์ชั่นที่เก่ากว่าอีกด้วย

ความสมบูรณ์ของระบบปฏิบัติการ

ซอฟต์แวร์ระบบปฏิบัติการของ Apple ได้รับการออกแบบมาโดยยึดถือความปลอดภัยเป็นสิ่งสำคัญ การออกแบบนี้ประกอบไปด้วยรากของความเชื่อถือฮาร์ดแวร์ซึ่งถูกนำมาใช้เพื่อเปิดใช้งานการบูตอย่างปลอดภัยและกระบวนการอัปเดตซอฟต์แวร์ที่ปลอดภัยซึ่งรวดเร็วและปลอดภัย ระบบปฏิบัติการของ Apple ยังใช้ความสามารถของฮาร์ดแวร์ที่ใช้ Silicon ที่สร้างขึ้นตามจุดประสงค์เพื่อช่วยป้องกันไม่ให้เกิดการใช้ประโยชน์ขณะที่ระบบทำงานอีกด้วย คุณสมบัติรันไทม์เหล่านี้จะปกป้องความสมบูรณ์ของโค้ดที่เชื่อถือแล้วในขณะที่โค้ดนั้นถูกเรียกใช้ สรุปแล้ว ซอฟต์แวร์ระบบปฏิบัติการของ Apple จะช่วยลดการโจมตีและเทคนิคการใช้ประโยชน์ต่างๆ ไม่ว่าจะมาจากแอปที่ประสงค์ร้าย จากเว็บ หรือผ่านช่องทางอื่นใดก็ตาม การปกป้องที่ระบุในที่นี้มีให้ใช้งานบนอุปกรณ์ที่มี SoC ที่ Apple ออกแบบและที่รองรับ ซึ่งรวมถึง iOS, iPadOS, tvOS, watchOS และตอนนี้รวมถึง macOS บน Mac ที่ใช้ Apple Silicon

คุณสมบัติ	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7	ตระกูล M1
การปกป้องความสมบูรณ์ของเคอร์เนล	✓	✓	✓	✓	✓	✓
การจำกัดสิทธิ์อย่างรวดเร็ว		✓	✓	✓	✓	✓
การปกป้องความสมบูรณ์ของหน่วยประมวลผลร่วมของระบบ			✓	✓	✓	✓
รหัสการตรวจสอบสิทธิ์ตัวชี้			✓	✓	✓	✓
ระดับชั้นการปกป้องหน้า		✓	✓	✓	✓	ดูหมายเหตุด้านล่าง

หมายเหตุ: ระดับชั้นการปกป้องหน้า (PPL) กำหนดให้แพลตฟอร์มเรียกใช้**เฉพาะ**โค้ดที่ลงชื่อและเชื่อถือแล้ว นี่เป็นโมเดลความปลอดภัยที่ไม่สามารถใช้ได้บน macOS

การปกป้องความสมบูรณ์ของเคอร์เนล

หลังจากที่เคอร์เนลของระบบปฏิบัติการเริ่มต้นทำงานแล้ว การปกป้องความสมบูรณ์ของเคอร์เนล (KIP) จะถูกเปิดใช้งานเพื่อช่วยป้องกันการแก้ไขโค้ดของเคอร์เนลและไดรเวอร์ ตัวควบคุมหน่วยความจำมอบพื้นที่หน่วยความจำทางกายภาพที่มีรหัสปกป้องซึ่ง iBoot ใช้ในการโหลดเคอร์เนลและส่วนขยายเคอร์เนล หลังจากที่การเริ่มต้นระบบเสร็จสมบูรณ์แล้ว ตัวควบคุมหน่วยความจำจะปฏิเสธการเขียนบนพื้นที่หน่วยความจำทางกายภาพที่มีรหัสปกป้อง หน่วยการจัดการหน่วยความจำ (MMU) ของหน่วยประมวลผลแอปพลิเคชันจะถูกกำหนดค่าเพื่อช่วยป้องกันการเทียบผังโค้ดที่มีสิทธิ์พิเศษจากหน่วยความจำทางกายภาพที่อยู่นอกพื้นที่หน่วยความจำที่มีรหัสปกป้อง และเพื่อช่วยป้องกันการเทียบผังแบบเขียนได้ของหน่วยความจำทางกายภาพภายในพื้นที่หน่วยความจำเคอร์เนล

ในการป้องกันไม่ให้กำหนดค่าอีกครั้ง ฮาร์ดแวร์ที่ใช้ในการเปิดใช้งาน KIP จะถูกล็อคหลังจากที่กระบวนการบูตเสร็จสมบูรณ์

การจำกัดสิทธิ์อย่างรวดเร็ว

เริ่มต้นด้วย A11 Bionic SoC และ S3 SoC ของ Apple พื้นฐานฮาร์ดแวร์ใหม่ได้มีการนำมาใช้ โดยพื้นฐานนี้ ซึ่งเรียกว่าการจำกัดสิทธิ์อย่างรวดเร็ว จะมีรีจิสเตอร์ CPU ที่จำกัดสิทธิ์ต่อเธรดอย่างรวดเร็ว ด้วยการจำกัดสิทธิ์อย่างรวดเร็ว (หรือเรียกอีกอย่างว่ารีจิสเตอร์ APRR) ระบบปฏิบัติการที่รองรับสามารถเอาสิทธิ์การดำเนินการออกจากหน่วยความจำได้โดยไม่ต้องใช้โอเวอร์เฮดของการเรียกระบบและ Page Table Walk หรือ Page Table Flush รีจิสเตอร์เหล่านี้ให้การเยียวยาอีกขั้นสำหรับการโจมตีจากเว็บ โดยเฉพาะกับโค้ดที่รวบรวมในระหว่างรันไทม์ (การรวบรวมแบบ Just In Time) เนื่องจากหน่วยความจำไม่สามารถเรียกใช้ได้อย่างมีประสิทธิภาพขณะที่มีการอ่านและเขียนไปพร้อมกัน

การปกป้องความสมบูรณ์ของหน่วยประมวลผลร่วมของระบบ

เฟิร์มแวร์ของหน่วยประมวลผลร่วมจะจัดการงานที่สำคัญของระบบเป็นจำนวนมาก ตัวอย่างเช่น Secure Enclave, หน่วยประมวลผลเซ็นเซอร์ภาพ และหน่วยประมวลผลร่วมของการเคลื่อนไหว ดังนั้นความปลอดภัยของเฟิร์มแวร์นี้จึงถือเป็นส่วนสำคัญของความปลอดภัยของระบบโดยรวม ในการป้องกันการแก้ไขเฟิร์มแวร์ของหน่วยประมวลผลร่วม Apple จะใช้กลไกที่เรียกว่า**การปกป้องความสมบูรณ์ของหน่วยประมวลผลร่วมของระบบ (SCIP)**

SCIP ทำงานคล้ายกับการปกป้องความสมบูรณ์ของเคอร์เนล (KIP) มาก: ในระหว่างการบูต iBoot จะโหลดเฟิร์มแวร์ของหน่วยประมวลผลร่วมแต่ละรายการไปยังพื้นที่หน่วยความจำที่มีรหัสปกป้อง ซึ่งเก็บรักษาและแยกออกจากพื้นที่ KIP โดย iBoot จะกำหนดค่า Memory Management Unit ของหน่วยประมวลผลร่วมแต่ละรายการเพื่อช่วยป้องกันดังต่อไปนี้:

- การเทียบผังที่สามารถเรียกใช้ได้นอกเหนือส่วนพื้นที่หน่วยความจำที่มีรหัสปกป้อง
- การเทียบผังแบบเขียนได้ภายในส่วนพื้นที่หน่วยความจำที่มีรหัสปกป้อง

นอกจากนี้ในระหว่างการบูต ในการกำหนดค่า SCIP สำหรับ Secure Enclave ระบบปฏิบัติการ Secure Enclave จะถูกใช้งาน หลังจากที่กระบวนการบูตเสร็จสมบูรณ์ ฮาร์ดแวร์ที่ใช้ในการเปิดใช้งาน SCIP จะถูกล็อค วิธีนี้ได้รับการออกแบบมาป้องกันการกำหนดค่าอีกครั้ง

รหัสการตรวจสอบสิทธิ์ตัวชี้

รหัสการตรวจสอบสิทธิ์ตัวชี้ (PAC) จะใช้เพื่อป้องกันการใช้ประโยชน์จากข้อผิดพลาดที่ทำให้หน่วยความจำเสียหาย ซอฟต์แวร์ระบบและแอปในตัวจะใช้ PAC เพื่อช่วยป้องกันการแก้ไขตัวชี้ฟังก์ชั่นและที่อยู่ส่งกลับ (ตัวชี้รหัส) PAC จะใช้ค่าลับแบบ 128 บิตห้าค่าเพื่อลงชื่อคำสั่งเคอร์เนลและข้อมูล และกระบวนการพื้นที่ผู้ใช้แต่ละกระบวนการจะมีกุญแจ B ของตัวเอง รายการจะได้รับการ salt และลงชื่อตามที่ระบุด้านล่างนี้

รายการ	กุญแจ	Salt
ที่อยู่ส่งกลับฟังก์ชั่น	IB	ที่อยู่พื้นที่จัดเก็บข้อมูล
ตัวชี้ฟังก์ชั่น	IA	0
ฟังก์ชั่นปิดกั้นการเรียกใช้	IA	ที่อยู่พื้นที่จัดเก็บข้อมูล
แคชวิธี Objective-C	IB	ที่อยู่พื้นที่จัดเก็บข้อมูล + คลาส + ตัวเลือก
รายการ C++ V-Table	IA	ที่อยู่พื้นที่จัดเก็บข้อมูล + แฮช (ชื่อวิธีไม่สมบูรณ์)
ป้าย Goto ที่มีการคำนวณ	IA	แฮช (ชื่อฟังก์ชั่น)
สถานะเธรดของเคอร์เนล	GA	•
รีจิสเตอร์สถานะเธรดของผู้ใช้	IA	ที่อยู่พื้นที่จัดเก็บข้อมูล
ตัวชี้ C++ V-Table	DA	0

ค่าลายเซ็นจะถูกจัดเก็บในบิตการเติมเต็มที่ไม่ได้ใช้ที่ด้านบนของตัวชี้ 64 บิต โดยลายเซ็นดังกล่าวจะได้รับการตรวจสอบยืนยันก่อนการใช้งาน และการเติมเต็มจะถูกกู้คืนเพื่อช่วยให้การรับรองที่อยู่ตัวชี้ฟังก์ชั่น การตรวจสอบยืนยันผลลัพธ์ในการยกเลิกไม่สำเร็จ การตรวจสอบยืนยันนี้จะทำให้การโจมตีในหลากหลายรูปแบบดำเนินการได้ยากขึ้น เช่น การโจมตีการเขียนโปรแกรมแบบย้อนกลับ (ROP) ซึ่งจะพยายามหลอกอุปกรณ์ให้เรียกใช้โค้ดที่มีอยู่โดยมีประสงค์ร้ายโดยการควบคุมที่อยู่ส่งกลับฟังก์ชั่นที่จัดเก็บอยู่บนสแต็ค

ระดับชั้นการปกป้องหน้า

ระดับชั้นการปกป้องหน้า (PPL) ใน iOS, iPadOS และ watchOS ได้รับการออกแบบมาเพื่อป้องกันไม่ให้มีการแก้ไขโค้ดพื้นที่ผู้ใช้หลังจากตรวจสอบยืนยันลายเซ็นโค้ดเสร็จ ด้วยการสร้างบนการปกป้องความสมบูรณ์ของเคอร์เนลและการจำกัดสิทธิ์อย่างรวดเร็ว PPL จัดการสิทธิ์การแทนที่ Page Table เพื่อให้แน่ใจว่ามีเพียง PPL เท่านั้นที่สามารถเปลี่ยนหน้าที่มีการปกป้องที่มีโค้ดผู้ใช้และ Page Table ระบบช่วยลดพื้นหน้าของการโจมตีเป็นอย่างมากด้วยการรองรับการบังคับใช้ความสมบูรณ์ของโค้ดทั้งระบบแม้ในขณะที่เคอร์เนลถูกโจมตี การปกป้องนี้จะไม่มีให้ใช้ใน macOS เนื่องจาก PPL สามารถใช้ได้บนระบบที่มีการลงชื่อโค้ดทั้งหมดที่เรียกใช้เท่านั้น

ความสามารถด้านความปลอดภัยของระบบ macOS เพิ่มเติม

ความสามารถด้านความปลอดภัยของระบบ macOS เพิ่มเติม

macOS ทำงานบนชุดของฮาร์ดแวร์ที่กว้างขึ้น (ตัวอย่างเช่น CPU ที่ใช้ Intel, CPU ที่ใช้ Intel ร่วมกับชิป Apple T2 Security และ SoC ที่ใช้ Apple Silicon) และรองรับกรณีการใช้งานการคำนวณทั่วไปที่หลากหลาย ในขณะที่ผู้ใช้บางรายใช้แอปพื้นฐานที่ติดตั้งมาให้แล้วหรือแอปที่มาจาก App Store ผู้ใช้รายอื่นเป็นเคอร์เนลแฮกเกอร์ที่จำเป็นต้องปิดใช้งานการปกป้องทั้งหมดของแพลตฟอร์มเพื่อให้สามารถเรียกใช้และทดสอบโค้ดดำเนินการของพวกเขาได้ด้วยความเชื่อถือระดับสูงสุด ผู้ใช้ส่วนใหญ่จะอยู่ระหว่างผู้ใช้สองประเภทดังกล่าว และในกลุ่มผู้ใช้เหล่านี้ หลายคนมีอุปกรณ์ต่อพ่วงและซอฟต์แวร์ที่ต้องใช้สิทธิ์เข้าถึงในระดับที่แตกต่างกันไป Apple ได้ออกแบบแพลตฟอร์ม macOS ด้วยวิธีการแบบผสานกับฮาร์ดแวร์ ซอฟต์แวร์ และบริการ ซึ่งเป็นแพลตฟอร์มที่มอบความปลอดภัยให้โดยการออกแบบและทำให้กำหนดค่า ปรับใช้ และจัดการได้ง่ายๆ แต่ยังคงความสามารถในการกำหนดค่าที่ผู้ใช้คาดหวัง macOS ยังมีเทคโนโลยีความปลอดภัยที่สำคัญซึ่งผู้เชี่ยวชาญด้าน IT ต้องการเพื่อช่วยปกป้องข้อมูลขององค์กรและรวมไว้ในสภาพแวดล้อมเครือข่ายที่ปลอดภัยขององค์กรอีกด้วย

ความสามารถต่อไปนี้รองรับและช่วยตอบสนองความต้องการด้านต่างๆ ของผู้ใช้ macOS ซึ่งรวมถึง

- ความปลอดภัยของดิสก์โวลุ่มระบบที่ลงชื่อ
- การปกป้องความสมบูรณ์ของระบบ
- แคชความเชื่อถือ
- การปกป้องสำหรับอุปกรณ์ต่อพ่วง
- การรองรับ Rosetta 2 (การแปลอัตโนมัติ) และความปลอดภัยสำหรับ Mac ที่ใช้ Apple Silicon
- การรองรับและการปกป้อง DMA
- การรองรับและความปลอดภัยของส่วนขยายเคอร์เนล (kext)
- การรองรับและความปลอดภัยของ Option ROM
- ความปลอดภัยของเฟิร์มแวร์ UEFI สำหรับคอมพิวเตอร์ Mac ที่ใช้ Intel

การปกป้องความสมบูรณ์ของระบบ

macOS ใช้สิทธิ์เคอร์เนลเพื่อจำกัดความสามารถในการเขียนของไฟล์ระบบที่สำคัญด้วยคุณสมบัติที่เรียกว่า**การปกป้องความสมบูรณ์ของระบบ (SIP)** คุณสมบัตินี้เป็นคุณสมบัติที่แตกต่างและนอกเหนือจากการปกป้องความสมบูรณ์ของเคอร์เนล (KIP) ด้านฮาร์ดแวร์ที่มีให้ใช้งานบน Mac ที่ใช้ Apple Silicon ซึ่งจะปกป้องการแก้ไขเคอร์เนลในหน่วยความจำ เทคโนโลยีการควบคุมการเข้าถึงแบบบังคับจะถูกนำมาใช้เพื่อให้การปกป้องนี้และการปกป้องระดับเคอร์เนลอื่นๆ อีกหลายรายการ ซึ่งรวมถึงการทำ Sandbox และ Data Vault

การควบคุมการเข้าถึงแบบบังคับ

macOS ใช้การควบคุมการเข้าถึงแบบบังคับ ซึ่งเป็นนโยบายที่กำหนดข้อจำกัดด้านความปลอดภัยที่นักพัฒนาสร้างขึ้นซึ่งไม่สามารถเขียนทับได้ วิธีการนี้จะแตกต่างจากการควบคุมการเข้าถึงแบบมีเงื่อนไขซึ่งอนุญาตให้ผู้ใช้เขียนทับนโยบายด้านความปลอดภัยตามการตั้งค่าของพวกเขาได้

ผู้ใช้จะไม่เห็นการควบคุมการเข้าถึงแบบบังคับ แต่การควบคุมเหล่านั้นจะเป็นเทคโนโลยีพื้นฐานที่ช่วยเปิดใช้งานคุณสมบัติที่สำคัญหลายอย่าง รวมถึงการทำ Sandbox การควบคุมโดยผู้ปกครอง การตั้งค่าที่ได้รับการจัดการ ส่วนขยาย และการปกป้องความสมบูรณ์ของระบบ

การปกป้องความสมบูรณ์ของระบบ

การปกป้องความสมบูรณ์ของระบบจะจำกัดส่วนประกอบให้เป็นแบบอ่านอย่างเดียวในตำแหน่งเฉพาะที่สำคัญของระบบไฟล์เพื่อช่วยป้องกันไม่ให้โค้ดที่ประสงค์ร้ายแก้ไขตำแหน่งของระบบไฟล์ การปกป้องความสมบูรณ์ของระบบเป็นการตั้งค่าเฉพาะสำหรับคอมพิวเตอร์ที่เปิดตามค่าเริ่มต้นเมื่อผู้ใช้อัปเกรดเป็น OS X 10.11 ขึ้นไป บน Mac ที่ใช้ Intel การปิดใช้งานการตั้งค่านี้จะเป็นการเอาการปกป้องสำหรับพาร์ติชั่นทั้งหมดบนอุปกรณ์จัดเก็บข้อมูลจริงออก macOS ปรับใช้นโยบายด้านความปลอดภัยนี้กับทุกกระบวนการที่ทำงานบนระบบ ไม่ว่าจะใช้งาน Sandbox หรือมีสิทธิ์ผู้ดูแลระบบก็ตาม

แคชความเชื่อถือ

หนึ่งในวัตถุที่รวมอยู่ในลำดับการบูตอย่างปลอดภัยคือแคชความเชื่อถือแบบคงที่ ซึ่งเป็นบันทึกที่เชื่อถือแล้วของไบนารี Mach-O ทั้งหมดที่มีการคัดลอกแบบมาสเตอร์ไปยังดิสก์โวลุ่มระบบที่ลงชื่อ Mach-O แต่ละรายการจะแสดงด้วยแฮชไดเรกทอรีโค้ด เพื่อการค้นหาอย่างมีประสิทธิภาพ แฮชเหล่านี้จะถูกเรียงก่อนจะถูกใส่ลงในแคชความเชื่อถือ ไดเรกทอรีโค้ดคือผลลัพธ์ของการดำเนินการลงชื่อที่ทำโดย `codesign(1)` ในการบังคับใช้แคชความเชื่อถือ SIP จะต้องเปิดใช้งานอยู่ ในการปิดใช้งานการบังคับใช้แคชความเชื่อถือบน Mac ที่ใช้ Apple Silicon การบูตอย่างปลอดภัยจะต้องกำหนดค่าเป็นความปลอดภัยแบบอนุญาต

เมื่อเรียกใช้ไบนารี (ไม่ว่าจะเพื่อสร้างกระบวนการใหม่หรือเทียบผังโค้ดที่เรียกใช้ได้ไปยังกระบวนการที่มีอยู่แล้ว) ไดเรกทอรีโค้ดของไบนารีจะถูกดึงข้อมูลและแฮช ถ้าพบแฮชผลลัพธ์ในแคชความเชื่อถือ การเทียบผังที่สามารถเรียกใช้ได้ที่สร้างขึ้นสำหรับไบนารีจะได้รับสิทธิ์ของแพลตฟอร์ม นั่นคือ การเทียบผังเหล่านั้นสามารถครอบครองสิทธิ์ใดๆ และทำงานได้โดยไม่ต้องตรวจสอบยืนยันเพิ่มเติมเกี่ยวกับความน่าเชื่อถือของลายเซ็น กระบวนการนี้จะตรงข้ามกับ Mac ที่ใช้ Intel ซึ่งสิทธิ์ของแพลตฟอร์มจะถูกส่งไปยังเนื้อหาระบบปฏิบัติการโดยใบรับรองของ Apple ที่ลงชื่อไบนารี (ใบรับรองนี้ไม่ได้จำกัดว่าสิทธิ์ใดที่ไบนารีสามารถมีได้)

ไบนารีที่ไม่ใช่แพลตฟอร์ม (ตัวอย่างเช่น โค้ดของบริษัทอื่นที่มีการรับรองแล้ว) จะต้องมีลำดับใบรับรองที่ถูกต้องจึงจะสามารถเรียกใช้ได้ และสิทธิ์ที่ไบนารีสามารถมีได้จะถูกจำกัดโดยโปรไฟล์การลงชื่อที่ออกให้กับนักพัฒนาโดย Apple Developer Program

ไบนารีทั้งหมดที่จัดส่งภายใน macOS จะมีการลงชื่อด้วย**ข้อมูลจำเพาะของแพลตฟอร์ม** บน Mac ที่ใช้ Apple Silicon ข้อมูลจำเพาะนี้จะใช้เพื่อระบุว่า แม้ว่าไบนารีจะมีการลงชื่อโดย Apple แฮชไดเรกทอรีโค้ดจะต้องมีอยู่ในแคชความเชื่อถือจึงจะสามารถเรียกใช้ได้ บน Mac ที่ใช้ Intel ข้อมูลจำเพาะของแพลตฟอร์มจะใช้เพื่อดำเนินการเพิกถอนแบบมีเป้าหมายของไบนารีจาก macOS เวอร์ชั่นที่เก่ากว่า การเพิกถอนแบบมีเป้าหมายนี้จะป้องกันไม่ให้ไบนารีเหล่านั้นเรียกใช้บนเวอร์ชั่นที่ใหม่กว่า

แคชความเชื่อถือแบบคงที่จะล็อคชุดของไบนารีอย่างสมบูรณ์ไปยัง macOS เวอร์ชั่นที่กำหนด ลักษณะการทำเช่นนี้จะช่วยป้องกันไบนารีที่ Apple ลงชื่ออย่างถูกต้องจากระบบปฏิบัติการที่เก่ากว่าไม่ให้ถูกนำเข้าไปยังเวอร์ชั่นที่ใหม่กว่าเพื่อให้ผู้โจมตีสามารถใช้ประโยชน์ได้

โค้ดแพลตฟอร์มที่จัดส่งภายนอกระบบปฏิบัติการ

Apple จัดส่งไบนารีบางรายการ เช่น Xcode และสแต็คเครื่องมือการพัฒนา ที่ไม่ได้ลงชื่อด้วยข้อมูลจำเพาะของแพลตฟอร์ม แม้จะเป็นเช่นนั้น Apple ก็ยังคงได้รับอนุญาตให้ดำเนินการด้วยสิทธิ์ของแพลตฟอร์มบน Mac ที่ใช้ Apple Silicon และ Mac ที่มีชิป T2 เนื่องจากซอฟต์แวร์แพลตฟอร์มนี้มีการจัดส่งอย่างอิสระจาก macOS ซอฟต์แวร์จึงไม่อยู่ภายใต้ลักษณะการทำงานการเพิกถอนที่กำหนดโดยแคชความเชื่อถือแบบคงที่

แคชความเชื่อถือแบบโหลดได้

Apple จัดส่งแพ็คเกจซอฟต์แวร์บางรายการพร้อมกับ**แคชความเชื่อถือแบบโหลดได้** แคชเหล่านี้มีโครงสร้างข้อมูลเดียวกันกับแคชความเชื่อถือแบบคงที่ แต่แม้ว่าแคชความเชื่อถือแบบคงที่จะมีเพียงรายการเดียว และเนื้อหาของแคชมักจะถูกล็อคอยู่ในช่วงอ่านอย่างเดียวเสมอหลังจากที่การเริ่มต้นทำงานในช่วงต้นของเคอร์เนลได้สิ้นสุดลง แคชความเชื่อถือแบบโหลดได้จะถูกเพิ่มไปยังระบบในระหว่างรันไทม์

แคชความเชื่อถือเหล่านี้มีการตรวจสอบสิทธิ์ผ่านกลไกเดียวกันกับกลไกที่ตรวจสอบสิทธิ์เฟิร์มแวร์การบูต (การปรับให้เป็นส่วนตัวโดยใช้บริการการลงชื่อที่เชื่อถือได้ของ Apple) หรือกลไกเดียวกันกับวัตถุที่มีการลงชื่อสากล (ซึ่งมีลายเซ็นที่ไม่ผูกกับอุปกรณ์ใดโดยเฉพาะ)

ตัวอย่างหนึ่งของแคชความเชื่อถือที่ปรับให้เป็นส่วนตัวคือแคชที่จัดส่งมาพร้อมกับภาพดิสก์ที่ใช้ดำเนินการการวินิจฉัยช่องบน Mac ที่ใช้ Apple Silicon แคชความเชื่อถือนี้มีการปรับให้เป็นส่วนตัว พร้อมกับภาพดิสก์ แล้วโหลดไปยังเคอร์เนลของคอมพิวเตอร์ Mac เป้าหมายขณะที่เครื่องบูตไปยังโหมดการวินิจฉัย แคชที่เชื่อถือได้ช่วยให้ซอฟต์แวร์ภายในภาพดิสก์ทำงานด้วยสิทธิ์ของแพลตฟอร์มได้

ตัวอย่างของแคชความเชื่อถือที่มีการลงชื่อสากลจะถูกจัดส่งพร้อมกับรายการอัปเดตซอฟต์แวร์ macOS แคชความเชื่อถือนี้จะอนุญาตให้ชิ้นส่วนของโค้ดภายในรายการอัปเดตซอฟต์แวร์ หรือที่เรียกว่า***สมองของการอัปเดต*** ทำงานด้วยสิทธิ์ของแพลตฟอร์ม สมองของการอัปเดตจะดำเนินการใดๆ เพื่อสร้างการอัปเดตซอฟต์แวร์ที่ระบบโฮสต์ไม่สามารถดำเนินการได้ในลักษณะที่สอดคล้องกันในเวอร์ชั่นต่างๆ

ความปลอดภัยของหน่วยประมวลผลอุปกรณ์ต่อพ่วงในคอมพิวเตอร์ Mac

ระบบการคำนวณสมัยใหม่ทั้งหมดมีหน่วยประมวลผลอุปกรณ์ต่อพ่วงในตัวหลายหน่วยประมวลผลที่ใช้กับงานต่างๆ เช่น ระบบเครือข่าย กราฟิก การจัดการพลังงาน และอื่นๆ หน่วยประมวลผลอุปกรณ์ต่อพ่วงเหล่านี้มักมีวัตถุประสงค์เดียวและมีประสิทธิภาพน้อยกว่า CPU หลักมาก อุปกรณ์ต่อพ่วงในตัวที่มีความปลอดภัยไม่เพียงพอจะกลายเป็นเป้าหมายที่ง่ายขึ้นต่อการใช้ประโยชน์จากผู้โจมตี ซึ่งเป็นวิธีที่ผู้โจมตีสามารถปล่อยไวรัสเข้าสู่ระบบปฏิบัติการได้อย่างต่อเนื่อง หลังจากที่ทำให้เฟิร์มแวร์หน่วยประมวลผลอุปกรณ์ต่อพ่วงติดไวรัสแล้ว ผู้โจมตีจะสามารถกำหนดเป้าหมายซอฟต์แวร์บน CPU หลักได้ หรือบันทึกข้อมูลที่สำคัญได้โดยตรง (ตัวอย่างเช่น อุปกรณ์อีเธอร์เน็ตจะสามารถดูเนื้อหาของแพ็คเกตที่ไม่ได้เข้ารหัสอยู่ได้)

เมื่อใดก็ตามที่เป็นไปได้ Apple จะทำงานเพื่อลดจำนวนหน่วยประมวลผลอุปกรณ์ต่อพ่วงที่จำเป็น และเพื่อหลีกเลี่ยงการออกแบบที่ต้องใช้เฟิร์มแวร์ แต่เมื่อต้องใช้หน่วยประมวลผลแบบแยกที่มีเฟิร์มแวร์เป็นของตนเอง ระบบจะพยายามช่วยทำให้มั่นใจว่าผู้โจมตีจะไม่สามารถโจมตีหน่วยประมวลผลนั้นต่อไปได้ ความพยายามนี้อาจเป็นการตรวจสอบยืนยันหน่วยประมวลผลด้วยวิธีใดวิธีหนึ่งจากสองวิธี:

- เรียกใช้หน่วยประมวลผลเพื่อให้ดาวน์โหลดเฟิร์มแวร์ที่ผ่านการตรวจสอบยืนยันแล้วจาก CPU หลักเมื่อเริ่มต้นระบบ
- ทำให้หน่วยประมวลผลอุปกรณ์ต่อพ่วงใช้ลำดับการบูตอย่างปลอดภัยของตัวเองเพื่อตรวจสอบยืนยันเฟิร์มแวร์ของหน่วยประมวลผลอุปกรณ์ต่อพ่วงทุกครั้งที่ Mac เริ่มต้นระบบ

Apple ทำงานร่วมกับผู้จำหน่ายในการตรวจสอบการใช้งาน และปรับปรุงการออกแบบของพวกเขาเพื่อรวมคุณสมบัติที่ต้องการ เช่น:

- การสร้างความมั่นใจในความรัดกุมของการเข้ารหัสขั้นต่ำ
- การสร้างความมั่นใจในการเพิกถอนแบบเต็มของเฟิร์มแวร์ที่ทราบว่ามีข้อบกพร่อง
- การปิดใช้งานอินเทอร์เฟซแก้ไขข้อบกพร่อง
- การลงชื่อเฟิร์มแวร์ด้วยกุญแจการเข้ารหัสที่จัดเก็บอยู่ในโมดูลรักษาความปลอดภัยฮาร์ดแวร์ (HSM) ที่ควบคุมโดย Apple

ในช่วงไม่กี่ปีที่ผ่านมา Apple ได้ทำงานร่วมกับผู้จำหน่ายภายนอกบางรายเพื่อใช้โครงสร้างข้อมูล “Image4” โค้ดการตรวจสอบยืนยัน และโครงสร้างพื้นฐานการลงชื่อแบบเดียวกัน ซึ่งใช้ใน Apple Silicon

เมื่อไม่มีการดำเนินการแบบไม่มีพื้นที่จัดเก็บข้อมูลหรือพื้นที่จัดเก็บข้อมูลที่มีการบูตอย่างปลอดภัยเป็นตัวเลือก การออกแบบจะบังคับให้ลงชื่อรับรองแบบเข้ารหัสและตรวจสอบยืนยันรายการอัปเดตเฟิร์มแวร์ก่อนจึงจะสามารถอัปเดตพื้นที่จัดเก็บข้อมูลแบบถาวรได้

Rosetta 2 บน Mac ที่ใช้ Apple Silicon

Mac ที่ใช้ Apple Silicon สามารถเรียกใช้โค้ดที่รวบรวมไว้สำหรับชุดคำสั่ง x86_64 ได้โดยใช้กลไกการแปลที่เรียกว่า **Rosetta** 2 การแปลที่มีให้ใช้แบ่งออกเป็นสองประเภท: Just In Time และ Ahead Of Time

การแปลแบบ Just In Time

ในวิธีการแปลแบบ Just In Time (JIT) วัตถุ Mach x86_64 จะมีการระบุในช่วงต้นของเส้นทางการเรียกใช้ภาพดิสก์ เมื่อพบภาพดิสก์เหล่านี้ เคอร์เนลจะถ่ายโอนการควบคุมไปยัง Stub การแปลแบบพิเศษของ Rosetta แทนที่จะไปยังตัวแก้ไขลิงก์ไดนามิก `dyld(1)` จากนั้น Stub การแปลจะแปลหน้า x86_64 ในระหว่างการเรียกใช้ภาพดิสก์ การแปลทั้งหมดนี้เกิดขึ้นภายในกระบวนการ เคอร์เนลจะยังคงตรวจสอบยืนยันแฮชโค้ดของ x86_64 แต่ละหน้ากับลายเซ็นโค้ดที่แนบมากับไบนารีเนื่องจากหน้ามีข้อบกพร่อง ในกรณีที่แฮชไม่ตรงกัน เคอร์เนลจะบังคับใช้นโยบายการเยียวยาที่เหมาะสมกับกระบวนการนั้น

การแปลแบบ Ahead Of Time

ในเส้นทางการแปลแบบ Ahead Of Time (AOT) ระบบจะอ่านไบนารี x86_64 จากพื้นที่จัดเก็บข้อมูลในเวลาที่ระบบถือว่าเหมาะสมที่สุดสำหรับการตอบสนองของโค้ดนั้น สิ่งแปลกปลอมที่แปลแล้วจะถูกเขียนไปยังพื้นที่จัดเก็บข้อมูลเป็นไฟล์วัตถุ Mach ประเภทพิเศษ ไฟล์นั้นจะคล้ายกับภาพดิสก์ที่เรียกใช้ได้ แต่จะถูกทำเครื่องหมายไว้เพื่อระบุว่าเป็นผลิตภัณฑ์ที่แปลแล้วของภาพดิสก์อื่น

ในโมเดลนี้ สิ่งแปลกปลอม AOT จะรับข้อมูลประจำตัวทั้งหมดจากภาพดิสก์ x86_64 ดั้งเดิมที่เรียกใช้ได้ ในการบังคับใช้การผูกมัดนี้ เอนทิตี้พื้นที่ผู้ใช้ที่มีสิทธิ์จะลงชื่อสิ่งแปลกปลอมการแปลโดยใช้กุญแจเฉพาะอุปกรณ์ที่จัดการโดย Secure Enclave กุญแจนี้จะเผยแพร่ไปยังเอนทิตี้พื้นที่ผู้ใช้ที่มีสิทธิ์เท่านั้น ซึ่งระบุเป็นเช่นนั้นโดยใช้สิทธิ์ที่จำกัด ไดเรกทอรีโค้ดที่สร้างขึ้นสำหรับสิ่งแปลกปลอมการแปลจะมีแฮชไดเรกทอรีโค้ดของภาพดิสก์ x86_64 ดั้งเดิมที่เรียกใช้ได้ ลายเซ็นที่อยู่บนตัวสิ่งแปลกปลอมการแปลเองจะเรียกว่า**ลายเซ็นเสริม**

วิธีการ AOT จะเริ่มต้นคล้ายกับวิธีการ JIT โดยเคอร์เนลจะถ่ายโอนการควบคุมไปยังรันไทม์ Rosetta แทนที่จะไปยังตัวแก้ไขลิงก์ไดนามิก `dyld(1)` แต่หลังจากนั้น รันไทม์ Rosetta จะส่งการสอบถามการสื่อสารระหว่างกระบวนการ (IPC) ไปยังบริการระบบ Rosetta ซึ่งจะถามว่ามีการแปล AOT ให้ใช้งานสำหรับภาพดิสก์ปัจจุบันที่เรียกใช้ได้หรือไม่ ถ้าพบ บริการ Rosetta จะให้ Handle กับการแปลนั้น และจะมีการเทียบผังกับกระบวนการและเรียกใช้ ในระหว่างการเรียกใช้ เคอร์เนลจะบังคับใช้แฮชไดเรกทอรีโค้ดของสิ่งแปลกปลอมการแปล ซึ่งได้รับตรวจสอบสิทธิ์โดยลายเซ็นที่มีรากฐานมาจากกุญแจการลงชื่อเฉพาะอุปกรณ์ แฮชไดเรกทอรีโค้ดของภาพดิสก์ x86_64 ดั้งเดิมจะไม่มีส่วนร่วมในกระบวนการนี้

สิ่งแปลกปลอมที่แปลแล้วจะถูกจัดเก็บไว้ใน Data Vault ซึ่งจะไม่มีเอนทิตี้ใดที่สามารถเข้าถึงได้ในระหว่างรันไทม์ ยกเว้นบริการ Rosetta บริการ Rosetta จัดการการเข้าถึงแคชของตัวเองโดยเผยแพร่ตัวอธิบายไฟล์แบบอ่านอย่างเดียวไปยังสิ่งแปลกปลอมการแปลแต่ละรายการ การทำเช่นนี้จะจำกัดการเข้าถึงแคชสิ่งแปลกปลอม AOT การสื่อสารระหว่างกระบวนการและพื้นที่ใช้งานแบบพึ่งพาของบริการนี้มีการตั้งใจทำให้แคบอย่างมากเพื่อจำกัดพื้นหน้าของการโจมตี

ถ้าแฮชไดเรกทอรีโค้ดของภาพดิสก์ x86_64 ดั้งเดิมไม่ตรงกับรายการเดียวกันที่เข้ารหัสอยู่ในลายเซ็นของสิ่งแปลกปลอมการแปล AOT ผลลัพธ์นี้จะถือว่าเทียบเท่ากับลายเซ็นโค้ดไม่ถูกต้อง และระบบจะดำเนินการการบังคับใช้ที่เหมาะสม

ถ้ากระบวนการระยะไกลสอบถามเคอร์เนลสำหรับสิทธิ์หรือคุณสมบัติข้อมูลประจำตัวโค้ดอื่นๆ ของรายการที่เรียกใช้ได้ที่แปลแบบ AOT คุณสมบัติข้อมูลประจำตัวของภาพดิสก์ x86_64 ดั้งเดิมจะถูกส่งกลับมา

เนื้อหาแคชความเชื่อถือแบบคงที่

macOS 11 ขึ้นไป จัดส่งมาพร้อมกับไบนารี Mach แบบ “fat” ที่มีส่วนของโค้ดเครื่องที่เป็น x86_64 และ arm64 บน Mac ที่ใช้ Apple Silicon ผู้ใช้อาจตัดสินใจที่จะเรียกใช้ส่วนที่เป็น x86_64 ของไบนารีระบบผ่านวิธีการ Rosetta ตัวอย่างเช่น เพื่อโหลดปลั๊กอินที่ไม่มีรูปแบบ arm64 ดั้งเดิม ในการรองรับวิธีการนี้ แคชความเชื่อถือแบบคงที่ซึ่งจัดส่งมาพร้อมกับ macOS โดยทั่วไปแล้ว ประกอบด้วยแฮชไดเรกเทอรีโค้ดสามรายการต่อไฟล์วัตถุ Mach หนึ่งไฟล์:

- แฮชไดเรกทอรีโค้ดของส่วน arm64
- แฮชไดเรกทอรีโค้ดของส่วน x86_64
- แฮชไดเรกทอรีโค้ดของการแปลแบบ AOT ของส่วน x86_64

ขั้นตอนการแปล Rosetta แบบ AOT เป็นขั้นตอนที่แน่นอนในลักษณะที่ให้ข้อมูลออกที่เหมือนกันไม่ว่าจะให้ข้อมูลเข้าใดก็ตาม ทั้งนี้จะไม่คำนึงถึงเวลาที่แปลหรืออุปกรณ์ที่ใช้แปล

ในระหว่างการสร้าง macOS ไฟล์วัตถุ Mach ทุกไฟล์จะถูกเรียกใช้ผ่านวิธีการแปล Rosetta แบบ AOT ที่เชื่อมโยงกับ macOS เวอร์ชั่นที่กำลังติดตั้ง แล้วแฮชไดเรกทอรีโค้ดผลลัพธ์จะถูกบันทึกไปยังแคชความเชื่อถือ เพื่อประสิทธิภาพที่ดี ผลิตภัณฑ์ที่แปลจริงจะไม่จัดส่งมาพร้อมกับระบบปฏิบัติการ และจะประกอบใหม่ตามความต้องการเมื่อผู้ใช้ร้องขอ

เมื่อเรียกใช้ภาพดิสก์ x86_64 บน Mac ที่ใช้ Apple Silicon ถ้าแฮชไดเรกทอรีโค้ดของภาพดิสก์นั้นอยู่ในแคชความเชื่อถือแบบคงที่ แฮชไดเรกทอรีโค้ดของสิ่งแปลกปลอม AOT ผลลัพธ์ก็ควรจะอยู่ในแคชความเชื่อถือแบบคงที่ **ด้วยเช่นกัน** ผลิตภัณฑ์ดังกล่าวจะไม่มีการลงชื่อโดยกุญแจเฉพาะอุปกรณ์ เนื่องจากอำนาจการลงชื่อนั้นมีรากฐานมาจากลำดับการบูตอย่างปลอดภัยของ Apple

โค้ด x86_64 ที่ไม่ได้ลงชื่อ

Mac ที่ใช้ Apple Silicon จะไม่อนุญาตให้เรียกใช้โค้ด arm64 ดั้งเดิมนอกจากจะแนบลายเซ็นที่ถูกต้องมาด้วย ลายเซ็นนี้อาจเรียบง่ายเหมือนกับลายเซ็นโค้ดเฉพาะกิจ (cf. `codesign(1)`) ที่ไม่มีข้อมูลประจำตัวจริงใดๆ จากครึ่งลับของคู่กุญแจแบบไม่สมมาตร (ซึ่งเป็นเพียงการวัดของไบนารีที่ไม่มีการตรวจสอบสิทธิ์)

เพื่อความเข้ากันได้กับไบนารี โค้ด x86_64 ที่แปลแล้วจะได้รับอนุญาตให้ทำงานผ่าน Rosetta โดยไม่มีข้อมูลลายเซ็นใดๆ ไม่มีข้อมูลประจำตัวเฉพาะที่ส่งไปยังโค้ดนี้ผ่านขั้นตอนการลงชื่อ Secure Enclave เฉพาะอุปกรณ์ และโค้ดก็ทำงานด้วยขีดจำกัดเดียวกันกับโค้ดดั้งเดิมที่ไม่ได้ลงชื่อที่ทำงานบน Mac ที่ใช้ Intel

การปกป้องการเข้าถึงหน่วยความจำโดยตรงสำหรับคอมพิวเตอร์ Mac

ในการทำให้ได้ปริมาณที่สามารถประมวลผลได้สูงบนอินเทอร์เฟซความเร็วสูง เช่น PCIe, FireWire, Thunderbolt และ USB คอมพิวเตอร์จะต้องรองรับการเข้าถึงหน่วยความจำโดยตรง (DMA) จากอุปกรณ์ต่อพ่วง นั่นคือจะต้องสามารถอ่านและเขียนไปยัง RAM ได้โดยไม่ต้องมีความเกี่ยวข้องที่ต่อเนื่องของ CPU ตั้งแต่ปี 2555 คอมพิวเตอร์ Mac ได้ใช้เทคโนโลยีมากมายในการปกป้อง DMA ซึ่งส่งผลให้มีชุดการปกป้อง DMA ที่ดีที่สุดและครอบคลุมที่สุดบน PC ใดๆ

การปกป้องการเข้าถึงหน่วยความจำโดยตรงสำหรับ Mac ที่ใช้ Apple Silicon

ระบบ Apple บนชิปประกอบด้วยหน่วยการจัดการหน่วยความจำข้อมูลเข้า/ข้อมูลออก (IOMMU) สำหรับเอเจ็นต์ DMA แต่ละรายการในระบบ รวมถึงพอร์ต PCIe และ Thunderbolt เนื่องจาก IOMMU แต่ละรายการจะมีชุดตารางการแปลที่อยู่เป็นของตัวเองเพื่อแปลคำขอ DMA อุปกรณ์ต่อพ่วงที่เชื่อมต่อโดย PCIe หรือ Thunderbolt สามารถเข้าถึงเฉพาะหน่วยความจำที่ได้เทียบผังสำหรับการใช้งาน อุปกรณ์ต่อพ่วงไม่สามารถเข้าถึงหน่วยความจำที่เป็นของส่วนอื่นของระบบได้ เช่น เคอร์เนลหรือเฟิร์มแวร์ หรือหน่วยความจำที่กำหนดไปยังอุปกรณ์ต่อพ่วงอื่น ถ้า IOMMU ตรวจพบว่าอุปกรณ์ต่อพ่วงพยายามเข้าถึงหน่วยความจำที่ไม่ได้เทียบผังสำหรับการใช้งานของอุปกรณ์ต่อพ่วงนั้น IOMMU จะสั่งทำงานเคอร์เนลแพนิก

การปกป้องการเข้าถึงหน่วยความจำโดยตรงสำหรับ Mac ที่ใช้ Intel

คอมพิวเตอร์ Mac ที่ใช้ Intel ที่มีเทคโนโลยีการสร้างสภาวะเสมือนจริงสำหรับ I/O ที่มีการสั่งการ (VT-d) ของ Intel จะเริ่มต้นการทำงาน IOMMU โดยเปิดใช้งานการเทียบผัง DMA ใหม่และการเทียบผังการขัดจังหวะใหม่ในช่วงต้นของกระบวนการบูตเพื่อลดคลาสช่องโหว่ด้านความปลอดภัยต่างๆ ฮาร์ดแวร์ IOMMU ของ Apple จะเริ่มการดำเนินการด้วยนโยบายการปฏิเสธตามค่าเริ่มต้น ดังนั้นทันทีที่เปิดระบบ ระบบจะเริ่มปิดกั้นคำขอ DMA จากอุปกรณ์ต่อพ่วง หลังจากเริ่มต้นการทำงานโดยซอฟต์แวร์แล้ว IOMMU จะเริ่มอนุญาตคำขอ DMA จากอุปกรณ์ต่อพ่วงไปยังพื้นที่หน่วยความจำที่ได้เทียบผังไว้อย่างชัดเจนสำหรับการใช้งาน

หมายเหตุ: การเทียบผังการขัดจังหวะสำหรับ PCIe ไม่จำเป็นบน Mac ที่ใช้ Apple Silicon เนื่องจาก IOMMU แต่ละรายการจะจัดการ MSI สำหรับอุปกรณ์ต่อพ่วงของตนเอง

นับตั้งแต่ macOS 11 คอมพิวเตอร์ Mac ทั้งหมดที่มีชิป Apple T2 Security จะใช้งานไดรเวอร์ UEFI ที่ช่วย DMA ในสภาพแวดล้อมวงแหวน 3 ที่จำกัดเมื่อไดรเวอร์เหล่านี้จับคู่กับอุปกรณ์ภายนอก คุณสมบัตินี้ช่วยลดช่องโหว่ด้านความปลอดภัยที่อาจเกิดขึ้นเมื่ออุปกรณ์ที่เป็นอันตรายติดต่อกับไดรเวอร์ UEFI ด้วยวิธีที่ไม่คาดคิดในขณะบูต โดยเฉพาะการลดผลกระทบของช่องโหว่ในการจัดการไดรเวอร์ของบัฟเฟอร์ DMA

ส่วนขยายเคอร์เนลใน macOS

นับตั้งแต่ macOS 11 เป็นต้นไป ถ้าส่วนขยายเคอร์เนลของบริษัทอื่น (kext) เปิดใช้งานอยู่ ระบบจะไม่สามารถโหลด kext ลงในเคอร์เนลตามคำร้องขอได้ แต่จะผสานกับ**คอลเลกชั่นเคอร์เนลเสริม (AuxKC)** แทน ซึ่งโหลดระหว่างกระบวนการบูต สำหรับ Mac ที่ใช้ Apple Silicon การวัดของ AuxKC จะลงชื่อเข้า LocalPolicy (สำหรับฮาร์ดแวร์ก่อนหน้า AuxKC จะอยู่บนดิสก์โวลุ่มข้อมูล) การสร้าง AuxKC ใหม่ต้องได้รับอนุญาตจากผู้ใช้และต้องเริ่มการทำงาน macOS ใหม่เพื่อโหลดการเปลี่ยนแปลงไปยังเคอร์เนล และต้องกำหนดค่าการบูตอย่างปลอดภัยเป็นความปลอดภัยแบบลดลง

สิ่งสำคัญ: ไม่แนะนำให้ใช้ kext กับ macOS อีกต่อไป kext มีความเสี่ยงต่อความสมบูรณ์และความน่าเชื่อถือของระบบปฏิบัติการ Apple แนะนำให้ผู้ใช้เลือกโซลูชั่นที่ไม่จำเป็นต้องขยายเคอร์เนล

ส่วนขยายเคอร์เนลใน Mac ที่ใช้ Apple Silicon

kext ต้องถูกเปิดใช้งานอย่างชัดเจนสำหรับ Mac ที่ใช้ Apple Silicon โดยการกดปุ่มเปิด/ปิดค้างไว้เมื่อเริ่มต้นระบบเพื่อเข้าสู่โหมด One True Recovery (1TR) จากนั้นดาวน์เกรดเป็นความปลอดภัยแบบลดลงและทำเครื่องหมายกล่องเพื่อเปิดใช้งานส่วนขยายเคอร์เนล การทำงานนี้ยังต้องป้อนรหัสผ่านของผู้ดูแลระบบเพื่ออนุญาตให้ดาวน์เกรดอีกด้วย การรวมกันของ 1TR และข้อกำหนดด้านรหัสผ่านทำให้ผู้โจมตีเฉพาะซอฟต์แวร์ที่เริ่มต้นจากภายใน macOS ส่ง kext เข้าไปยัง macOS ได้ยากขึ้น ซึ่งจากนั้นผู้โจมตีจะสามารถใช้ประโยชน์เพื่อรับสิทธิ์เคอร์เนลแบบพิเศษได้

หลังจากผู้ใช้อนุญาตให้โหลด kext โฟลว์การโหลดส่วนขยายเคอร์เนลที่ผู้ใช้อนุญาตข้างต้นจะถูกใช้เพื่ออนุญาตให้ติดตั้ง kext การอนุญาตที่ใช้สำหรับโฟลว์ข้างต้นจะยังถูกใช้เพื่อบันทึกแฮช SHA384 ของรายการ kext ที่ผู้ใช้อนุญาต (UAKL) ใน LocalPolicy อีกด้วย จากนั้นดีมอนการจัดการเคอร์เนล (`kmd`) จะรับผิดชอบในการตรวจสอบความถูกต้องเฉพาะ kext ที่พบใน UAKL เท่านั้นเพื่อรวมเข้ากับ AuxKC

- ถ้าเปิดใช้งานการปกป้องความสมบูรณ์ของระบบ (SIP) ลายเซ็นของ kext แต่ละรายการจะได้รับการตรวจสอบยืนยันก่อนถูกรวมเข้าใน AuxKC
- ถ้า SIP ปิดใช้งานอยู่ ลายเซ็น kext จะไม่ถูกบังคับใช้

วิธีการนี้จะทำให้โฟลว์ความปลอดภัยที่อนุญาตที่นักพัฒนาหรือผู้ใช้ที่ไม่ได้เป็นส่วนหนึ่งของ Apple Developer Program สามารถทดสอบ kext ก่อนลงชื่อได้

หลังจากสร้าง AuxKC การวัดจะถูกส่งไปยัง Secure Enclave เพื่อลงชื่อและรวมไว้ในโครงสร้างข้อมูล Image4 ซึ่ง iBoot สามารถประเมินได้เมื่อเริ่มต้นระบบ คำขอ kext จะถูกสร้างในฐานะส่วนหนึ่งของการสร้าง AuxKC ด้วยเช่นกัน คำขอนี้ประกอบด้วยรายการของ kext ที่ถูกรวมอยู่ใน AuxKC จริงๆ เนื่องจากชุดดังกล่าวอาจเป็นชุดย่อยของ UAKL หากพบ kext ที่ถูกแบน แฮช SHA384 ของโครงสร้างข้อมูล Image4 ของ AuxKC และคำขอ kext จะรวมอยู่ใน LocalPolicy iBoot จะใช้แฮช Image4 ของ AuxKC สำหรับการตรวจสอบยืนยันเพิ่มเติมเมื่อเริ่มต้นระบบเพื่อช่วยให้การรับรองว่าไม่สามารถเริ่มต้นระบบไฟล์ Image4 ของ AuxKC ที่ลงชื่อด้วย Secure Enclave แบบเก่าด้วย LocalPolicy ใหม่ได้ ระบบย่อย เช่น Apple Pay จะใช้คำขอ kext เพื่อระบุว่ามี kext ที่กำลังโหลดซึ่งอาจรบกวนความน่าไว้วางใจของ macOS ถ้ามี แสดงว่าความสามารถของ Apple Pay อาจถูกปิดใช้งาน

ทางเลือกสำหรับ kext (macOS 10.15 ขึ้นไป)

macOS 10.15 ช่วยให้นักพัฒนาขยายขีดความสามารถของ macOS ได้โดยการติดตั้งและจัดการส่วนขยายระบบที่ทำงานในพื้นที่ผู้ใช้มากกว่าที่ระดับเคอร์เนล ด้วยการทำงานในพื้นที่ผู้ใช้ นั่นหมายความว่าส่วนขยายของระบบจะขยายความเสถียรและความปลอดภัยของ macOS แม้ว่าตามปกติแล้ว kext มีการเข้าถึงระบบปฏิบัติการทั้งระบบแบบเต็ม แต่ส่วนขยายที่ทำงานในพื้นที่ผู้ใช้จะได้รับเฉพาะสิทธิ์ที่จำเป็นในการใช้งานฟังก์ชั่นที่ระบุเท่านั้น

นักพัฒนาสามารถใช้เฟรมเวิร์ค รวมถึง DriverKit, EndpointSecurity และ NetworkExtension เพื่อเขียนไดรเวอร์สำหรับอินเทอร์เฟซ USB และอินเทอร์เฟซมนุษย์ เครื่องมือรักษาความปลอดภัยปลายทาง (เช่น การป้องกันข้อมูลสูญหายหรือเอเจ็นต์ปลายทางอื่นๆ) และ VPN และเครื่องมือเครือข่าย ทั้งหมดนี้ทำได้โดยไม่ต้องเขียน kext เอเจนต์ความปลอดภัยของบริษัทอื่นควรใช้เฉพาะเมื่อเอเจนต์เหล่านั้นใช้ประโยชน์จาก API หรือมีแผนงานที่สมบูรณ์สำหรับเปลี่ยนไปใช้เอเจนต์และอยู่ห่างจากส่วนขยายเคอร์เนล

การโหลดส่วนขยายเคอร์เนลที่ได้รับอนุญาตจากผู้ใช้

ในการปรับปรุงความปลอดภัย ผู้ใช้ต้องให้ความยินยอมในการโหลดส่วนขยายเคอร์เนลที่ติดตั้งด้วยหรือหลังการติดตั้ง macOS 10.13 กระบวนการนี้เรียกว่า**การโหลดส่วนขยายเคอร์เนลที่ได้รับอนุญาตจากผู้ใช้** โดยต้องได้รับอนุญาตจากผู้ดูแลระบบเพื่ออนุญาตให้ใช้ส่วนขยายเคอร์เนล ส่วนขยายเคอร์เนลจะไม่ต้องขออนุญาตใช้งานหากเป็นกรณีดังต่อไปนี้:

- ติดตั้งอยู่บน Mac เมื่อเรียกใช้ macOS 10.12 หรือก่อนหน้านี้
- มาแทนที่ส่วนขยายที่ได้รับอนุญาตก่อนหน้านี้
- ได้รับอนุญาตให้โหลดได้โดยไม่ได้รับความยินยอมจากผู้ใช้โดยใช้เครื่องมือบรรทัดคำสั่ง `spctl` ซึ่งจะใช้ได้เมื่อบูต Mac จาก recoveryOS
- ได้รับอนุญาตให้โหลดได้โดยใช้การกำหนดค่าการจัดการอุปกรณ์เคลื่อนที่ (MDM)

  เมื่อเริ่มต้นใช้งานด้วย macOS 10.13.2 ผู้ใช้สามารถใช้ MDM เพื่อระบุรายการส่วนขยายเคอร์เนลที่โหลดโดยไม่ได้รับความยินยอมจากผู้ใช้ได้ ตัวเลือกนี้ต้องใช้กับ Mac ที่ใช้ macOS 10.13.2 ซึ่งได้รับการลงทะเบียนใน MDM ผ่าน Apple School Manager, Apple Business Manager หรือการลงทะเบียน MDM ที่ทำโดยผู้ใช้

ความปลอดภัยของ Option ROM ใน macOS

หมายเหตุ: Mac ที่ใช้ Apple Silicon ปัจจุบันไม่รองรับ Option ROM

ความปลอดภัยของ Option ROM ใน Mac ที่มีชิป Apple T2 Security

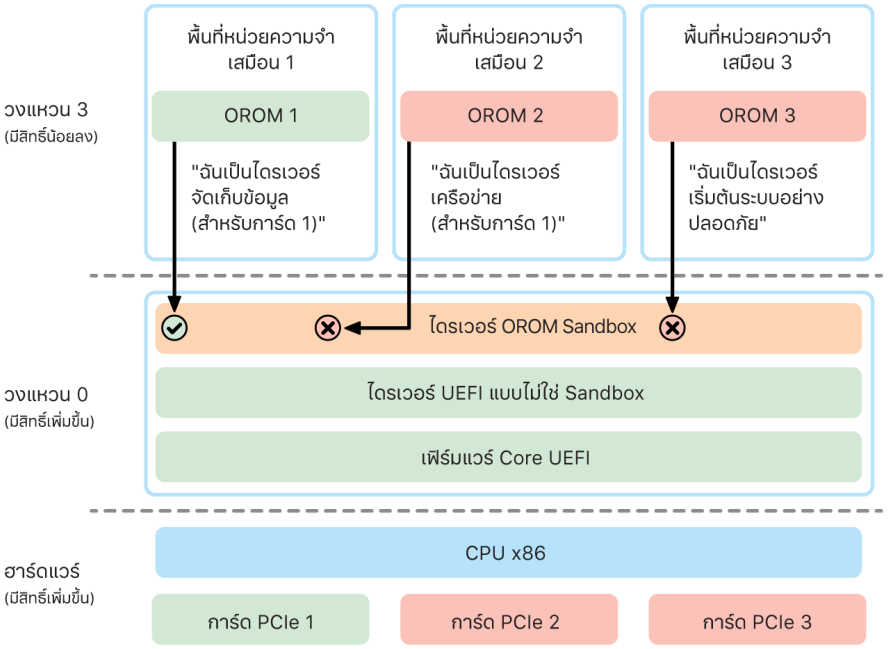
ทั้งอุปกรณ์ Thunderbolt และ PCIe อาจมี "Option ROM (OROM)" ที่ต่อกับอุปกรณ์ได้ (โดยทั่วไปแล้ว สิ่งนี้ไม่ใช่ ROM จริง แต่จะเป็นชิปที่สามารถเขียนซ้ำได้ซึ่งใช้จัดเก็บเฟิร์มแวร์) บนระบบที่ใช้ UEFI เฟิร์มแวร์ดังกล่าวมักจะเป็นไดรเวอร์ UEFI ซึ่งถูกอ่านโดยเฟิร์มแวร์ UEFI และถูกเรียกใช้ โค้ดที่เรียกใช้จะเริ่มต้นการทำงานและกำหนดฮาร์ดแวร์ที่เป็นที่เก็บโค้ดดังกล่าว เพื่อให้ฮาร์ดแวร์นั้นสามารถใช้งานได้จากเฟิร์มแวร์ในส่วนที่เหลือ ความสามารถนี้เป็นสิ่งจำเป็นเพื่อให้ฮาร์ดแวร์เฉพาะของบริษัทอื่นสามารถโหลดและดำเนินการในช่วงระยะการเริ่มต้นระบบครั้งแรกสุดได้ ตัวอย่างเช่น การเริ่มต้นระบบจากอาร์เรย์ RAID ภายนอก

อย่างไรก็ตาม โดยทั่วไปแล้วเนื่องจาก OROM สามารถเขียนซ้ำได้ ถ้าผู้โจมตีเขียนทับ OROM ของอุปกรณ์ต่อพ่วงที่ถูกต้อง โค้ดของผู้โจมตีจะดำเนินการก่อนในกระบวนการบูต และสามารถแทรกแซงสภาพแวดล้อมการดำเนินการและละเมิดความสมบูรณ์ของซอฟต์แวร์ที่โหลดในภายหลังได้ ในทำนองเดียวกัน ถ้าผู้โจมตีนำอุปกรณ์ของตัวเองที่เป็นอันตรายมาใช้กับระบบ พวกเขาก็จะสามารถเรียกใช้โค้ดที่เป็นอันตรายได้

ใน macOS 10.12.3 ลักษณะการทำงานของคอมพิวเตอร์ Mac ที่จำหน่ายหลังจากปี 2011 นั้นได้ถูกเปลี่ยนไม่ให้เรียกใช้ OROM ตามค่าเริ่มต้นในขณะที่บูต Mac เว้นแต่จะมีการกดชุดคำสั่งแป้นพิมพ์เป็นพิเศษ การกดชุดคำสั่งแป้นพิมพ์นี้จะป้องกัน OROM ที่เป็นอันตรายซึ่งถูกนำเข้ามาในลำดับการบูตของ macOS โดยไม่ตั้งใจ ลักษณะการทำงานเริ่มต้นของยูทิลิตี้รหัสผ่านเฟิร์มแวร์ก็ถูกเปลี่ยนไปเช่นกันเพื่อที่ว่าเมื่อผู้ใช้ตั้งรหัสผ่านเฟิร์มแวร์ OROM จะไม่สามารถดำเนินการได้แม้ว่าจะมีการกดชุดคำสั่งแป้นพิมพ์ก็ตาม สิ่งนี้ได้ช่วยป้องกันไม่ให้ผู้โจมตีทางกายภาพนำ OROM ที่เป็นอันตรายมาใช้โดยเจตนา สำหรับผู้ใช้ที่ยังคงต้องใช้งาน OROM ในขณะที่มีชุดรหัสผ่านเฟิร์มแวร์ ก็สามารถกำหนดค่าตัวเลือกที่ไม่ใช่ค่าเริ่มต้นโดยใช้เครื่องมือบรรทัดคำสั่ง `firmwarepasswd` ใน macOS ได้

ความปลอดภัยของ Sandbox ของ OROM

ใน macOS 10.15 เฟิร์มแวร์ UEFI ได้รับการอัปเดตเพื่อให้มีกลไกสำหรับการทำ Sandbox OROM และสำหรับการยกเลิกสิทธิ์ โดยทั่วไปแล้วเฟิร์มแวร์ UEFI จะเรียกใช้โค้ดทั้งหมด รวมถึง OROM ที่ระดับสิทธิ์สูงสุดของ CPU ซึ่งเรียกว่า วงแหวน 0 และมีพื้นที่หน่วยความจำเสมือนเดียวที่มีการใช้งานร่วมกันสำหรับโค้ดและข้อมูลทั้งหมด วงแหวน 0 อยู่ในระดับสิทธิ์ที่เคอร์เนล macOS ทำงาน ในขณะที่ระดับสิทธิ์ที่ต่ำกว่า ซึ่งคือ วงแหวน 3 จะเป็นที่ที่แอปต่างๆ ทำงาน ส่วน Sandbox ของ OROM นั้นได้ยกเลิกสิทธิ์ OROM แล้วโดยใช้การแยกหน่วยความจำเสมือนอย่างที่เคอร์เนลทำ จากนั้นทำให้ OROM ทำงานในวงแหวน 3



Sandbox จะจำกัดทั้งอินเทอร์เฟซที่ OROM สามารถเรียกใช้ได้ (ซึ่งคล้ายกับการเรียกระบบที่ฟิลเตอร์ในเคอร์เนล) และประเภทของอุปกรณ์ที่ OROM สามารถลงทะเบียนได้ (ซึ่งคล้ายกับการอนุญาตของแอป) อย่างมีนัยสำคัญเพิ่มเติม ประโยชน์ของการออกแบบนี้คือ OROM ที่เป็นอันตรายจะไม่สามารถเขียนที่ใดก็ได้โดยตรงภายในหน่วยความจำวงแหวน 0 ได้อีกต่อไป แต่จะจำกัดอยู่ในอินเทอร์เฟซ Sandbox ที่แคบมากและมีการกำหนดอย่างชัดเจน อินเทอร์เฟซที่มีการจำกัดนี้จึงช่วยลดพื้นหน้าของการโจมตีได้อย่างมาก และบังคับให้ผู้โจมตีออกจาก Sandbox และยกระดับสิทธิ์

ความปลอดภัยของเฟิร์มแวร์ UEFI ใน Mac ที่ใช้ Intel

Mac ที่ใช้ Intel ที่มีชิป Apple T2 Security มอบความปลอดภัยโดยใช้เฟิร์มแวร์ UEFI (Intel)

ภาพรวม

ตั้งแต่ปี 2006 คอมพิวเตอร์ Mac ที่มี CPU ที่ใช้ Intel จะใช้เฟิร์มแวร์ของ Intel ที่ใช้ชุดการพัฒนา (EDK) ของอินเทอร์เฟซเฟิร์มแวร์แบบขยาย (EFI) เวอร์ชั่น 1 หรือเวอร์ชั่น 2 โค้ดที่ใช้ EDK2 เป็นไปตามข้อมูลจำเพาะของ Unified Extensible Firmware Interface (UEFI) โดยส่วนนี้จะอ้างอิงถึงเฟิร์มแวร์ Intel ว่าเป็น**เฟิร์มแวร์ UEFI** เฟิร์มแวร์ UEFI เป็นโค้ดแรกสำหรับเรียกใช้บนชิป Intel

สำหรับ Mac ที่ใช้ Intel ที่ไม่มีชิป Apple T2 Security รากของความเชื่อถือสำหรับเฟิร์มแวร์ UEFI จะเป็นชิปที่ใช้จัดเก็บเฟิร์มแวร์นั้น รายการอัปเดตเฟิร์มแวร์ UEFI จะลงชื่อแบบดิจิตอลโดย Apple และตรวจสอบยืนยันโดยเฟิร์มแวร์ก่อนที่จะอัปเดตพื้นที่จัดเก็บข้อมูล ในการช่วยป้องกันการโจมตีแบบย้อนกลับ รายการอัปเดตจะต้องมีเวอร์ชั่นที่ใหม่กว่าเวอร์ชั่นที่มีอยู่เสมอ อย่างไรก็ตาม ผู้โจมตีที่เข้าถึง Mac ทางกายภาพอาจสามารถใช้ฮาร์ดแวร์เพื่อเชื่อมต่อกับชิปจัดเก็บข้อมูลเฟิร์มแวร์และอัปเดตชิปเพื่อให้มีเนื้อหาที่เป็นอันตรายได้ เช่นเดียวกัน ถ้าพบช่องโหว่ในกระบวนการบูตช่วงต้นของเฟิร์มแวร์ UEFI (ก่อนที่จะจำกัดการเขียนชิปจัดเก็บข้อมูล) สิ่งนี้ยังอาจทำให้เกิดการติดไวรัสของเฟิร์มแวร์ UEFI แบบถาวรได้ด้วย นี่เป็นข้อจำกัดทางสถาปัตยกรรมของฮาร์ดแวร์ที่พบได้ทั่วไปใน PC ส่วนใหญ่ที่ใช้ Intel และมีอยู่ในคอมพิวเตอร์ Mac ที่ใช้ Intel ทุกเครื่องที่ไม่มีชิป T2

ในการช่วยป้องกันการโจมตีทางกายภาพที่ทำลายเฟิร์มแวร์ UEFI คอมพิวเตอร์ Mac มีการออกแบบใหม่ให้ความเชื่อถือมีรากฐานมาจากเฟิร์มแวร์ UEFI ในชิป T2 บนคอมพิวเตอร์ Mac เหล่านี้ รากของความเชื่อถือสำหรับเฟิร์มแวร์ UEFI จะเป็นเฟิร์มแวร์ T2 โดยเฉพาะ ตามที่อธิบายในกระบวนการบูต

องค์ประกอบย่อยของ Intel Management Engine (ME)

องค์ประกอบย่อยหนึ่งองค์ประกอบที่จัดเก็บอยู่ภายในเฟิร์มแวร์ UEFI คือเฟิร์มแวร์ **Intel Management Engine (ME)** หน่วยประมวลผลแบบแยกต่างหากและระบบย่อยภายในชิป Intel ที่เรียกว่า ME โดยหลักแล้วจะใช้เพื่อปกป้องลิขสิทธิ์เสียงและวิดีโอบน Mac ที่มีเฉพาะกราฟิกของ Intel เท่านั้น ในการลดพื้นหน้าของการโจมตีของส่วนประกอบย่อยนี้ให้น้อยลง Mac ที่ใช้ Intel จะใช้งานเฟิร์มแวร์ ME แบบกำหนดเองซึ่งส่วนประกอบส่วนใหญ่ได้ถูกเอาออกไปแล้ว เนื่องจากผลลัพธ์ที่ได้คือเฟิร์มแวร์ ME ของ Mac ที่มีขนาดเล็กกว่าบิลด์ขนาดเล็กที่สุดเริ่มต้นที่ Intel มีให้ใช้งาน ส่วนประกอบหลายๆ ส่วนที่เคยเป็นเป้าหมายของการโจมตีสาธารณะจากนักวิจัยด้านความปลอดภัยในอดีตก็ไม่มีอยู่อีกต่อไป

โหมดการจัดการระบบ (SMM)

หน่วยประมวลผล Intel มีโหมดการดำเนินการพิเศษซึ่งแตกต่างจากการทำงานปกติ ที่เรียกว่า**โหมดการจัดการระบบ (SMM)** โดยแรกเริ่มมีการนำมาใช้เพื่อจัดการกับการดำเนินงานที่มีเวลาเป็นปัจจัยสำคัญ เช่น การจัดการพลังงาน อย่างไรก็ตาม คอมพิวเตอร์ Mac ใช้ไมโครคอนโทรลเลอร์แบบแยกส่วนซึ่งเรียกว่า**ตัวควบคุมการจัดการระบบ (SMC)** เพื่อดำเนินการทำงานดังกล่าวมานานแล้ว เนื่องจาก SMC ได้รวมเข้ากับชิป T2 แล้ว จึงไม่ใช่ไมโครคอนโทรลเลอร์แบบแยกอีกต่อไป

ความปลอดภัยของระบบสำหรับ watchOS

Apple Watch ใช้ความสามารถด้านความปลอดภัยของแพลตฟอร์มด้านฮาร์ดแวร์หลายรายการที่เหมือนกันกับที่ iOS และ iPadOS ใช้ ตัวอย่างเช่น Apple Watch:

- ดำเนินการการบูตที่ปลอดภัยและการอัปเดตซอฟต์แวร์ที่ปลอดภัย
- รักษาความสมบูรณ์ของระบบปฏิบัติการ
- ช่วยปกป้องข้อมูลทั้งบนอุปกรณ์และเมื่อสื่อสารกับ iPhone ที่จับคู่กันอยู่หรืออินเทอร์เน็ต

เทคโนโลยีที่รองรับประกอบด้วยเทคโนโลยีที่ระบุในรายการความปลอดภัยของระบบ (เช่น KIP, SKP และ SCIP) รวมถึงเทคโนโลยีการปกป้องข้อมูล พวงกุญแจ และเครือข่าย

การอัปเดต watchOS

watchOS สามารถกำหนดค่าให้ทำการอัปเดตข้ามคืนได้ โปรดดูที่กระเป๋ากุญแจ (Keybag) สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีการจัดเก็บรหัส Apple Watch และใช้ในระหว่างการอัปเดต

การตรวจจับข้อมือ

ถ้าการตรวจจับข้อมือถูกเปิดใช้งานอยู่ อุปกรณ์จะล็อคโดยอัตโนมัติหลังจากที่ถอดออกจากข้อมือของผู้ใช้ได้ไม่นาน ถ้าการตรวจจับข้อมือถูกปิดใช้งานอยู่ ศูนย์ควบคุมจะมีตัวเลือกให้สำหรับล็อค Apple Watch เมื่อ Apple Watch ล็อคอยู่ ผู้ใช้จะสามารถใช้ Apple Pay ได้ด้วยการป้อนรหัสบน Apple Watch เท่านั้น การตรวจจับข้อมือปิดใช้โดยใช้แอป Apple Watch บน iPhone การตั้งค่านี้ยังสามารถบังคับใช้ได้โดยใช้โซลูชั่น การจัดการอุปกรณ์เคลื่อนที่ (MDM) อีกด้วย

การล็อคการเข้าใช้งานเครื่อง

เมื่อ “ค้นหา Mac ของฉัน” เปิดใช้อยู่บน iPhone นาฬิกา Apple Watch ที่จับคู่อยู่กับ iPhone เครื่องนั้นจะสามารถใช้การล็อคการเข้าใช้เครื่องได้ การล็อคการเข้าใช้เครื่องทำให้การใช้หรือขาย Apple Watch ที่สูญหายหรือถูกขโมยเป็นเรื่องยากขึ้นด้วย การล็อคการเข้าใช้เครื่องต้องใช้ Apple ID และรหัสผ่านของผู้ใช้เพื่อเลิกจับคู่ ลบ หรือเปิดใช้งาน Apple Watch อีกครั้ง

การจับคู่อย่างปลอดภัยกับ iPhone

Apple Watch สามารถจับคู่กับ iPhone ได้ครั้งละหนึ่งเครื่อง เมื่อเลิกจับคู่ Apple Watch แล้ว iPhone จะสื่อสารคำสั่งให้ลบเนื้อหาและข้อมูลทั้งหมดออกจากนาฬิกา

การจับคู่ Apple Watch กับ iPhone ได้รับการรักษาความปลอดภัยโดยใช้กระบวนการทำงาน out-of-band เพื่อแลกเปลี่ยนกุญแจสาธารณะ ตามด้วยการเชื่อมโยงความลับบลูทูธพลังงานต่ำ (BLE) ที่แชร์ Apple Watch จะแสดงรูปแบบเคลื่อนไหว ซึ่งจะได้รับการจับภาพบนกล้อง iPhone รูปแบบประกอบด้วยความลับที่เข้ารหัสซึ่งใช้สำหรับการจับคู่ BLE 4.1 แบบ out-of-band การป้อน BLE Passkey แบบมาตรฐานใช้เพื่อเป็นวิธีการจับคู่แบบสำรอง หากจำเป็น

หลังจากสร้างเซสชั่น BLE และเข้ารหัสโดยใช้โปรโตคอลความปลอดภัยสูงสุดที่มีให้ใช้งานในข้อกำหนดหลักของบลูทูธแล้ว iPhone และ Apple Watch จะแลกเปลี่ยนกุญแจโดยใช้สิ่งใดสิ่งหนึ่งต่อไปนี้:

- กระบวนการที่ปรับจากบริการข้อมูลประจำตัว (IDS) ของ Apple ดังที่อธิบายในภาพรวมความปลอดภัยของ iMessage
- การแลกเปลี่ยนกุญแจโดยใช้ IKEv2/IPsec การเริ่มแลกเปลี่ยนกุญแจได้รับการตรวจสอบสิทธิ์โดยใช้กุญแจเซสชั่นบลูทูธ (สำหรับสถานการณ์การจับคู่) หรือกุญแจ IDS (สำหรับสถานการณ์การอัปเดตระบบปฏิบัติการ) อุปกรณ์แต่ละเครื่องจะสร้างคู่กุญแจสาธารณะแบบสุ่มและกุญแจส่วนตัว Ed25519 แบบ 256 บิต และแลกเปลี่ยนกุญแจสาธารณะระหว่างเริ่มกระบวนการแลกเปลี่ยนกุญแจ

หมายเหตุ: กลไกที่ใช้สำหรับการแลกเปลี่ยนกุญแจและการเข้ารหัสจะแตกต่างกันไป ทั้งนี้ขึ้นอยู่กับเวอร์ชั่นของระบบปฏิบัติการบน iPhone และ Apple Watch โดยอุปกรณ์ iPhone ที่ใช้ iOS 13 ขึ้นไป เมื่อจับคู่กับ Apple Watch ที่ใช้ watchOS 6 ขึ้นไปจะใช้เพียง IKEv2/IPsec สำหรับการแลกเปลี่ยนกุญแจและการเข้ารหัส

หลังจากแลกเปลี่ยนกุญแจ:

- กุญแจเซสชั่นบลูทูธจะถูกละทิ้งและการสื่อสารทั้งหมดระหว่าง iPhone กับ Apple Watch จะได้รับการเข้ารหัสโดยใช้วิธีใดวิธีหนึ่งข้างต้น พร้อมทั้งลิงก์บลูทูธ, Wi-Fi และเซลลูลาร์ที่เข้ารหัสทำหน้าที่ให้ชั้นการเข้ารหัสชั้นที่สอง
- (IKEv2/IPsec เท่านั้น) กุญแจจะถูกเก็บไว้ในพวงกุญแจของระบบและใช้สำหรับตรวจสอบสิทธิ์ของเซสชั่น IKEv2/IPsec ระหว่างอุปกรณ์ในอนาคต การสื่อสารเพิ่มเติมระหว่างอุปกรณ์เหล่านี้ได้รับการเข้ารหัสและปกป้องความสมบูรณ์โดยใช้ AES-256-GCM หรือ ChaCha20-Poly1305 (กุญแจ 256 บิต) บนอุปกรณ์ iPhone ที่ใช้ iOS 15 ขึ้นไปที่จับคู่กับ Apple Watch Series 4 ขึ้นไปที่ใช้ watchOS 8 ขึ้นไป

ที่อยู่ของอุปกรณ์บลูทูธพลังงานต่ำจะสลับเปลี่ยนทุกๆ 15 นาทีเพื่อลดความเสี่ยงที่อุปกรณ์จะถูกติดตามในพื้นที่ใกล้เคียงหากมีใครก็ตามใช้การกระจายของข้อมูลจำเพาะแบบถาวร

ในการรองรับแอปที่จำเป็นต้องสตรีมข้อมูล การเข้ารหัสจะถูกดำเนินการด้วยวิธีที่อธิบายไว้แล้วในความปลอดภัยของ FaceTime โดยใช้บริการข้อมูลประจำตัว (IDS) ของ Apple ที่ให้บริการโดย iPhone ที่จับคู่อยู่หรือการเชื่อมต่อกับอินเทอร์เน็ตโดยตรง

Apple Watch ใช้พื้นที่จัดเก็บข้อมูลแบบเข้ารหัสด้านฮาร์ดแวร์และการปกป้องไฟล์และรายการพวงกุญแจแบบคลาส กระเป๋ากุญแจ (Keybag) ที่ควบคุมด้วยสิทธิ์การเข้าถึงสำหรับรายการพวงกุญแจถูกใช้ด้วยเช่นกัน กุญแจที่ใช้เพื่อสื่อสารระหว่างApple Watch และ iPhone ยังได้รับการรักษาความปลอดภัยโดยใช้การปกป้องแบบคลาสอีกด้วย โปรดดูที่ กระเป๋ากุญแจ (Keybag) สำหรับการปกป้องข้อมูล สำหรับข้อมูลเพิ่มเติม

ปลดล็อคอัตโนมัติและ Apple Watch

เพื่อความสะดวกที่มากขึ้นเมื่อใช้อุปกรณ์ของ Apple หลายๆ เครื่อง อุปกรณ์บางเครื่องสามารถปลดล็อคอุปกรณ์เครื่องอื่นได้โดยอัตโนมัติในบางสถานการณ์ การการปลดล็อคอัตโนมัติรองรับการใช้งานสามอย่างนี้:

- Apple Watch สามารถปลดล็อคได้โดย iPhone
- Mac สามารถปลดล็อคได้โดย Apple Watch
- iPhone สามารถปลดล็อคได้โดย Apple Watch เมื่อตรวจพบว่าจมูกและปากของผู้ใช้ถูกปิดอยู่

กรณีการใช้งานทั้งสามอย่างนี้สร้างอยู่บนพื้นฐานเบื้องต้นเดียวกัน: โปรโตคอล Station-to-Station (STS) ที่ได้รับการตรวจสอบสิทธิ์ร่วมกัน พร้อมกับกุญแจระยะยาวที่แลกเปลี่ยนกันในขณะที่คุณสมบัติถูกเปิดใช้งาน และกุญแจเซสชั่นชั่วคราวที่ไม่ซ้ำกันซึ่งติดต่อสำหรับแต่ละคำขอ แม้ว่าจะมีช่องทางการสื่อสารพื้นฐาน ช่องทาง STS จะมีการติดต่อโดยตรงระหว่าง Secure Enclave ในอุปกรณ์ทั้งสองเครื่อง และข้อมูลการเข้ารหัสทั้งหมดจะถูกเก็บไว้ในโดเมนที่ปลอดภัยนั้น (ยกเว้นคอมพิวเตอร์ Mac ที่ไม่มี Secure Enclave ซึ่งจะยุติช่องทาง STS ในเคอร์เนล)

การปลดล็อค

ลำดับการปลดล็อคที่สมบูรณ์สามารถแยกออกได้เป็นสองระยะ ระยะแรก อุปกรณ์ที่ถูกปลดล็อค (“เป้าหมาย”) จะร้างความลับการปลดล็อคการเข้ารหัสแล้วส่งความลับนั้นไปยังอุปกรณ์ที่ดำเนินการปลดล็อค (“อุปกรณ์ริเริ่ม”) หลังจากนั้น อุปกรณ์ริเริ่มจะดำเนินการปลดล็อคโดยใช้ความลับที่สร้างขึ้นก่อนหน้านี้

ในการเปิดใช้งานการปลดล็อคอัตโนมัติ อุปกรณ์ทั้งสองจะเชื่อมต่อกันโดยใช้การเชื่อมต่อ BLE หลังจากนั้น ความลับการปลดล็อคแบบ 32 ไบต์ที่สุ่มสร้างขึ้นโดยอุปกรณ์เป้าหมายจะส่งไปยังอุปกรณ์ริเริ่มผ่านช่องทาง STS ในระหว่างการปลดล็อคด้วยชีวมิติหรือรหัส อุปกรณ์เป้าหมายจะห่อกุญแจที่ได้จากรหัส (PDK) ด้วยความลับการปลดล็อคและจะละทิ้งความลับการปลดล็อคออกจากหน่วยความจำ

ในการดำเนินการปลดล็อค อุปกรณ์จะเริ่มการเชื่อมต่อ BLE ใหม่แล้วใช้ Wi-Fi แบบเพียร์ทูเพียร์เพื่อประมาณระยะห่างระหว่างอุปกรณ์ทั้งสองอย่างปลอดภัย ถ้าอุปกรณ์อยู่ในระยะที่ระบุและเป็นไปตามนโยบายความปลอดภัยที่กำหนด อุปกรณ์ริเริ่มจะส่งความลับการปลดล็อคไปยังเป้าหมายผ่านช่องทาง STS เป้าหมายจะสร้างความลับการปลดล็อคแบบ 32 ไบต์ใหม่แล้วส่งความลับนั้นกลับไปยังอุปกรณ์ริเริ่ม ถ้าความลับการปลดล็อคปัจจุบันที่ถูกส่งจากอุปกรณ์ริเริ่มสามารถถอดรหัสข้อมูลการปลดล็อคได้สำเร็จ อุปกรณ์เป้าหมายจะถูกปลดล็อคและ PDK จะถูกห่อด้วยความลับการปลดล็อคใหม่ สุดท้าย ความลับการปลดล็อคและ PDK ใหม่จะถูกละทิ้งจากหน่วยความจำของเป้าหมาย

นโยบายความปลอดภัยการปลดล็อคอัตโนมัติของ Apple Watch

เพื่อความสะดวกยิ่งขึ้น iPhone สามารถปลดล็อค Apple Watch ได้โดยตรงหลังจากการเริ่มต้นระบบครั้งแรก โดยที่ผู้ใช้ไม่จำเป็นต้องป้อนรหัสบน Apple Watch เองก่อน ในการทำเช่นนี้ได้ ความลับการปลดล็อคแบบสุ่ม (สร้างขึ้นในระหว่างลำดับการปลดล็อคแรกสุดหลังการเปิดใช้งานคุณสมบัติ) จะถูกใช้สำหรับสร้างข้อมูลที่ฝากไว้ระยะยาว ซึ่งจัดเก็บอยู่ในกระเป๋ากุญแจ (Keybag) ของ Apple Watch ข้อมูลความลับที่ฝากไว้จะถูกจัดเก็บอยู่ในพวงกุญแจ iPhone และจะถูกใช้ในการเริ่มต้นเซสชั่นใหม่หลังจาก Apple Watch แต่ละเรือนเริ่มการทำงานเครื่องใหม่

นโยบายความปลอดภัยการปลดล็อคอัตโนมัติของ iPhone

นโยบายความปลอดภัยเพิ่มเติมที่บังคับใช้กับการปลดล็อค iPhone อัตโนมัติด้วย Apple Watch ผู้ใช้ไม่สามารถใช้ Apple Watch แทน Face ID เพื่อการทำงานอื่นบน iPhone ได้ ตัวอย่างเช่น Apple Pay หรือการอนุญาตแอป เมื่อ Apple Watch ปลดล็อค iPhone ที่จับคู่กันได้สำเร็จ นาฬิกาจะแสดงการแจ้งเตือนและเล่นการสะกิดที่เกี่ยวข้อง ถ้าผู้ใช้แตะปุ่มล็อค iPhone ในการแจ้งเตือน นาฬิกาจะส่งคำสั่งล็อคผ่าน BLE เมื่อ iPhone ได้รับคำสั่งล็อค โทรศัพท์จะปิดใช้งานทั้ง Face ID และการปลดล็อคโดยใช้ Apple Watch การปลดล็อค iPhone ในครั้งถัดไปจะต้องดำเนินการด้วยรหัสของ iPhone

การปลดล็อค iPhone ที่จับคู่กันโดย Apple Watch (เมื่อเปิดใช้งาน) ได้สำเร็จจะต้องเป็นไปตามเกณฑ์ต่อไปนี้:

- iPhone จะต้องถูกปลดล็อคโดยใช้วิธีการอื่นอย่างน้อยหนึ่งครั้งหลังจาก Apple Watch ที่เกี่ยวข้องถูกวางบนข้อมือและปลดล็อคอยู่
- เซ็นเซอร์จะต้องตรวจพบได้ว่าจมูกและปากถูกปิดอยู่
- ระยะห่างที่วัดได้จะต้องเป็น 2-3 เมตรหรือน้อยกว่า
- Apple Watch จะต้องไม่อยู่ในโหมดเวลาเข้านอน
- Apple Watch หรือ iPhone จะต้องถูกปลดล็อคเมื่อเมื่อไม่นานมานี้ หรือ Apple Watch จะต้องมีบันทึกการเคลื่อนไหวทางกายภาพที่ระบุได้ว่าผู้สวมใส่เคลื่อนไหวอยู่ (ตัวอย่างเช่น ไม่ได้นอนหลับอยู่)
- iPhone จะต้องถูกปลดล็อคอย่างน้อยหนึ่งครั้งใน 6.5 ชั่วโมงที่ผ่านมา
- iPhone จะต้องอยู่ในสถานะที่ Face ID ได้รับการอนุญาตให้ดำเนินการปลดล็อคอุปกรณ์ได้ (โปรดดูที่ Face ID, Touch ID, รหัส และรหัสผ่าน สำหรับข้อมูลเพิ่มเติม)

อนุญาตใน macOS ด้วย Apple Watch

เมื่อการปลดล็อคโดยอัตโนมัติด้วย Apple Watch เปิดใช้งานอยู่ คุณจะสามารถใช้ Apple Watch แทนที่หรือร่วมกับ Touch ID เพื่ออนุญาตการตรวจสอบความถูกต้องและการแจ้งการตรวจสอบสิทธิ์จากรายการต่อไปนี้ได้:

- macOS และแอปของ Apple ที่ขอตรวจสอบความถูกต้อง
- แอปของบุคคลหรือบริษัทอื่นที่ขอตรวจสอบสิทธิ์
- รหัสผ่าน Safari ที่บันทึก
- โน้ตที่ปลอดภัย

การใช้ Wi-Fi, cellular, iCloud และ Gmail อย่างปลอดภัย

เมื่อ Apple Watch ไม่ได้อยู่ในช่วงสัญญาณบลูทูธ จะสามารถใช้ Wi-Fi หรือเซลลูลาร์แทนได้ Apple Watch จะเข้าร่วมเครือข่าย Wi-Fi ที่เคยเข้าร่วมบน iPhone ที่จับคู่แล้วโดยอัตโนมัติ และมีการเชื่อมข้อมูลประจำตัวกับ Apple Watch ในขณะที่ทั้งสองอุปกรณ์อยู่ในระยะสัญญาณ ลักษณะการทำงานของการเข้าร่วมอัตโนมัติเช่นนี้สามารถกำหนดค่าแบบรายเครือข่ายได้ในส่วน Wi-Fi ของแอปการตั้งค่าบน Apple Watch เครือข่าย Wi-Fi ที่ยังไม่เคยเชื่อมต่อมาก่อนบนอุปกรณ์ทั้งสองเครื่องสามารถเข้าร่วมได้ด้วยตัวเองในส่วน Wi-Fi ของแอปการตั้งค่าบน Apple Watch

เมื่อ Apple Watch และ iPhone อยู่นอกระยะทำการ Apple Watch จะเชื่อมต่อกับเซิร์ฟเวอร์ iCloud และ Gmail โดยตรงเพื่อดึงข้อมูลแอปเมล ซึ่งแตกต่างจากการเชื่อมข้อมูลแอปเมลกับ iPhone ที่จับคู่อยู่ผ่านทางอินเทอร์เน็ต สำหรับบัญชี Gmail ผู้ใช้จะต้องตรวจสอบสิทธิ์กับ Google ในส่วนแอปเมลของแอป Watch บน iPhone โทเค็น OAuth ที่ได้รับจาก Google จะถูกส่งไปยัง Apple Watch ในรูปแบบที่เข้ารหัสผ่านทางบริการข้อมูลประจำตัว (IDS) ของ Apple เพื่อทำให้สามารถใช้ในการดึงข้อมูลแอปเมลได้ โทเค็น OAuth จะไม่ถูกนำไปใช้ในการเชื่อมต่อกับเซิร์ฟเวอร์ Gmail จาก iPhone ที่จับคู่อยู่

การสร้างหมายเลขแบบสุ่ม

ตัวสร้างหมายเลขแบบสุ่มการเข้ารหัสแฝง (CPRNG) เป็นหน่วยโครงสร้างที่สำคัญสำหรับซอฟต์แวร์ที่ปลอดภัย ด้วยเหตุนี้ Apple จึงมอบซอฟต์แวร์ CPRNG ที่เชื่อถือได้ซึ่งทำงานในเคอร์เนลของ iOS, iPadOS, macOS, tvOS และ watchOS โดยมีหน้าที่ในการรวบรวม Entropy ดิบจากระบบและมีหมายเลขแบบสุ่มที่ปลอดภัยให้กับผู้บริโภคทั้งในเคอร์เนลและพื้นที่ผู้ใช้

แหล่ง Entropy

CPRNG เคอร์เนลมาจากแหล่ง Entropy หลายแหล่งในระหว่างบูตและตลอดระยะเวลาใช้งานอุปกรณ์ แหล่ง Entropy เหล่านี้รวมถึง (ขึ้นอยู่กับความพร้อมใช้งาน):

- TRNG ฮาร์ดแวร์ของ Secure Enclave
- จิทเทอร์ตามเวลาที่รวบรวมในระหว่างการบูต
- Entropy ที่รวบรวมจากการขัดจังหวะของฮาร์ดแวร์
- ไฟล์ Seed ที่ใช้ในการเก็บรักษา Entropy ในระหว่างการบูต
- คำสั่งแบบสุ่มของ Intel เช่น RDSEED และ RDRAND (บน Mac ที่ใช้ Intel เท่านั้น)

CPRNG เคอร์เนล

CPRNG เคอร์เนลเป็นการออกแบบที่มาจาก Fortuna ซึ่งมีเป้าหมายระดับความปลอดภัยแบบ 256 บิต และมีหมายเลขแบบสุ่มคุณภาพสูงให้กับผู้บริโภคในพื้นที่ผู้ใช้โดยใช้ API ต่อไปนี้:

- การเรียกระบบ `getentropy`(2)
- อุปกรณ์แบบสุ่ม (/dev/random)

CPRNG เคอร์เนลจะยอมรับ Entropy ที่ผู้ใช้กำหนดผ่านการเขียนไปยังอุปกรณ์แบบสุ่ม

อุปกรณ์การวิจัยด้านความปลอดภัยของ Apple

อุปกรณ์การวิจัยด้านความปลอดภัยของ Apple เป็น iPhone ที่รวมเข้าด้วยกันโดยเฉพาะซึ่งช่วยให้นักวิจัยด้านความปลอดภัยสามารถดำเนินการวิจัยเกี่ยวกับ iOS ได้โดยไม่ต้องทำลายหรือปิดใช้งานคุณสมบัติด้านความปลอดภัยของแพลตฟอร์มของ iPhone อุปกรณ์นี้จะช่วยให้นักวิจัยสามารถไซด์โหลดเนื้อหาที่ทำงานด้วยสิทธิ์ที่เทียบเท่ากับแพลตฟอร์มได้ ดังนั้นจึงสามารถดำเนินการวิจัยบนแพลตฟอร์มที่ใกล้เคียงยิ่งขึ้นกับโมเดลของอุปกรณ์การผลิตได้

เพื่อช่วยให้มั่นใจว่าอุปกรณ์ของผู้ใช้ไม่ได้รับผลกระทบจากนโยบายการปฏิบัติงานอุปกรณ์การวิจัยความปลอดภัย การเปลี่ยนแปลงนโยบายจะถูกปรับใช้ใน iBoot และในคอลเลกชั่นเคอร์เนลบูต ซึ่งจะทำให้การบูตบนฮาร์ดแวร์ผู้ใช้ไม่สำเร็จ iBoot การวิจัยจะตรวจสอบสถานะการหลอมรวมใหม่และเข้าสู่ลูปแพนิกหากทำงานบนฮาร์ดแวร์ที่ไม่ได้หลอมรวมกับการวิจัย

ระบบย่อยรหัสลิขิตช่วยให้นักวิจัยโหลดแคชความเชื่อถือและภาพดิสก์ที่ปรับให้เป็นส่วนตัวที่มีเนื้อหาที่สอดคล้องกันได้ มีการใช้มาตรการเชิงลึกในการป้องกันจำนวนมากซึ่งได้รับการออกแบบมาเพื่อให้แน่ใจว่าให้แน่ใจว่าระบบย่อยนี้ไม่อนุญาตให้ดำเนินการกับอุปกรณ์ของผู้ใช้:

- `launchd` จะไม่โหลดรายการคุณสมบัติ launchd ของ `cryptexd` หากตรวจพบว่าอุปกรณ์ของลูกค้าปกติ
- `cryptexd` จะยกเลิก หากตรวจพบว่าอุปกรณ์ของลูกค้าปกติ
- `AppleImage4` ไม่ได้จำหน่าย Nonce ที่ใช้สำหรับการตรวจสอบยืนยันการเข้ารหัสการวิจัยบนอุปกรณ์ของลูกค้าทั่วไป
- เซิร์ฟเวอร์การลงชื่อปฏิเสธที่จะปรับแต่งภาพดิสก์ cryptex สำหรับอุปกรณ์ที่ไม่อยู่ในรายการอนุญาตอย่างชัดเจน

ในการเคารพความเป็นส่วนตัวของนักวิจัยด้านความปลอดภัย ระบบจะส่งเฉพาะการวัด (เช่น แฮช) ของไฟล์ปฏิบัติการหรือแคชเคอร์เนลและข้อมูลจำเพาะอุปกรณ์การวิจัยด้านความปลอดภัยไปยัง Apple ระหว่างการตั้งค่าส่วนบุคคล Apple ไม่ได้รับเนื้อหาของ cryptex ที่โหลดลงในอุปกรณ์

ในการหลีกเลี่ยงสถานการณ์ที่ผู้ไม่ประสงค์ดีพยายามปลอมแปลงอุปกรณ์การวิจัยเป็นอุปกรณ์ของผู้ใช้เพื่อหลอกล่อเป้าหมายให้ใช้งานในชีวิตประจำวัน อุปกรณ์การวิจัยด้านความปลอดภัยมีความแตกต่างดังนี้:

- อุปกรณ์การวิจัยด้านความปลอดภัยจะเริ่มต้นระบบขณะชาร์จเท่านั้น ซึ่งสามารถใช้สาย Lightning หรือที่ชาร์จที่สามารถใช้งานร่วมกับ Qi ได้ ถ้าอุปกรณ์ไม่ชาร์จระหว่างการเริ่มต้นระบบ อุปกรณ์จะเข้าสู่โหมดการกู้คืน ถ้าผู้ใช้เริ่มชาร์จและเริ่มการทำงานอุปกรณ์ใหม่ อุปกรณ์จะเริ่มการทำงานตามปกติ ทันทีที่ XNU เริ่ม อุปกรณ์ไม่ต้องชาร์จเพื่อทำงานต่อ
- คำว่า **อุปกรณ์การวิจัยด้านความปลอดภัย** แสดงอยู่ด้านล่างโลโก้ Apple ในระหว่างเริ่มต้นระบบ iBoot
- เคอร์เนล XNU บูตในโหมดรายละเอียด
- มีข้อความสลักอยู่ที่ด้านข้างของอุปกรณ์ที่ระบุว่า “ทรัพย์สินของ Apple” เป็นความลับและมีเจ้าของ โทร +1 877 595 1125”

ต่อไปนี้เป็นมาตรการเพิ่มเติมที่นำไปใช้ในซอฟต์แวร์ที่แสดงขึ้นหลังจากการบูต:

- คำว่า **อุปกรณ์การวิจัยด้านความปลอดภัย** แสดงขึ้นในระหว่างการตั้งค่าอุปกรณ์
- คำว่า **อุปกรณ์การวิจัยด้านความปลอดภัย** แสดงอยู่บนหน้าจอล็อคและในแอปการตั้งค่า

อุปกรณ์การวิจัยด้านความปลอดภัยช่วยให้นักวิจัยมีความสามารถดังต่อไปนี้ ซึ่งอุปกรณ์ของผู้ใช้ไม่มี:

- โค้ดปฏิบัติการไซด์โหลดลงในอุปกรณ์โดยให้สิทธิ์ตามอำเภอใจในระดับการอนุญาตเดียวกันกับส่วนประกอบระบบปฏิบัติการของ Apple
- เริ่มต้นบริการเมื่อเริ่มต้นระบบ
- คงเนื้อหาในการเริ่มการทำงานใหม่

- ใช้สิทธิ์ `research.com.apple.license-to-operate` เพื่ออนุญาตให้กระบวนการทำการดีบั๊กกระบวนการอื่นๆ บนระบบ รวมถึงกระบวนการของระบบ

  พื้นที่ชื่อ `research.` ได้รับการยอมรับโดยตัวแปร RESEARCH ของส่วนขยายเคอร์เนล AppleMobileFileIntegrity เท่านั้น กระบวนการใดๆ ที่มีสิทธิ์นี้จะสิ้นสุดลงในอุปกรณ์ของลูกค้าระหว่างการตรวจสอบลายเซ็น
- ตั้งค่าส่วนบุคคลและกู้คืนแคชเคอร์เนลแบบกำหนดเอง

การเข้ารหัสและการปกป้องข้อมูล

ภาพรวมการเข้ารหัสและการปกป้องข้อมูล

ความสามารถของลำดับการบูตอย่างปลอดภัย ความปลอดภัยของระบบ และความปลอดภัยของแอปทั้งหมดนี้ช่วยตรวจสอบให้แน่ใจว่าโค้ดและแอปที่เชื่อถือเท่านั้นที่สามารถทำงานได้บนอุปกรณ์ อุปกรณ์ Apple มีคุณสมบัติการเข้ารหัสเพิ่มเติมเพื่อปกป้องข้อมูลของผู้ใช้ ถึงแม้ว่าส่วนอื่นของโครงสร้างระบบความปลอดภัยมีพฤติกรรมที่กระทบต่อความมั่นคงปลอดภัยของข้อมูล (ตัวอย่างเช่น หากอุปกรณ์สูญหายหรือเรียกใช้โค้ดที่ไม่เชื่อถือ) คุณสมบัติเหล่านี้ทั้งหมดเป็นประโยชน์กับทั้งผู้ใช้และผู้ดูแลระบบ IT โดยให้การปกป้องข้อมูลส่วนบุคคลและขององค์กร และให้วิธีการล้างข้อมูลระยะไกลโดยทันทีและสมบูรณ์ในกรณีที่อุปกรณ์ถูกขโมยหรือสูญหาย

อุปกรณ์ iOS และ iPadOS ใช้วิธีการเข้ารหัสไฟล์ที่เรียกว่า**การปกป้องข้อมูล** ขณะที่ข้อมูลบน Mac ที่ใช้ Intel ได้รับการปกป้องด้วยเทคโนโลยีการเข้ารหัสดิสก์โวลุ่มที่เรียกว่า **FileVault** Mac ที่ใช้ Apple Silicon จะใช้โมเดลแบบผสมที่รองรับการปกป้องข้อมูล โดยมีข้อจำกัดสองข้อ: ไม่รองรับการปกป้องที่คลาส (D) ซึ่งเป็นระดับต่ำสุดและระดับเริ่มต้น (คลาส C) จะใช้กุญแจดิสก์โวลุ่มและทำหน้าที่เหมือนกับ FileVault บน Mac ที่ใช้ Intel ในทุกกรณี ลำดับการจัดการกุญแจมีรากฐานอยู่ใน Silicon เฉพาะของ Secure Enclave และกลไก AES เฉพาะรองรับการเข้ารหัสสายความเร็วและช่วยให้แน่ใจว่าจะไม่มีการเปิดเผยกุญแจการเข้ารหัสระยะยาวไปยังระบบปฏิบัติการเคอร์เนลหรือ CPU (ซึ่งอาจทำให้ไม่ปลอดภัย) (Mac ที่ใช้ Intel ที่มี T1 หรือไม่มี Secure Enclave จะไม่ใช้ Silicon เฉพาะเพื่อปกป้องกุญแจการเข้ารหัส FileVault ของตัวเอง)

นอกจากจะใช้การปกป้องข้อมูลและ FileVault เพื่อช่วยป้องกันการเข้าถึงข้อมูลแบบไม่ได้รับอนุญาตแล้ว Apple ยังใช้**เคอร์เนลระบบปฏิบัติการ**ในการบังคับใช้การปกป้องและการรักษาความปลอดภัยอีกด้วย เคอร์เนลจะใช้ตัวควบคุมการเข้าถึงแอป Sandbox (ซึ่งจำกัดข้อมูลที่แอปสามารถเข้าถึงได้) และกลไกที่เรียกว่า Data Vault (ซึ่งจำกัดการเข้าถึงข้อมูลของแอปจากแอปอื่นๆ ที่ร้องขอทั้งหมด แทนที่จะจำกัดการร้องขอที่แอปสามารถทำได้)

รหัสและรหัสผ่าน

Apple จะใช้รหัสใน iOS และ iPadOS และรหัสผ่านใน macOS เพื่อปกป้องข้อมูลผู้ใช้จากการโจมตีที่เป็นอันตราย ยิ่งรหัสหรือรหัสผ่านยาวเท่าไร ก็ยิ่งปลอดภัยมากเท่านั้น และยิ่งป้องกันการโจมตีแบบ Brute-Force ได้ง่ายขึ้น Apple บังคับใช้การหน่วงเวลา (สำหรับ iOS และ iPadOS) และจำกัดการพยายามป้อนรหัสผ่าน (สำหรับ Mac) เพื่อเพิ่มการป้องกันจากการโจมตี

การตั้งค่ารหัสอุปกรณ์หรือรหัสผ่านใน iOS และ iPadOS จะเป็นการเปิดใช้งานการปกป้องข้อมูลโดยอัตโนมัติ การปกป้องข้อมูลยังเปิดใช้งานบนอุปกรณ์อื่นๆ ที่มีระบบ Apple บนชิป (SoC) เช่น Mac ที่มี Apple Silicon, Apple TV, และ Apple Watch อีกด้วย Apple ใช้โปรแกรมเข้ารหัสดิสก์โวลุ่ม **FileVault** ในตัวสำหรับ macOS

รหัสและรหัสผ่านที่ปลอดภัยสูงช่วยเพิ่มความปลอดภัยได้อย่างไร

iOS และ iPadOS รองรับรหัสตัวเลขและตัวอักษรหกหลัก สี่หลัก และการกำหนดความยาวตามอำเภอใจ นอกจากการปลดล็อคอุปกรณ์ รหัสและรหัสผ่านยังมอบ Entropy สำหรับกุญแจการเข้ารหัสบางรายการอีกด้วย ซึ่งหมายความว่าผู้ไม่ประสงค์ดีที่ได้อุปกรณ์ไปจะไม่สามารถเข้าถึงข้อมูลในคลาสการปกป้องเฉพาะโดยไม่มีรหัสได้

รหัสหรือรหัสผ่านจะเชื่อมโยงกับ UID ของอุปกรณ์ ดังนั้นการโจมตีแบบ Brute-force จะต้องทำบนอุปกรณ์ที่จะโจมตี ตัวนับการทำซ้ำจำนวนมากใช้เพื่อทำให้การโจมตีแต่ละครั้งช้าลง ตัวนับการทำซ้ำมีการปรับเทียบเพื่อให้การโจมตีหนึ่งครั้งใช้เวลาประมาณ 80 มิลลิวินาที ซึ่งแท้จริงแล้ว การลองผสมรหัสทั้งหมดของรหัสตัวเลขและตัวอักษรหกหลักซึ่งมีตัวอักษรตัวพิมพ์เล็กและตัวเลขจะใช้เวลามากกว่าห้าปีครึ่ง

ยิ่งรหัสผู้ใช้มีความยากมากขึ้นเท่าใด กุญแจการเข้ารหัสจะยิ่งมีความปลอดภัยสูงขึ้นเท่านั้น และด้วยการใช้ Face ID และ Touch ID ผู้ใช้จะสามารถสร้างรหัสที่ปลอดภัยได้สูงกว่ารหัสที่ใช้ได้ในเชิงปฏิบัติ รหัสที่ปลอดภัยมากขึ้นนี้จะช่วยเพิ่มปริมาณ Entropy ที่มีประสิทธิภาพซึ่งช่วยปกป้องกุญแจการเข้ารหัสที่ใช้สำหรับการปกป้องข้อมูล โดยไม่ส่งผลด้านลบต่อประสบการณ์การใช้งานของผู้ใช้ที่ต้องปลดล็อคอุปกรณ์หลายครั้งตลอดวัน

ถ้าป้อนรหัสผ่านที่ยาวและมีเพียงตัวเลขเท่านั้น ปุ่มตัวเลขจะแสดงบนหน้าจอล็อคแทนแป้นพิมพ์แบบเต็ม รหัสตัวเลขที่ยาวจะป้อนได้ง่ายกว่ารหัสตัวเลขและตัวอักษรที่สั้นกว่า ในขณะที่ให้การป้องกันในระดับเดียวกัน

ผู้ใช้สามารถกำหนดรหัสตัวเลขและตัวอักษรที่ยาวขึ้นได้โดยเลือก กำหนดรหัสตัวอักษรและตัวเลขเอง ในตัวเลือกรหัสในการตั้งค่า > Touch ID และรหัส หรือ Face ID และรหัส

การส่งต่อไปยังการหน่วงเวลาป้องกันการโจมตีแบบ Brute-Force ได้อย่างไร (iOS, iPadOS)

สำหรับ iOS และ iPadOS เพื่อเพิ่มการป้องกันจากการโจมตีแบบ Brute-Force อาจมีการหน่วงเวลาที่เพิ่มขึ้นหลังจากการป้อนรหัสที่ไม่ถูกต้องบนหน้าจอล็อคดังที่แสดงในตารางด้านล่าง

ความพยายาม	การหน่วงเวลาที่บังคับใช้
1-4	ไม่มี
5	1 นาที
6	5 นาที
7-8	15 นาที
9	1 ชั่วโมง

ถ้าตัวเลือกลบข้อมูลเปิดใช้อยู่ (ในการตั้งค่า > Touch ID และรหัส) หลังจากป้อนรหัสไม่ถูกต้อง 10 ครั้งติดต่อกัน เนื้อหาและการตั้งค่าทั้งหมดจะถูกเอาออกจากพื้นที่จัดเก็บข้อมูล ความพยายามในการป้อนรหัสที่ไม่ถูกต้องซึ่งเป็นรหัสเดียวกันซ้ำๆ จะไม่ถูกนับเป็นการป้อนรหัสผิดที่ติดต่อกันมากกว่าหนึ่งครั้ง การตั้งค่านี้ยังใช้งานเป็นนโยบายการดูแลจัดการได้ผ่านโซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) ที่รองรับคุณสมบัตินี้และผ่าน Microsoft Exchange ActiveSync และยังสามารถปรับลดจำนวนครั้งในการป้อนรหัสให้ต่ำลงมาได้

บนอุปกรณ์ที่ใช้ Secure Enclave การหน่วงเวลาจะถูกบังคับใช้โดย Secure Enclave ถ้าอุปกรณ์เริ่มการทำงานเครื่องใหม่ในระหว่างช่วงการหน่วงเวลา การหน่วงเวลาจะยังคงใช้งานอยู่ โดยตัวจับเวลาจะเริ่มต้นใหม่สำหรับช่วงเวลาปัจจุบัน

การหน่วงเวลาที่เพิ่มขึ้นช่วยป้องกันการโจมตีแบบ Brute-Force (macOS) ได้อย่างไร

ในการช่วยป้องกันการโจมตีด้วย Brute-force เมื่อ Mac เริ่มต้นระบบ ผู้ใช้พยายามป้อนรหัสผ่านในหน้าต่างเข้าสู่ระบบหรือใช้โหมดดิสก์เป้าหมายได้ไม่เกิน 10 ครั้ง และการหน่วงเวลาที่เพิ่มขึ้นจะถูกกำหนดขึ้นหลังจากป้อนรหัสผิดตามจำนวนครั้งที่กำหนด การหน่วงเวลาถูกบังคับใช้โดย Secure Enclave ถ้า Mac เริ่มการทำงานเครื่องใหม่ในระหว่างช่วงการหน่วงเวลา การหน่วงเวลาจะยังคงใช้งานอยู่ โดยตัวจับเวลาจะเริ่มต้นใหม่สำหรับช่วงเวลาปัจจุบัน

ตารางด้านล่างแสดงการหน่วงเวลาระหว่างการพยายามป้อนรหัสผ่านบน Mac ที่มี Apple Silicon และ Mac ที่มีชิป T2

ความพยายาม	การหน่วงเวลาที่บังคับใช้
5	1 นาที
6	5 นาที
7	15 นาที
8	15 นาที
9	1 ชั่วโมง
10	ปิดใช้งาน

ในการช่วยป้องกันไม่ให้มัลแวร์ทำให้สูญเสียข้อมูลถาวรโดยการพยายามโจมตีรหัสผ่านของผู้ใช้ การจำกัดเหล่านี้จะไม่ได้ใช้งานหลังจากที่ผู้ใช้เข้าสู่ระบบ Mac เสร็จเรียบร้อย แต่ถูกกำหนดขึ้นอีกครั้งหลังจากรีบูต ถ้าป้อนรหัสผ่านครบ 10 ครั้งแล้ว จะสามารถป้อนรหัสผ่านได้อีก 10 ครั้งหลังจากบูตไปยัง recoveryOS และถ้าป้อนรหัสผ่านจนครบ 10 ครั้งแล้วเช่นกัน จะสามารถป้อนรหัสผ่านเพิ่มเติมได้อีก 10 ครั้งสำหรับกลไกการกู้คืน FileVault แต่ละกลไก (การกู้คืน iCloud, รหัสการกู้คืน FileVault และกุญแจองค์กร) สำหรับการป้อนรหัสผ่านเพิ่มเติมสูงสุด 30 ครั้ง หลังจากป้อนรหัสผ่านเพิ่มเติมเหล่านั้นครบแล้ว Secure Enclave จะไม่สามารถดำเนินการตามคำร้องใดๆ เพื่อถอดรหัสดิสก์โวลุ่มหรือตรวจสอบความถูกต้องรหัสผ่านได้อีกต่อไป และข้อมูลบนไดรฟ์จะไม่สามารถกู้คืนได้

ในการปกป้องข้อมูลในการตั้งค่าองค์กร ฝ่ายไอทีควรกำหนดและบังคับใช้นโยบายการกำหนดค่า FileVault โดยใช้โซลูชั่น MDM องค์กรจะมีตัวเลือกมากมายสำหรับจัดการดิสก์โวลุ่มที่ถูกเข้ารหัส รวมถึงรหัสการกู้คืนขององค์กร รหัสการกู้คืนส่วนบุคคล (ซึ่งสามารถเลือกที่จะจัดเก็บด้วย MDM สำหรับข้อมูลที่ฝากได้) หรือกุญแจทั้งสองประเภท การหมุนเวียนของกุญแจก็สามารถตั้งค่าเป็นนโยบายใน MDM ได้ด้วยเช่นกัน

บน Mac ที่มีชิป Apple T2 Security รหัสผ่านจะทำหน้าที่คล้ายคลึงกัน ยกเว้นว่ากุญแจที่สร้างขึ้นจะใช้สำหรับการเข้ารหัส FileVault แทนการปกป้องข้อมูล macOS ยังเสนอตัวเลือกการกู้คืนรหัสผ่านเพิ่มเติม:

- การกู้คืน iCloud
- การกู้คืน FileVault
- กุญแจ FileVault สำหรับองค์กร

การปกป้องข้อมูล

ภาพรวมการปกป้องข้อมูล

Apple ใช้เทคโนโลยีที่เรียกว่าการปกป้องข้อมูลเพื่อปกป้องข้อมูลที่จัดเก็บไว้ในพื้นที่จัดเก็บข้อมูลแบบแฟลชบนอุปกรณ์ที่มี Apple SoC เช่น iPhone, iPad, Apple Watch, Apple TV และ Mac ที่มี Apple Silicon อุปกรณ์สามารถตอบสนองต่อเหตุการณ์ทั่วไป เช่น สายเรียกเข้า ในขณะเดียวกันก็ให้การเข้ารหัสข้อมูลผู้ใช้ในระดับสูงได้ด้วยการปกป้องข้อมูล แอประบบบางแอป (เช่น ข้อความ เมล ปฏิทิน รายชื่อ รูปภาพ) และค่าข้อมูลสุขภาพจะใช้การปกป้องข้อมูลโดยค่าเริ่มต้น แอปของบริษัทอื่นจะได้รับการปกป้องนี้โดยอัตโนมัติ

การปรับใช้

การปกป้องข้อมูลมีการปรับใช้โดยการสร้างและจัดการลำดับชั้นของกุญแจ และสร้างโดยใช้เทคโนโลยีการเข้ารหัสฮาร์ดแวร์ที่สร้างในอุปกรณ์ Apple การปกป้องข้อมูลมีการควบคุมแบบรายไฟล์โดยการกำหนดคลาสให้กับไฟล์แต่ละไฟล์ ความสามารถในการเข้าถึงจะกำหนดตามคลาสกุญแจว่ามีการปลดล็อคหรือไม่ APFS (Apple File System) ช่วยให้ระบบไฟล์สามารถแบ่งย่อยกุญแจเป็นแบบรายขอบเขตเพิ่มเติมได้แล้ว (ซึ่งส่วนของไฟล์สามารถมีกุญแจได้หลายรายการ)

ทุกครั้งที่ไฟล์บนดิสก์โวลุ่มข้อมูลถูกสร้าง การปกป้องข้อมูลจะสร้างกุญแจใหม่แบบ 256 บิต (**กุญแจรายไฟล์**) และส่งกุญแจไปยังกลไกฮาร์ดแวร์ AES ซึ่งจะใช้กุญแจเพื่อเข้ารหัสไฟล์ตามที่เขียนลงในพื้นที่จัดเก็บข้อมูลแบบแฟลช สำหรับอุปกรณ์ตระกูล A14, A15 และ M1 การเข้ารหัสจะใช้ AES-256 ในโหมด XTS ซึ่งกุญแจ 256 บิตต่อไฟล์จะผ่านฟังก์ชั่นการสร้างกุญแจ (NIST Special Publication 800-108) เพื่อให้ได้มาซึ่ง Tweak 256 บิต และกุญแจการเข้ารหัส 256 บิต รุ่นฮาร์ดแวร์ของ A9 ถึง A13, S5, S6 และ S7 ใช้ AES-128 ในโหมด XTS โดยกุญแจ 256 บิตต่อไฟล์จะถูกแยกออกเพื่อให้ได้มาซึ่ง Tweak 128 บิตและกุญแจการเข้ารหัส 128 บิต

ใน Mac ที่มี Apple Silicon การปกป้องข้อมูลจะมีค่าเริ่มต้นเป็น Class C (ให้ดูที่ คลาสการปกป้องข้อมูล) แต่จะใช้กุญแจดิสก์โวลุ่มแทนกุญแจแบบรายขอบเขตหรือรายไฟล์ ซึ่งจะสร้างโมเดลความปลอดภัยของ FileVault ขึ้นใหม่สำหรับข้อมูลผู้ใช้อย่างมีประสิทธิภาพ ผู้ใช้ยังคงต้องเลือกใช้ FileVault เพื่อรับการปกป้องเต็มรูปแบบจากการเชื่อมโยงลำดับชั้นกุญแจการเข้ารหัสด้วยรหัสผ่านของผู้ใช้ นักพัฒนายังสามารถเลือกใช้คลาสการปกป้องที่สูงขึ้นได้ ซึ่งจะใช้กุญแจรายไฟล์หรือรายขอบเขต

การปกป้องข้อมูลในอุปกรณ์ Apple

บนอุปกรณ์ Apple ที่มีการปกป้องข้อมูล แต่ละไฟล์จะได้รับการปกป้องด้วยกุญแจรายไฟล์ (หรือรายขอบเขต) ที่ไม่ซ้ำกัน กุญแจที่ถูกห่อโดยใช้อัลกอริทึมการห่อกุญแจ NIST AED จะถูกห่อเพิ่มเติมด้วยหนึ่งในกุญแจคลาสหลายรายการ ทั้งนี้ขึ้นอยู่กับวิธีเข้าถึงไฟล์ตามปกติ จากนั้นกุญแจรายไฟล์ที่ถูกห่อจะจัดเก็บไว้ในเมตาดาต้าของไฟล์

อุปกรณ์ที่ใช้รูปแบบระบบไฟล์ APFS อาจจะรองรับการโคลนของไฟล์ (สำเนาที่ไม่มีค่าใช้จ่ายใดๆ โดยใช้เทคโนโลยีการเขียนไฟล์แบบ Copy-on-write) ถ้าไฟล์ถูกโคลน โคลนแต่ละครึ่งจะได้รับกุญแจใหม่เพื่อยอมรับการเขียนที่จะเกิดขึ้น ข้อมูลใหม่จึงถูกเขียนไปที่สื่อด้วยกุญแจใหม่ เมื่อเวลาผ่านไป ไฟล์อาจประกอบด้วยขอบเขตหลายอย่าง (หรือหลายส่วน) โดยแต่ละขอบเขตจะเทียบผังเข้ากับกุญแจที่แตกต่างกัน อย่างไรก็ตาม ขอบเขตทั้งหมดที่รวมถึงไฟล์จะได้รับการป้องกันโดยคลาสกุญแจเดียวกัน

เมื่อเปิดไฟล์ เมตาดาต้าของไฟล์นั้นจะถูกถอดรหัสด้วยกุญแจระบบไฟล์ โดยเปิดเผยกุญแจรายไฟล์ที่ถูกห่ออยู่และสัญลักษณ์ที่บอกว่าปกป้องด้วยคลาสใด กุญแจรายไฟล์ (หรือรายขอบเขต) จะถูกแกะห่อด้วยคลาสกุญแจ จากนั้นส่งมอบให้กับกลไก AES ของฮาร์ดแวร์ ซึ่งจะถอดรหัสไฟล์ตามที่มีการอ่านจากพื้นที่จัดเก็บข้อมูลแบบแฟลช การจัดการกุญแจไฟล์ที่ถูกห่อทั้งหมดจะเกิดขึ้นใน Secure Enclave โดยจะไม่เปิดเผยกุญแจไฟล์ให้กับหน่วยประมวลผลแอปพลิเคชัน เมื่อเริ่มต้นระบบ Secure Enclave จะเจรจาขอกุญแจชั่วคราวกับกลไก AES เมื่อ Secure Enclave แกะห่อกุญแจของไฟล์ กุญแจจะถูกห่ออีกครั้งด้วยกุญแจชั่วคราวและถูกส่งกลับไปที่หน่วยประมวลผลแอปพลิเคชัน

เมตาดาต้าของไฟล์ทั้งหมดในระบบไฟล์ดิสก์โวลุ่มข้อมูลจะเข้ารหัสด้วยกุญแจดิสก์โวลุ่มแบบสุ่ม ซึ่งถูกสร้างขึ้นเมื่อติดตั้งระบบปฏิบัติการเป็นครั้งแรกหรือเมื่อผู้ใช้ลบข้อมูลอุปกรณ์ กุญแจนี้จะถูกเข้ารหัสและห่อด้วยกุญแจการห่อกุญแจที่มีเพียง Secure Enclave เท่านั้นที่รู้จักสำหรับการจัดเก็บข้อมูลระยะยาว กุญแจการห่อกุญแจจะเปลี่ยนไปทุกครั้งที่ผู้ใช้ลบข้อมูลอุปกรณ์ บน A9 SoC (และเวอร์ชั่นที่ใหม่กว่า) Secure Enclave จะใช้ Entropy ซึ่งสนับสนุนโดยระบบป้องกันการเล่นซ้ำเพื่อให้สามารถลบออกได้ และเพื่อปกป้องกุญแจการห่อกุญแจที่มีอยู่ในแอสเซทอื่นๆ โปรดดูที่ พื้นที่จัดเก็บข้อมูลแบบถาวรที่ปลอดภัย สำหรับข้อมูลเพิ่มเติม

เช่นเดียวกับกุญแจรายไฟล์หรือรายขอบเขต กุญแจเมตาดาต้าของดิสก์โวลุ่มข้อมูลจะไม่เปิดเผยกุญแจไฟล์ให้กับหน่วยประมวลผลแอปพลิเคชันโดยตรง Secure Enclave จะให้เวอร์ชั่นรายบูตแบบชั่วคราวแทน เมื่อจัดเก็บ กุญแจระบบไฟล์ที่เข้ารหัสจะถูกห่อเพิ่มเติมด้วย "กุญแจที่ลบได้" ที่จัดเก็บอยู่ในพื้นที่จัดเก็บข้อมูลที่ลบได้หรือโดยใช้กุญแจการห่อกุญแจสื่อ ซึ่งปกป้องโดยกลไกการป้องกันการเล่นซ้ำของ Secure Enclave กุญแจนี้จะไม่มีการรักษาความลับของข้อมูลให้เพิ่มเติม แต่ออกแบบมาให้ลบได้อย่างรวดเร็วตามคำร้องขอ (เมื่อผู้ใช้เลือกตัวเลือก "ลบข้อมูลเนื้อหาและการตั้งค่าทั้งหมด" หรือเมื่อผู้ใช้หรือผู้ดูแลระบบออกคำสั่งล้างข้อมูลระยะไกลจากโซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM), Microsoft Exchange ActiveSync หรือ iCloud) การลบกุญแจในลักษณะนี้จะทำให้ไฟล์ทั้งหมดไม่สามารถเข้าถึงได้แบบเข้ารหัส

เนื้อหาของไฟล์อาจมีการเข้ารหัสด้วยกุญแจรายไฟล์ (หรือรายขอบเขต) อย่างน้อยหนึ่งรายการ ซึ่งจะห่อด้วยคลาสกุญแจและจัดเก็บในเมตาดาต้าของไฟล์ ซึ่งเข้ารหัสด้วยกุญแจระบบไฟล์ คลาสกุญแจได้รับการปกป้องด้วยค่า UID ฮาร์ดแวร์ และสำหรับบางคลาสก็จะได้รับการปกป้องด้วยรหัสของผู้ใช้ ลำดับชั้นนี้ให้ทั้งความยืดหยุ่นและการทำงานที่ดี ตัวอย่างเช่น การเปลี่ยนคลาสของไฟล์จำเป็นต้องห่อซ้ำเฉพาะกุญแจรายไฟล์เท่านั้น และการเปลี่ยนรหัสจะห่อคลาสกุญแจซ้ำ

คลาสการปกป้องข้อมูล

เมื่อสร้างไฟล์ใหม่บนอุปกรณ์ที่รองรับการปกป้องข้อมูล แอปที่สร้างไฟล์จะกำหนดคลาสของไฟล์นั้น คลาสแต่ละคลาสจะใช้นโยบายที่ต่างกันเพื่อระบุว่าข้อมูลจะเข้าถึงได้เมื่อใด คลาสและนโยบายเบื้องต้นมีการอธิบายในส่วนต่อไปนี้ Mac ที่ใช้ Apple Silicon ไม่รองรับคลาส D: ไม่มีการปกป้อง และมีการสร้างขอบเขตความปลอดภัยรอบๆ การเข้าสู่ระบบและออกจากระบบ (ไม่ใช่การล็อคหรือปลดล็อคเหมือนบน iPhone, iPad และ iPod touch)

คลาส	ประเภทการปกป้อง
คลาส A: การปกป้องแบบสมบูรณ์	NSFileProtectionComplete
คลาส B: ปกป้องหากไม่เปิดอยู่	NSFileProtectionCompleteUnlessOpen
คลาส C: ปกป้องจนกว่าจะมีการตรวจสอบสิทธิ์ของผู้ใช้รายแรก **หมายเหตุ:** macOS ใช้กุญแจดิสก์โวลุ่มเพื่อสร้างคุณลักษณะการปกป้องของ FileVault ใหม่	NSFileProtectionCompleteUntilFirstUserAuthentication
คลาส D: ไม่มีการปกป้อง **หมายเหตุ:** ไม่รองรับบน macOS	NSFileProtectionNone

การปกป้องแบบสมบูรณ์

NSFileProtectionComplete: คลาสกุญแจได้รับการปกป้องโดยกุญแจที่ได้มาจากรหัสหรือรหัสผ่านของผู้ใช้และค่า UID ของอุปกรณ์ ไม่นานหลังจากที่ผู้ใช้ล็อคอุปกรณ์ (10 วินาที หากการตั้งค่าต้องใส่รหัสผ่านถูกตั้งไว้เป็นทันที) คลาสกุญแจที่ถอดรหัสแล้วจะถูกยกเลิก ทำให้ข้อมูลทั้งหมดในคลาสนี้ไม่สามารถเข้าถึงได้จนกว่าผู้ใช้จะป้อนรหัสอีกครั้งหรือปลดล็อค (เข้าสู่ระบบ) อุปกรณ์ โดยใช้ Face ID หรือ Touch ID

ใน macOS ไม่นานหลังจากที่ผู้ใช้คนล่าสุดออกจากระบบ คลาสกุญแจที่ถอดรหัสจะถูกละทิ้ง โดยทำให้ข้อมูลทั้งหมดในคลาสนี้ไม่สามารถเข้าถึงได้จนกว่าผู้ใช้จะป้อนรหัสอีกครั้ง หรือเข้าสู่ระบบอุปกรณ์โดยใช้ Touch ID

ปกป้องหากไม่เปิดอยู่

NSFileProtectionCompleteUnlessOpen: ไฟล์บางไฟล์อาจต้องเขียนในขณะที่อุปกรณ์ล็อคอยู่ หรือขณะที่ผู้ใช้ออกจากระบบแล้ว ตัวอย่างที่ดีของกรณีนี้คือไฟล์แนบอีเมลที่ดาวน์โหลดอยู่ในพื้นหลัง ลักษณะงานเช่นนี้ทำได้โดยการใช้การเข้ารหัสเส้นโค้งรูปไข่แบบไม่สมมาตร (ECDH บน Curve25519) กุญแจรายไฟล์โดยทั่วไปจะถูกปกป้องด้วยกุญแจที่ได้มาโดยใช้ข้อตกลงกุญแจ One-Pass Diffie-Hellman ตามที่อธิบายใน NIST SP 800-56A

กุญแจสาธารณะชั่วคราวสำหรับข้อตกลงจะจัดเก็บไปพร้อมกับกุญแจรายไฟล์ที่ถูกห่อ KDF คือ ฟังก์ชั่นการแปรผันกุญแจที่ต่อกัน (ตัวเลือก 1 ที่ได้รับอนุญาต) ตามที่อธิบายใน 5.8.1 ของ NIST SP 800-56A ID อัลกอริทึมถูกละเว้น PartyUInfo และ PartyVInfo คือกุญแจสาธารณะชั่วคราวและกุญแจสาธารณะแบบคงที่ตามลำดับ SHA256 ใช้เป็นฟังก์ชั่นการแฮช ทันทีที่ปิดไฟล์ กุญแจรายไฟล์จะถูกล้างจากหน่วยความจำ ในการเปิดไฟล์อีกครั้ง ความลับที่แชร์จะถูกสร้างอีกครั้งโดยใช้กุญแจส่วนตัวของคลาสปกป้องหากไม่เปิดอยู่ และกุญแจสาธารณะชั่วคราวของไฟล์ ซึ่งจะใช้เพื่อแกะห่อกุญแจรายไฟล์ที่ใช้ในการถอดรหัสไฟล์

ใน macOS ส่วนที่เป็นส่วนตัวของ NSFileProtectionCompleteUnlessOpen จะสามารถเข้าถึงได้ตราบใดที่ผู้ใช้บนระบบเข้าสู่ระบบอยู่หรือได้รับการตรวจสอบสิทธิ์

ปกป้องจนกว่าจะมีการตรวจสอบสิทธิ์ของผู้ใช้รายแรก

NSFileProtectionCompleteUntilFirstUserAuthentication: คลาสนี้ทำงานเหมือนกับการปกป้องแบบสมบูรณ์ เว้นแต่เพียงคลาสกุญแจที่ถอดรหัสจะไม่ถูกลบออกจากหน่วยความจำเมื่อล็อคอุปกรณ์หรือผู้ใช้ออกจากระบบ การปกป้องในคลาสนี้มีคุณลักษณะคล้ายกับการเข้ารหัสแบบเต็มในคอมพิวเตอร์เดสก์ท็อป และปกป้องข้อมูลจากการโจมตีที่เกี่ยวข้องกับการรีบูต นี่เป็นคลาสค่าเริ่มต้นสำหรับข้อมูลแอปของบุคคลหรือบริษัทอื่นทั้งหมดที่ไม่ได้ถูกกำหนดคลาสการปกป้องข้อมูลให้

ใน macOS คลาสนี้ใช้กุญแจดิสก์โวลุ่มซึ่งสามารถเข้าถึงได้ตราบใดที่ดิสก์โวลุ่มต่อเชื่อมอยู่ และทำหน้าที่เหมือนกับ FileVault

ไม่มีการปกป้อง

NSFileProtectionNone: คลาสกุญแจนี้ได้รับการปกป้องด้วยค่า UID เท่านั้น และมีการจัดเก็บในพื้นที่จัดเก็บข้อมูลที่ลบได้ เนื่องจากกุญแจทั้งหมดที่จำเป็นต้องใช้เพื่อถอดรหัสไฟล์ในคลาสนี้มีการจัดเก็บบนอุปกรณ์ การเข้ารหัสจึงให้ประโยชน์ของการล้างข้อมูลระยะไกลอย่างรวดเร็วเท่านั้น ถ้าระบบไม่ได้กำหนดคลาสการปกป้องข้อมูลให้ไฟล์ ไฟล์จะยังคงจัดเก็บในรูปแบบที่เข้ารหัส (เช่นเดียวกับข้อมูลทั้งหมดบนอุปกรณ์ iOS และ iPadOS)

สิ่งนี้ไม่รองรับใน macOS

หมายเหตุ: ใน macOS สำหรับดิสก์โวลุ่มที่ไม่สัมพันธ์กันกับระบบปฏิบัติการที่บูต คลาสการปกป้องข้อมูลทั้งหมดจะสามารถเข้าถึงได้ตราบใดที่ดิสก์โวลุ่มต่อเชื่อมอยู่ คลาสการปกป้องข้อมูลที่เป็นค่าเริ่มต้นคือ NSFileProtectionCompleteUntilFirstUserAuthentication ฟังก์ชั่นของกุญแจรายขอบเขตมีให้ใช้ทั้งสำหรับ Rosetta 2 และแอปดั้งเดิม

กระเป๋ากุญแจ (Keybag) สำหรับการปกป้องข้อมูล

กุญแจสำหรับคลาสการปกป้องข้อมูลของทั้งไฟล์และพวงกุญแจจะถูกเก็บรวบรวมและจัดการในกระเป๋ากุญแจ (Keybag) บน iOS, iPadOS, watchOS และ tvOS ระบบปฏิบัติการเหล่านี้จะใช้กระเป๋ากุญแจ (Keybag) ต่อไปนี้: ผู้ใช้ อุปกรณ์ ข้อมูลสำรอง ข้อมูลที่ฝาก และข้อมูลสำรอง iCloud

กระเป๋ากุญแจ (Keybag) ผู้ใช้

กระเป๋ากุญแจ (Keybag) ผู้ใช้ คือที่ที่จัดเก็บคลาสกุญแจที่ถูกห่อซึ่งใช้ในการทำงานปกติของอุปกรณ์ ตัวอย่างเช่น เมื่อป้อนรหัส รหัส **NSFileProtectionComplete** จะโหลดจากกระเป๋ากุญแจ (Keybag) ผู้ใช้แล้วแกะห่อออก ไฟล์นี้เป็นไฟล์รายการคุณสมบัติ (.plist) แบบไบนารีที่จัดเก็บอยู่ในคลาสไม่มีการปกป้อง

สำหรับอุปกรณ์ที่มี SoC เวอร์ชั่นก่อนหน้า A9 เนื้อหาไฟล์แบบ .plist จะถูกเข้ารหัสด้วยกุญแจที่อยู่ในพื้นที่จัดเก็บข้อมูลที่ลบได้ ในการให้ความปลอดภัยกับกระเป๋ากุญแจ (Keybag) กุญแจนี้จะถูกล้างและสร้างใหม่ทุกครั้งที่ผู้ใช้เปลี่ยนรหัสของตน

สำหรับอุปกรณ์ที่มี SoC เวอร์ชั่น A9 ขึ้นไป ไฟล์ .plist จะมีกุญแจที่ระบุว่ากระเป๋ากุญแจ (Keybag) ถูกจัดเก็บไว้ในล็อคเกอร์ที่ได้รับการปกป้องโดย nonce ป้องกันการเล่นซ้ำที่ควบคุมโดย Secure Enclave

Secure Enclave จะจัดการกระเป๋ากุญแจ (Keybag) และสามารถสอบถามเกี่ยวกับสถานะการล็อคของอุปกรณ์ได้ โดยจะแจ้งว่าอุปกรณ์ไม่ได้ล็อคอยู่เมื่อสามารถเข้าถึงคลาสกุญแจทั้งหมดในกระเป๋ากุญแจ (Keybag) ผู้ใช้ได้ และได้แกะห่อสำเร็จแล้วเท่านั้น

กระเป๋ากุญแจ (Keybag) อุปกรณ์

กระเป๋ากุญแจ (Keybag) อุปกรณ์ใช้เพื่อจัดเก็บคลาสกุญแจที่ถูกห่อสำหรับการทำงานที่เกี่ยวข้องกับข้อมูลเฉพาะอุปกรณ์ อุปกรณ์ iPadOS ที่กำหนดค่าสำหรับการใช้งานที่แชร์ในบางครั้งจำเป็นต้องใช้การเข้าถึงเอกสารสิทธิ์ก่อนที่ผู้ใช้รายใดเข้าสู่ระบบ ดังนั้นจะต้องใช้กระเป๋ากุญแจ (Keybag) ที่ไม่ได้รับการปกป้องด้วยรหัสของผู้ใช้

iOS และ iPadOS ไม่รองรับการเข้ารหัสแบบแยกของเนื้อหาระบบไฟล์รายผู้ใช้ ซึ่งหมายความว่าระบบจะใช้คลาสกุญแจจากกระเป๋ากุญแจ (Keybag) อุปกรณ์เพื่อห่อกุญแจรายไฟล์ อย่างไรก็ตามพวงกุญแจจะใช้คลาสกุญแจจากกระเป๋ากุญแจ (Keybag) ผู้ใช้เพื่อปกป้องรายการในพวงกุญแจของผู้ใช้ ในอุปกรณ์ iOS และ iPadOS ที่กำหนดค่าสำหรับใช้โดยผู้ใช้เพียงคนเดียว (การกำหนดค่าเริ่มต้น) กระเป๋ากุญแจ (Keybag) อุปกรณ์และกระเป๋ากุญแจ (Keybag) ผู้ใช้จะเป็นอันเดียวกัน และได้รับการปกป้องด้วยรหัสของผู้ใช้

กระเป๋ากุญแจ (Keybag) ของข้อมูลสำรอง

กระเป๋ากุญแจ (Keybag) ของข้อมูลสำรองจะถูกสร้างขึ้นเมื่อ Finder (macOS 10.15 ขึ้นไป) หรือ iTunes (ใน macOS 10.14 หรือก่อนหน้านี้) สำรองข้อมูลแบบเข้ารหัสและจัดเก็บในคอมพิวเตอร์ที่สำรองข้อมูลของอุปกรณ์อยู่ กระเป๋ากุญแจ (Keybag) ใหม่จะถูกสร้างขึ้นด้วยกุญแจชุดใหม่ และข้อมูลที่สำรองไว้จะถูกเข้ารหัสอีกครั้งไปยังกุญแจใหม่เหล่านั้น ตามที่อธิบายก่อนหน้านี้ รายการพวงกุญแจที่ไม่สามารถเคลื่อนย้ายได้จะยังคงถูกห่อด้วยกุญแจที่ได้จากค่า UID ซึ่งทำให้สามารถกู้คืนรายการเหล่านั้นไปที่อุปกรณ์ดั้งเดิมที่สำรองข้อมูลนั้นได้ แต่จะทำให้เข้าถึงไม่ได้ในอุปกรณ์เครื่องอื่น

กระเป๋ากุญแจ (Keybag) ที่ปกป้องด้วยชุดรหัสผ่าน มีการเรียกใช้งานผ่านการทำซ้ำนับ 10 ล้านครั้งของฟังก์ชั่นการรับกุญแจ PBKDF2 แม้จะมีตัวนับการทำซ้ำที่สูง แต่ไม่มีการผูกกับอุปกรณ์เฉพาะเครื่อง ดังนั้นในทางทฤษฎีแล้วจึงสามารถพยายามโจมตีกระเป๋ากุญแจ (Keybag) ของข้อมูลสำรองด้วย Brute-force โดยใช้คอมพิวเตอร์หลายเครื่องพร้อมกันได้ ภัยคุกคามนี้สามารถถูกจำกัดได้โดยใช้รหัสผ่านที่มีความปลอดภัยสูงพอ

ถ้าผู้ใช้เลือกไม่เข้ารหัสข้อมูลสำรอง ไฟล์เหล่านั้นจะไม่ถูกเข้ารหัสไม่ว่าจะอยู่ในคลาสการปกป้องข้อมูลใด แต่พวงกุญแจจะยังคงได้รับการปกป้องด้วยกุญแจที่มาจากค่า UID นี่จึงเป็นสาเหตุที่รายการพวงกุญแจจะโยกย้ายไปยังอุปกรณ์เครื่องใหม่เฉพาะเมื่อตั้งค่ารหัสผ่านข้อมูลสำรองไว้เท่านั้น

กระเป๋ากุญแจ (Keybag) ของข้อมูลที่ฝาก

กระเป๋ากุญแจ (Keybag) ของข้อมูลที่ฝากจะใช้เพื่อเชื่อมข้อมูลกับ Finder (ใน macOS 10.15 ขึ้นไป) หรือ iTunes (macOS 10.14 หรือก่อนหน้านี้) ผ่าน USB และการจัดการอุปกรณ์ (MDM) กระเป๋ากุญแจ (Keybag) นี้อนุญาตให้ Finder หรือ iTunes สำรองข้อมูลและเชื่อมข้อมูลโดยไม่ต้องเรียกขอให้ผู้ใช้ป้อนรหัส และอนุญาตให้โซลูชั่น MDM ล้างรหัสของผู้ใช้จากระยะไกลได้ กระเป๋ากุญแจ (Keybag) นี้มีการจัดเก็บในคอมพิวเตอร์ที่ใช้เพื่อเชื่อมข้อมูลกับ Finder หรือ iTunes หรือบนโซลูชั่น MDM ที่จัดการอุปกรณ์จากระยะไกล

กระเป๋ากุญแจ (Keybag) ของข้อมูลที่ฝากจะปรับปรุงประสบการณ์ของผู้ใช้ในระหว่างการเชื่อมข้อมูลอุปกรณ์ ซึ่งต้องใช้การเข้าถึงคลาสทั้งหมดของข้อมูล เมื่ออุปกรณ์ที่ล็อคด้วยรหัสเชื่อมต่อกับ Finder หรือ iTunes ครั้งแรก ผู้ใช้จะได้รับแจ้งให้ป้อนรหัส จากนั้นอุปกรณ์จะสร้างกระเป๋ากุญแจ (Keybag) ของข้อมูลที่ฝากที่มีคลาสกุญแจเดียวกันกับที่ใช้บนอุปกรณ์ที่ถูกปกป้องด้วยกุญแจที่สร้างใหม่ กระเป๋ากุญแจ (Keybag) ของข้อมูลที่ฝากและกุญแจที่ปกป้องจะถูกแยกระหว่างอุปกรณ์และโฮสต์หรือเซิร์ฟเวอร์ โดยข้อมูลจะถูกจัดเก็บในอุปกรณ์ในคลาสปกป้องจนกว่าจะมีการตรวจสอบสิทธิ์ของผู้ใช้รายแรก นี่เป็นสาเหตุที่รหัสอุปกรณ์จะต้องได้รับการป้อนก่อนที่ผู้ใช้จะสำรองข้อมูลกับ Finder หรือ iTunes เป็นครั้งแรกหลังจากรีบูต

ในกรณีของรายการอัปเดตซอฟต์แวร์ผ่านทางอากาศ (OTA) ผู้ใช้จะได้รับแจ้งขอรหัสเมื่อเริ่มต้นการอัปเดต ขั้นตอนนี้ใช้เพื่อสร้างโทเค็นการปลดล็อคครั้งเดียวอย่างปลอดภัย ซึ่งจะปลดล็อคกระเป๋ากุญแจ (Keybag) ผู้ใช้หลังจากการอัปเดต โทเค็นนี้ไม่สามารถสร้างได้โดยปราศจากการป้อนรหัสของผู้ใช้ และโทเค็นที่สร้างก่อนหน้าใดๆ จะถูกยกเลิกการใช้งานหากรหัสของผู้ใช้เปลี่ยน

โทเค็นการปลดล็อคครั้งเดียวใช้สำหรับการติดตั้งรายการอัปเดตซอฟต์แวร์ทั้งแบบต้องจัดการหรือแบบไม่ต้องจัดการ โทเค็นจะถูกเข้ารหัสด้วยกุญแจที่มาจากค่าปัจจุบันของตัวนับทางเดียวใน Secure Enclave, ค่า UUID ของกระเป๋ากุญแจ (Keybag) และค่า UID ของ Secure Enclave

บน SoC A9 (ขึ้นไป) โทเค็นการปลดล็อคแบบครั้งเดียวจะไม่พึ่งพาตัวนับหรือพื้นที่จัดเก็บข้อมูลที่ลบได้อีกต่อไป แต่จะได้รับการปกป้องโดย Nonce ป้องกันการเล่นซ้ำที่ควบคุมโดย Secure Enclave

โทเค็นการปลดล็อคครั้งเดียวสำหรับรายการอัปเดตซอฟต์แวร์ที่ต้องจัดการจะหมดอายุหลังผ่านไป 20 นาที ใน iOS 13 และ iPadOS 13.1 ขึ้นไป โทเค็นจะจัดเก็บอยู่ในล็อคเกอร์ที่ได้รับการปกป้องโดย Secure Enclave ก่อน iOS 13 โทเค็นนี้จะถูกส่งออกจาก Secure Enclave และเขียนไปที่พื้นที่จัดเก็บข้อมูลที่ลบได้ หรือได้รับการปกป้องโดยกลไกการป้องกันการเล่นซ้ำของ Secure Enclave นาฬิกานับถอยหลังของนโยบายจะเพิ่มตัวนับหากอุปกรณ์ไม่เริ่มการทำงานใหม่ภายใน 20 นาที

รายการอัปเดตซอฟต์แวร์ที่ไม่ต้องจัดการจะเกิดขึ้นเมื่อระบบตรวจพบรายการอัปเดตที่พร้อมให้ดาวน์โหลด และเมื่อหนึ่งรายการอัปเดตต่อไปนี้เป็นจริง:

- มีการกำหนดค่าการอัปเดตอัตโนมัติใน iOS 12 ขึ้นไป
- ผู้ใช้เลือก ติดตั้งในภายหลัง เมื่อได้รับแจ้งให้อัปเดต

หลังจากที่ผู้ใช้ป้อนรหัสของตัวเอง โทเค็นการปลดล็อคแบบครั้งเดียวจะถูกสร้างขึ้นและยังคงสามารถใช้ใน Secure Enclave ได้มากถึง 8 ชั่วโมง ถ้ายังไม่มีรายการอัปเดต โทเค็นการปลดล็อคแบบครั้งเดียวนี้จะถูกทำลายในการล็อคทุกครั้ง และจะถูกสร้างขึ้นในการปลดล็อคที่เกิดขึ้นในภายหลังทุกๆ ครั้ง การปลดล็อคแต่ละครั้งจะเริ่มการทำงานหน้าต่าง 8 ชั่วโมงใหม่ หลังจาก 8 ชั่วโมง นาฬิกานับถอยหลังของนโยบายจะทำให้โทเค็นการปลดล็อคแบบครั้งเดียวไม่สามารถใช้งานได้

กระเป๋ากุญแจ (Keybag) ข้อมูลสำรอง iCloud

กระเป๋ากุญแจ (Keybag) ข้อมูลสำรอง iCloud คล้ายคลึงกับกระเป๋ากุญแจ (Keybag) ข้อมูลสำรอง คลาสกุญแจทั้งหมดในกระเป๋ากุญแจ (Keybag) นี้ไม่สมมาตร (ใช้งาน Curve25519 เหมือนกับคลาสการปกป้องข้อมูลแบบปกป้องหากไม่เปิดอยู่) กระเป๋ากุญแจ (Keybag) แบบไม่สมมาตรยังใช้สำหรับข้อมูลสำรองในส่วนการกู้คืนพวงกุญแจของพวงกุญแจ iCloud อีกด้วย

การปกป้องกุญแจในโหมดการบูตอื่นๆ

การปกป้องข้อมูลได้รับการออกแบบให้เข้าถึงข้อมูลผู้ใช้ได้เฉพาะหลังจากที่ตรวจสอบสิทธิ์สำเร็จเท่านั้น และเข้าถึงได้เฉพาะผู้ใช้ที่อนุญาตเท่านั้น คลาสการปกป้องข้อมูลได้รับการออกแบบให้รองรับกรณีการใช้งานที่หลากหลาย เช่น ความสามารถในการอ่านและเขียนข้อมูลบางส่วนแม้อุปกรณ์จะล็อคอยู่ (แต่ต้องหลังจากปลดล็อคครั้งแรกแล้ว) ระบบมีขั้นตอนเพิ่มเติมที่ต้องดำเนินการเพื่อปกป้องสิทธิ์เข้าถึงข้อมูลผู้ใช้ในระหว่างโหมดบูตอื่นๆ เช่น ขั้นตอนที่ใช้กับโหมดอัปเดตเฟิร์มแวร์อุปกรณ์ (DFU), โหมดการกู้คืน, การวินิจฉัยของ Apple หรือแม้แต่ในระหว่างการอัปเดตซอฟต์แวร์ ความสามารถเหล่านี้มีการอ้างอิงจากการผสมผสานระหว่างคุณสมบัติด้านฮาร์ดแวร์และซอฟต์แวร์ และมีการขยายเพิ่มขึ้นขณะที่ Silicon ที่ Apple ออกแบบได้พัฒนาขึ้น

คุณสมบัติ	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, ตระกูล M1
การกู้คืน: คลาสการปกป้องข้อมูลทุกคลาสที่ได้รับการปกป้อง	✓	✓	✓	✓	✓
การบูตอื่นๆ ของโหมด DFU, การกู้คืน และการอัปเดตซอฟต์แวร์: คลาส A, B และ C ที่ได้รับการปกป้อง		✓	✓	✓	✓

กลไก Secure Enclave AES มาพร้อมกับบิต Seed ของซอฟต์แวร์ที่สามารถล็อคได้ เมื่อกุญแจถูกสร้างขึ้นจาก UID ระบบจะรวมบิต Seed อยู่ในฟังก์ชั่นการแปรผันกุญแจเพื่อสร้างลำดับชั้นเพิ่มเติมของกุญแจขึ้นมา วิธีใช้บิต Seed จะแตกต่างกันไปตามระบบบนชิป:

- สำหรับ A10 SoC และ S3 SoC ของ Apple บิต Seed จะมีอยู่ในกุญแจแต่ละดอกที่ได้รับการปกป้องด้วยรหัสของผู้ใช้ บิต Seed จะถูกตั้งค่าสำหรับกุญแจที่ต้องใช้รหัสของผู้ใช้ (เช่น กุญแจการปกป้องข้อมูลคลาส A, คลาส B, และคลาส C) และจะไม่มีอยู่ในกุญแจที่ไม่จำเป็นต้องใช้รหัสของผู้ใช้ (เช่น กุญแจเมตาดาต้าของระบบไฟล์และกุญแจคลาส D)
- ใน iOS 13 ขึ้นไปและ iPadOS 13.1 ขึ้นไปบนอุปกรณ์ที่มี A10 ขึ้นไป ข้อมูลของผู้ใช้ทั้งหมดทำให้ไม่สามารถเข้าถึงได้ด้วยการเข้ารหัสเมื่ออุปกรณ์บูตไปยังโหมดการวินิจฉัย การทำเช่นนี้ทำได้โดยการแนะนำบิต Seed เพิ่มเติมที่มีการตั้งค่าควบคุมความสามารถในการเข้าถึงกุญแจสื่อ ซึ่งจำเป็นต้องใช้เพื่อเข้าถึงเมตาดาต้า (ดังนั้นจึงรวมไปถึงเนื้อหาของไฟล์ทั้งหมด) บนดิสก์โวลุ่มข้อมูลที่เข้ารหัสด้วยการปกป้องข้อมูล การปกป้องนี้รวมไฟล์ที่ได้รับการปกป้องในทุกคลาส (A, B, C และ D) ไม่เพียงไฟล์ที่ต้องใช้รหัสของผู้ใช้เท่านั้น
- Secure Enclave Boot ROM บน A12 SoC จะล็อคบิต Seed ของรหัสหากหน่วยประมวลผลแอปพลิเคชันเข้าสู่โหมดอัปเกรดเฟิร์มแวร์อุปกรณ์ (DFU) หรือ โหมดการกู้คืน เมื่อรหัสบิต Seed ถูกล็อค การทำงานใดๆ ที่จะเปลี่ยนรหัสผ่านจะไม่สามารถดำเนินการได้ วิธีนี้ได้รับการออกแบบมาเพื่อป้องกันเข้าถึงข้อมูลที่ได้รับการปกป้องโดยรหัสของผู้ใช้

การกู้คืนอุปกรณ์หลังจากที่เข้าสู่โหมด DFU จะทำให้อุปกรณ์นั้นกลับสู่สภาพที่ใช้งานได้และรับรองได้ว่าจะมีเฉพาะรหัสที่ Apple ลงชื่อรับรองที่ไม่ได้แก้ไขเท่านั้น สามารถเข้าสู่โหมด DFU ได้ด้วยตัวเอง

ดูบทความบริการช่วยเหลือของ Apple ต่อไปนี้เกี่ยวกับวิธีเปลี่ยนอุปกรณ์ในโหมด DFU:

อุปกรณ์	บทความ
iPhone, iPad, iPod touch	ถ้าคุณลืมรหัส iPhone ของคุณ
Apple TV	ถ้าคุณเห็นสัญลักษณ์เตือนบน Apple TV
Mac ที่ใช้ Apple Silicon	ฟื้นฟูหรือกู้คืน Mac ที่ใช้ Apple Silicon

การปกป้องข้อมูลผู้ใช้ขณะที่ถูกโจมตี

ผู้โจมตีที่พยายามดึงข้อมูลผู้ใช้มักจะลองใช้เทคนิคที่หลากหลาย: ดึงข้อมูลที่เข้ารหัสไว้ไปยังสื่ออื่นเพื่อโจมตีแบบ Brute-force หรือควบคุมเวอร์ชั่นของระบบปฏิบัติการ หรือไม่ก็เปลี่ยนแปลงหรือทำให้นโยบายความปลอดภัยของอุปกรณ์อ่อนแอลงเพื่อให้โจมตีได้ง่ายขึ้น การโจมตีข้อมูลบนอุปกรณ์มักจะต้องมีการสื่อสารกับอุปกรณ์โดยใช้อินเทอร์เฟซทางกายภาพอย่าง Lightning หรือ USB อุปกรณ์ Apple มีคุณสมบัติต่างๆ ที่ช่วยป้องกันการโจมตีเหล่านั้น

อุปกรณ์ Apple รองรับเทคโนโลยีที่เรียกว่า **Sealed Key Protection (SKP)** ที่ได้รับการออกแบบมาเพื่อให้แน่ใจว่าข้อมูลการเข้ารหัสนั้นจะถูกทำให้ไม่สามารถใช้งานได้ภายนอกอุปกรณ์ หรือจะถูกใช้หากตรวจสอบว่ามีการควบคุมเวอร์ชั่นของระบบปฏิบัติการหรือการตั้งค่าความปลอดภัยโดยที่ไม่ได้รับอนุญาตจากผู้ใช้อย่างเหมาะสมหรือไม่ คุณสมบัตินี้**ไม่ได้**มาจาก Secure Enclave แต่รองรับโดยการลงทะเบียนฮาร์ดแวร์ที่อยู่ชั้นล่างลงไปเพื่อเพิ่มการปกป้องอีกหนึ่งชั้นให้กับกุญแจที่จำเป็นต่อการถอดรหัสข้อมูลผู้ใช้ที่แยกต่างหากจาก Secure Enclave

หมายเหตุ: SKP มีให้ใช้เฉพาะบนอุปกรณ์ที่มี SoC ที่ Apple ออกแบบเท่านั้น

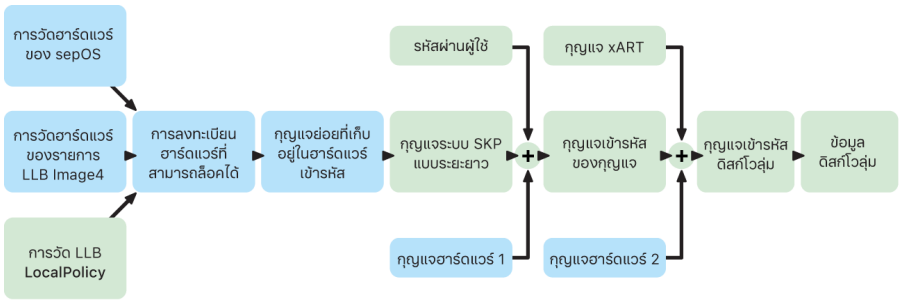
คุณสมบัติ	A10	A11, S3	A12, S4	A13, S5	A14, A15, S6, S7, ตระกูล M1
Sealed Key Protection	✓	✓	✓	✓	✓

iPhone และ iPad สามารถกำหนดค่าให้เปิดใช้งานการเชื่อมต่อข้อมูลเฉพาะในสภาพแวดล้อมที่บ่งบอกว่าอุปกรณ์อยู่ภายใต้การควบคุมทางกายภาพของผู้ใช้ที่ได้รับอนุญาต

Sealed Key Protection (SKP)

บนอุปกรณ์ Apple ที่รองรับการปกป้องข้อมูล กุญแจการเข้ารหัสกุญแจ (KEK) จะได้รับการปกป้อง (หรือปิดผนึก) ด้วยการวัดของซอฟต์แวร์บนระบบ และผูกกับ UID ที่มีให้ใช้งานจาก Secure Enclave เท่านั้น บน Mac ที่ใช้ Apple Silicon การปกป้องของ KEK มีการเพิ่มความแข็งแกร่งโดยการรวมข้อมูลเกี่ยวกับนโยบายความปลอดภัยบนระบบ เนื่องจาก macOS รองรับการเปลี่ยนแปลงนโยบายด้านความปลอดภัยที่สำคัญ (ตัวอย่างเช่น การปิดใช้งานการบูตอย่างปลอดภัยหรือ SIP) ที่ไม่รองรับบนแพลตฟอร์มอื่น บน Mac ที่ใช้ Apple Silicon การปกป้องนี้ครอบคลุมกุญแจ FileVault เนื่องจาก FileVault มีการใช้การปกป้องข้อมูล (คลาส C)

กุญแจที่มาจากการเชื่อมโยงรหัสผ่านผู้ใช้, กุญแจ SKP ระยะยาว และกุญแจฮาร์ดแวร์ 1 (UID จาก Secure Enclave) จะเรียกว่า **กุญแจที่ได้จากรหัส** กุญแจนี้จะใช้เพื่อปกป้องกระเป๋ากุญแจ (Keybag) ของผู้ใช้ (บนทุกแพลตฟอร์มที่รองรับ) และ KEK (ใน macOS เท่านั้น) และเมื่อเปิดใช้งานการปลดล็อคด้วยชีวมิติหรือการปลดล็อคอัตโนมัติด้วยอุปกรณ์เครื่องอื่น เช่น Apple Watch



ตัวตรวจสอบการบูตของ Secure Enclave จะบันทึกข้อมูลการวัด Secure Enclave OS ที่โหลด เมื่อ Boot ROM ของหน่วยประมวลผลแอปพลิเคชันวัดรายการ Image4 ที่แนบกับ LLB รายการดังกล่าวจะมีการวัดของเฟิร์มแวร์ที่จับคู่กับระบบอื่นๆ ทั้งหมดที่โหลดด้วยเช่นกัน LocalPolicy มีการกำหนดค่าความปลอดภัยหลักสำหรับ macOS ที่โหลด นอกจากนี้ LocalPolicy ยังมีช่อง `nsih` ซึ่งเป็นแฮชของรายการ Image4 ใน macOS อีกด้วย รายการ Image4 ใน macOS ประกอบด้วยการวัดเฟิร์มแวร์ที่จับคู่กับ macOS ทั้งหมดและวัตถุการบูต macOS หลักๆ เช่น คอลเลกชั่นเคอร์เนลบูตหรือแฮชรากดิสก์โวลุ่มระบบที่ลงชื่อ (SSV)

ถ้าผู้โจมตีสามารถเปลี่ยนส่วนประกอบเฟิร์มแวร์ ซอฟต์แวร์ หรือการกำหนดค่าที่วัดข้างต้นได้ ผู้โจมตีจะแก้ไขการวัดที่จัดเก็บอยู่ในการลงทะเบียนฮาร์ดแวร์ การแก้ไขของการวัดทำให้ **System Measurement Root Key (SMRK)** ที่ได้จากฮาร์ดแวร์การเข้ารหัสมีการรับการวัดเป็นค่าอื่น ซึ่งจะทำลายตราประทับบนลำดับชั้นกุญแจอย่างมีประสิทธิภาพ ซึ่งทำให้ไม่สามารถเข้าถึง **System Measurement Device Key (SMDK)** ได้ จึงทำให้ไม่สามารถเข้าถึง KEK และข้อมูลได้

อย่างไรก็ตาม เมื่อระบบไม่ได้ถูกโจมตี ระบบจะต้องรองรับรายการอัปเดตซอฟต์แวร์ที่มีสิทธิ์อย่างถูกต้องที่จะเปลี่ยนการวัดเฟิร์มแวร์และช่อง `nsih` ใน LocalPolicy เป็นการวัด macOS แบบใหม่ ในระบบอื่นที่พยายามรวมการวัดเฟิร์มแวร์แต่ไม่มีแหล่งข้อมูลของความจริงที่ใช้งานได้ ระบบจะต้องใช้ผู้ใช้ในการปิดใช้งานความปลอดภัย อัปเดตซอฟต์แวร์ และเปิดใช้งานอีกครั้งเพื่อให้สามารถบันทึกข้อมูลฐานการวัดใหม่ได้ การทำเช่นนี้จะเพิ่มความเสี่ยงที่ผู้โจมตีจะสามารถดัดแปลงเฟิร์มแวร์ในระหว่างการอัปเดตซอฟต์แวร์เป็นอย่างมาก ระบบได้รับการช่วยเหลือจากการที่รายการ Image4 มีการวัดที่จำเป็นทั้งหมด ฮาร์ดแวร์ที่ถอดรหัส SMDK ด้วย SMRK เมื่อการวัดตรงกันระหว่างการบูตปกติ ยังสามารถเข้ารหัส SMDK กับ SMRK ที่จะเสนอในอนาคตได้อีกด้วย ด้วยการระบุการวัดที่คาดหวังไว้หลังจากอัปเดตซอฟต์แวร์ ฮาร์ดแวร์จะสามารถเข้ารหัส SMDK ที่สามารถเข้าถึงได้ในระบบปฏิบัติการปัจจุบันเพื่อให้ยังคงสามารถเข้าถึงได้ในระบบปฏิบัติการในอนาคต เช่นเดียวกัน เมื่อลูกค้าเปลี่ยนการตั้งค่าอย่างถูกต้องใน LocalPolicy แล้ว SMDK จะต้องถูกเข้ารหัสไปยัง SMRK ในอนาคต โดยอิงจากการวัดของ LocalPolicy ที่ LLB จะคำนวณเมื่อเริ่มการทำงานใหม่ครั้งถัดไป

การเปิดใช้งานการเชื่อมต่อข้อมูลอย่างปลอดภัยใน iOS และ iPadOS

สำหรับอุปกรณ์ iOS หรือ iPadOS หากไม่มีการสร้างการเชื่อมต่อข้อมูลเมื่อเร็วๆ นี้ ผู้ใช้ต้องใช้ Face ID, Touch ID หรือรหัสเพื่อเปิดใช้งานการเชื่อมต่อข้อมูลผ่านอินเทอร์เฟซ Lightning, USB หรือ Smart Connector วิธีการนี้จะจำกัดการโจมตีผ่านทางอุปกรณ์เชื่อมต่อทางกายภาพ เช่น ที่ชาร์จที่เป็นอันตราย ในขณะที่ยังคงสามารถใช้งานอุปกรณ์เสริมอื่นๆ ภายในระยะเวลาที่เหมาะสมได้ ถ้าเวลาผ่านไปมากกว่าหนึ่งชั่วโมงนับจากเวลาที่อุปกรณ์ iOS หรือ iPadOS ล็อคหรือการเชื่อมต่อข้อมูลของอุปกรณ์เสริมหยุดลง อุปกรณ์จะไม่อนุญาตให้มีการเชื่อมต่อข้อมูลครั้งใหม่จนกว่าอุปกรณ์จะถูกปลดล็อค ในระหว่างระยะเวลาหนึ่งชั่วโมงนี้ ระบบจะอนุญาตเพียงการเชื่อมต่อข้อมูลจากอุปกรณ์เสริมที่เคยเชื่อมต่อกับอุปกรณ์ในขณะที่อยู่ในสถานะปลดล็อคแล้วเท่านั้น อุปกรณ์เสริมเหล่านี้จะถูกจดจำเป็นเวลา 30 วันหลังจากการเชื่อมต่อกับอุปกรณ์เสริมครั้งล่าสุด เมื่ออุปกรณ์เสริมที่ไม่ทราบชื่อพยายามเปิดการเชื่อมต่อข้อมูลในช่วงเวลานี้ จะเป็นการปิดใช้งานการเชื่อมต่อข้อมูลอุปกรณ์เสริมทั้งหมดผ่าน Lighting, USB และ Smart Connector จนกว่าอุปกรณ์จะถูกปลดล็อคอีกครั้ง ระยะเวลาหนึ่งชั่วโมงนี้:

- ช่วยให้มั่นใจได้ว่าผู้ใช้ที่มีการเชื่อมต่อกับ Mac หรือ PC, อุปกรณ์เสริม หรือใช้สายเชื่อมต่อกับ CarPlay อยู่เป็นประจำ ไม่จำเป็นจะต้องป้อนรหัสทุกครั้งที่เชื่อมต่ออุปกรณ์ของตัวเอง
- เป็นสิ่งจำเป็น เนื่องจากระบบนิเวศของอุปกรณ์เสริมไม่มีวิธีการที่น่าเชื่อถือในการเข้ารหัสเพื่อระบุอุปกรณ์เสริมก่อนที่จะสร้างการเชื่อมต่อข้อมูล

นอกจากนี้แล้ว ถ้าระยะเวลาผ่านไปเกินกว่า 3 วันนับจากวันที่สร้างการเชื่อมต่อข้อมูลกับอุปกรณ์เสริม อุปกรณ์จะไม่อนุญาตการเชื่อมต่อครั้งใหม่ในทันทีหลังจากที่อุปกรณ์ล็อค การดำเนินการนี้มีจุดประสงค์เพื่อเพิ่มการปกป้องให้กับผู้ใช้ที่ไม่ได้ใช้อุปกรณ์เสริมรูปแบบดังกล่าวบ่อยมากนัก การเชื่อมต่อข้อมูลผ่าน Lightning, USB และ Smart Connector ยังถูกปิดใช้งานเมื่อใดก็ตามที่อุปกรณ์อยู่ในสถานะที่ต้องใช้รหัสในการเปิดใช้งานการตรวจสอบสิทธิ์แบบชีวมิติอีกครั้งด้วยเช่นกัน

ผู้ใช้สามารถเลือกเปิดใช้งานการเชื่อมต่อข้อมูลแบบเปิดตลอดเวลาอีกครั้งได้ในการตั้งค่า (การตั้งค่าอุปกรณ์ช่วยเหลือบางเครื่องจะเปิดใช้งานการเชื่อมต่อนี้โดยอัตโนมัติ)

บทบาทของ Apple File System

Apple File System (APFS) คือระบบไฟล์ความเป็นเจ้าของที่ได้รับการออกแบบมาพร้อมกับการเข้ารหัส APFS ทำงานได้บนแพลตฟอร์มทั้งหมดของ Apple ซึ่งได้แก่ iPhone, iPad, iPod touch, Mac, Apple TV และ Apple Watch APFS ที่ปรับให้เหมาะสมกับพื้นที่จัดเก็บข้อมูลแฟลช/SSD มีการเข้ารหัสที่ปลอดภัย, เมตาดาต้าแบบ Copy-on-write, การแชร์พื้นที่, การโคลนไฟล์และไดเรกทอรี, สแนปช็อต, การปรับขนาดไดเรกทอรีอย่างรวดเร็ว, การบันทึกแบบดั้งเดิมที่มีความปลอดภัยระดับจุลภาค และพื้นฐานระบบไฟล์ที่ปรับปรุงแล้ว รวมถึงการออกแบบแบบ Copy-on-write ที่ไม่ซ้ำกัน ซึ่งใช้การรวมกันของ I/O เพื่อมอบประสิทธิภาพการทำงานสูงสุดขณะที่ให้ความมั่นใจถึงความน่าเชื่อด้านข้อมูล

การแชร์พื้นที่

APFS จะจัดสรรพื้นที่จัดเก็บข้อมูลตามคำร้องขอ เมื่อตัวบรรจุ APFS เดี่ยวมีดิสก์โวลุ่มจำนวนมาก พื้นที่ว่างของตัวบรรจุจะถูกแชร์และสามารถจัดสรรไปยังดิสก์โวลุ่มใดๆ ตามต้องการได้ แต่ละดิสก์โวลุ่มจะใช้เพียงส่วนหนึ่งของตัวบรรจุทั้งหมด จึงมีพื้นที่ว่างเท่ากับขนาดทั้งหมดของตัวบรรจุ ลบด้วยพื้นที่ว่างที่ใช้ในดิสก์โวลุ่มทั้งหมดในตัวบรรจุ

ดิสก์โวลุ่มหลายดิสก์

ใน macOS 10.15 ขึ้นไป ตัวบรรจุ APFS ที่ใช้ในการเริ่มต้นระบบ Mac จะต้องประกอบด้วยดิสก์โวลุ่มอย่างน้อยห้ารายการ โดยสามรายการแรกจะซ่อนไม่ให้ผู้ใช้เห็น:

- **ดิสก์โวลุ่มก่อนเริ่มต้นระบบ:** ดิสก์โวลุ่มนี้ไม่มีการเข้ารหัสและมีข้อมูลที่จำเป็นสำหรับการบูตแต่ละดิสก์โวลุ่มระบบในตัวบรรจุ
- **ดิสก์โวลุ่ม VM:** ดิสก์โวลุ่มนี้ไม่มีการเข้ารหัสและใช้โดย macOS ในการจัดเก็บไฟล์การสับเปลี่ยนที่เข้ารหัส
- **ดิสก์โวลุ่มการกู้คืน:** ดิสก์โวลุ่มนี้ไม่มีการเข้ารหัสและต้องพร้อมใช้งานโดยไม่ต้องปลดล็อคดิสก์โวลุ่มระบบเพื่อเริ่มต้นระบบใน recoveryOS
- **ดิสก์โวลุ่มระบบ:** มีดังต่อไปนี้:
  - ไฟล์ที่จำเป็นทั้งหมดสำหรับเริ่มต้นทำงาน Mac
  - แอปทั้งหมดที่ติดตั้งในตัวโดย macOS (แอปที่เคยมีอยู่ในโฟลเดอร์ /Applications ตอนนี้อยู่ใน /System/Applications)

  หมายเหตุ: ตามค่าเริ่มต้น ไม่มีกระบวนการใดสามารถเขียนไปยังดิสก์โวลุ่มระบบได้ แม้กระทั่งกระบวนการระบบของ Apple
- **ดิสก์โวลุ่มข้อมูล:** มีข้อมูลที่สามารถเปลี่ยนแปลงได้ เช่น:
  - ข้อมูลใดๆ ภายในโฟลเดอร์ของผู้ใช้ ซึ่งรวมถึงรูปภาพ เพลง วิดีโอ และเอกสาร
  - แอปที่ผู้ใช้ติดตั้ง รวมถึงแอปพลิเคชัน AppleScript และ Automator
  - เฟรมเวิร์คและดีมอนแบบกำหนดเองที่ผู้ใช้ องค์กร หรือแอปของบริษัทอื่นเป็นผู้ติดตั้ง
  - ตำแหน่งที่ตั้งอื่นๆ ที่ผู้ใช้เป็นเจ้าของและเขียนได้ เช่น /Applications, /Library, /Users, /Volumes, /usr/local, /private, /var และ /tmp

ดิสก์โวลุ่มข้อมูลถูกสร้างขึ้นสำหรับดิสก์โวลุ่มระบบเพิ่มเติมแต่ละดิสก์ ดิสก์โวลุ่มก่อนเริ่มต้นระบบ ดิสก์โวลุ่ม VM และดิสก์โวลุ่มการกู้คืนจะไม่ถูกทำสำเนาแต่จะถูกแชร์ทั้งหมด

สำหรับ macOS 11 ขึ้นไป ดิสก์โวลุ่มระบบจะได้รับการบันทึกแบบสแนปช็อต ระบบปฏิบัติการจะเริ่มต้นระบบจากสแนปช็อตของดิสก์โวลุ่ม ไม่ใช่จากการต่อเชื่อมแบบอ่านอย่างเดียวของดิสก์โวลุ่มระบบที่ผันแปรได้เท่านั้น

ใน iOS และ iPadOS พื้นที่จัดเก็บข้อมูลจะแบ่งออกเป็นอย่างน้อยสองดิสก์โวลุ่ม APFS:

- ดิสก์โวลุ่มระบบ
- ดิสก์โวลุ่มข้อมูล

การปกป้องข้อมูลในพวงกุญแจ

แอปหลายตัวจำเป็นต้องจัดการรหัสผ่านและข้อมูลสั้นๆ ที่เป็นความลับ เช่น กุญแจและโทเค็นการเข้าสู่ระบบ พวงกุญแจมอบวิธีที่ปลอดภัยในการจัดเก็บรายการเหล่านี้ ระบบปฏิบัติการที่หลากหลายของ Apple ใช้กลไกที่แตกต่างกันเพื่อบังคับใช้การรับประกันที่เชื่อมโยงกับคลาสการปกป้องพวงกุญแจต่างๆ ใน macOS (ซึ่งรวมถึง Mac ที่ใช้ Apple Silicon) ระบบไม่ได้ใช้การปกป้องข้อมูลโดยตรงเพื่อบังคับใช้การรับประกันเหล่านี้

ภาพรวม

รายการพวงกุญแจจะเข้ารหัสโดยใช้กุญแจ AES-256-GCM ที่แตกต่างกันสองแบบ ซึ่งได้แก่ กุญแจตาราง (เมตาดาต้า) และกุญแจต่อแถว (กุญแจลับ) เมตาดาต้าพวงกุญแจ (คุณลักษณะทั้งหมดนอกเหนือจาก kSecValue) จะถูกเข้ารหัสด้วยกุญแจเมตาดาต้าเพื่อค้นหาอย่างเร็ว และค่าลับ (kSecValueData) จะถูกเข้ารหัสด้วยกุญแจลับ กุญแจเมตาดาต้าได้รับการปกป้องโดย Secure Enclave แต่จะถูกแคชในหน่วยประมวลผลแอปพลิเคชันเพื่ออนุญาตให้ใช้การสอบถามแบบเร็วของพวงกุญแจ กุญแจลับต้องใช้การส่งข้อมูลแบบไปกลับผ่านทาง Secure Enclave อยู่เสมอ

พวงกุญแจถูกใช้เป็นฐานข้อมูล SQLite ที่จัดเก็บในระบบไฟล์ ฐานข้อมูลมีเพียงฐานเดียว โดยดีมอน `securityd` จะกำหนดว่ารายการพวงกุญแจใดที่กระบวนการทำงานหรือแอปสามารถเข้าถึงได้ API การเข้าถึงพวงกุญแจส่งผลให้มีการเรียกไปยังดีมอน ซึ่งจะสอบถามการให้สิทธิ์ “keychain-access-groups,” “application-identifier,” และ “application-group” ของแอป กลุ่มสิทธิ์อนุญาตรายการพวงกุญแจให้สามารถแชร์ระหว่างแอปได้ แทนที่จะจำกัดการเข้าถึงไปที่กระบวนการทำงานเดียว

รายการพวงกุญแจสามารถแชร์ได้ระหว่างแอปต่างๆ จากนักพัฒนารายเดียวกันเท่านั้น ในการแชร์รายการพวงกุญแจ แอปของบริษัทอื่นจะใช้กลุ่มการเข้าถึงที่มีคำนำหน้าระบุหน้ากลุ่มเหล่านั้นผ่าน Apple Developer Program ในกลุ่มแอปพลิเคชัน ข้อกำหนดคำนำหน้าและกลุ่มแอปพลิเคชันที่ไม่เหมือนกันมีการบังคับใช้ผ่านการลงชื่อโค้ด โปรไฟล์การกำหนดสิทธิ์ และโปรแกรมนักพัฒนาของ Apple

ข้อมูลพวงกุญแจได้รับการปกป้องโดยใช้โครงสร้างคลาสที่คล้ายคลึงกับที่ใช้ในการปกป้องข้อมูลของไฟล์ คลาสเหล่านี้มีลักษณะการทำงานเหมือนกับคลาสการปกป้องข้อมูลของไฟล์ แต่ใช้กุญแจและฟังก์ชั่นที่เป็นเอกลักษณ์

ความพร้อมใช้งาน	การปกป้องข้อมูลไฟล์	การปกป้องข้อมูลในพวงกุญแจ
เมื่อปลดล็อค	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
เมื่อล็อค	NSFileProtectionCompleteUnlessOpen	ไม่มี
หลังจากปลดล็อคครั้งแรก	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
ตลอดเวลา	NSFileProtectionNone	kSecAttrAccessibleAlways
รหัสถูกเปิดใช้งาน	ไม่มี	kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly

แอปที่ใช้บริการดึงข้อมูลใหม่ของพื้นหลังสามารถใช้ **kSecAttrAccessibleAfterFirstUnlock** สำหรับรายการพวงกุญแจที่จำเป็นต้องได้รับการเข้าถึงในระหว่างการอัปเดตพื้นหลังได้

คลาส **kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly** จะทำงานเหมือนกับ **kSecAttrAccessibleWhenUnlocked** อย่างไรก็ตาม คลาสนี้จะใช้ได้เฉพาะเมื่ออุปกรณ์ได้รับการกำหนดค่าด้วยรหัสเท่านั้น คลาสนี้จะมีอยู่ในระบบกระเป๋ากุญแจ (Keybag) เท่านั้น โดยมีคุณสมบัติดังต่อไปนี้:

- ไม่เชื่อมข้อมูลกับพวงกุญแจ iCloud
- ไม่ถูกสำรองข้อมูล
- ไม่ได้รวมอยู่ในกระเป๋ากุญแจ (keybag) ของผู้ดูแลผลประโยชน์ของคู่สัญญา (escrow)

ถ้าลบหรือรีเซ็ตรหัส รายการต่างๆ จะกลายเป็นรายการที่ไร้ประโยชน์โดยการทิ้งคลาสกุญแจไป

คลาสพวงกุญแจอื่นๆ มีส่วนของ “อุปกรณ์นี้เท่านั้น” ซึ่งจะได้รับการปกป้องด้วยค่า UID เสมอ เมื่อถูกคัดลอกจากอุปกรณ์ในระหว่างการสำรองข้อมูล โดยจะกลายเป็นรายการที่ไร้ประโยชน์หากจัดเก็บลงในอุปกรณ์เครื่องอื่น Apple ได้รักษาสมดุลระหว่างความปลอดภัยและความสามารถในการใช้งานไว้อย่างรอบคอบโดยการเลือกคลาสพวงกุญแจที่ขึ้นอยู่กับประเภทของข้อมูลที่ได้รับการรักษาความปลอดภัย และเมื่อจำเป็นสำหรับ iOS และ iPadOS ตัวอย่างเช่น ใบรับรอง VPN จะต้องสามารถใช้งานได้เสมอ เพื่อให้อุปกรณ์รักษาการเชื่อมต่ออย่างต่อเนื่อง แต่รายการนี้จะถูกจัดเป็น “ไม่สามารถเคลื่อนย้ายได้” จึงไม่สามารถย้ายไปยังอุปกรณ์อีกเครื่องได้

การปกป้องคลาสข้อมูลในพวงกุญแจ

การปกป้องคลาสที่ระบุด้านล่างมีการบังคับใช้สำหรับรายการในพวงกุญแจ

รายการ	**สามารถเข้าถึงได้**
รหัสผ่าน Wi-Fi	หลังจากปลดล็อคครั้งแรก
บัญชีเมล	หลังจากปลดล็อคครั้งแรก
บัญชี Microsoft Exchange ActiveSync	หลังจากปลดล็อคครั้งแรก
รหัสผ่าน VPN	หลังจากปลดล็อคครั้งแรก
LDAP, CalDAV, CardDAV	หลังจากปลดล็อคครั้งแรก
โทเค็นบัญชีเครือข่ายสังคม	หลังจากปลดล็อคครั้งแรก
กุญแจการเข้ารหัสการแจ้ง Handoff	หลังจากปลดล็อคครั้งแรก
โทเค็น iCloud	หลังจากปลดล็อคครั้งแรก
กุญแจ iMessage	หลังจากปลดล็อคครั้งแรก
รหัสผ่านการแชร์ในพื้นที่	เมื่อปลดล็อค
รหัสผ่าน Safari	เมื่อปลดล็อค
ที่คั่นหน้า Safari	เมื่อปลดล็อค
ข้อมูลสำรอง Finder/iTunes	เมื่อล็อคแล้ว ไม่สามารถเคลื่อนย้ายได้
กุญแจส่วนตัวที่ติดตั้งโดยโปรไฟล์การกำหนดค่า	เมื่อล็อคแล้ว ไม่สามารถเคลื่อนย้ายได้
ใบรับรอง VPN	ตลอดเวลา ไม่สามารถเคลื่อนย้ายได้
กุญแจ Bluetooth®	ตลอดเวลา ไม่สามารถเคลื่อนย้ายได้
โทเค็นบริการการแจ้งผลักข้อมูลของ Apple (APNs)	ตลอดเวลา ไม่สามารถเคลื่อนย้ายได้
ใบรับรอง iCloud และกุญแจส่วนตัว	ตลอดเวลา ไม่สามารถเคลื่อนย้ายได้
รหัส PIN ของซิม	ตลอดเวลา ไม่สามารถเคลื่อนย้ายได้
ใบรับรองที่ติดตั้งโดยโปรไฟล์การกำหนดค่า	ตลอดเวลา
โทเค็น “ค้นหาของฉัน”	ตลอดเวลา
ข้อความเสียง	ตลอดเวลา

การควบคุมการเข้าถึงพวงกุญแจ

พวงกุญแจสามารถใช้รายการควบคุมสิทธิ์ (ACL) เพื่อตั้งค่านโยบายสำหรับข้อกำหนดการช่วยการเข้าถึงและข้อกำหนดการตรวจสอบสิทธิ์ รายการสามารถกำหนดเงื่อนไขที่ต้องมีการแสดงตนของผู้ใช้โดยระบุว่า ผู้ใช้จะไม่สามารถเข้าถึงได้เว้นแต่จะมีการตรวจสอบสิทธิ์โดยใช้ Face ID, Touch ID หรือโดยการป้อนรหัสหรือรหัสผ่านของอุปกรณ์ การเข้าถึงรายการยังสามารถถูกจำกัดได้ด้วยการกำหนดว่าการลงทะเบียน Face ID หรือ Touch ID ต้องไม่มีการเปลี่ยนแปลงตั้งแต่เพิ่มรายการ การจำกัดนี้จะช่วยป้องกันไม่ให้ผู้โจมตีเพิ่มลายนิ้วมือของตัวเองเพื่อเข้าถึงรายการในพวงกุญแจ ACL มีการประเมินภายใน Secure Enclave และจะปล่อยสู่เคอร์เนลเมื่อตรงตามข้อจำกัดที่ระบุเท่านั้น

สถาปัตยกรรมพวงกุญแจใน macOS

macOS ยังให้การเข้าถึงพวงกุญแจเพื่อจัดเก็บชื่อผู้ใช้และรหัสผ่าน รวมถึงข้อมูลประจำตัวดิจิตอล กุญแจการเข้ารหัส และโน้ตที่ปลอดภัยอย่างสะดวกและปลอดภัยอีกด้วย ซึ่งสามารถเข้าถึงได้ด้วยการเปิดแอปการเข้าถึงพวงกุญแจใน /Applications/Utilities/ การใช้พวงกุญแจจะช่วยให้ไม่จำเป็นต้องป้อนหรือแม้แต่จดจำเอกสารสิทธิ์สำหรับแหล่งข้อมูลแต่ละแห่ง พวงกุญแจเริ่มต้นรายการแรกสร้างขึ้นสำหรับผู้ใช้ Mac แต่ละราย แต่ผู้ใช้สามารถสร้างพวงกุญแจอื่นๆ เพื่อวัตถุประสงค์เฉพาะ

นอกจากการพึ่งพาพวงกุญแจผู้ใช้ macOS จะใช้พวงกุญแจระดับระบบจำนวนหนึ่งคงแอสเซทการตรวจสอบสิทธิ์ซึ่งไม่ใช่แอสเซทเฉพาะผู้ใช้ เช่น เอกสารสิทธิ์เครือข่ายและข้อมูลประจำตัวของโครงสร้างกุญแจสาธารณะ (PKI) รากของระบบซึ่งเป็นหนึ่งในพวงกุญแจเหล่านี้ไม่สามารถเปลี่ยนได้และจัดเก็บใบรับรองของหน่วยงานให้บริการออกใบรับรอง (CA) ระดับ PKI อินเทอร์เน็ตเพื่อให้ทำงานทั่วไปได้อย่างง่ายดาย เช่น บริการธนาคารออนไลน์และอีคอมเมิร์ซ ผู้ใช้สามารถปรับใช้ใบรับรอง CA ที่ได้รับการเตรียมใช้งานภายในด้วยลักษณะที่คล้ายกันในคอมพิวเตอร์ Mac ที่ได้รับการจัดการเพื่อช่วยตรวจสอบความถูกต้องของไซต์และบริการภายในได้

FileVault

การเข้ารหัสดิสก์โวลุ่มด้วย FileVault ใน macOS

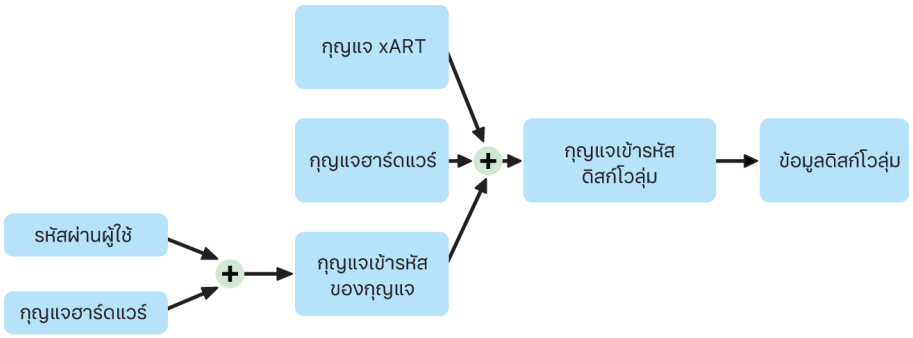
คอมพิวเตอร์ Mac มี FileVault ซึ่งเป็นความสามารถของการเข้ารหัสในตัวเพื่อรักษาความปลอดภัยของข้อมูลทั้งหมดในเครื่อง FileVault ใช้อัลกอริทึมการเข้ารหัสข้อมูล AES-XTS เพื่อปกป้องดิสก์โวลุ่มแบบเต็มบนอุปกรณ์จัดเก็บข้อมูลภายในและถอดออกได้

FileVault บน Mac ที่ใช้ Apple Silicon มีการใช้โดยใช้การปกป้องข้อมูลคลาส C ที่มีกุญแจดิสก์โวลุ่ม บน Mac ที่มีชิป Apple T2 Security และ Mac ที่ใช้ Apple Silicon อุปกรณ์จัดเก็บข้อมูลภายในที่เข้ารหัสที่เชื่อมต่อกับ Secure Enclave โดยตรงจะใช้ความสามารถด้านความปลอดภัยของฮาร์ดแวร์ของตัวเอง รวมถึงความสามารถของกลไก AES หลังจากผู้ใช้เปิดใช้ FileVault บน Mac จะต้องใช้เอกสารสิทธิ์ของผู้ใช้ในระหว่างกระบวนการเริ่มต้นระบบ

พื้นที่จัดเก็บข้อมูลภายในที่มี FileVault เปิดใช้อยู่

ในกรณีที่ไม่มีข้อมูลยืนยันตัวตนที่ถูกต้องหรือรหัสการกู้คืนแบบเข้ารหัส ดิสก์โวลุ่ม APFS ภายในจะยังคงเข้ารหัสอยู่และได้รับการปกป้องจากการเข้าถึงที่ไม่ได้รับอนุญาต แม้ว่าอุปกรณ์พื้นที่จัดเก็บข้อมูลจะถูกเอาออกและเชื่อมต่อกับคอมพิวเตอร์เครื่องอื่น ใน macOS 10.15 สิ่งนี้จะรวมทั้งดิสก์โวลุ่มระบบและดิสก์โวลุ่มข้อมูล ตั้งแต่ macOS 11 เป็นต้นไป ดิสก์โวลุ่มระบบจะได้รับการปกป้องโดยคุณสมบัติดิสก์โวลุ่มระบบที่ลงชื่อ (SSV) แต่ดิสก์โวลุ่มข้อมูลจะยังคงได้รับการปกป้องด้วยการเข้ารหัส การเข้ารหัสดิสก์โวลุ่มภายในบน Mac ที่ใช้ Apple Silicon และ Mac ที่มีชิป T2 ถูกปรับใช้โดยการสร้างและจัดการลำดับชั้นของกุญแจ และสร้างบนเทคโนโลยีการเข้ารหัสฮาร์ดแวร์ภายในชิป ลำดับชั้นของกุญแจนี้ออกแบบมาเพื่อให้บรรลุสิ่เป้าหมายนี้พร้อมกัน:

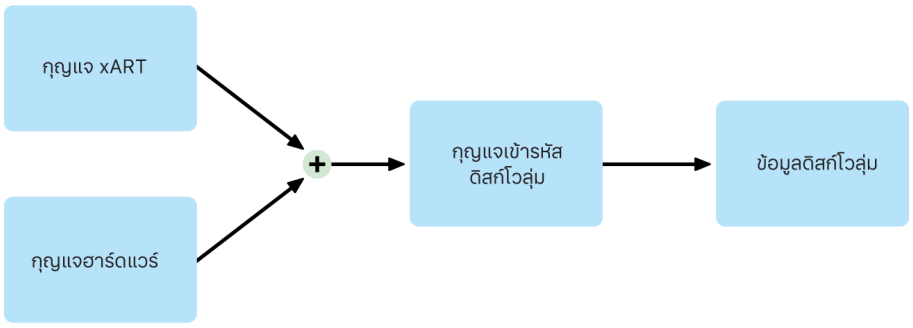
- ต้องใช้รหัสของผู้ใช้สำหรับการถอดรหัส
- ปกป้องระบบจากการโจมตีด้วย Brute-force โดยตรงกับสื่อในพื้นที่จัดเก็บข้อมูลที่เอาออกจาก Mac
- มอบวิธีที่รวดเร็วและปลอดภัยสำหรับการลบข้อมูลเนื้อหาผ่านการลบข้อมูลการเข้ารหัสที่จำเป็น
- ช่วยให้ผู้ใช้เปลี่ยนรหัสผ่าน (และใช้กุญแจการเข้ารหัสเพื่อปกป้องไฟล์) ได้โดยไม่ต้องเข้ารหัสดิสก์โวลุ่มทั้งหมดอีกครั้ง



บน Mac ที่ใช้ Apple Silicon และ Mac ที่มีชิป T2 การจัดการกุญแจ FileVault ทั้งหมดจะเกิดขึ้นใน Secure Enclave กุญแจการเข้ารหัสไม่เปิดเผยกุญแจไฟล์ให้กับ Intel CPU โดยตรง ดิสก์โวลุ่ม APFS ทั้งหมดสร้างด้วยกุญแจการเข้ารหัสดิสก์โวลุ่มตามค่าเริ่มต้น เนื้อหาของดิสก์โวลุ่มและเมตาดาต้าเข้ารหัสด้วยกุญแจการเข้ารหัสดิสก์โวลุ่มนี้ ซึ่งจะถูกห่อด้วยคลาสกุญแจ คลาสกุญแจได้รับการปกป้องโดยการรวมรหัสผ่านของผู้ใช้และ UID ฮาร์ดแวร์เข้าด้วยกันเมื่อเปิดใช้ FileVault อยู่

พื้นที่จัดเก็บข้อมูลภายในที่มี FileVault ปิดใช้อยู่

ถ้าไม่ได้เปิดใช้ FileVault อยู่ใน Mac ที่ใช้ Apple Silicon หรือ Mac ที่มีชิป T2 ในระหว่างกระบวนการเริ่มต้นผู้ช่วยตั้งค่า ดิสก์โวลุ่มจะยังคงเข้ารหัสอยู่ แต่กุญแจการเข้ารหัสดิสก์โวลุ่มจะได้รับการปกป้องด้วย UID ฮาร์ดแวร์เท่านั้นใน Secure Enclave



ถ้าเปิดใช้ FileVault ในภายหลัง ซึ่งกระบวนการจะเริ่มขึ้นทันทีเนื่องจากเข้ารหัสข้อมูลอยู่แล้ว กลไกการป้องกันการเล่นซ้ำจะช่วยป้องกันไม่ให้ใช้กุญแจเก่า (ขึ้นอยู่กับ UID ฮาร์ดแวร์เท่านั้น) ถอดรหัสดิสก์โวลุ่ม จากนั้นดิสก์โวลุ่มจะได้รับการปกป้องโดยการรวมรหัสผ่านของผู้ใช้และ UID ฮาร์ดแวร์เข้าด้วยกันดังที่อธิบายไว้ก่อนหน้านี้

การลบดิสก์โวลุ่ม FileVault

เมื่อลบดิสก์โวลุ่ม กุญแจการเข้ารหัสดิสก์โวลุ่มจะถูกลบอย่างปลอดภัยด้วย Secure Enclave ซึ่งจะช่วยป้องกันการเข้าถึงด้วยกุญแจนี้ในอนาคต แม้แต่การเข้าถึงโดย Secure Enclave นอกจากนี้ กุญแจการเข้ารหัสดิสก์โวลุ่มทั้งหมดจะห่อด้วยกุญแจสื่อ กุญแจสื่อนี้จะไม่มีการรักษาความลับของข้อมูลให้เพิ่มเติม แต่กุญแจสื่อนี้ออกแบบมาเพื่อทำให้การลบข้อมูลรวดเร็วและปลอดภัย เพราะหากไม่มีกุญแจสื่อ จะไม่สามารถถอดรหัสได้

บน Mac ที่ใช้ Apple Silicon และ Mac ที่มีชิป T2 กุญแจสื่อมีโอกาสที่สูงจะถูกลบโดยเทคโนโลยีที่รองรับของ Secure Enclave ตัวอย่างเช่น คำสั่ง MDM ระยะไกล การลบกุญแจสื่อในลักษณะนี้จะทำให้ดิสก์โวลุ่มไม่สามารถเข้าถึงได้แบบเข้ารหัส

อุปกรณ์จัดเก็บข้อมูลแบบถอดออกได้

การเข้ารหัสของอุปกรณ์จัดเก็บข้อมูลแบบถอดออกได้จะไม่ใช้ความสามารถด้านความปลอดภัยของ Secure Enclave และการเข้ารหัสของอุปกรณ์จะดำเนินการในลักษณะเดียวกันกับ Mac ที่ใช้ Intel ที่ไม่มีชิป T2

การจัดการ FileVault ใน macOS

ใน macOS องค์กรสามารถจัดการ FileVault ได้โดยใช้ SecureToken หรือโทเค็นการเริ่มต้นระบบ

การใช้โทเค็นที่ปลอดภัย

Apple File System (APFS) ใน macOS 10.13 ขึ้นไปเปลี่ยนวิธีสร้างกุญแจการเข้ารหัส FileVault ใน macOS เวอร์ชั่นก่อนหน้าบนดิสก์โวลุ่ม CoreStorage กุญแจที่ใช้อยู่ในกระบวนการการเข้ารหัส FileVault ถูกสร้างเมื่อผู้ใช้หรือองค์กรเปิดใช้ FileVault บน Mac ใน macOS บนดิสก์โวลุ่ม APFS กุญแจจะถูกสร้างในระหว่างการสร้างผู้ใช้ การตั้งรหัสผ่านแรกของผู้ใช้ หรือในระหว่างที่ผู้ใช้ของ Mac เข้าสู่ระบบเป็นครั้งแรก สำหรับการปรับใช้กุญแจการเข้ารหัสนี้ กรณีที่จะมีการสร้างกุญแจและวิธีการจัดเก็บกุญแจนี้เป็นส่วนหนึ่งของคุณสมบัติที่เรียกว่า**โทเค็นที่ปลอดภัย** โทเค็นที่ปลอดภัยเป็นเวอร์ชั่นที่ถูกห่อของกุญแจสำหรับการเข้ารหัสกุญแจ (KEK) โดยเฉพาะซึ่งได้รับการปกป้องด้วยรหัสผ่านของผู้ใช้

เมื่อมีการปรับใช้ FileVault บน APFS ผู้ใช้สามารถทำสิ่งต่างๆ เหล่านี้ต่อไปได้:

- ใช้เครื่องมือและกระบวนการที่มีอยู่ เช่น กุญแจการกู้คืนส่วนบุคคล (PRK) ที่สามารถจัดเก็บด้วยโซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) สำหรับการฝากได้
- สร้างและใช้รหัสการกู้คืนขององค์กร (IRK)
- เลื่อนการเปิดใช้งาน FileVault จนกว่าผู้ใช้จะเข้าสู่ระบบหรือออกจากระบบ Mac

ใน macOS 11 การตั้งรหัสผ่านเริ่มต้นสำหรับผู้ใช้ที่ใช้งาน Mac เป็นครั้งแรกส่งผลให้ผู้ใช้ได้รับโทเค็นที่ปลอดภัย ในบางเวิร์คโฟลว์ที่อาจเป็นลักษณะการทำงานที่ไม่พึงประสงค์ การมอบโทเค็นที่ปลอดภัยรายการแรกจะกำหนดให้ผู้ใช้เข้าสู่ระบบ เช่นเดียวกับก่อนหน้านี้ ในการป้องกันไม่ให้สิ่งนี้เกิดขึ้น ให้เพิ่ม `;DisabledTags;SecureToken` ไปยังคุณลักษณะ `AuthenticationAuthority` ของผู้ใช้ที่สร้างขึ้นด้วยโปรแกรม ก่อนที่จะตั้งรหัสผ่านของผู้ใช้ ดังที่แสดงอยู่ด้านล่าง:

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

การใช้โทเค็นการเริ่มต้นระบบ

macOS 10.15 เปิดตัวคุณสมบัติใหม่ซึ่งเป็น**โทเค็นการเริ่มต้นระบบ** เพื่อช่วยในการมอบโทเค็นที่ปลอดภัยให้กับทั้งบัญชีอุปกรณ์เคลื่อนที่และบัญชีผู้ดูแลระบบที่สร้างด้วยการลงทะเบียนอุปกรณ์ (“ผู้ดูแลระบบที่มีการจัดการ”) สำหรับ macOS 11 โทเค็นการเริ่มต้นระบบสามารถมอบโทเค็นที่ปลอดภัยให้กับผู้ใช้ที่เข้าสู่ระบบคอมพิวเตอร์ Mac ซึ่งรวมถึงบัญชีผู้ใช้ภายในเครื่องด้วย การใช้คุณสมบัติโทเค็นการเริ่มต้นระบบใหม่ของ macOS 10.15 ขึ้นไป ต้องใช้:

- การลงทะเบียน Mac ใน MDM โดยใช้ Apple School Manager หรือ Apple Business Manager ซึ่งทำให้ Mac ได้รับการกำกับดูแล
- การรองรับผู้จำหน่าย MDM

สำหรับ macOS 10.15.4 ขึ้นไป โทเค็นการเริ่มต้นระบบจะถูกสร้างและฝากไว้กับ MDM ในการเข้าสู่ระบบครั้งแรกโดยผู้ใช้ที่เปิดใช้งานโทเค็นความปลอดภัย หากโซลูชั่น MDM รองรับคุณสมบัตินี้ โทเค็นการเริ่มต้นระบบยังสามารถสร้างและฝากไปยัง MDM โดยใช้เครื่องมือบรรทัดคำสั่ง `profiles` ได้เช่นกัน หากจำเป็น

สำหรับ macOS 11 โทเค็นการเริ่มต้นระบบยังสามารถใช้ได้มากกว่าเพียงเพื่อมอบโทเค็นที่ปลอดภัยให้กับบัญชีผู้ใช้บน Mac ที่มี Apple Silicon จะสามารถใช้โทเค็นการเริ่มต้นระบบ (หากมี) เพื่ออนุญาตการติดตั้งทั้งส่วนขยายเคอร์เนลและรายการอัปเดตซอฟต์แวร์ได้เมื่อจัดการโดยใช้ MDM

วิธีการที่ Apple ปกป้องข้อมูลส่วนบุคคลของผู้ใช้

การปกป้องการเข้าถึงข้อมูลผู้ใช้ของแอป

นอกจากการเข้ารหัสข้อมูลในเครื่องแล้ว อุปกรณ์ Apple ยังช่วยป้องกันไม่ให้แอปต่างๆ เข้าถึงข้อมูลส่วนบุคคลของผู้ใช้โดยไม่ได้รับสิทธิ์อีกด้วย โดยใช้เทคโนโลยีต่างๆ ซึ่งรวมถึง Data Vault ในการตั้งค่าใน iOS และ iPadOS หรือการตั้งค่าระบบใน macOS ผู้ใช้สามารถดูได้ว่าได้อนุญาตให้แอปใดบ้างเข้าถึงข้อมูลบางอย่าง เช่นเดียวกับการมอบหรือถอนสิทธิ์การเข้าถึงในอนาคตทั้งหมด การเข้าถึงจะบังคับใช้ในรายการต่อไปนี้:

- **iOS, iPadOS และ macOS:** ปฏิทิน กล้อง รายชื่อ ไมโครโฟน รูปภาพ เตือนความจำ การรู้จำคำพูด
- **iOS และ iPadOS:** บลูทูธ บ้าน สื่อ แอปสื่อและ Apple Music การเคลื่อนไหวและฟิตเนส
- **iOS และ watchOS:** สุขภาพ
- **macOS:** การตรวจสอบข้อมูลเข้า (ตัวอย่างเช่น การกดปุ่มบนแป้นพิมพ์) การแจ้ง การบันทึกหน้าจอ (ตัวอย่างเช่น ภาพหน้าจอแบบนิ่งและวิดีโอ) การตั้งค่าระบบ

ใน iOS 13.4 ขึ้นไป และ iPadOS 13.4 ขึ้นไป แอปของบริษัทอื่นทั้งหมดจะได้รับการปกป้องข้อมูลโดยอัตโนมัติใน Data Vault Data Vault ช่วยป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต แม้กระทั่งการเข้าถึงข้อมูลจากกระบวนการที่ไม่ได้อยู่ใน Sandbox คลาสเพิ่มเติมใน iOS 15 ขึ้นไป ได้แก่ เครือข่ายในพื้นที่ การโต้ตอบในพื้นที่ใกล้เคียง เซ็นเซอร์การวิจัยและข้อมูลการใช้งาน รวมถึงโฟกัส

ถ้าผู้ใช้ลงชื่อเข้า iCloud อยู่ แอปใน iOS และ iPadOS จะได้รับสิทธิ์เข้าถึง iCloud Drive ตามค่าเริ่มต้น ผู้ใช้สามารถควบคุมการเข้าถึงของแต่ละแอปได้ใน iCloud ในการตั้งค่า นอกจากนี้ iOS และ iPadOS ยังมอบการจำกัดที่ได้รับการออกแบบมาเพื่อป้องกันไม่ให้มีการเคลื่อนย้ายข้อมูลระหว่างแอปและบัญชีที่ติดตั้งโดยโซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) กับแอปและบัญชีที่ผู้ใช้ติดตั้งเองอีกด้วย

การปกป้องการเข้าถึงข้อมูลสุขภาพของผู้ใช้

HealthKit มีคลังจัดเก็บส่วนกลางสำหรับข้อมูลสุขภาพและฟิตเนสบน iPhone และ Apple Watch HealthKit ยังทำงานกับอุปกรณ์สุขภาพและฟิตเนสโดยตรง เช่น ตัววัดอัตราการเต้นของหัวใจที่ใช้บลูทูธพลังงานต่ำ (BLE) ที่ใช้งานร่วมกันได้ และหน่วยประมวลผลร่วมของการเคลื่อนไหวมีอยู่ในตัวอุปกรณ์ iOS เครื่องต่างๆ การโต้ตอบทั้งหมดของ HealthKit กับแอปสุขภาพและฟิตเนส สถาบันการดูแลสุขภาพ และอุปกรณ์สุขภาพและฟิตเนสจะต้องได้รับสิทธิ์จากผู้ใช้ ข้อมูลเหล่านี้จะมีการจัดเก็บในคลาสการปกป้องข้อมูลแบบปกป้องหากไม่เปิดอยู่ การเข้าถึงข้อมูลจะสิ้นสุดลงภายใน 10 นาทีหลังจากที่อุปกรณ์ล็อค และสามารถเข้าถึงข้อมูลได้ในครั้งต่อไปที่ผู้ใช้ป้อนรหัสหรือใช้ Face ID หรือ Touch ID ในการปลดล็อคอุปกรณ์

กำเก็บรวบรวมและจัดเก็บข้อมูลสุขภาพและฟิตเนส

HealthKit ยังเก็บรวบรวมและจัดเก็บข้อมูลการจัดการ เช่น สิทธิ์การเข้าถึงสำหรับแอป ชื่อของอุปกรณ์ที่เชื่อมต่อกับ HealthKit และข้อมูลกำหนดการที่ใช้เพื่อเริ่มใช้งานแอปเมื่อมีข้อมูลใหม่เข้ามา ข้อมูลนี้จะจัดเก็บโดยใช้คลาสการปกป้องข้อมูลแบบปกป้องจนกว่าจะมีการตรวจสอบสิทธิ์ของผู้ใช้รายแรก ไฟล์บันทึกชั่วคราวจะจัดเก็บบันทึกสุขภาพที่มีการสร้างเมื่ออุปกรณ์ถูกล็อค เช่น เมื่อผู้ใช้ออกกำลังกาย ข้อมูลเหล่านี้จะมีการจัดเก็บในคลาสการปกป้องข้อมูลแบบปกป้องหากไม่ได้เปิดอยู่ เมื่ออุปกรณ์ถูกปลดล็อค ไฟล์บันทึกชั่วคราวจะถูกนำเข้าไปที่ฐานข้อมูลสุขภาพหลัก จากนั้นจะถูกลบเมื่อการผสานข้อมูลเสร็จสมบูรณ์

ข้อมูลสุขภาพสามารถจัดเก็บบน iCloud ได้ การเข้ารหัสแบบต้นทางถึงปลายทางสำหรับข้อมูลสุขภาพต้องใช้ iOS 12 ขึ้นไปและการตรวจสอบสิทธิ์สองปัจจัย ไม่เช่นนั้น ข้อมูลของผู้ใช้จะยังคงถูกเข้ารหัสในพื้นที่จัดเก็บข้อมูลและการส่งข้อมูล แต่จะไม่ถูกเข้ารหัสแบบต้นทางถึงปลายทาง หลังจากที่ผู้ใช้เปิดใช้การตรวจสอบสิทธิ์สองปัจจัยและอัปเดตเป็น iOS 12 ขึ้นไป ข้อมูลสุขภาพของผู้ใช้จะเปลี่ยนไปใช้การเข้ารหัสแบบต้นทางถึงปลายทาง

ถ้าผู้ใช้สำรองข้อมูลอุปกรณ์ของตัวเองโดยใช้ Finder (ใน macOS 10.15 ขึ้นไป) หรือ iTunes (macOS 10.14 หรือก่อนหน้า) ข้อมูลสุขภาพจะถูกจัดเก็บเมื่อข้อมูลสำรองถูกเข้ารหัสเท่านั้น

บันทึกสุขภาพทางคลินิก

ผู้ใช้สามารถลงชื่อเข้าระบบสุขภาพที่รองรับภายในแอปสุขภาพเพื่อรับสำเนาของบันทึกสุขภาพทางคลินิกของตัวเองได้ ในระหว่างที่เชื่อมต่อผู้ใช้ไปยังระบบสุขภาพ ผู้ใช้จะตรวจสอบสิทธิ์โดยใช้เอกสารสิทธิ์ไคลเอ็นต์ OAuth 2 หลังจากการเชื่อมต่อ ข้อมูลบันทึกสุขภาพทางคลินิกจะถูกดาวน์โหลดโดยตรงจากสถาบันทางการแพทย์โดยใช้การเชื่อมต่อ TLS 1.3 ที่มีรหัสปกป้อง เมื่อดาวน์โหลดแล้ว บันทึกสุขภาพทางคลินิกจะถูกจัดเก็บอย่างปลอดภัยพร้อมกับข้อมูลสุขภาพอื่นๆ

ความสมบูรณ์ของข้อมูลสุขภาพ

ข้อมูลที่จัดเก็บในฐานข้อมูลจะรวมถึงเมตาดาต้าเพื่อติดตามแหล่งที่มาของบันทึกข้อมูลแต่ละอัน เมตาดาต้านี้รวมถึงตัวข้อมูลจำเพาะของแอปที่ระบุชี้ว่าแอปใดที่จัดเก็บบันทึก นอกจากนี้ รายการเมตาดาต้าเพิ่มเติมอาจรวมถึงสำเนาที่ลงชื่อดิจิตอลของบันทึกด้วย ทั้งนี้เพื่อความสมบูรณ์ของข้อมูลสำหรับบันทึกที่สร้างโดยอุปกรณ์ที่ได้รับความเชื่อถือ รูปแบบที่ใช้สำหรับลายมือชื่อดิจิตอลคือ Cryptographic Message Syntax (CMS) ที่ระบุใน RFC 5652

การเข้าถึงข้อมูลสุขภาพโดยแอปของบุคคลหรือบริษัทอื่น

การเข้าถึงไปที่ HealthKit API ถูกควบคุมโดยสิทธิ์ และแอปต้องปฏิบัติตามข้อจำกัดเรื่องวิธีที่ข้อมูลจะถูกใช้ ตัวอย่างเช่น แอปไม่ได้รับอนุญาตให้ใช้งานข้อมูลสุขภาพเพื่อการโฆษณา แอปยังต้องแสดงนโยบายความเป็นส่วนตัวที่ระบุรายละเอียดการใช้งานข้อมูลสุขภาพแก่ผู้ใช้ด้วย

การเข้าใช้งานข้อมูลสุขภาพโดยแอปได้รับการควบคุมโดยการตั้งค่าความเป็นส่วนตัวของผู้ใช้ ผู้ใช้จะได้รับคำขอให้อนุญาตการเข้าถึงเมื่อแอปร้องขอข้อมูลสุขภาพ คล้ายกับการขอใช้แอปรายชื่อ แอปรูปภาพ และทรัพยากร iOS อื่นๆ อย่างไรก็ตามสำหรับข้อมูลสุขภาพ แอปจะได้รับสิทธิ์เข้าถึงแยกต่างหากสำหรับการอ่านและเขียนข้อมูล เช่นเดียวกับสิทธิ์แยกต่างหากสำหรับข้อมูลสุขภาพแต่ละประเภท ผู้ใช้สามารถดูและเพิกถอนสิทธิ์ที่อนุญาตให้เข้าถึงข้อมูลสุขภาพได้ใน การตั้งค่า > สุขภาพ > การเข้าถึงข้อมูลและอุปกรณ์

ถ้าอนุญาตให้เขียนข้อมูล แอปพลิเคชันจะสามารถอ่านข้อมูลที่เขียนโดยแอปได้ด้วย ถ้าอนุญาตให้อ่านข้อมูล แอปจะสามารถอ่านข้อมูลที่เขียนโดยแหล่งที่มาทั้งหมดได้ อย่างไรก็ตาม แอปไม่สามารถกำหนดสิทธิ์ที่อนุญาตให้กับแอปอื่นได้ นอกจากนี้ แอปไม่สามารถสรุปได้ว่าตัวแอปเองได้รับสิทธิ์การอ่านข้อมูลสุขภาพหรือไม่ เมื่อแอปไม่มีสิทธิ์อ่าน การสอบถามทั้งหมดจะไม่ได้รับข้อมูลกลับมา ซึ่งเหมือนกับการตอบสนองที่ฐานข้อมูลว่างเปล่าจะส่งกลับ สิ่งนี้ได้รับการออกแบบมาเพื่อป้องกันแอปจากการแทรกแซงสถานะสุขภาพของผู้ใช้โดยการเรียนรู้ว่าข้อมูลประเภทใดที่ผู้ใช้ติดตามอยู่

ID ทางแพทย์สำหรับผู้ใช้

แอปสุขภาพให้ตัวเลือกแก่ผู้ใช้ในการกรอกแบบฟอร์ม ID ทางแพทย์ด้วยข้อมูลที่อาจสำคัญหากเกิดเหตุฉุกเฉินทางการแพทย์ จะมีการป้อนข้อมูลหรืออัปเดตด้วยตัวเอง และไม่เชื่อมข้อมูลกับข้อมูลในฐานข้อมูลสุขภาพ

ดูข้อมูล ID ทางแพทย์ได้โดยแตะปุ่มฉุกเฉินบนหน้าจอล็อค ข้อมูลจัดเก็บในอุปกรณ์โดยใช้คลาสการปกป้องข้อมูลแบบไม่มีการปกป้อง ดังนั้นข้อมูลดังกล่าวจึงสามารถเข้าถึงได้โดยไม่ต้องป้อนรหัสของอุปกรณ์ ID ทางแพทย์เป็นคุณสมบัติเสริมที่ช่วยให้ผู้ใช้สามารถตัดสินใจได้ว่าจะสร้างสมดุลระหว่างความกังวลด้านความปลอดภัยและความเป็นส่วนตัวได้อย่างไร ข้อมูลนี้จะสำรองอยู่ในข้อมูลสำรอง iCloud ใน iOS 13 หรือก่อนหน้านี้ ใน iOS 14 นั้น ID ทางแพทย์จะถูกเชื่อมข้อมูลระหว่างอุปกรณ์โดยใช้ CloudKit และมีคุณลักษณะการเข้ารหัสเหมือนกับข้อมูลสุขภาพในส่วนที่เหลือ

การแชร์ข้อมูลสุขภาพ

สำหรับ iOS 15 แอปสุขภาพช่วยให้ผู้ใช้มีตัวเลือกในการแชร์ข้อมูลสุขภาพกับผู้ใช้รายอื่น ข้อมูลสุขภาพจะถูกแชร์ระหว่างผู้ใช้สองคนโดยใช้การเข้ารหัส iCloud แบบแบบต้นทางถึงปลายทาง และ Apple จะไม่สามารถเข้าถึงข้อมูลที่ส่งผ่านการแชร์สุขภาพได้ ในการใช้คุณสมบัตินี้ ทั้งผู้ใช้ที่ส่งและรับข้อมูลจะต้องใช้งาน iOS 15 ขึ้นไป และเปิดใช้งานการตรวจสอบสิทธิ์สองปัจจัย

ผู้ใช้ยังสามารถเลือกที่จะแชร์ข้อมูลสุขภาพกับผู้ให้บริการด้านการดูแลสุขภาพโดยใช้คุณสมบัติแชร์กับผู้ให้บริการในแอปสุขภาพ ข้อมูลที่แชร์โดยใช้คุณสมบัตินี้มีให้เฉพาะสถาบันสุขภาพที่ผู้ใช้เลือกโดยใช้การเข้ารหัสแบบต้นทางถึงปลายทาง และ Apple จะไม่ได้รักษาหรือเข้าถึงกุญแจการเข้ารหัสเพื่อถอดรหัส ดู หรือเข้าถึงข้อมูลสุขภาพที่แชร์ผ่านคุณสมบัติแชร์กับผู้ให้บริการ รายละเอียดเพิ่มเติมเกี่ยวกับวิธีที่การออกแบบบริการนี้ปกป้องข้อมูลสุขภาพของผู้ใช้สามารถพบได้ในส่วนความปลอดภัยและความเป็นส่วนตัวของคู่มือการลงทะเบียน Apple สำหรับองค์กรด้านการดูแลสุขภาพ

การลงชื่อและการเข้ารหัสแบบดิจิตอล

รายการควบคุมสิทธิ์

ข้อมูลพวงกุญแจถูกแบ่งพาร์ติชั่นและปกป้องด้วยรายการควบคุมสิทธิ์ (ACL) ดังนั้น เอกสารสิทธิ์ที่จัดเก็บโดยแอปของบริษัทอื่นจึงไม่สามารถเข้าถึงได้ด้วยแอปที่มีข้อมูลประจำตัวแตกต่างกัน ยกเว้นว่าผู้ใช้จะตั้งใจอนุญาตแอปเหล่านั้น การปกป้องนี้มีกลไกสำหรับรักษาความปลอดภัยให้กับเอกสารสิทธิ์ในการตรวจสอบสิทธิ์ในอุปกรณ์ Apple กับแอปและบริการมากมายภายในองค์กร

เมล

ในแอปเมล ผู้ใช้สามารถส่งข้อความที่ลงชื่อและเข้ารหัสแบบดิจิตอลได้ แอปเมลจะค้นหาที่อยู่อีเมล ชื่อเรื่อง หรือชื่อเรื่องอื่นๆ ที่ยึดตามตัวพิมพ์ใหญ่-เล็ก RFC 5322 ที่เหมาะสมโดยอัตโนมัติในใบรับรองที่มีการลงชื่อและการเข้ารหัสแบบดิจิตอลบนโทเค็น Personal Identification Verification (PIV) ที่แนบมาด้วยในสมาร์ทการ์ดที่ใช้งานร่วมกันได้ ถ้าบัญชีอีเมลที่กำหนดค่าตรงกับที่อยู่อีเมลบนใบรับรองที่มีการลงชื่อและเข้ารหัสแบบดิจิตอลบนโทเค็น PIV ที่แนบมาด้วย แอปเมลจะแสดงปุ่มลงชื่อในแถบเครื่องมือของหน้าต่างข้อความใหม่โดยอัตโนมัติ ถ้าแอปเมลมีใบรับรองการเข้ารหัสอีเมลของผู้รับหรือสามารถค้นหาใบรับรองนั้นได้ใน Global Address List (GAL) ของ Microsoft Exchange ไอคอนปลดล็อคแล้วจะแสดงขึ้นในแถบเครื่องมือข้อความใหม่ ไอคอนกุญแจล็อคอยู่ระบุว่าข้อความจะถูกส่งโดยเข้ารหัสด้วยกุญแจสาธารณะของผู้รับ

S/MIME รายข้อความ

iOS, iPadOS และ macOS รองรับ S/MIME รายข้อความ หมายความว่าผู้ใช้ S/MIME สามารถเลือกที่จะลงชื่อและเข้ารหัสข้อความเสมอตามค่าเริ่มต้น หรือเลือกที่จะลงชื่อและเข้ารหัสข้อความทีละข้อความได้

ข้อมูลประจำตัวที่ใช้กับ S/MIME สามารถส่งมอบไปยังอุปกรณ์ Apple ได้โดยใช้โปรไฟล์การกำหนดค่า, โซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM), โปรโตคอลการลงทะเบียนใบรับรองอย่างง่าย (SCEP) หรือ Microsoft Active Directory Certificate Authority

สมาร์ทการ์ด

macOS 10.12 ขึ้นไปมีการรองรับดั้งเดิมสำหรับบัตร PIV บัตรเหล่านี้ถูกใช้อย่างกว้างขวางในเชิงพาณิชย์และในองค์กรรัฐบาลสำหรับการตรวจสอบสิทธิ์สองปัจจัย การลงชื่อแบบดิจิตอล และการเข้ารหัส

สมาร์ทการ์ดจะมีข้อมูลประจำตัวดิจิตอลมากกว่าหนึ่งรายการที่มีกุญแจสาธารณะและกุญแจส่วนตัวหนึ่งคู่และใบรับรองที่เกี่ยวข้อง การปลดล็อคสมาร์ทการ์ดด้วย Personal Identification Number (PIN) มอบการเข้าถึงกุญแจส่วนตัวที่ใช้สำหรับการตรวจสอบสิทธิ์ การเข้ารหัส และการสร้างกุญแจ ใบรับรองกำหนดว่ากุญแจสามารถใช้สำหรับอะไรได้ คุณลักษณะอะไรที่เกี่ยวข้อง และได้รับการยืนยัน (ลงชื่อ) โดยใบรับรองของผู้ให้บริการออกใบรับรอง (CA) แล้วหรือไม่

สมาร์ทการ์ดสามารถใช้สำหรับการตรวจสอบสิทธิ์สองปัจจัย สองปัจจัยที่จำเป็นในการปลดล็อคบัตรคือ “สิ่งที่ผู้ใช้มี” (บัตร) และ “สิ่งที่ผู้ใช้ทราบ” (รหัส PIN) macOS 10.12 ขึ้นไปยังมีการรองรับดั้งเดิมสำหรับการตรวจสอบสิทธิ์หน้าต่างเข้าสู่ระบบสมาร์ทการ์ดและการตรวจสอบสิทธิ์ใบรับรองสำหรับลูกข่ายบน Safari นอกจากนี้ยังรองรับการตรวจสอบสิทธิ์ Kerberos โดยใช้คู่กุญแจ (PKINIT) สำหรับการลงชื่อเข้าครั้งเดียวไปยังบริการที่รองรับ Kerberos ในการเรียนรู้เพิ่มเติมเกี่ยวกับสมาร์ทการ์ดและ macOS ให้ดูที่ข้อมูลเบื้องต้นเกี่ยวกับการรวมสมาร์ทการ์ดใน **Apple Platform Deployment**

ภาพดิสก์ที่เข้ารหัส

ใน macOS ภาพดิสก์ที่เข้ารหัสทำหน้าที่เป็นตัวบรรจุที่ปลอดภัยซึ่งผู้ใช้สามารถกู้คืนหรือถ่ายโอนเอกสารที่เป็นความลับและไฟล์อื่นๆ ได้ ภาพดิสก์ที่เข้ารหัสสร้างโดยการใช้ยูทิลิตี้ดิสก์ซึ่งอยู่ใน /Applications/Utilities/ ภาพดิสก์สามารถเข้ารหัสได้โดยใช้การเข้ารหัส AES 128 บิต หรือ 256 บิต เนื่องจากภาพดิสก์ที่ต่อเชื่อมเป็นดิสก์โวลุ่มภายในที่เชื่อมต่อกับ Mac ผู้ใช้จึงสามารถคัดลอก ย้าย และเปิดไฟล์และโฟลเดอร์ที่จัดเก็บอยู่ในนั้นได้ ด้วย FileVault เนื้อหาของภาพดิสก์ถูกเข้ารหัสและถอดรหัสในแบบเรียลไทม์ ด้วยภาพดิสก์ที่เข้ารหัส ผู้ใช้สามารถแลกเปลี่ยนเอกสาร ไฟล์ และโฟลเดอร์ได้อย่างปลอดภัยโดยการบันทึกภาพดิสก์ที่เข้ารหัสไปยังสื่อที่สามารถถอดออกได้ ส่งเป็นไฟล์แนบในข้อความอีเมล หรือจัดเก็บในเซิร์ฟเวอร์ระยะไกล โปรดดูที่คู่มือผู้ใช้ยูทิลิตี้ดิสก์สำหรับข้อมูลเพิ่มเติมเกี่ยวกับภาพดิสก์ที่เข้ารหัส

ความปลอดภัยของแอป

ภาพรวมความปลอดภัยของแอป

ทุกวันนี้ แอปเป็นหนึ่งในองค์ประกอบที่สำคัญที่สุดของสถาปัตยกรรมความปลอดภัยสมัยใหม่ ในขณะที่แอปให้ประโยชน์ด้านการทำงานที่น่ามหัศจรรย์สำหรับผู้ใช้ แต่ก็มีโอกาสที่จะส่งผลกระทบต่อความปลอดภัยระบบ ความเสถียร และข้อมูลผู้ใช้ในทางลบหากไม่ได้รับการดูแลอย่างเหมาะสม

เนื่องจากสาเหตุนี้ Apple จึงมอบการปกป้องหลายชั้นเพื่อช่วยให้มั่นใจว่าแอปปราศจากมัลแวร์ที่รู้จักและไม่ถูกรบกวน การป้องกันเพิ่มเติมจะบังคับให้การเข้าถึงจากแอปไปยังข้อมูลของผู้ใช้ต้องอาศัยสื่อกลางที่ได้รับการดูแล การควบคุมความปลอดภัยเหล่านี้มอบแพลตฟอร์มสำหรับแอปที่มีความเสถียรและปลอดภัย และช่วยให้นักพัฒนาแอปหลายพันคนสามารถส่งมอบแอปหลายพันรายการสำหรับ iOS, iPadOS และ macOS ได้โดยไม่ส่งผลกระทบต่อความสมบูรณ์ของระบบโดยรวม และผู้ใช้สามารถเข้าถึงแอปเหล่านี้บนอุปกรณ์ Apple ได้โดยไม่ต้องกลัวไวรัส มัลแวร์ หรือการโจมตีที่ไม่ได้รับอนุญาต

บน iPhone, iPad และ iPod touch แอปทั้งหมดจะได้รับจาก App Store และแอปทั้งหมดจะอยู่ใน Sandbox เพื่อมอบการควบคุมที่รัดกุมที่สุด

บน Mac แอปหลายแอปจะได้รับจาก App Store แต่ผู้ใช้ Mac ยังสามารถดาวน์โหลดและใช้แอปจากอินเทอร์เน็ตได้อีกด้วย ในการรองรับการดาวน์โหลดผ่านทางอินเทอร์เน็ตอย่างปลอดภัย macOS จะเพิ่มการควบคุมหลายชั้นอันดับแรก ตามค่าเริ่มต้นแล้ว ใน macOS 10.15 ขึ้นไป แอปทั้งหมดของ Mac จะต้องได้รับการรับรองโดย Apple ก่อนเพื่อให้เริ่มใช้งานได้ ข้อกำหนดนี้ช่วยให้มั่นใจได้ว่าแอปเหล่านี้จะไม่มีมัลแวร์ที่รู้จัก โดยไม่จำเป็นว่าต้องเป็นแอปที่ดาวน์โหลดจากใน App Store นอกจากนี้แล้ว macOS ยังมีการป้องกันไวรัสที่ล้ำสมัยเพื่อปิดกั้นมัลแวร์ และเอาออกหากจำเป็นอีกด้วย

เพื่อเป็นการควบคุมเพิ่มเติมทั่วทั้งแพลตฟอร์ม การทำให้แอปอยู่ใน Sandbox จะช่วยปกป้องข้อมูลผู้ใช้ไม่ให้แอปต่างๆ เข้าถึงโดยไม่ได้รับอนุญาต และใน macOS ข้อมูลที่อยู่ในพื้นที่ที่สำคัญจะได้รับการปกป้อง ซึ่งช่วยให้การรับรองว่าผู้ใช้ยังคงเป็นผู้ควบคุมการเข้าถึงไฟล์จากแอปทั้งหมดในเดสก์ท็อป เอกสาร รายการดาวน์โหลด และพื้นที่อื่นๆ ไม่ว่าแอปที่พยายามจะเข้าถึงจะทำให้ตัวเองอยู่ใน Sandbox หรือไม่ก็ตาม

ความสามารถดั้งเดิม	เทียบเท่าบริษัทอื่น
รายการปลั๊กอินที่ไม่ได้รับอนุญาตและส่วนขยาย Safari ที่ไม่ได้รับอนุญาต	คำนิยามไวรัส/มัลแวร์
การกักกันไฟล์	คำนิยามไวรัส/มัลแวร์
ลายเซ็น XProtect/YARA	คำนิยามไวรัส/มัลแวร์ การป้องกันปลายทาง
Gatekeeper	การป้องกันปลายทาง บังคับการลงชื่อโค้ดบนแอปต่างๆ เพื่อช่วยให้การรับรองว่าจะมีซอฟต์แวร์ที่เชื่อถือแล้วเท่านั้นที่สามารถใช้งานได้
eficheck (จำเป็นสำหรับ Mac ที่ไม่มีชิป Apple T2 Security)	การป้องกันปลายทาง การตรวจจับ Rootkit

ความสามารถดั้งเดิม	เทียบเท่าบริษัทอื่น
ไฟร์วอลล์แอปพลิเคชัน	การป้องกันปลายทาง ไฟร์วอลล์
ฟิลเตอร์แพ็คเกต (pf)	โซลูชั่นไฟร์วอลล์
การปกป้องความสมบูรณ์ของระบบ	สร้างไว้ใน macOS
การควบคุมการเข้าถึงแบบบังคับ	สร้างไว้ใน macOS
รายการที่ไม่รวม kext	สร้างไว้ใน macOS
การลงชื่อโค้ดแอปที่บังคับ	สร้างไว้ใน macOS
การรับรองแอป	สร้างไว้ใน macOS

ความปลอดภัยของแอปใน iOS และ iPadOS

ข้อมูลเบื้องต้นเกี่ยวกับความปลอดภัยของแอปสำหรับ iOS และ iPadOS

iOS และ iPadOS ไม่อนุญาตให้ผู้ใช้ติดตั้งแอปที่ไม่ได้ลงชื่อซึ่งอาจเป็นอันตรายจากเว็บไซต์อื่น หรือใช้งานแอปที่ไม่ได้รับความเชื่อถือ ซึ่งแตกต่างจากแพลตฟอร์มอุปกรณ์เคลื่อนที่อื่นๆ ในระหว่างรันไทม์ ลายเซ็นรหัสจะตรวจสอบว่าหน้าหน่วยความจำโปรแกรมปฏิบัติงานทั้งหมดว่าเป็นแบบเดียวกับที่โหลดหรือไม่ เพื่อช่วยให้มั่นใจว่าแอปไม่ได้ถูกแก้ไขหลังจากที่ติดตั้งหรืออัปเดตล่าสุด

หลังจากที่แอปได้รับการตรวจสอบยืนยันว่ามาจากแหล่งที่ได้รับอนุญาต iOS และ iPadOS จะบังคับใช้มาตรการความปลอดภัยที่ออกแบบมาเพื่อป้องกันการทำให้ความปลอดภัยของแอปอื่นหรือระบบที่เหลือบกพร่อง

กระบวนการลงชื่อโค้ดของแอปใน iOS และ iPadOS

Apple มอบความปลอดภัยของแอปสำหรับ iOS และ iPadOS ผ่านสิ่งต่างๆ เช่น ระบบการลงชื่อโค้ดแบบบังคับ การลงชื่อเข้าสำหรับนักพัฒนาแอปที่เข้มงวด และอื่นๆ

การลงชื่อโค้ดที่บังคับ

หลังจากที่เคอร์เนลของ iOS และ iPadOS เริ่มทำงาน เคอร์เนลนั้นจะควบคุมกระบวนการทำงานของผู้ใช้และแอปที่สามารถทำงานได้ ในการช่วยทำให้มั่นใจว่าแอปทั้งหมดมาจากแหล่งที่รู้จักและได้รับการอนุญาตและไม่ได้ถูกรบกวน iOS และ iPadOS จะกำหนดให้โปรแกรมปฏิบัติการทั้งหมดต้องได้รับการลงชื่อโดยใช้ใบรับรองที่ออกโดย Apple แอปที่มาพร้อมอุปกรณ์ เช่น แอปเมลและ Safari จะได้รับการลงชื่อโดย Apple แอปของบริษัทอื่นจะต้องได้รับการตรวจสอบความถูกต้องและลงชื่อโดยใช้ใบรับรองที่ออกโดย Apple การลงชื่อโค้ดที่บังคับเป็นการต่อยอดแนวคิดลำดับการตรวจสอบความน่าเชื่อถือจากระบบปฏิบัติการไปที่แอป และช่วยป้องกันแอปของบริษัทอื่นไม่ให้โหลดโค้ดที่ไม่ได้ลงชื่อหรือไม่ให้ใช้โค้ดที่แก้ไขตัวเอง

นักพัฒนาลงชื่อแอปของตัวเองอย่างไร

นักพัฒนาของ Apple สามารถลงชื่อแอปผ่านการตรวจสอบความถูกต้องของใบรับรอง (ผ่าน Apple Developer Program) ได้ นักพัฒนายังสามารถฝังเฟรมเวิร์คลงในแอปของตนและตรวจสอบความถูกต้องโค้ดนั้นด้วยใบรับรองที่ออกโดย Apple (ผ่านสตริงตัวระบุทีม) ได้อีกด้วย

- **การตรวจสอบความถูกต้องของใบรับรอง:** ในการพัฒนาและติดตั้งแอปในอุปกรณ์ iOS หรือ iPadOS นักพัฒนาต้องลงทะเบียนกับ Apple และเข้าร่วม Apple Developer Program ตัวตนจริงของนักพัฒนาแต่ละราย ไม่ว่าจะเป็นบุคคลหรือธุรกิจจะได้รับการตรวจสอบยืนยันโดย Apple ก่อนที่ใบรับรองของนักพัฒนาจะออก ใบรับรองนี้ทำให้นักพัฒนาแอปสามารถลงชื่อแอปและส่งแอปไปยัง App Store เพื่อการแจกจ่ายได้ ผลลัพธ์ก็คือแอปทั้งหมดใน App Store ถูกส่งโดยบุคคลหรือองค์กรที่ระบุตัวตนได้ จึงเป็นการช่วยขัดขวางการสร้างแอปที่เป็นอันตราย แอปยังได้รับการตรวจสอบโดย Apple เพื่อช่วยให้แน่ใจว่าทำงานตามที่อธิบายโดยทั่วไปและไม่มีข้อผิดพลาดหรือปัญหาอื่นๆ ที่เห็นได้อย่างชัดเจน นอกเหนือจากเทคโนโลยีตามที่กล่าวถึงแล้ว กระบวนการคัดสรรนี้ยังให้ความมั่นใจแก่ผู้ใช้ถึงคุณภาพของแอปที่พวกเขาซื้อ
- **การตรวจสอบความถูกต้องลายเซ็นโค้ด:** iOS และ iPadOS อนุญาตให้นักพัฒนาฝังเฟรมเวิร์คลงในแอปของตน ซึ่งสามารถใช้งานได้โดยตัวแอปเองหรือโดยส่วนขยายที่ฝังอยู่ภายในแอป ในการปกป้องระบบและแอปอื่นไม่ให้โหลดโค้ดของบริษัทอื่นภายในพื้นที่ที่อยู่ของตน ระบบจะตรวจสอบความถูกต้องลายเซ็นโค้ดของคลังไดนามิกทั้งหมดที่ประมวลผลลิงก์เมื่อเวลาเริ่มทำงาน การตรวจสอบยืนยันนี้ทำได้ผ่านตัวระบุทีม (ID ทีม) ซึ่งได้มาจากใบรับรองที่ออกโดย Apple ตัวระบุชี้ทีมคือสตริงตัวอักษรและตัวเลข 10 อักขระ ตัวอย่างเช่น 1A2B3C4D5F โปรแกรมอาจเชื่อมกับคลังแพลตฟอร์มใดๆ ที่มาพร้อมระบบหรือคลังใดๆ ที่มีข้อมูลจำเพาะของทีมเดียวกันในลายเซ็นโค้ดเป็นโปรแกรมปฏิบัติงานหลัก เนื่องจากการจัดส่งโปรแกรมปฏิบัติงานเป็นส่วนหนึ่งของระบบไม่มีข้อมูลจำเพาะของทีม โปรแกรมจะสามารถเชื่อมกับคลังที่จัดส่งมากับตัวระบบเองเท่านั้นได้

การตรวจสอบยืนยันแอปภายในที่เป็นกรรมสิทธิ์

ธุรกิจที่ได้รับเลือกยังสามารถเขียนแอปภายในที่เป็นกรรมสิทธิ์เพื่อใช้ภายในองค์กรและแจกจ่ายให้กับพนักงานของตนได้ ธุรกิจและองค์กรสามารถสมัครเข้าร่วม Apple Developer Enterprise Program (ADEP) ได้ โปรดดูที่ เว็บไซต์ Apple Developer Enterprise Program สำหรับข้อมูลเพิ่มเติมและเพื่อตรวจสอบข้อกำหนดคุณสมบัติ หลังจากที่องค์กรเข้าเป็นสมาชิกของ ADEP แล้ว องค์กรจะสามารถลงทะเบียนเพื่อรับโปรไฟล์กำหนดสิทธิ์ที่อนุญาตให้แอปภายในที่เป็นกรรมสิทธิ์ขององค์กรสามารถทำงานบนอุปกรณ์ที่ได้รับอนุญาตได้

ผู้ใช้จะต้องติดตั้งโปรไฟล์กำหนดสิทธิ์เพื่อเรียกใช้แอปเหล่านี้ ทั้งนี้เพื่อช่วยให้การรับรองว่าจะมีเฉพาะผู้ใช้ที่ควรได้สิทธิ์ขององค์กรเท่านั้นที่จะสามารถโหลดแอปลงในอุปกรณ์ iOS และ iPadOS ของตนเองได้ แอปที่ติดตั้งผ่านการจัดการอุปกรณ์เคลื่อนที่ (MDM) จะได้รับความเชื่อถือแบบโดยนัย เนื่องจากความสัมพันธ์ระหว่างองค์กรและอุปกรณ์ได้ถูกสร้างขึ้นเรียบร้อยแล้ว ไม่เช่นนั้น ผู้ใช้จะต้องอนุญาตโปรไฟล์การกำหนดสิทธิ์ของแอปในการตั้งค่า องค์กรยังสามารถจำกัดไม่ให้ผู้ใช้อนุมัติแอปจากนักพัฒนาที่ไม่รู้จักได้ ในการเปิดใช้แอปภายในที่เป็นกรรมสิทธิ์ครั้งแรก อุปกรณ์จะต้องได้รับการยืนยันเชิงบวกจาก Apple ว่าแอปนั้นได้รับอนุญาตให้ทำงาน

ความปลอดภัยของกระบวนการรันไทม์ใน iOS และ iPadOS

iOS และ iPadOS ช่วยรับรองความปลอดภัยของรันไทม์โดยการใช้ “Sandbox”, สิทธิ์ที่ประกาศ และการสุ่มเค้าโครงพื้นที่ที่อยู่ (ASLR)

การทำ Sandbox

แอปบุคคลหรือบริษัทอื่นทั้งหมดจะอยู่ใน “Sandbox” จึงถูกจำกัดจากการเข้าถึงไฟล์ที่จัดเก็บโดยแอปอื่นหรือจากการเปลี่ยนแปลงกับอุปกรณ์ การทำ Sandbox ได้รับการออกแอบบมาเพื่อป้องกันไม่ให้แอปเก็บข้อมูลหรือแก้ไขข้อมูลที่จัดเก็บโดยแอปอื่น แอปแต่ละตัวมีสารบบเริ่มต้นเฉพาะสำหรับไฟล์ของแอป ซึ่งจะมีการกำหนดแบบสุ่มเมื่อติดตั้งแอป ถ้าแอปของบริษัทอื่นต้องการเข้าถึงข้อมูลนอกเหนือจากข้อมูลของตนเอง แอปจะต้องใช้บริการที่ iOS และ iPadOS มีบริการให้อย่างชัดแจ้งเท่านั้น

ไฟล์ระบบและทรัพยากรยังถูกป้องกันจากแอปของผู้ใช้อีกด้วย โดยคุณสมบัติส่วนมากของไฟล์ระบบและทรัพยากร iOS และ iPadOS จะทำงานในฐานะ “mobile” ของผู้ใช้ที่ไม่ได้รับสิทธิพิเศษ และแอปของบุคคลหรือบริษัทอื่นทั้งหมดก็จะทำงานในฐานะนี้เช่นกัน ขณะที่พาร์ติชั่นระบบปฏิบัติการทั้งพาร์ติชั่นจะต่อเชื่อมเป็นแบบอ่านอย่างเดียว เครื่องมือที่ไม่จำเป็น เช่น บริการการเข้าสู่ระบบระยะไกลจะไม่รวมอยู่ในซอฟต์แวร์ระบบ และ API ไม่อนุญาตให้แอปยกระดับสิทธิ์ของตนเพื่อแก้ไขแอปอื่นหรือตัว iOS และ iPadOS เองได้

การใช้การให้สิทธิ์

การเข้าถึงข้อมูลผู้ใช้และคุณสมบัติ เช่น iCloud และความสามารถในการเพิ่มฟังก์ชั่นของแอปของบริษัทอื่นจะถูกควบคุมโดยใช้สิทธิ์ที่ประกาศ โดยสิทธิ์คือคู่ค่ากุญแจที่มีการลงชื่อเข้าแอปและอนุญาตการตรวจสอบสิทธิ์นอกเหนือไปจากปัจจัยรันไทม์ เช่น ID ผู้ใช้ของ UNIX เนื่องจากสิทธิ์มีการลงชื่อแบบดิจิตอล จึงไม่สามารถเปลี่ยนแปลงได้ สิทธิ์มีการใช้เป็นอย่างมากโดยแอประบบและดีมอนเพื่อทำงานที่ต้องได้รับสิทธิ์เฉพาะที่กระบวนการทำงานต้องทำงานในระดับราก สิ่งนี้ช่วยลดโอกาสของการยกระดับสิทธิ์โดยแอประบบหรือดีมอนที่มีพฤติกรรมที่กระทบต่อความมั่นคงปลอดภัยของข้อมูลได้เป็นอย่างมาก

นอกจากนี้ แอปจะสามารถทำการประมวลผลพื้นหลังผ่าน API ที่ระบบมีให้ได้เท่านั้น ซึ่งช่วยให้แอปทำงานต่อไปได้โดยไม่ลดทอนประสิทธิภาพการทำงาน หรือส่งผลกระทบอย่างมากต่ออายุการใช้งานแบตเตอรี่

การสุ่มเค้าโครงพื้นที่ที่อยู่

การสุ่มเค้าโครงพื้นที่ที่อยู่ (ASLR) จะช่วยปกป้องการแอบแฝงใช้ประโยชน์ของข้อผิดพลาดที่ทำให้หน่วยความจำเสียหาย แอปในตัวใช้ ASLR ซึ่งช่วยสุ่มพื้นที่หน่วยความจำทั้งหมดเมื่อเริ่มเปิดทำงาน นอกเหนือจากการทำงานเมื่อเปิดใช้งาน ASLR จะสุ่มจัดเรียงที่อยู่หน่วยความจำของรหัสประมวลผล คลังระบบ และโครงสร้างโปรแกรมที่เกี่ยวข้อง ซึ่งช่วยลดโอกาสของการแอบแฝงใช้ประโยชน์ต่างๆ ได้มากขึ้น ตัวอย่างเช่น ความพยายามโจมตี return-to-libc เพื่อหลอกอุปกรณ์ให้ใช้งานโค้ดที่เป็นอันตรายโดยการควบคุมที่อยู่หน่วยความจำของสแต็คและคลังระบบ การสุ่มตำแหน่งของสิ่งเหล่านี้ทำให้การโจมตียากขึ้นในการปฏิบัติการ โดยเฉพาะอย่างยิ่งบนอุปกรณ์หลายเครื่อง Xcode และสภาพแวดล้อมการพัฒนา iOS หรือ iPadOS จะผสานโปรแกรมของบริษัทอื่นเข้ากับการเปิดใช้การรองรับ ASLR โดยอัตโนมัติ

คุณสมบัติ Execute Never

iOS และ iPadOS มอบการปกป้องเพิ่มเติมโดยใช้คุณสมบัติ Execute Never (XN) ของ ARM ซึ่งจะทำเครื่องหมายหน้าหน่วยความจำเป็นไม่สามารถปฏิบัติงานได้ หน้าหน่วยความจำที่มีเครื่องหมายเป็นทั้งเขียนได้และปฏิบัติงานได้จะสามารถใช้ได้เฉพาะแอปที่อยู่ในเงื่อนไขที่ควบคุมเหล่านี้อย่างไม่ผิดเพี้ยนเท่านั้น: เคอร์เนลจะตรวจสอบตัวตนของสิทธิ์การเซ็นชื่อโค้ดไดนามิกของ Apple เท่านั้น แม้ในกรณีนั้น เฉพาะการเรียกใช้ `mmap` แบบเดี่ยวเท่านั้นที่จะสามารถทำเพื่อร้องขอหน้าปฏิบัติงานได้และเขียนได้ซึ่งจะได้รับที่อยู่แบบสุ่ม Safari ใช้งานฟังก์ชั่นการทำงานนี้สำหรับคอมไพเลอร์ JavaScript Just-in-Time (JIT) ของ Safari

การรองรับส่วนขยายใน iOS, iPadOS และ macOS

iOS, iPadOS และ macOS อนุญาตให้แอปมอบฟังก์ชั่นการทำงานให้แอปอื่นได้โดยการให้ส่วนขยาย ส่วนขยายคือไบนารีโปรแกรมปฏิบัติงานที่ลงชื่อด้วยวัตถุประสงค์พิเศษซึ่งรวมเป็นแพ็คเกจอยู่ภายในแอป ในระหว่างการติดตั้งระบบจะตรวจหาส่วนขยายโดยอัตโนมัติและทำให้สามารถใช้งานกับแอปอื่นได้โดยใช้ระบบการจับคู่

จุดขยาย

พื้นที่ระบบที่รองรับส่วนขยายเรียกว่า**จุดขยาย** จุดขยายแต่ละจุดให้ API และบังคับใช้นโยบายสำหรับพื้นที่นั้น ระบบจะกำหนดว่าส่วนขยายใดที่ใช้งานได้โดยอิงตามจุดขยายกับกฎเกณฑ์การจับคู่เฉพาะ ระบบจะเริ่มต้นกระบวนการทำงานส่วนขยายตามที่จำเป็นและจัดการระยะเวลาใช้งานโดยอัตโนมัติ สามารถใช้สิทธิ์เพื่อจำกัดความพร้อมใช้งานของส่วนขยายกับแอประบบบางแอปได้ ตัวอย่างเช่น วิดเจ็ตมุมมองวันนี้ จะแสดงเฉพาะในศูนย์การแจ้งเตือน และการแชร์ส่วนขยายสามารถใช้งานได้เฉพาะจากบานหน้าต่างการแชร์เท่านั้น ตัวอย่างของจุดขยายคือวิดเจ็ตวันนี้ การแชร์ การทำงาน การแก้ไขรูปภาพ ตัวจัดหาไฟล์ และแป้นพิมพ์แบบกำหนดเอง

ส่วนขยายสื่อสารได้อย่างไร

ส่วนขยายจะทำงานในพื้นที่ที่อยู่ของตนเอง การสื่อสารระหว่างส่วนขยายและแอปตั้งแต่ที่มีการเปิดใช้งานใช้การสื่อสารระหว่างกระบวนการทำงานซึ่งอาศัยสื่อกลางโดยเฟรมเวิร์กระบบ ส่วนขยายและแอปจะไม่มีสิทธิ์เข้าถึงไฟล์หรือหน่วยความจำของอีกฝ่าย ส่วนขยายได้รับการออกแบบมาให้แยกจากส่วนอื่นๆ ทั้งจากแอปที่มีส่วนขยายดังกล่าวและจากแอปที่ใช้งานส่วนขยาย โดยจะอยู่ใน Sandbox เหมือนกับแอปของบริษัทอื่นทั้งหมด และมีตัวบรรจุแยกจากตัวบรรจุของแอปที่มีส่วนขยายนั้นๆ อย่างไรก็ตาม ส่วนขยายเหล่านี้จะสามารถเข้าถึงการควบคุมความเป็นส่วนตัวได้ในระดับเดียวกับแอปคอนเทนเนอร์ ดังนั้นถ้าผู้ใช้อนุญาตให้แอปเข้าถึงแอปรายชื่อ ส่วนขยายที่ฝังอยู่ในแอปนี้จะได้รับอนุญาตด้วย แต่ส่วนขยายที่แอปนี้เปิดใช้งานจะไม่ได้รับอนุญาต

วิธีใช้แป้นพิมพ์แบบกำหนดเอง

แป้นพิมพ์แบบกำหนดเองเป็นส่วนขยายประเภทพิเศษ เนื่องจากเปิดใช้งานโดยผู้ใช้ให้กับทั้งระบบ หลังจากเปิดใช้งานแล้ว ส่วนขยายแป้นพิมพ์จะถูกใช้กับช่องข้อความทั้งหมด ยกเว้นช่องรหัสและมุมมองข้อความแบบปลอดภัย ในการจำกัดการถ่ายโอนข้อมูลผู้ใช้ แป้นพิมพ์แบบกำหนดเองจะทำงานตามค่าเริ่มต้นใน Sandbox ที่มีข้อจำกัดอย่างมาก ซึ่งปิดกั้นการเข้าถึงเครือข่าย รวมไปถึงบริการที่ทำงานเครือข่ายแทนกระบวนการทำงาน และ API ที่จะอนุญาตส่วนขยายให้แทรกแซงการพิมพ์ข้อมูล นักพัฒนาแป้นพิมพ์แบบกำหนดเองสามารถร้องขอให้ส่วนขยายของตนมี Open Access ซึ่งจะช่วยให้ระบบเรียกใช้ส่วนขยายใน Sandbox เริ่มต้นหลังจากได้รับความยินยอมจากผู้ใช้

MDM และส่วนขยาย

สำหรับอุปกรณ์ที่ลงทะเบียนในโซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) ส่วนขยายของเอกสารและแป้นพิมพ์จะทำตามกฎเกณฑ์ของ Managed Open In ตัวอย่างเช่น โซลูชั่น MDM สามารถช่วยป้องกันผู้ใช้ไม่ให้ส่งออกเอกสารจากแอปที่ได้รับการจัดการไปยังผู้ให้บริการเอกสารที่ไม่ได้รับการจัดการ หรือช่วยป้องกันผู้ใช้จากการใช้แป้นพิมพ์ที่ไม่ได้รับการจัดการด้วยแอปที่ได้รับการจัดการได้ นอกจากนี้ นักพัฒนาแอปสามารถป้องกันการใช้งานส่วนขยายแป้นพิมพ์ของบริษัทอื่นภายในแอปของตนได้

การปกป้องแอปและกลุ่มของแอปใน iOS และ iPadOS

ใน iOS และ iPadOS องค์กรสามารถปกป้องแอปให้ปลอดภัยได้โดยใช้ IOS SDK และโดยเข้าร่วมกลุ่มของแอปที่พอร์ทัลนักพัฒนาของ Apple

การใช้งานการปกป้องข้อมูลในแอป

ชุดการพัฒนาซอฟต์แวร์ iOS (SDK) สำหรับ iOS และ iPadOS มี API แบบครบชุดที่ทำให้นักพัฒนาของบริษัทอื่นและของ Apple สามารถใช้งานการปกป้องข้อมูลได้อย่างง่ายดาย และช่วยรับรองระดับการปกป้องแอปที่สูงที่สุด การปกป้องข้อมูลสามารถใช้งานได้สำหรับ API ของไฟล์และฐานข้อมูล ซึ่งรวมถึง NSFileManager, CoreData, NSData และ SQLite

ฐานข้อมูลแอปเมล (รวมถึงไฟล์แนบ), หนังสือที่ได้รับการจัดการ, ที่คั่นหน้า Safari, ภาพเริ่มต้นแอป และข้อมูลตำแหน่งที่ตั้งจะถูกจัดเก็บผ่านการเข้ารหัสด้วยคุณแจที่ถูกปกป้องด้วยรหัสของผู้ใช้บนอุปกรณ์ด้วยเช่นกัน ปฏิทิน (ไม่รวมไฟล์แนบ), รายชื่อ, เตือนความจำ, โน้ต, ข้อความ และรูปภาพ จะใช้สิทธิ์การปกป้อง การปกป้องข้อมูลจนกว่าจะมีการตรวจสอบสิทธิ์ของผู้ใช้รายแรก

แอปที่ผู้ใช้ติดตั้งที่ไม่ได้เลือกคลาสการปกป้องข้อมูลเฉพาะจะได้รับการปกป้องจนกว่าจะมีการตรวจสอบสิทธิ์ของผู้ใช้รายแรกเป็นค่าเริ่มต้น

การเข้าร่วมกลุ่มของแอป

แอปและส่วนขยายของบัญชีนักพัฒนาสามารถแชร์เนื้อหาได้เมื่อกำหนดค่าให้เป็นส่วนหนึ่งของกลุ่มของแอป นักพัฒนาสามารถเลือกสร้างกลุ่มที่เหมาะสมบนพอร์ทัลนักพัฒนาของ Apple และใส่ชุดของแอปและส่วนขยายที่ต้องการได้ เมื่อกำหนดค่าให้เป็นส่วนหนึ่งของกลุ่มของแอป แอปจะมีสิทธิ์เข้าถึงดังต่อไปนี้:

- ตัวบรรจุบนดิสก์โวลุ่มที่แชร์สำหรับจัดเก็บข้อมูล ซึ่งจะอยู่บนอุปกรณ์ตราบเท่าที่ยังติดตั้งแอปจากกลุ่มนี้อย่างน้อยหนึ่งแอป
- การตั้งค่าที่แชร์
- รายการพวงกุญแจที่แชร์

พอร์ทัลนักพัฒนาของ Apple จะช่วยให้การรับรองว่า ID กลุ่ม (GID) ของแอปจะไม่ซ้ำกันตลอดทั้งระบบของแอป

การตรวจสอบยืนยันอุปกรณ์เสริมใน iOS และ iPadOS

โปรแกรมสิทธิ์การใช้งาน Made for iPhone, iPad และ iPod touch (MFi) ให้สิทธิ์ผู้ผลิตอุปกรณ์เสริมใช้งานโปรโตคอลอุปกรณ์เสริม iPod (iAP) และคอมโพเนนต์ฮาร์ดแวร์สนับสนุนที่จำเป็น

เมื่ออุปกรณ์เสริม MFi สื่อสารกับอุปกรณ์ iOS หรือ iPadOS โดยใช้หัวต่อ Lightning หรือ USB-C ผ่านบลูทูธ อุปกรณ์จะขอให้อุปกรณ์เสริมยืนยันว่าได้รับการอนุญาตจาก Apple โดยการตอบสนองกับใบรับรองที่ Apple ออกให้ ซึ่งจะได้รับการตรวจสอบยืนยันโดยอุปกรณ์ จากนั้นอุปกรณ์จะส่งคำถาม ซึ่งอุปกรณ์เสริมจะต้องตอบด้วยข้อความตอบที่ลงชื่อไว้ กระบวนการทำงานนี้ทั้งหมดจะได้รับการจัดการโดยวงจรแบบผสาน (IC) ที่ผลิตมาเป็นการเฉพาะซึ่ง Apple จัดหาให้กับผู้ผลิตอุปกรณ์เสริมที่ได้รับอนุญาตและโปร่งใสกับตัวอุปกรณ์เสริมเอง

อุปกรณ์เสริมสามารถร้องขอการเข้าถึงวิธีการส่งข้อมูลและคุณสมบัติการทำงานต่างๆ ได้ ตัวอย่างเช่น การเข้าถึงสตรีมเสียงดิจิตอลผ่านสาย Lightning หรือ USB-C รับข้อมูลตำแหน่งที่ตั้งผ่านบลูทูธ การตรวจสอบสิทธิ์ IC ได้รับการออกแบบมาเพื่อรับรองว่าเฉพาะอุปกรณ์เสริมที่ได้รับอนุญาตเท่านั้นที่ได้รับสิทธิ์เข้าถึงอุปกรณ์แบบเต็ม ถ้าอุปกรณ์เสริมไม่รองรับการตรวจสอบสิทธิ์ สิทธิ์การเข้าถึงจะถูกจำกัดเพียงเสียงอนาล็อคและการควบคุมการเล่นเสียงแบบอนุกรม (UART) บางส่วนจำนวนน้อยเท่านั้น

AirPlay ยังใช้การตรวจสอบสิทธิ์ IC เพื่อตรวจสอบยืนยันว่าตัวรับได้รับการอนุญาตโดย Apple การสตรีมเสียง AirPlay และวิดีโอ CarPlay จะใช้ MFi-SAP (โปรโตคอลการเชื่อมโยงที่ปลอดภัย) ซึ่งเข้ารหัสการสื่อสารระหว่างอุปกรณ์เสริมและอุปกรณ์โดยใช้ AES128 ในโหมด Counter (CTR) กุญแจชั่วคราวจะมีการแลกเปลี่ยนโดยใช้การแลกเปลี่ยนกุญแจ ECDH (Curve25519) และลงชื่อโดยใช้กุญแจ RSA แบบ 1024 บิตของการตรวจสอบสิทธิ์ IC ซึ่งเป็นส่วนหนึ่งของโปรโตคอล Station-to-Station (STS)

ความปลอดภัยของแอปใน macOS

ข้อมูลเบื้องต้นเกี่ยวกับความปลอดภัยของแอปสำหรับ macOS

ความปลอดภัยของแอปใน macOS ประกอบด้วยชั้นที่ซ้อนกันจำนวนหนึ่ง โดยมีชั้นแรกเป็นตัวเลือกสำหรับการใช้งานเฉพาะแอปที่ได้รับการลงชื่อและเชื่อถือแล้วจาก App Store เท่านั้น นอกจากนี้ macOS ยังสร้างการปกป้องหลายชั้นเพื่อช่วยให้มั่นใจว่าแอปที่ดาวน์โหลดจากอินเทอร์เน็ตจะปราศจากมัลแวร์ที่รู้จัก macOS มีเทคโนโลยีที่ตรวจจับและเอามัลแวร์ออก และมีการปกป้องเพิ่มเติมที่ออกแบบมาเพื่อป้องกันไม่ให้แอปที่ไม่ได้รับการเชื่อถือเข้าถึงข้อมูลของผู้ใช้ บริการของ Apple เช่น การรับรองและการอัปเดต XProtect ได้รับการออกแบบมาเพื่อช่วยป้องกันการติดตั้งมัลแวร์ บริการเหล่านี้จะค้นหามัลแวร์ที่อาจหลีกเลี่ยงการตรวจจับในตอนแรกได้เมื่อจำเป็น จากนั้นจะเอามัลแวร์ออกอย่างรวดเร็วและมีประสิทธิภาพ ท้ายที่สุดแล้ว ผู้ใช้ macOS ก็สามารถทำงานได้อย่างอิสระภายในโมเดลการรักษาความปลอดภัยที่เหมาะสมสำหรับผู้ใช้ รวมถึงการเรียกใช้โค้ดที่ไม่ได้ลงชื่อและโค้ดที่ไม่ได้รับการเชื่อถือ

กระบวนการลงชื่อโค้ดของแอปใน macOS

แอปทั้งหมดจาก App Store จะมีการลงชื่อโดย Apple การลงชื่อนี้ได้รับการออกแบบมาเพื่อให้มั่นใจว่าแอปเหล่านั้นไม่ถูกรบกวนหรือดัดแปลง Apple จะลงชื่อแอปต่างๆ ที่มาพร้อมอุปกรณ์ Apple

ใน macOS 10.15 แอปทั้งหมดที่แจกจ่ายภายนอก App Store จะต้องเซ็นชื่อโดยนักพัฒนาโดยใช้ใบรับรอง ID นักพัฒนาที่ออกโดย Apple (ประกอบด้วยกุญแจส่วนตัว) และได้รับการรับรองโดย Apple ในการทำงานภายใต้การตั้งค่าเริ่มต้นของ Gatekeeper แอปที่พัฒนาโดยบริษัทจะต้องถูกลงชื่อด้วย ID นักพัฒนาที่ออกโดย Apple เพื่อทำให้ผู้ใช้สามารถตรวจสอบความสมบูรณ์ของตัวเองได้

ใน macOS การลงชื่อโค้ดและการรับรองจะทำงานแยกจากกัน และสามารถดำเนินการได้โดยผู้ใช้งานที่ต่างกันเพื่อเป้าหมายที่แตกต่างกัน การลงชื่อโค้ดจะดำเนินการโดยนักพัฒนาโดยใช้ใบรับรอง ID ของนักพัฒนา (ออกโดย Apple) และการตรวจสอบยืนยันของลายเซ็นนี้จะยืนยันกับผู้ใช้ว่าซอฟต์แวร์ของนักพัฒนายังไม่ถูกดัดแปลงนับตั้งแต่ที่นักพัฒนาสร้างและลงชื่อซอฟต์แวร์นี้ การรับรองสามารถดำเนินการโดยใครก็ได้ในห่วงโซ่การเผยแพร่ของซอฟต์แวร์และยืนยันว่า Apple ได้รับสำเนาของโค้ดสำหรับตรวจสอบหามัลแวร์และไม่พบมัลแวร์ที่รู้จัก ข้อมูลออกของการรับรองคือบัตรผ่าน ซึ่งจะถูกจัดเก็บอยู่ในเซิร์ฟเวอร์ของ Apple และสามารถแนบรวมกับแอปได้ (โดยใครก็ได้) โดยไม่ต้องตรวจสอบยืนยันลายเซ็นของนักพัฒนา

การควบคุมการเข้าถึงที่บังคับ (MAC) จะใช้การลงชื่อโค้ดเพื่อเปิดใช้งานสิทธิ์ที่ได้รับการปกป้องโดยระบบ ตัวอย่างเช่น แอปที่ร้องขอการเข้าถึงผ่านไฟร์วอลล์จะต้องลงชื่อด้วยโค้ดพร้อมกับสิทธิ์ MAC ที่เหมาะสม

Gatekeeper และการปกป้องแบบรันไทม์ใน macOS

macOS มีเทคโนโลยี Gatekeeper และการปกป้องแบบรันไทม์เพื่อช่วยให้การรับรองว่าจะมีแค่ซอฟต์แวร์ที่เชื่อถือแล้วเท่านั้นที่สามารถใช้งานได้บน Mac ของผู้ใช้

Gatekeeper

macOS มีเทคโนโลยีความปลอดภัยที่เรียกว่า **Gatekeeper** ซึ่งออกแบบมาเพื่อช่วยให้มั่นใจว่าจะมีเพียงซอฟต์แวร์ที่เชื่อถือได้เท่านั้นที่ทำงานบน Mac ของผู้ใช้ เมื่อผู้ใช้ดาวน์โหลดและเปิดแอป ปลั๊กอินหรือแพ็คเกจตัวติดตั้งจากภายนอก App Store แล้ว Gatekeeper จะตรวจสอบยืนยันว่าซอฟต์แวร์มาจากนักพัฒนาที่ได้รับการยืนยันตัวตน ได้รับการรับรองโดย Apple ว่าปราศจากเนื้อหาที่ทราบว่าเป็นอันตราย และไม่ได้ถูกดัดแปลง นอกจากนี้ Gatekeeper จะร้องขอการอนุญาตจากผู้ใช้ก่อนที่จะเปิดซอฟต์แวร์ที่ดาวน์โหลดแล้วเป็นครั้งแรกเพื่อตรวจสอบให้แน่ใจว่าผู้ใช้ไม่ได้ถูกหลอกให้ใช้งานโปรแกรมปฏิบัติการที่ผู้ใช้เชื่อว่าเป็นเพียงแค่ไฟล์ข้อมูล

ตามค่าเริ่มต้น Gatekeeper จะช่วยให้การรับรองว่าซอฟต์แวร์ที่ดาวน์โหลดแล้วทั้งหมดถูกลงชื่อโดย App Store หรือลงชื่อโดยนักพัฒนาที่ได้รับการลงทะเบียนและได้รับการรับรองโดย Apple แล้ว ทั้งกระบวนการตรวจสอบของ App Store และวิธีการรับรองได้รับการออกแบบมารับรองว่าแอปเหล่านั้นไม่มีมัลแวร์ที่รู้จัก ดังนั้น ตามค่าเริ่มต้นแล้ว **ซอฟต์แวร์ทั้งหมดใน macOS จะถูกตรวจสอบหาเนื้อหาที่ทราบว่าประสงค์ร้ายในครั้งแรกที่ถูกเปิด ไม่ว่าเนื้อหาดังกล่าวจะถูกนำเข้ามาบน Mac ด้วยวิธีการใดก็ตาม**

ผู้ใช้และองค์กรมีตัวเลือกในการอนุญาตเฉพาะซอฟต์แวร์ที่ติดตั้งจาก App Store เท่านั้น นอกจากนี้ ผู้ใช้ยังสามารถเขียนทับนโยบายของ Gatekeeper เพื่อเปิดซอฟต์แวร์ใดก็ได้ เว้นแต่ว่าจะถูกจำกัดโดยโซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) องค์กรสามารถใช้ MDM ในการกำหนดค่าการตั้งค่าของ Gatekeeper ได้ ซึ่งรวมถึงการอนุญาตซอฟต์แวร์ที่ถูกลงชื่อด้วยข้อมูลประจำตัวอื่น ถ้าจำเป็น Gatekeeper ยังสามารถปิดใช้งานอย่างสมบูรณ์ได้อีกด้วย

Gatekeeper ยังปกป้องจากการการแพร่กระจายของปลั๊กอินที่เป็นอันตรายที่มากับแอปที่ไม่เป็นอันตรายอีกด้วย ในกรณีนี้ การใช้แอปจะสั่งทำงานการโหลดปลั๊กอินที่เป็นอันตรายโดยที่ผู้ใช้ไม่รู้ตัว Gatekeeper จะเปิดแอปจากตำแหน่งแบบอ่านอย่างเดียวแบบสุ่มเมื่อจำเป็น วิธีนี้ได้รับการออกแบบมาเพื่อป้องกันการโหลดปลั๊กอินที่แจกจ่ายพร้อมกับแอปโดยอัตโนมัติ

การปกป้องรันไทม์

ไฟล์ระบบ ทรัพยากร และเคอร์เนลจะถูกป้องกันจากพื้นที่แอปของผู้ใช้ แอปทั้งหมดจาก App Store จะอยู่ใน Sandbox เพื่อจำกัดการเข้าถึงข้อมูลที่จัดเก็บโดยแอปอื่น ถ้าแอปจาก App Store ต้องการเข้าถึงข้อมูลจากแอปอื่น App Store สามารถทำได้โดยใช้ API และบริการที่ให้บริการโดย macOS

การป้องกันมัลแวร์ใน macOS

Apple ดำเนินกระบวนการข้อมูลภัยคุกคามเพื่อระบุและปิดกั้นมัลแวร์อย่างรวดเร็ว

การป้องกันสามชั้น

โครงสร้างการป้องกันมัลแวร์มีสามชั้น:

1 **ป้องกันการเปิดใช้หรือการเรียกใช้มัลแวร์:** App Store หรือ Gatekeeper ร่วมกับการรับรอง

2 **ปิดกั้นมัลแวร์ไม่ให้ทำงานบนระบบของลูกค้า:** Gatekeeper, การรับรองและ XProtect

3 **เยียวยามัลแวร์ที่ถูกเรียกใช้แล้ว:** XProtect

การป้องกันชั้นแรกออกแบบมาเพื่อยับยั้งการแพร่กระจายของมัลแวร์ และป้องกันไม่ให้มัลแวร์เปิดใช้งานได้แม้แต่ครั้งเดียว นี่คือเป้าหมายของ App Store และ Gatekeeper ที่ทำงานร่วมกับการรับรอง

ชั้นถัดไปของการป้องกันคือการช่วยทำให้แน่ใจว่าหากมัลแวร์แสดงขึ้นบน Mac เครื่องใดก็ตาม มัลแวร์จะถูกระบุและปิดกั้นอย่างรวดเร็ว ทั้งเพื่อหยุดการแพร่กระจายและเพื่อเยียวยาระบบ Mac ที่มัลแวร์ได้ปักหลักแล้ว XProtect พร้อมด้วย Gatekeeper และการรับรองจะเพิ่มเข้ามาในการป้องกันชั้นนี้

ในขั้นสุดท้าย XProtect จะทำหน้าที่แก้ไขมัลแวร์ที่สามารถดำเนินการได้สำเร็จ

การป้องกันเหล่านี้จะรวมกันเพื่อรองรับแนวปฏิบัติที่ดีที่สุดในการป้องกันไวรัสและมัลแวร์ ด้านล่างคือคำอธิบายเพิ่มเติมสำหรับการป้องกันเหล่านี้ Mac ที่ใช้ Apple Silicon มีการปกป้องเพิ่มเติมเพื่อจำกัดความเสียหายจากมัลแวร์ที่อาจเกิดขึ้นเมื่อมีการเรียกใช้มัลแวร์สำเร็จ ให้ดูที่ การปกป้องการเข้าถึงข้อมูลผู้ใช้ของแอป สำหรับวิธีที่ macOS สามารถช่วยปกป้องข้อมูลผู้ใช้จากมัลแวร์ได้ และ ความสมบูรณ์ของระบบปฏิบัติการ สำหรับวิธีที่ macOS สามารถจำกัดการทำงานของมัลแวร์บนระบบได้

การรับรอง

การรับรองเป็นบริการการสแกนมัลแวร์ที่ Apple ให้บริการ นักพัฒนาที่ต้องการเผยแพร่แอปสำหรับ macOS ภายนอก App Store จะส่งแอปของตนเพื่อสแกน ซึ่งเป็นส่วนหนึ่งของกระบวนการเผยแพร่ Apple จะสแกนซอฟต์แวร์นี้เพื่อตรวจหามัลแวร์ที่รู้จัก และหากไม่พบ ก็จะออกตั๋วรับรองให้ ปกตินักพัฒนาจะแนบตั๋วนี้รวมกับแอปของตนเพื่อให้ Gatekeeper สามารถตรวจสอบยืนยันและเปิดใช้แอปได้แม้จะออฟไลน์

Apple ยังสามารถออกตั๋วเพิกถอนให้กับแอปที่ประสงค์ร้ายได้เช่นกัน แม้ว่าก่อนหน้านี้จะมีการรับรองไปแล้วก็ตาม macOS จะตรวจสอบตั๋วเพิกถอนใหม่ๆ เป็นประจำเพื่อให้ Gatekeeper มีข้อมูลล่าสุดและสามารถปิดกั้นการเปิดใช้ไฟล์เหล่านั้นได้ กระบวนการนี้สามารถปิดกั้นแอปที่ประสงค์ร้ายได้อย่างรวดเร็วมากเนื่องจากมีการอัปเดตในเบื้องหลังบ่อยกว่ามากเมื่อเทียบกับรายการอัปเดตในเบื้องหลังที่ผลักข้อมูลลายเซ็น XProtect ใหม่ๆ นอกจากนี้ การปกป้องนี้ยังสามารถปรับใช้กับทั้งแอปที่มีการปรับใช้ไปก่อนหน้านี้และแอปที่ยังไม่มีการปรับใช้อีกด้วย

XProtect

macOS มีเทคโนโลยีป้องกันไวรัสในตัวที่เรียกว่า **XProtect** สำหรับการตรวจจับและกำจัดมัลแวร์ด้วยลายเซ็น ระบบจะใช้ลายเซ็น YARA ซึ่งเป็นเครื่องมือที่ใช้ตรวจจับมัลแวร์โดยอิงจากลายเซ็น และเป็นเครื่องมือที่ Apple อัปเดตอย่างสม่ำเสมอ Apple จะตรวจสอบการติดมัลแวร์และสเตรน แล้วอัปเดตลายเซ็นโดยอัตโนมัติโดยไม่เกี่ยวข้องกับรายการอัปเดตของระบบ ทั้งนี้เพื่อช่วยป้องกัน Mac ไม่ให้ติดมัลแวร์ XProtect จะตรวจจับและปิดกั้นการดำเนินการของมัลแวร์ที่รู้จักโดยอัตโนมัติ ใน macOS 10.15 ขึ้นไป XProtect จะตรวจสอบหาเนื้อหาที่ทราบว่าประสงค์ร้ายเมื่อใดก็ตามที่:

- แอปเปิดใช้เป็นครั้งแรก
- มีการเปลี่ยนแปลงแอป (ในระบบไฟล์)
- ลายเซ็น XProtect อัปเดตแล้ว

เมื่อ XProtect ตรวจจับมัลแวร์ที่รู้จัก ซอฟต์แวร์จะถูกปิดกั้นและผู้ใช้จะได้รับการแจ้งเตือนและได้รับตัวเลือกสำหรับย้ายซอฟต์แวร์ไปยังถังขยะ

หมายเหตุ: การรับรองมีประสิทธิภาพกับไฟล์ที่รู้จัก (หรือแฮชไฟล์) และสามารถใช้กับแอปที่เปิดใช้ไปแล้วก่อนหน้านี้ได้ กฎเกณฑ์ที่อิงจากลายเซ็นของ XProtect เป็นกฎเกณฑ์ที่ครอบคลุมมากกว่าแฮชไฟล์แบบเฉพาะ จึงสามารถค้นหารูปแบบต่างๆ ที่ Apple ยังไม่เคยเห็นได้ XProtect จะสแกนเฉพาะแอปที่มีการเปลี่ยนแปลงหรือสแกนการเปิดใช้แอปครั้งแรก

XProtect ยังมีเทคโนโลยีในการแก้ไขการติดไวรัสหากมัลแวร์เข้าสู่ Mac แล้วอีกด้วย ตัวอย่างเช่น มีกลไกที่แก้ไขการติดไวรัสตามการอัปเดตที่ส่งจาก Apple โดยอัตโนมัติ (ซึ่งเป็นส่วนหนึ่งของการอัปเดตอัตโนมัติของไฟล์ข้อมูลระบบและการอัปเดตความปลอดภัย) นอกจากนี้ยังเอามัลแวร์ออกเมื่อได้รับข้อมูลที่อัปเดต และยังคงตรวจหาการติดไวรัสเป็นระยะ XProtect จะไม่จะเริ่มต้นระบบของ Mac อีกครั้งโดยอัตโนมัติ

รายการอัปเดตความปลอดภัยอัตโนมัติของ XProtect

Apple จะออกรายการอัปเดตสำหรับ XProtect โดยอัตโนมัติ โดยอิงตามข้อมูลภัยคุกคามล่าสุดที่มี ตามค่าเริ่มต้น macOS จะตรวจสอบรายการอัปเดตเหล่าโดยอัตโนมัติทุกวัน รายการอัปเดตการรับรอง ซึ่งเผยแพร่โดยใช้การเชื่อมข้อมูล CloudKit นั้นเกิดขึ้นบ่อยกว่ามาก

Apple จะตอบสนองอย่างไรเมื่อพบมัลแวร์ใหม่

เมื่อพบมัลแวร์ตัวใหม่ อาจมีการดำเนินการต่างๆ ในหลายขั้นตอน:

- ใบรับรอง ID ของนักพัฒนาทุกใบที่เกี่ยวข้องจะถูกเพิกถอน
- มีการออกตั๋วเพิกถอนการรับรองให้กับทุกไฟล์ (แอปและไฟล์ที่เกี่ยวข้อง)
- มีการพัฒนาและเผยแพร่ลายเซ็น XProtect

  ลายเซ็นเหล่านี้ยังถูกปรับใช้แบบย้อนหลังกับซอฟต์แวร์ที่ได้รับการรับรองไปแล้วอีกด้วย และการตรวจจับใดๆ ที่เป็นการตรวจจับใหม่อาจส่งผลให้การทำงานอย่างน้อยหนึ่งรายการที่เกิดขึ้นไปแล้วเกิดขึ้นอีกครั้ง

ท้ายที่สุดแล้ว การตรวจพบมัลแวร์จะนำไปสู่ชุดขั้นตอนต่างๆ ที่ใช้เวลาเป็นวินาที ชั่วโมง และวันตามมา เพื่อมอบการปกป้องที่ดีที่สุดกับผู้ใช้ Mac

การควบคุมการเข้าถึงไฟล์ของแอปใน macOS

Apple เชื่อมั่นว่าผู้ใช้ควรได้รับความโปร่งใส ความยินยอม และการควบคุมแบบเต็มรูปแบบต่อสิ่งที่แอปดำเนินการกับข้อมูลของผู้ใช้ ใน macOS 10.15 รุ่นนี้ถูกบังคับใช้โดยระบบเพื่อช่วยให้แน่ใจว่าแอปทั้งหมดจะรับความยินยอมของผู้ใช้ก่อนที่จะเข้าถึงไฟล์ในเอกสาร, รายการดาวน์โหลด, เดสก์ท็อป, iCloud Drive และดิสก์โวลุ่มเครือข่าย ใน macOS 10.13 ขึ้นไป แอปที่ต้องการเข้าถึงอุปกรณ์พื้นที่จัดเก็บข้อมูลแบบเต็มจะต้องถูกเพิ่มในการตั้งค่าระบบอย่างชัดแจ้ง นอกจากนี้ การช่วยการเข้าถึงและความสามารถของการทำงานอัตโนมัติจะต้องใช้สิทธิ์ของผู้ใช้เพื่อช่วยให้การรับรองว่าจะไม่หลีกเลี่ยงการปกป้องอื่นๆ ระบบอาจขอผู้ใช้หรือผู้ใช้อาจจำเป็นต้องเปลี่ยนการตั้งค่าใน การตั้งค่าระบบ > ความปลอดภัยและความเป็นส่วนตัว > ความเป็นส่วนตัว ทั้งนี้ขึ้นอยู่กับนโยบายการเข้าถึง

รายการ	แอปแจ้งผู้ใช้	ผู้ใช้จะต้องแก้ไขการตั้งค่าความเป็นส่วนตัวของระบบ
การช่วยการเข้าถึง		✓
การเข้าถึงพื้นที่จัดเก็บข้อมูลภายในแบบเต็ม		✓
ไฟล์และโฟลเดอร์ **หมายเหตุ:** รวมถึงเดสก์ท็อป เอกสาร การดาวน์โหลด ดิสก์โวลุ่มเครือข่าย และดิสก์โวลุ่มที่ถอดออกได้	✓	
การทำงานอัตโนมัติ (กิจกรรมของ Apple)	✓	

รายการในถังขยะของผู้ใช้ได้รับการปกป้องจากแอปใดๆ ก็ตามที่ใช้การเข้าถึงดิสก์แบบเต็ม ผู้ใช้จะไม่ได้รับการแจ้งสำหรับการเข้าถึงแอป ถ้าผู้ใช้ต้องการให้แอปเข้าถึงไฟล์ จะต้องย้ายไฟล์เหล่านั้นจากถังขยะไปยังตำแหน่งอื่น

ผู้ใช้ที่เปิดใช้ FileVault บน Mac จะถูกขอให้ระบุข้อมูลประจำตัวที่ถูกต้องก่อนที่จะดำเนินกระบวนการบูตต่อและเข้าถึงโหมดเริ่มต้นใช้งานพิเศษได้ ในกรณีที่ไม่มีข้อมูลยืนยันตัวตนที่ถูกต้องหรือรหัสการกู้คืน ดิสก์โวลุ่มทั้งหมดจะยังคงเข้ารหัสอยู่และได้รับการปกป้องจากการเข้าถึงที่ไม่ได้รับอนุญาต แม้ว่าอุปกรณ์พื้นที่จัดเก็บข้อมูลจะถูกเอาออกและเชื่อมต่อกับคอมพิวเตอร์เครื่องอื่น

ในการปกป้องข้อมูลในการตั้งค่าองค์กร ฝ่าย IT ควรกำหนดและบังคับใช้นโยบายการกำหนดค่า FileVault โดยใช้ การจัดการอุปกรณ์เคลื่อนที่ (MDM) องค์กรจะมีตัวเลือกมากมายสำหรับจัดการดิสก์โวลุ่มที่ถูกเข้ารหัส รวมถึงรหัสการกู้คืนขององค์กร รหัสการกู้คืนส่วนบุคคล (ซึ่งสามารถเลือกที่จะจัดเก็บด้วย MDM สำหรับข้อมูลที่ฝากได้) หรือกุญแจทั้งสองประเภท การหมุนเวียนของกุญแจก็สามารถตั้งค่าเป็นนโยบายใน MDM ได้ด้วยเช่นกัน

คุณสมบัติความปลอดภัยในแอปโน้ต

แอปโน้ตมีคุณสมบัติโน้ตที่ปลอดภัยบน iPhone, iPad, Mac และเว็บไซต์ iCloud ซึ่งทำให้ผู้ใช้สามารถปกป้องเนื้อหาของโน้ตฉบับที่ต้องการปกป้องได้ ผู้ใช้ยังสามารถแชร์โน้ตกับผู้อื่นได้อย่างปลอดภัย

โน้ตที่ปลอดภัย

โน้ตที่ปลอดภัยจะถูกเข้ารหัสแบบต้นทางถึงปลายทางโดยใช้วลีรหัสผ่านที่ผู้ใช้กำหนดและจำเป็นต้องใช้เพื่อดูโน้ตบนอุปกรณ์ iOS, iPadOS, macOS และเว็บไซต์ iCloud บัญชี iCloud แต่ละบัญชี (รวมถึงบัญชีอุปกรณ์ “On my”) สามารถมีวลีรหัสผ่านที่แตกต่างกันได้

เมื่อผู้ใช้ดำเนินการป้องกันโน้ต จะได้กุญแจแบบ 16 ไบต์จากวลีรหัสผ่านของผู้ใช้โดยใช้ PBKDF2 และ SHA256 โน้ตและไฟล์แนบทั้งหมดของโน้ตจะถูกเข้ารหัสโดยใช้ AES ที่มีโหมด Galois/ตัวนับ (AES-GCM) บันทึกใหม่จะถูกสร้างใน Core Data และ CloudKit เพื่อจัดเก็บโน้ตที่เข้ารหัส ไฟล์แนบ แท็ก และเวคเตอร์การเริ่มต้นทำงาน หลังจากที่บันทึกใหม่ถูกสร้างขึ้น ข้อมูลที่ไม่ได้เข้ารหัสต้นฉบับจะถูกลบออก ไฟล์แนบที่รองรับการเข้ารหัสประกอบด้วย ภาพ ภาพสเก็ตช์ ตาราง แผนที่ และเว็บไซต์ โน้ตที่มีไฟล์แนบประเภทอื่นๆ จะเข้ารหัสไม่ได้ และจะไม่สามารถเพิ่มไฟล์แนบที่ไม่รองรับลงในโน้ตที่ปลอดภัยได้

ในการดูโน้ตที่ปลอดภัย ผู้ใช้จะต้องป้อนวลีรหัสผ่านหรือตรวจสอบสิทธิ์โดยใช้ Face ID หรือ Touch ID หลังจากที่ตรวจสอบสิทธิ์ผู้ใช้เสร็จแล้ว ไม่ว่าเพื่อดูหรือสร้างโน้ตที่ปลอดภัยก็ตาม แอปโน้ตจะเปิดเซสชั่นที่ปลอดภัย ในระหว่างที่เปิดเซสชั่นที่ปลอดภัยอยู่ ผู้ใช้สามารถดูหรือป้องกันโน้ตอื่นๆ ได้โดยไม่ต้องตรวจสอบสิทธิ์เพิ่มเติม อย่างไรก็ตาม เซสชั่นที่ปลอดภัยจะปรับใช้กับโน้ตที่ปกป้องด้วยวลีรหัสผ่านที่กำหนดเท่านั้น ผู้ใช้จะยังต้องตรวจสอบสิทธิ์สำหรับโน้ตที่ได้รับการปกป้องโดยวลีรหัสผ่านอื่น เซสชั่นที่ปลอดภัยจะปิดลงเมื่อ:

- ผู้ใช้แตะปุ่มล็อคตอนนี้ในแอปโน้ต
- โน้ตสลับไปทำงานในเบื้องหลังนานเกิน 3 นาที (8 นาทีใน macOS)
- การล็อคของอุปกรณ์ iOS หรือ iPadOS

ในการเปลี่ยนวลีรหัสผ่านของโน้ตที่ปลอดภัย ผู้ใช้จะต้องป้อนวลีรหัสผ่านปัจจุบัน เนื่องจาก Face ID และ Touch ID จะไม่สามารถใช้งานได้เมื่อเปลี่ยนวลีรหัสผ่าน หลังจากเลือกวลีรหัสผ่านใหม่แล้ว แอปโน้ตจะห่อกุญแจของโน้ตทั้งหมดที่มีอยู่ในบัญชีเดียวกันและถูกเข้ารหัสโดยวลีรหัสผ่านก่อนหน้านี้อีกครั้ง

ถ้าผู้ใช้ป้อนวลีรหัสผ่านผิดติดกันสามครั้ง แอปโน้ตจะแสดงคำใบ้ที่ผู้ใช้กำหนดไว้เองหากผู้ใช้กำหนดไว้ในระหว่างการตั้งค่า ถ้าผู้ใช้ยังคงจำวลีรหัสผ่านไม่ได้ ผู้ใช้สามารถรีเซ็ตได้ในการตั้งค่าของแอปโน้ต คุณสมบัตินี้ทำให้ผู้ใช้สามารถสร้างโน้ตที่ปลอดภัยฉบับใหม่ด้วยวลีรหัสผ่านใหม่ได้ แต่จะไม่ทำให้ผู้ใช้สามารถดูโน้ตที่ได้รับการรักษาความปลอดภัยฉบับก่อนหน้าได้ ผู้ใช้ยังคงสามารถดูโน้ตที่ได้รับการรักษาความปลอดภัยฉบับก่อนหน้าได้หากนึกวลีรหัสผ่านออก การรีเซ็ตวลีรหัสผ่านต้องใช้วลีรหัสผ่านของบัญชี iCloud ของผู้ใช้

โน้ตที่แชร์

โน้ตที่ไม่ได้ถูกเข้ารหัสแบบต้นทางถึงปลายทางด้วยวลีรหัสผ่านจะสามารถแชร์กับผู้อื่นได้ โน้ตที่แชร์จะยังคงใช้ประเภทข้อมูลที่เข้ารหัส CloudKit สำหรับข้อความหรือไฟล์แนบที่ผู้ใช้ป้อนลงในโน้ต แอสเซทถูกเข้ารหัสอยู่เสมอด้วยกุญแจที่เข้ารหัสใน CKRecord เมตาดาต้าอย่างเช่นการสร้างหรือแก้ไขวันที่ จะไม่ถูกเข้ารหัส CloudKit จัดการกระบวนการโดยผู้เข้าร่วมสามารถเข้ารหัสและถอดรหัสข้อมูลของกันและกันได้

คุณสมบัติความปลอดภัยในแอปคำสั่งลัด

ในแอปคำสั่งลัด คำสั่งลัดจะเชื่อมข้อมูลกับอุปกรณ์ Apple ทุกเครื่องโดยใช้ iCloud แทนก็ได้ นอกจากนี้ยังแชร์คำสั่งลัดกับผู้ใช้คนอื่นผ่าน iCloud ได้ด้วย คำสั่งลัดจะถูกจัดเก็บในรูปแบบเข้ารหัสในตัวเครื่อง

คำสั่งลัดแบบกำหนดเองนั้นสามารถใช้งานได้สะดวกเนื่องจากคล้ายคลึงกับสคริปต์หรือโปรแกรม เมื่อดาวน์โหลดคำสั่งลัดจากอินเทอร์เน็ต ผู้ใช้จะได้รับคำเตือนว่าคำสั่งลัดยังไม่ได้รับการตรวจสอบโดย Apple และให้โอกาสในการตรวจสอบคำสั่งลัด ในการปกป้องผู้ใช้จากคำสั่งลัดที่ประสงค์ร้าย คำนิยามมัลแวร์ที่อัปเดตจะถูกดาวน์โหลดเพื่อระบุคำสั่งลัดที่ประสงค์ร้ายเมื่อเรียกใช้งาน

คำสั่งลัดแบบกำหนดเองยังสั่งทำงาน JavaScript ที่ระบุผู้ใช้บนเว็บไซต์ใน Safari เมื่อใช้งานจากแผ่นงานการแชร์อีกด้วย ตัวอย่างเช่น ในการปกป้องผู้ใช้จาก JavaScript ที่ประสงค์ร้ายที่หลอกให้ผู้ใช้สั่งทำงานสคริปต์บนเว็บไซต์สังคมออนไลน์ที่เก็บข้อมูลของผู้ใช้ JavaScript จะถูกตรวจสอบความถูกต้องสำหรับคำนิยามมัลแวร์ที่กล่าวไว้ข้างต้น ครั้งแรกที่ผู้ใช้สั่งทำงาน JavaScript บนโดเมน ผู้ใช้จะได้รับแจ้งให้อนุญาตคำสั่งลัดที่มี JavaScript สั่งทำงานบนหน้าเว็บปัจจุบันสำหรับโดเมนนั้น

ความปลอดภัยของบริการ

ภาพรวมความปลอดภัยของบริการ

Apple ได้สร้างชุดของบริการที่สมบูรณ์เพื่อช่วยให้ผู้ใช้ได้รับอรรถประโยชน์และประสิทธิภาพการทำงานจากอุปกรณ์ได้มากยิ่งขึ้น บริการเหล่านี้มีความสามารถที่มีประสิทธิภาพสำหรับการจัดเก็บข้อมูลบนคลาวด์ การเชื่อมข้อมูล การจัดเก็บรหัสผ่าน การตรวจสอบสิทธิ์ การชำระเงิน การส่งข้อความ การสื่อสาร และอื่นๆ และในขณะเดียวกันก็ปกป้องความเป็นส่วนตัวของผู้ใช้และความปลอดภัยของข้อมูลผู้ใช้ด้วย

บทนี้ครอบคลุมถึงเทคโนโลยีความปลอดภัยที่ใช้บน iCloud, ในการลงชื่อเข้าด้วย Apple, Apple Pay, iMessage, Apple Messages for Business, FaceTime, “ค้นหาของฉัน” และคุณสมบัติความต่อเนื่อง

หมายเหตุ: บริการของ Apple และเนื้อหาบางอย่างมีให้ใช้ในบางประเทศหรือภูมิภาคเท่านั้น

Apple ID และ Apple ID ที่ได้รับการจัดการ

ภาพรวมความปลอดภัยของ Apple ID

Apple ID คือบัญชีที่ใช้ในการลงชื่อเข้าบริการของ Apple เป็นเรื่องสำคัญที่ผู้ใช้ต้องเก็บ Apple ID ของตนให้ปลอดภัยเพื่อป้องกันการเข้าถึงบัญชีของตนโดยไม่ได้รับอนุญาต ในการช่วยป้องกันเรื่องนี้ Apple ID ต้องใช้รหัสผ่านที่ปลอดภัยสูงซึ่ง:

- ต้องมีอักขระอย่างน้อยแปดตัว
- ต้องมีทั้งตัวอักษรและตัวเลข
- ต้องไม่มีอักขระเดียวกันอยู่ติดกันตั้งแต่สามตัวขึ้นไป
- ต้องไม่เป็นรหัสผ่านที่ใช้กันอย่างแพร่หลาย

แนะนำให้ผู้ใช้เพิ่มความปลอดภัยให้มากกว่าที่แนะนำ โดยการเพิ่มตัวอักษรพิเศษและเครื่องหมายวรรคตอนเพื่อทำให้รหัสผ่านของตนมีความปลอดภัยสูงขึ้น

Apple ยังแจ้งเตือนผู้ใช้ทางอีเมลหรือการแจ้งเตือนแบบผลักข้อมูล หรือทั้งสองทาง เมื่อมีการเปลี่ยนแปลงที่สำคัญในบัญชีของผู้ใช้อีกด้วย ตัวอย่างเช่น หากรหัสผ่านหรือข้อมูลการเรียกเก็บเงินมีการเปลี่ยนแปลง หรือมีการใช้ Apple ID เพื่อลงชื่อเข้าบนอุปกรณ์เครื่องใหม่ ถ้ามีจุดผิดปกติไป ผู้ใช้จะได้รับคำแนะนำให้เปลี่ยนรหัสผ่าน Apple ID ของตนโดยทันที

นอกจากนี้ Apple ยังใช้นโยบายและขั้นตอนหลายอย่างที่ออกแบบมาเพื่อป้องกันบัญชีผู้ใช้ ซึ่งประกอบด้วยการจำกัดจำนวนครั้งในการพยายามลงชื่อเข้าหรือพยายามรีเซ็ตรหัสผ่าน การตรวจสอบการหลอกลวงอยู่ตลอดเวลาเพื่อช่วยระบุการโจมตีในขณะที่เกิดขึ้น และการตรวจสอบนโยบายอย่างสม่ำเสมอที่ทำให้ Apple สามารถปรับตัวเข้ากับข้อมูลใหม่ซึ่งอาจส่งผลต่อความปลอดภัยของผู้ใช้ได้

หมายเหตุ: นโยบายรหัสผ่านของ Apple ID ที่ได้รับการจัดการจะกำหนดโดยผู้ดูแลระบบใน Apple School Manager หรือ Apple Business Manager

การตรวจสอบสิทธิ์สองปัจจัย

Apple ใช้**การตรวจสอบสิทธิ์สองปัจจัย**เป็นค่าเริ่มต้นเพื่อช่วยให้ผู้ใช้รักษาความปลอดภัยบัญชีของตนได้มากขึ้น ซึ่งเป็นการรักษาความปลอดภัยอีกชั้นหนึ่งสำหรับ Apple ID คุณสมบัตินี้ออกแบบมาเพื่อรับรองว่าเจ้าของบัญชีเท่านั้นที่สามารถเข้าถึงบัญชีได้ แม้ว่าผู้อื่นจะทราบรหัสผ่านก็ตาม เมื่อใช้การตรวจสอบสิทธิ์สองปัจจัย บัญชีของผู้ใช้จะสามารถเข้าถึงได้จากบนอุปกรณ์ที่เชื่อถือแล้วเท่านั้น เช่น iPhone, iPad, iPod touch หรือ Mac ของผู้ใช้หรือบนอุปกรณ์อื่นๆ หลังจากตรวจสอบยืนยันจนเสร็จจากอุปกรณ์ที่เชื่อถือแล้วเหล่านี้หรือจากเบอร์โทรศัพท์ที่เชื่อถือแล้ว ในการลงชื่อเข้าเป็นครั้งแรกในอุปกรณ์เครื่องใหม่ คุณต้องใช้ข้อมูลสองส่วนซึ่งประกอบด้วยรหัสผ่าน Apple ID และรหัสการตรวจสอบยืนยันหกหลักที่จะแสดงบนอุปกรณ์ที่เชื่อถือแล้วของผู้ใช้หรือส่งไปที่เบอร์โทรศัพท์ที่เชื่อถือแล้ว โดยการป้อนรหัสนี้ ถือว่าผู้ใช้ยืนยันว่าตนเชื่อถือในอุปกรณ์เครื่องใหม่นี้และยืนยันว่าอุปกรณ์ดังกล่าวมีความปลอดภัยที่จะลงชื่อเข้า เนื่องจากรหัสผ่านเพียงอย่างเดียวไม่เพียงพอที่จะเข้าถึงบัญชีของผู้ใช้ได้อีกต่อไป การตรวจสอบสิทธิ์สองปัจจัยจึงจะช่วยเพิ่มความปลอดภัยให้กับ Apple ID ของผู้ใช้และข้อมูลส่วนบุคคลทั้งหมดที่ผู้ใช้จัดเก็บไว้กับ Apple คุณสมบัตินี้รวมอยู่โดยตรงใน iOS, iPadOS, macOS, tvOS, watchOS และระบบการตรวจสอบสิทธิ์ที่เว็บไซต์ของ Apple ใช้

เมื่อผู้ใช้ลงชื่อเข้าเว็บไซต์ของ Apple โดยใช้เว็บเบราว์เซอร์ คำขอปัจจัยที่สองจะถูกส่งไปยังอุปกรณ์ที่เชื่อถือแล้วทุกเครื่องที่ผูกกับบัญชี iCloud ของผู้ใช้เพื่อร้องขอการอนุญาตเซสชั่นเว็บ ถ้าผู้ใช้ลงชื่อเข้าเว็บไซต์ของ Apple จากเบราว์เซอร์บนอุปกรณ์ที่เชื่อถือแล้ว ผู้ใช้จะเห็นรหัสการตรวจสอบยืนยันแสดงขึ้นบนอุปกรณ์ที่ตนกำลังใช้ เมื่อผู้ใช้ป้อนโค้ดบนอุปกรณ์นั้น เซสชั่นเว็บจะได้รับอนุญาต

การรีเซ็ตรหัสผ่านและกู้คืนบัญชี

ถ้าลืมรหัสผ่านของบัญชี Apple ID ผู้ใช้สามารถรีเซ็ตรหัสผ่านบนอุปกรณ์ที่เชื่อถือแล้วได้ ถ้าไม่มีอุปกรณ์ที่เชื่อถือแต่ทราบรหัสผ่าน ผู้ใช้สามารถใช้เบอร์โทรศัพท์ที่เชื่อถือในการตรวจสอบสิทธิ์ผ่านการตรวจสอบยืนยันทาง SMS ได้ นอกจากนี้ ในการกู้คืนโดยทันทีสำหรับ Apple ID คุณสามารถใช้รหัสที่เคยใช้ก่อนหน้าเพื่อรีเซ็ตร่วมกับ SMS ได้ ถ้าไม่สามารถใช้ตัวเลือกเหล่านี้ได้ จะต้องทำตามกระบวนการกู้คืนบัญชี โปรดดูบทความบริการช่วยเหลือของ Apple วิธีใช้การกู้คืนบัญชีเมื่อคุณไม่สามารถรีเซ็ตรหัสผ่าน Apple ID ได้ สำหรับข้อมูลเพิ่มเติม

ความปลอดภัยของ Apple ID ที่ได้รับการจัดการ

Apple ID ที่ได้รับการจัดการจะทำหน้าที่คล้ายกับ Apple ID แต่องค์กรหรือสถาบันการศึกษาจะเป็นเจ้าของและเป็นผู้ควบคุม องค์กรเหล่านี้สามารถรีเซ็ตรหัสผ่าน จำกัดการซื้อสินค้าและการสื่อสารต่างๆ เช่น FaceTime และแอปข้อความ และตั้งค่าสิทธิ์ตามบทบาทสำหรับพนักงาน เจ้าหน้าที่ ครูอาจารย์ และนักเรียนได้

สำหรับ Apple ID ที่ได้รับการจัดการ บางบริการจะถูกปิดใช้งาน (ตัวอย่างเช่น Apple Pay, พวงกุญแจ iCloud, HomeKit และ “ค้นหาของฉัน”)

การตรวจสอบ Apple ID ที่ได้รับการจัดการ

Apple ID ที่ได้รับการจัดการยังรองรับ**การตรวจสอบ**อีกด้วย ซึ่งทำให้องค์กรสามารถปฏิบัติตามกฎหมายและระเบียบข้อบังคับเกี่ยวกับความเป็นส่วนตัวได้ ผู้ดูแลระบบ ผู้จัดการ หรือครูอาจารย์ของ Apple School Manager สามารถตรวจสอบบัญชี Apple ID ที่ได้รับการจัดการแบบเจาะจงบัญชีได้

ผู้ตรวจสอบสามารถตรวจสอบได้เฉพาะบัญชีที่อยู่ภายใต้ตนเองในลำดับชั้นขององค์กรเท่านั้น ตัวอย่างเช่น ครูอาจารย์จะสามารถตรวจสอบนักเรียนได้ ผู้จัดการจะสามารถตรวจสอบครูอาจารย์และนักเรียนได้ และผู้ดูแลระบบจะสามารถตรวจสอบผู้จัดการ ครูอาจารย์ และนักเรียนได้

เมื่อมีการร้องขอเอกสารสิทธิ์ของการตรวจสอบโดยใช้ Apple School Manager จะมีการสร้างบัญชีพิเศษที่สามารถเข้าถึงได้เฉพาะ Apple ID ที่ได้รับการจัดการที่ถูกร้องขอให้ตรวจสอบเท่านั้น จากนั้นผู้ตรวจสอบจะสามารถอ่านและแก้ไขเนื้อหาของผู้ใช้ที่จัดเก็บอยู่บน iCloud หรือในแอปที่ใช้กับ CloudKit ได้ การร้องขอการเข้าถึงเพื่อตรวจสอบทุกครั้งจะถูกเก็บบันทึกการใช้งานไว้ใน Apple School Manager บันทึกการใช้งานจะแสดงว่าผู้ตรวจสอบเป็นใคร แสดง Apple ID ที่ได้รับการจัดการที่ผู้ตรวจสอบร้องขอการเข้าถึง แสดงเวลาที่ร้องขอ และแสดงว่าได้มีการตรวจสอบเกิดขึ้นหรือไม่

Apple ID ที่ได้รับการจัดการและอุปกรณ์ส่วนบุคคล

Apple ID ที่ได้รับการจัดการยังสามารถใช้กับอุปกรณ์ iOS และ iPadOS และคอมพิวเตอร์ Mac ส่วนบุคคลได้ด้วยเช่นกัน นักเรียนจะลงชื่อเข้า iCloud โดยใช้ Apple ID ที่ได้รับการจัดการที่ออกโดยสถาบันและใช้รหัสผ่านเพิ่มเติมสำหรับใช้ในเครื่อง ซึ่งทำหน้าที่เป็นปัจจัยที่สองของกระบวนการตรวจสอบสิทธิ์สองปัจจัยของ Apple ID ขณะที่นักเรียนใช้ Apple ID ที่ได้รับการจัดการบนอุปกรณ์ส่วนบุคคล ผู้ใช้จะไม่สามารถใช้งานพวงกุญแจ iCloud ได้ และสถาบันอาจจะจำกัดคุณสมบัติอื่นๆ เช่น FaceTime หรือแอปข้อความ เอกสาร iCloud ใดๆ ที่นักเรียนสร้างในขณะที่ลงชื่อเข้าจะถูกตรวจสอบได้ตามที่อธิบายไว้ก่อนหน้านี้ในส่วนนี้

iCloud

ภาพรวมความปลอดภัยของ iCloud

iCloud จัดเก็บรายชื่อ ปฏิทิน รูปภาพ เอกสาร และอื่นๆ ของผู้ใช้และทำให้ข้อมูลอัปเดตอยู่เสมอในอุปกรณ์ทุกเครื่องของผู้ใช้โดยอัตโนมัติ iCloud ยังสามารถใช้โดยแอปของบริษัทอื่นเพื่อจัดเก็บและเชื่อมข้อมูลเอกสาร เช่นเดียวกับค่ากุญแจสำหรับข้อมูลแอปตามที่ระบุโดยนักพัฒนาได้อีกด้วย ผู้ใช้ตั้งค่า iCloud โดยลงชื่อเข้าด้วย Apple ID และเลือกบริการที่พวกเขาต้องการใช้ ผู้ดูแลระบบ IT สามารถปิดใช้งานคุณสมบัติ iCloud บางอย่าง เช่น iCloud Drive และข้อมูลสำรอง iCloud ได้โดยใช้โปรไฟล์การกำหนดค่าการจัดการอุปกรณ์เคลื่อนที่ (MDM)

iCloud ใช้วิธีการด้านความปลอดภัยที่ทรงพลังและใช้นโยบายที่เข้มงวดในการปกป้องข้อมูลของผู้ใช้ ข้อมูล iCloud ส่วนใหญ่จะถูกเข้ารหัสบนอุปกรณ์ของผู้ใช้ก่อนด้วยกุญแจ iCloud ที่อุปกรณ์สร้างขึ้นมาเอง จากนั้นจะถูกอัปโหลดไปยังเซิร์ฟเวอร์ iCloud สำหรับข้อมูลที่ไม่ได้เข้ารหัสแบบต้นทางถึงปลายทาง อุปกรณ์ของผู้ใช้จะอัปโหลดกุญแจ iCloud เหล่านี้ไปยังโมดูลรักษาความปลอดภัยฮาร์ดแวร์ของ iCloud ในศูนย์ข้อมูลของ Apple อย่างปลอดภัย กระบวนการนี้ทำให้ Apple สามารถช่วยเหลือผู้ใช้ในการกู้คืนข้อมูลและถอดรหัสข้อมูลในนามของผู้ใช้ได้ทุกเมื่อที่ผู้ใช้ต้องการ (ตัวอย่างเช่น เมื่อผู้ใช้ลงชื่อเข้าบนอุปกรณ์ใหม่ กู้คืนจากข้อมูลสำรอง หรือเข้าถึงข้อมูล iCloud ของตนบนเว็บ) การย้ายข้อมูลระหว่างอุปกรณ์ของผู้ใช้และเซิร์ฟเวอร์ iCloud มีการเข้ารหัสแยกจากกันในระหว่างการส่งผ่านด้วย TLS และเซิร์ฟเวอร์ iCloud จะจัดเก็บข้อมูลผู้ใช้ด้วยการเข้ารหัสอีกชั้นหนึ่งขณะที่ข้อมูลพักอยู่

เมื่อมีกุญแจการเข้ารหัสที่ Apple ใช้ได้ กุญแจเหล่านั้นจะได้รับการเก็บรักษาในศูนย์ข้อมูลของ Apple ในระหว่างการประมวลผลข้อมูลที่จัดเก็บไว้ในศูนย์ข้อมูลของบริษัทอื่น กุญแจการเข้ารหัสเหล่านี้จะเข้าถึงได้โดยซอฟต์แวร์ของ Apple ที่ทำงานบนเซิร์ฟเวอร์ที่ปลอดภัยเท่านั้น และในขณะดำเนินการประมวลผลที่จำเป็นเท่านั้น สำหรับความเป็นส่วนตัวและความปลอดภัยเพิ่มเติม บริการของ Apple จำนวนมากใช้การเข้ารหัสแบบต้นทางถึงปลายทาง ซึ่งหมายความว่ามีเพียงผู้ใช้เท่านั้นที่สามารถเข้าถึงข้อมูล iCloud ของตนได้ และเข้าถึงได้เฉพาะจากอุปกรณ์ที่เชื่อถือแล้วซึ่งผู้ใช้ลงชื่อเข้าไว้ด้วย Apple ID ของตน

Apple เสนอสองตัวเลือกให้กับผู้ใช้ในการเข้ารหัสและปกป้องข้อมูลที่จัดเก็บอยู่บน iCloud:

- **การปกป้องข้อมูลมาตรฐาน (การตั้งค่าเริ่มต้น):** ข้อมูล iCloud ของผู้ใช้จะถูกเข้ารหัส กุญแจการเข้ารหัสจะถูกเก็บรักษาในศูนย์ข้อมูลของ Apple และ Apple สามารถช่วยเหลือด้านการกู้คืนข้อมูลและบัญชีได้ เฉพาะข้อมูล iCloud บางส่วน ซึ่งมี 14 หมวดหมู่ รวมถึงข้อมูลสุขภาพและรหัสผ่านในพวงกุญแจ iCloud ที่จะมีการเข้ารหัสแบบต้นทางถึงปลายทาง
- **การปกป้องข้อมูลขั้นสูงสำหรับ iCloud:** การตั้งค่าแบบไม่บังคับที่ให้การปกป้องข้อมูลคลาวด์ระดับสูงสุดของ Apple ถ้าผู้ใช้เลือกที่จะเปิดใช้การปกป้องข้อมูลขั้นสูง อุปกรณ์ที่เชื่อถือแล้วของผู้ใช้จะยังคงมีสิทธิ์เพียงหนึ่งเดียวในการเข้าถึงกุญแจการเข้ารหัสสำหรับข้อมูล iCloud ส่วนใหญ่ของผู้ใช้ ดังนั้นข้อมูลนั้นจะได้รับการปกป้องโดยใช้การเข้ารหัสแบบต้นทางถึงปลายทาง เมื่อคุณเปิดใช้การปกป้องข้อมูลขั้นสูง จำนวนหมวดหมู่ข้อมูลที่ใช้การเข้ารหัสแบบต้นทางถึงปลายทางจะเพิ่มขึ้นเป็น 23 หมวดหมู่ และรวมข้อมูลสำรอง รูปภาพ โน้ต และอื่นๆ ของ iCloud

ข้อมูล iCloud หมวดหมู่ที่ระบุเฉพาะซึ่งมีการปกป้องด้วยการเข้ารหัสแบบต้นทางถึงปลายทางจะระบุอยู่ในบทความบริการช่วยเหลือของ Apple ภาพรวมความปลอดภัยของข้อมูล iCloud

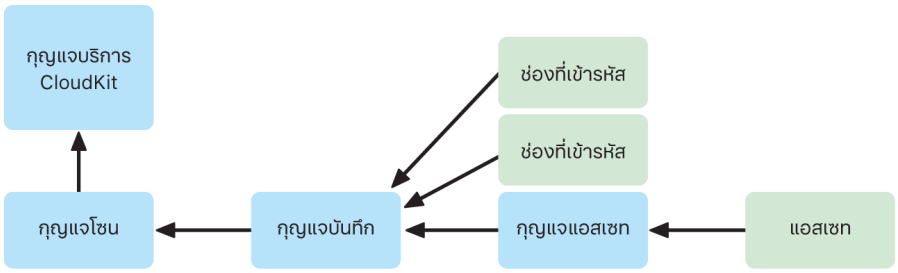
การเข้ารหัส iCloud

การเข้ารหัสข้อมูลใน iCloud มีความสัมพันธ์อย่างใกล้ชิดกับโมเดลการจัดเก็บข้อมูล โดยเริ่มจากเฟรมเวิร์ค CloudKit และ API ที่อนุญาตให้แอปและซอฟต์แวร์ระบบจัดเก็บข้อมูลบน iCloud ในนามของผู้ใช้ และทำให้ทุกอย่างตรงกันล่าสุดอยู่เสมอบนอุปกรณ์ต่างๆ และบนเว็บ

การเข้ารหัส CloudKit

CloudKit เป็นเฟรมเวิร์คที่ทำให้นักพัฒนาแอปสามารถจัดเก็บข้อมูลค่ากุญแจ ข้อมูลที่มีโครงสร้าง และแอสเซท (ข้อมูลขนาดใหญ่ที่จัดเก็บแยกต่างหากจากฐานข้อมูล เช่น ภาพหรือวิดีโอ) บน iCloud ได้ CloudKit รองรับทั้งฐานข้อมูลแบบสาธารณะและส่วนตัว โดยจัดกลุ่มอยู่ในตัวบรรจุ ฐานข้อมูลแบบสาธารณะมีการแชร์ทั่วโลก โดยปกติจะใช้สำหรับแอสเซททั่วไป และไม่ได้เข้ารหัส ฐานข้อมูลแบบส่วนตัวจะจัดเก็บข้อมูล iCloud ของผู้ใช้แต่ละราย

CloudKit ใช้ลำดับชั้นของกุญแจที่ตรงกับโครงสร้างของข้อมูล ฐานข้อมูลแบบส่วนตัวของตัวบรรจุแต่ละตัวจะได้รับการปกป้องโดยลำดับชั้นกุญแจซึ่งมีรากฐานอยู่ในกุญแจแบบไม่สมมาตรที่เรียกว่า**กุญแจบริการ CloudKit** กุญแจเหล่านี้จะไม่ซ้ำกันสำหรับผู้ใช้ iCloud แต่ละรายและจะถูกสร้างขึ้นบนอุปกรณ์ที่เชื่อถือแล้วของผู้ใช้ เมื่อข้อมูลถูกเขียนไปยัง CloudKit กุญแจบันทึกทั้งหมดจะถูกสร้างขึ้นบนอุปกรณ์ที่เชื่อถือแล้วของผู้ใช้และจะถูกรวมเข้ากับลำดับชั้นกุญแจที่เหมาะสมก่อนที่ข้อมูลจะถูกอัปโหลด



บริการของ Apple จำนวนมากซึ่งแสดงในบทความบริการช่วยเหลือของ Apple ภาพรวมความปลอดภัยของข้อมูล iCloud ใช้การเข้ารหัสแบบต้นทางถึงปลายทางโดยที่กุญแจบริการ CloudKit ได้รับการปกป้องโดยการเชื่อมข้อมูลพวงกุญแจ iCloud สำหรับตัวบรรจุ CloudKit เหล่านี้ กุญแจบริการจะถูกจัดเก็บอยู่ในพวงกุญแจ iCloud ของผู้ใช้และแชร์ลักษณะความปลอดภัยของพวงกุญแจ iCloud โดยกุญแจบริการจะมีเฉพาะบนอุปกรณ์ที่เชื่อถือแล้วของผู้ใช้ และไม่สามารถเข้าถึงได้โดย Apple หรือบริษัทอื่นๆ ในกรณีที่อุปกรณ์สูญหาย ผู้ใช้สามารถกู้คืนข้อมูลพวงกุญแจ iCloud ของตนได้โดยใช้การกู้คืนพวงกุญแจ iCloud ที่ปลอดภัย ผู้ติดต่อการกู้คืนบัญชี หรือรหัสการกู้คืนบัญชี

การจัดการกุญแจการเข้ารหัส

ความปลอดภัยของข้อมูลที่เข้ารหัสใน CloudKit ขึ้นอยู่กับความปลอดภัยของกุญแจการเข้ารหัสที่สอดคล้องกัน กุญแจบริการ CloudKit แบ่งออกเป็นสองหมวดหมู่ ได้แก่ กุญแจที่เข้ารหัสแบบต้นทางถึงปลายทางและกุญแจที่มีให้ใช้หลังจากการตรวจสอบสิทธิ์

- **กุญแจบริการที่เข้ารหัสแบบต้นทางถึงปลายทาง:** สำหรับบริการ iCloud ที่เข้ารหัสแบบต้นทางถึงปลายทาง กุญแจส่วนตัวบริการ CloudKit ที่เกี่ยวข้องจะไม่ถูกทำให้มีใช้บนเซิร์ฟเวอร์ของ Apple คู่กุญแจบริการซึ่งรวมถึงกุญแจส่วนตัวจะถูกสร้างขึ้นภายในอุปกรณ์ที่เชื่อถือแล้วของผู้ใช้และถ่ายโอนไปยังอุปกรณ์อื่นๆ ของผู้ใช้โดยใช้ความปลอดภัยของพวงกุญแจ iCloud แม้ว่าการกู้คืนและความต่อเนื่องของการเชื่อมข้อมูลพวงกุญแจ iCloud จะดูแลโดยเซิร์ฟเวอร์ของ Apple เซิร์ฟเวอร์เหล่านี้จะถูกป้องกันในเชิงการเข้ารหัสเพื่อไม่ให้เข้าถึงข้อมูลพวงกุญแจของผู้ใช้ ในกรณีที่ร้ายแรงที่สุดของการสูญเสียการเข้าถึงพวงกุญแจ iCloud และกลไกการกู้คืนทั้งหมด ข้อมูลที่เข้ารหัสแบบต้นทางถึงปลายทางใน CloudKit จะสูญหาย Apple ไม่สามารถช่วยกู้คืนข้อมูลนี้ได้
- **กุญแจบริการที่มีให้ใช้หลังจากการตรวจสอบสิทธิ์:** สำหรับบริการอื่นๆ เช่น รูปภาพและ iCloud Drive กุญแจบริการจะถูกจัดเก็บอยู่ในโมดูลรักษาความปลอดภัยฮาร์ดแวร์ของ iCloud ในศูนย์ข้อมูลของ Apple และสามารถเข้าถึงได้จากบางบริการของ Apple เมื่อผู้ใช้ลงชื่อเข้า iCloud บนอุปกรณ์เครื่องใหม่และตรวจสอบสิทธิ์ Apple ID ของตน เซิร์ฟเวอร์ของ Apple จะเข้าถึงกุญแจเหล่านี้ได้โดยไม่ต้องมีการโต้ตอบหรือการป้อนข้อมูลเพิ่มเติมจากผู้ใช้ ตัวอย่างเช่น หลังจากลงชื่อเข้า iCloud.com ผู้ใช้สามารถดูรูปภาพของตนทางออนไลน์ได้ทันที กุญแจบริการเหล่านี้คือกุญแจที่**มีให้ใช้หลังจากการตรวจสอบสิทธิ์**

การปกป้องข้อมูลขั้นสูงสำหรับ iCloud

การปกป้องข้อมูลขั้นสูงสำหรับ iCloud เป็นการตั้งค่าแบบไม่บังคับที่ให้การปกป้องข้อมูลคลาวด์ระดับสูงสุดของ Apple เมื่อผู้ใช้เปิดใช้การปกป้องข้อมูลขั้นสูง อุปกรณ์ที่เชื่อถือแล้วของผู้ใช้จะยังคงมีสิทธิ์เพียงหนึ่งเดียวในการเข้าถึงกุญแจการเข้ารหัสสำหรับข้อมูล iCloud ส่วนใหญ่ของผู้ใช้ ดังนั้นข้อมูลนั้นจะได้รับการปกป้องด้วย**การเข้ารหัสแบบต้นทางถึงปลายทาง** สำหรับผู้ใช้ที่เปิดใช้การปกป้องข้อมูลขั้นสูง จำนวนหมวดหมู่ข้อมูลทั้งหมดที่มีการปกป้องโดยใช้การเข้ารหัสแบบต้นทางถึงปลายทางจะเพิ่มขึ้นจาก 14 เป็น 23 หมวดหมู่ และรวมข้อมูลสำรอง รูปภาพ โน้ต และอื่นๆ ของ iCloud

การปกป้องข้อมูลขั้นสูงสำหรับ iCloud จะมีให้ใช้งานสำหรับผู้ใช้ในสหรัฐอเมริกาก่อนสิ้นปี 2022 และจะเริ่มเผยแพร่ไปยังส่วนอื่นๆ ของโลกภายในต้นปี 2023

การปกป้องข้อมูลขั้นสูงมีแนวคิดที่เรียบง่าย: กุญแจบริการ CloudKit ทั้งหมดที่ถูกสร้างบนอุปกรณ์แล้วอัปโหลดไปยังโมดูลรักษาความปลอดภัยฮาร์ดแวร์ของ iCloud (HSM) ที่**มีให้ใช้หลังจากการตรวจสอบสิทธิ์**ในศูนย์ข้อมูลของ Apple จะถูกลบออกจาก HSM เหล่านั้นและจะถูกเก็บไว้ทั้งหมดภายในโดเมนการปกป้องพวงกุญแจ iCloud ของบัญชีแทน กุญแจบริการเหล่านี้จะมีการจัดการเหมือนกับกุญแจบริการที่**เข้ารหัสแบบต้นทางถึงปลายทาง**ซึ่งมีอยู่แล้ว ซึ่งหมายความว่า Apple จะไม่สามารถอ่านหรือเข้าถึงกุญแจเหล่านี้ได้อีกต่อไป

การปกป้องข้อมูลขั้นสูงยังปกป้องช่อง CloudKit ที่นักพัฒนาของบริษัทอื่นเลือกทำเครื่องหมายว่าเข้ารหัสแล้วและปกป้องแอสเซท CloudKit ทั้งหมดโดยอัตโนมัติอีกด้วย

การเปิดใช้งานการปกป้องข้อมูลขั้นสูง

เมื่อผู้ใช้เปิดใช้การปกป้องข้อมูลขั้นสูง อุปกรณ์ที่เชื่อถือแล้วของผู้ใช้จะดำเนินการสองอย่าง: อย่างแรก อุปกรณ์จะสื่อสารความตั้งใจของผู้ใช้ที่จะเปิดใช้การปกป้องข้อมูลขั้นสูงไปยังอุปกรณ์อื่นๆ ที่เข้าร่วมการเข้ารหัสแบบต้นทางถึงปลายทาง อุปกรณ์จะทำเช่นนั้นโดยเขียนค่าใหม่ ซึ่งลงชื่อโดยกุญแจภายในอุปกรณ์ ลงในเมตาดาต้าอุปกรณ์ของพวงกุญแจ iCloud เซิร์ฟเวอร์ของ Apple จะไม่สามารถเอาการรับรองนี้ออกหรือแก้ไขการรับรองนี้ได้ขณะที่การรับรองถูกเชื่อมข้อมูลกับอุปกรณ์อื่นๆ ของผู้ใช้

อย่างที่สอง อุปกรณ์จะเริ่มต้นการเอากุญแจบริการ**ที่มีให้ใช้หลังจากการตรวจสอบสิทธิ์**ออกจากศูนย์ข้อมูลของ Apple เนื่องจากกุญแจเหล่านี้มีการปกป้องโดย HSM ของ iCloud การลบนี้จะเป็นไปอย่างทันที ถาวร และไม่สามารถเพิกถอนได้ หลังจากที่กุญแจถูกลบ Apple จะไม่สามารถเข้าถึงข้อมูล**ใดๆ** ที่ปกป้องโดยกุญแจบริการของผู้ใช้ได้อีกต่อไป ในตอนนี้ อุปกรณ์จะเริ่มกระบวนการหมุนเวียนกุญแจแบบไม่ตรงกัน ซึ่งจะสร้างกุญแจบริการใหม่สำหรับแต่ละบริการที่มีกุญแจบนเซิร์ฟเวอร์ของ Apple ก่อนหน้านี้ ถ้าการหมุนเวียนกุญแจไม่สำเร็จเนื่องจากเครือข่ายถูกรบกวนหรือมีข้อผิดพลาดอื่นๆ อุปกรณ์จะพยายามหมุนเวียนกุญแจซ้ำๆ จนกว่าจะสำเร็จ

หลังจากหมุนเวียนกุญแจบริการสำเร็จ ข้อมูลใหม่ที่เขียนไปยังบริการจะไม่สามารถถอดรหัสได้ด้วยกุญแจบริการเก่า ข้อมูลจะได้รับการปกป้องด้วยกุญแจใหม่ที่ควบคุมโดยอุปกรณ์ที่เชื่อถือแล้วของผู้ใช้เท่านั้น และยังไม่เคยมีให้ Apple ใช้งาน

การปกป้องข้อมูลขั้นสูงและการเข้าถึงเว็บ iCloud.com

เมื่อผู้ใช้เปิดใช้การปกป้องข้อมูลขั้นสูงเป็นครั้งแรก การเข้าถึงเว็บไปยังข้อมูลของผู้ใช้ที่ iCloud.com จะถูกปิดใช้โดยอัตโนมัติ ที่เป็นเช่นนี้เนื่องจากเซิร์ฟเวอร์เว็บ iCloud ไม่สามารถเข้าถึงกุญแจที่ต้องใช้ในการถอดรหัสและแสดงข้อมูลของผู้ใช้ได้อีกต่อไป ผู้ใช้สามารถเลือกที่จะเปิดใช้การเข้าถึงเว็บอีกครั้ง และใช้การเข้าร่วมของอุปกรณ์ที่เชื่อถือแล้วของตนเพื่อเข้าถึงข้อมูล iCloud ของตนที่เข้ารหัสอยู่บนเว็บได้

หลังจากเปิดใช้การเข้าถึงเว็บแล้ว ผู้ใช้จะต้องอนุญาตการลงชื่อเข้าเว็บบนอุปกรณ์ที่เชื่อถือแล้วเครื่องใดเครื่องหนึ่งของตนทุกครั้งที่ผู้ใช้เยี่ยมชม iCloud.com การอนุญาตจะ “ปกป้อง” อุปกรณ์ในการเข้าถึงเว็บ ในอีกหนึ่งชั่วโมงถัดไป อุปกรณ์นี้จะยอมรับคำขอจากเซิร์ฟเวอร์ที่ระบุเฉพาะของ Apple เพื่ออัปโหลดกุญแจบริการแต่ละรายการ แต่จะจำกัดเฉพาะกุญแจที่สอดคล้องกับรายการอนุญาตของบริการที่เข้าถึงได้ตามปกติบน iCloud.com กล่าวอีกนัยหนึ่งคือ แม้ว่าผู้ใช้จะอนุญาตการลงชื่อเข้าเว็บแล้ว คำขอเซิร์ฟเวอร์จะไม่สามารถทำให้อุปกรณ์ของผู้ใช้อัปโหลดกุญแจบริการสำหรับข้อมูลที่ไม่ต้องการให้ดูบน iCloud.com ได้ (เช่น ข้อมูลสุขภาพหรือรหัสผ่านในพวงกุญแจ iCloud) เซิร์ฟเวอร์ของ Apple จะร้องขอเฉพาะกุญแจบริการที่จำเป็นในการถอดรหัสข้อมูลที่ระบุเฉพาะที่ผู้ใช้ร้องเข้าเพื่อเข้าถึงบนเว็บเท่านั้น ทุกครั้งที่มีการอัปโหลดกุญแจบริการ กุญแจจะถูกเข้ารหัสโดยใช้กุญแจชั่วคราวที่ผูกกับเซสชั่นเว็บที่ผู้ใช้อนุญาต และการแจ้งเตือนจะแสดงบนอุปกรณ์ของผู้ใช้ โดยจะแสดงบริการ iCloud ที่มีข้อมูลที่กำลังถูกทำให้มีให้ใช้งานแบบชั่วคราวบนเซิร์ฟเวอร์ของ Apple

การรักษาตัวเลือกของผู้ใช้

การตั้งค่าการปกป้องข้อมูลขั้นสูงและการเข้าถึงเว็บ iCloud.com สามารถแก้ไขได้โดยผู้ใช้เท่านั้น ค่าเหล่านี้จะถูกจัดเก็บในเมตาดาต้าอุปกรณ์ของพวงกุญแจ iCloud ของผู้ใช้และสามารถเปลี่ยนแปลงได้จากอุปกรณ์ที่เชื่อถือแล้วเครื่องใดเครื่องหนึ่งของผู้ใช้เท่านั้น เซิร์ฟเวอร์ของ Apple ไม่สามารถแก้ไขการตั้งค่าเหล่านี้ในนามของผู้ใช้ และไม่สามารถย้อนการตั้งค่ากลับเป็นการกำหนดค่าก่อนหน้าได้

ผลกระทบด้านความปลอดภัยของการแชร์และการใช้งานร่วมกัน

โดยส่วนใหญ่แล้ว เมื่อผู้ใช้แชร์เนื้อหาเพื่อใช้งานร่วมกัน ตัวอย่างเช่น ด้วยโน้ตที่แชร์ เตือนความจำที่แชร์ โฟลเดอร์ที่แชร์ใน iCloud Drive หรือคลังรูปภาพ iCloud ที่แชร์ และผู้ใช้ทุกรายได้เปิดใช้การปกป้องข้อมูลขั้นสูงไว้ เซิร์ฟเวอร์ของ Apple จะถูกใช้เพื่อสร้างการแชร์เท่านั้น แต่จะไม่สามารถเข้าถึงกุญแจการเข้ารหัสสำหรับข้อมูลที่แชร์ได้ เนื้อหาจะยังคงเข้ารหัสแบบต้นทางถึงปลายทางและเข้าถึงได้เฉพาะบนอุปกรณ์ที่เชื่อถือแล้วของผู้เข้าร่วมเท่านั้น สำหรับกระบวนการแชร์แต่ละรายการ Apple อาจจัดเก็บชื่อและรูปย่อแสดงแทนด้วยการปกป้องข้อมูลมาตรฐานเพื่อแสดงตัวอย่างสำหรับผู้ใช้ที่ได้รับ

การเลือกตัวเลือก “ทุกคนที่มีลิงก์” เมื่อเปิดใช้งานการใช้งานร่วมกันจะทำให้เนื้อหามีให้ใช้งานบนเซิร์ฟเวอร์ของ Apple ภายใต้การปกป้องข้อมูลมาตรฐาน เนื่องจากเซิร์ฟเวอร์จะต้องให้การเข้าถึงกับทุกคนที่เปิด URL

การใช้งาน iWork ร่วมกันและคุณสมบัติการแชร์อัลบั้มในรูปภาพไม่รองรับการปกป้องข้อมูลขั้นสูง เมื่อผู้ใช้ใช้งานร่วมกันบนเอกสาร iWork หรือเปิดเอกสาร iWork จากโฟลเดอร์ที่แชร์ใน iCloud Drive กุญแจการเข้ารหัสสำหรับเอกสารจะถูกอัปโหลดอย่างปลอดภัยไปยังเซิร์ฟเวอร์ของ iWork ในศูนย์ข้อมูลของ Apple ที่เป็นเช่นนี้เนื่องจากการใช้งานร่วมกันแบบเรียลไทม์ใน iWork ต้องใช้การดูแลจากฝั่งเซิร์ฟเวอร์เพื่อสร้างความสอดคล้องให้กับการเปลี่ยนแปลงเอกสารระหว่างผู้เข้าร่วม รูปภาพที่เพิ่มไปยังการแชร์อัลบั้มจะถูกจัดเก็บด้วยการปกป้องข้อมูลมาตรฐาน เนื่องจากคุณสมบัตินี้อนุญาตให้แชร์อัลบั้มแบบสาธารณะบนเว็บได้

การปิดใช้งานการปกป้องข้อมูลขั้นสูง

ผู้ใช้สามารถปิดใช้การปกป้องข้อมูลขั้นสูงได้ตลอดเวลา ถ้าผู้ใช้ต้องการทำเช่นนั้น:

1 ขั้นแรกอุปกรณ์ของผู้ใช้จะบันทึกตัวเลือกใหม่ในเมตาดาต้าการเข้าร่วมของพวงกุญแจ iCloud และการตั้งค่านี้จะเชื่อมข้อมูลอย่างปลอดภัยไปยังอุปกรณ์ทั้งหมดของผู้ใช้

2 อุปกรณ์ของผู้ใช้จะอัปโหลดกุญแจบริการสำหรับบริการทั้งหมด**ที่มีให้ใช้หลังจากการตรวจสอบสิทธิ์**ไปยัง HSM ของ iCloud ในศูนย์ข้อมูลของ Apple อย่างปลอดภัย กุญแจเหล่านี้ไม่รวมกุญแจสำหรับบริการที่เข้ารหัสแบบต้นทางถึงปลายทางภายใต้การปกป้องข้อมูลมาตรฐาน เช่น พวงกุญแจ iCloud และสุขภาพ

อุปกรณ์จะอัปโหลดทั้งกุญแจบริการดั้งเดิม ซึ่งสร้างขึ้นก่อนที่จะมีการเปิดใช้การปกป้องข้อมูลขั้นสูง และกุญแจบริการใหม่ที่สร้างขึ้นหลังจากที่ผู้ใช้เปิดใช้คุณสมบัติ การทำเช่นนี้จะทำให้ข้อมูลทั้งหมดในบริการเหล่านี้เข้าถึงได้หลังจากการตรวจสอบสิทธิ์และจะทำให้บัญชีกลับไปใช้การปกป้องข้อมูลมาตรฐาน ซึ่งจะทำให้ Apple สามารถช่วยเหลือผู้ใช้ในการกู้คืนข้อมูลส่วนใหญ่ได้อีกครั้งในกรณีที่ผู้ใช้สูญเสียการเข้าถึงบัญชีของตน

ข้อมูล iCloud ที่ไม่ได้รับความคุ้มครองจากการปกป้องข้อมูลขั้นสูง

เนื่องจากความจำเป็นในการใช้งานร่วมกับระบบอีเมล รายชื่อ และปฏิทินทั่วโลก เมล รายชื่อ และปฏิทิน iCloud จึงไม่มีการเข้ารหัสแบบต้นทางถึงปลายทาง

iCloud จัดเก็บข้อมูลบางส่วนโดยไม่มีการปกป้องจากกุญแจบริการ CloudKit เฉพาะผู้ใช้ แม้ว่าการปกป้องข้อมูลขั้นสูงจะเปิดใช้อยู่ ช่องบันทึก CloudKit จะต้องประกาศอย่างชัดแจ้งว่า “เข้ารหัสแล้ว” ในสคีมาของตัวบรรจุจึงจะได้รับการปกป้อง และการอ่านและเขียนช่องที่เข้ารหัสจำเป็นต้องใช้ API เฉพาะ วันที่และเวลาที่แก้ไขไฟล์หรือวัตถุจะถูกใช้เพื่อเรียงข้อมูลของผู้ใช้ และเช็คซัมของข้อมูลไฟล์และรูปภาพจะถูกใช้เพื่อช่วย Apple ลบรายการที่ซ้ำกันและปรับขนาดพื้นที่จัดเก็บข้อมูล iCloud และอุปกรณ์ของผู้ใช้ให้เหมาะสม ทั้งหมดนี้ทำได้โดยไม่ต้องเข้าถึงตัวไฟล์และรูปภาพเอง รายละเอียดเกี่ยวกับการใช้การเข้ารหัสสำหรับข้อมูลบางหมวดหมู่มีอยู่ในบทความบริการช่วยเหลือของ Apple ภาพรวมความปลอดภัยของข้อมูล iCloud

การตัดสินใจอย่างการใช้เช็คซัมเพื่อลบข้อมูลที่ซ้ำกัน ซึ่งเป็นเทคนิคที่รู้จักกันดีที่เรียกว่า**การเข้ารหัสแบบบรรจบกัน** เป็นส่วนหนึ่งของการออกแบบดั้งเดิมของบริการ iCloud เมื่อเปิดตัว เมตาดาต้านี้จะถูกเข้ารหัสเสมอ แต่ Apple จะจัดเก็บกุญแจการเข้ารหัสด้วยการปกป้องข้อมูลมาตรฐาน ในการเสริมความปลอดภัยให้กับผู้ใช้ทุกรายอย่างต่อเนื่อง Apple มุ่งมั่นที่จะทำให้มีการเข้ารหัสแบบต้นทางถึงปลายทางกับข้อมูลมากขึ้น ซึ่งรวมถึงเมตาดาต้าประเภทนี้เมื่อเปิดใช้การปกป้องข้อมูลขั้นสูง

ข้อกำหนดการปกป้องข้อมูลขั้นสูง

ข้อกำหนดในการเปิดใช้การปกป้องข้อมูลขั้นสูงสำหรับ iCloud มีดังนี้:

- บัญชีของผู้ใช้ต้องรองรับการเข้ารหัสแบบต้นทางถึงปลายทาง การเข้ารหัสแบบต้นทางถึงปลายทางต้องใช้การตรวจสอบสิทธิ์สองปัจจัยสำหรับ Apple ID และรหัสหรือรหัสผ่านของผู้ใช้ที่ตั้งค่าไว้บนอุปกรณ์ที่เชื่อถือแล้ว โปรดดูบทความบริการช่วยเหลือของ Apple การตรวจสอบสิทธิ์สองปัจจัยสำหรับ Apple ID
- อุปกรณ์ที่ผู้ใช้ลงชื่อเข้าด้วย Apple ID ของตัวเองจะต้องอัปเดตเป็น iOS 16.2, iPadOS 16.2, macOS 13.1, tvOS 16.2, watchOS 9.2 และ iCloud สำหรับ Windows เวอร์ชั่นล่าสุด ข้อกำหนดนี้จะป้องกันไม่ให้ iOS, iPadOS, macOS, tvOS หรือ watchOS เวอร์ชั่นก่อนหน้าจัดการกุญแจบริการที่เพิ่งสร้างขึ้นใหม่อย่างไม่ถูกต้องโดยอัปโหลดกุญแจเหล่านั้นซ้ำไปยัง HSM **ที่มีให้ใช้หลังจากการตรวจสอบสิทธิ์** ซึ่งเป็นความพยายามที่ผิดพลาดในการซ่อมแซมสถานะบัญชี
- ผู้ใช้จะต้องตั้งค่าวิธีการกู้คืนทางเลือกอย่างน้อยหนึ่งวิธี ไม่ว่าจะเป็นผู้ติดต่อการกู้คืนอย่างน้อยหนึ่งคนหรือรหัสการกู้คืนหนึ่งรหัส ซึ่งผู้ใช้สามารถใช้เพื่อกู้คืนข้อมูล iCloud ของตนได้หากสูญเสียการเข้าถึงบัญชี

ถ้าวิธีการกู้คืนไม่ได้ผล เช่น ถ้าข้อมูลของผู้ติดต่อการกู้คืนเก่าเกินไป หรือผู้ใช้ลืมวิธีการเหล่านั้น Apple จะไม่สามารถช่วยกู้คืนข้อมูล iCloud ที่เข้ารหัสแบบต้นทางถึงปลายทางของผู้ใช้ได้

การปกป้องข้อมูลขั้นสูงสำหรับ iCloud สามารถเปิดใช้ได้เฉพาะกับ Apple ID เท่านั้น ไม่รองรับ Apple ID ที่มีการจัดการและบัญชีบุตรหลาน (แตกต่างกันไปตามประเทศหรือภูมิภาค)

ความปลอดภัยของข้อมูลสำรอง iCloud

iCloud สำรองข้อมูลต่างๆ เช่น การตั้งค่าอุปกรณ์ ข้อมูลแอป รูปภาพและวิดีโอในม้วนฟิล์ม และการสนทนาในแอปข้อความ ทุกวันผ่าน Wi-Fi ข้อมูลสำรอง iCloud จะเกิดขึ้นก็ต่อเมื่ออุปกรณ์ล็อคอยู่ เชื่อมต่ออยู่กับแหล่งจ่ายไฟ และมีการเข้าถึงอินเทอร์เน็ตผ่าน Wi-Fi ข้อมูลสำรอง iCloud คำนึงถึงการเข้ารหัสพื้นที่จัดเก็บข้อมูลที่ใช้ใน iOS และ iPadOS จึงได้รับการออกแบบให้เก็บรักษาข้อมูลให้ปลอดภัยในขณะที่อนุญาตให้มีการสำรองข้อมูลและกู้คืนข้อมูลส่วนที่เพิ่มแบบที่ไม่ต้องจัดการ ตามค่าเริ่มต้นแล้ว กุญแจบริการข้อมูลสำรอง iCloud จะมีการสำรองข้อมูลอย่างปลอดภัยไปยังโมดูลรักษาความปลอดภัยฮาร์ดแวร์ของ iCloud ในศูนย์ข้อมูลของ Apple และเป็นส่วนหนึ่งของข้อมูลหมวดหมู่ที่มีให้ใช้หลังจากการตรวจสอบสิทธิ์ สำหรับผู้ใช้ที่เปิดใช้การปกป้องข้อมูลขั้นสูงสำหรับ iCloud กุญแจบริการข้อมูลสำรอง iCloud จะมีการปกป้องด้วยการเข้ารหัสแบบต้นทางถึงปลายทาง และมีให้ใช้เฉพาะบนอุปกรณ์ที่เชื่อถือแล้วของผู้ใช้เท่านั้น

เมื่อไฟล์ถูกสร้างในคลาสการปกป้องข้อมูลที่ไม่สามารถเข้าถึงได้เมื่ออุปกรณ์ล็อคอยู่ กุญแจรายไฟล์ของไฟล์เหล่านั้นจะถูกเข้ารหัสโดยใช้คลาสกุญแจจากกระเป๋ากุญแจ (Keybag) ข้อมูลสำรอง iCloud และสำรองข้อมูลไฟล์เหล่านั้นไปยัง iCloud ในสถานะดั้งเดิมที่เข้ารหัสแล้ว ไฟล์ทั้งหมดจะถูกเข้ารหัสในระหว่างการส่งข้าม และเมื่อถูกจัดเก็บ จะมีการเข้ารหัสโดยใช้กุญแจที่อิงตามบัญชี ตามที่ได้อธิบายไว้ในการเข้ารหัส CloudKit

กระเป๋ากุญแจ (Keybag) ข้อมูลสำรอง iCloud ประกอบด้วยกุญแจ (Curve25519) แบบไม่สมมาตรสำหรับคลาสการปกป้องข้อมูลที่ไม่สามารถเข้าถึงได้เมื่ออุปกรณ์ล็อคอยู่ ชุดการสำรองข้อมูลจะถูกจัดเก็บในบัญชี iCloud ของผู้ใช้ และประกอบด้วยสำเนาของไฟล์ของผู้ใช้ และกระเป๋ากุญแจ (Keybag) ข้อมูลสำรอง iCloud กระเป๋ากุญแจ (Keybag) ข้อมูลสำรอง iCloud จะถูกปกป้องด้วยกุญแจแบบสุ่ม ซึ่งจะได้รับการจัดเก็บพร้อมกับชุดการสำรองข้อมูลด้วยเช่นกัน รหัสผ่าน iCloud ของผู้ใช้ไม่ใช่รหัสผ่านสำหรับการเข้ารหัส ดังนั้นการเปลี่ยนแปลงรหัสผ่าน iCloud จะไม่ทำให้ข้อมูลสำรองที่มีอยู่ไม่สามารถใช้งานได้

เมื่อกู้คืน ไฟล์ที่ได้รับการสำรองข้อมูล กระเป๋ากุญแจ (Keybag) ข้อมูลสำรอง iCloud และกุญแจสำหรับกระเป๋ากุญแจ (Keybag) จะถูกดึงข้อมูลจากบัญชี iCloud ของผู้ใช้ กระเป๋ากุญแจ (Keybag) ข้อมูลสำรอง iCloud จะถูกถอดรหัสโดยใช้กุญแจของกระเป๋ากุญแจ (Keybag) จากนั้นกุญแจรายไฟล์ในกระเป๋ากุญแจ (Keybag) จะถูกใช้เพื่อถอดรหัสไฟล์ในชุดการสำรองข้อมูล ซึ่งจะถูกเขียนเป็นไฟล์ใหม่ไปยังระบบไฟล์ จึงเป็นการเข้ารหัสไฟล์เหล่านั้นใหม่ตามคลาสการปกป้องข้อมูล

เนื้อหาต่อไปนี้จะสำรองข้อมูลโดยใช้ข้อมูลสำรอง iCloud:

- บันทึกสำหรับเพลง ภาพยนตร์ รายการทีวี แอป และหนังสือที่ซื้อ ข้อมูลสำรอง iCloud ของผู้ใช้ประกอบด้วยข้อมูลเกี่ยวกับเนื้อหาที่ซื้อซึ่งแสดงอยู่บนอุปกรณ์ของผู้ใช้ แต่ไม่ใช่ตัวเนื้อหาที่ซื้อนั้นเอง เมื่อผู้ใช้กู้คืนจากข้อมูลสำรอง iCloud เนื้อหาที่ซื้อของผู้ใช้จะถูกดาวน์โหลดจาก iTunes Store, App Store, แอป Apple TV หรือ Apple Books โดยอัตโนมัติ เนื้อหาบางประเภทจะไม่ถูกดาวน์โหลดโดยอัตโนมัติในบางประเทศหรือภูมิภาค และสินค้าที่ซื้อก่อนหน้านี้อาจจะไม่มีให้บริการหากได้รับการคืนเงินแล้วหรือไม่มีสินค้าอยู่ในร้านที่เกี่ยวข้องแล้ว โดยประวัติการซื้อสินค้าแบบสมบูรณ์จะผูกกับ Apple ID ของผู้ใช้
- รูปภาพและวิดีโอบนอุปกรณ์ของผู้ใช้ โปรดทราบว่าถ้าผู้ใช้เปิดใช้ “รูปภาพ iCloud” ใน iOS 8.1, iPadOS 13.1 หรือ OS X 10.10.3 ขึ้นไป รูปภาพและวิดีโอของผู้ใช้จะถูกจัดเก็บบน iCloud อยู่แล้ว ดังนั้นรูปภาพและวิดีโอจะไม่ถูกรวมในข้อมูลสำรอง iCloud ของผู้ใช้
- รายชื่อ กิจกรรมปฏิทิน รายการเตือนความจำ และโน้ต
- การตั้งค่าอุปกรณ์
- ข้อมูลของแอป
- หน้าจอโฮมและการจัดระเบียบแอป
- การกำหนดค่า HomeKit
- ข้อมูล ID ทางแพทย์
- รหัสผ่านเสียงบันทึก (หากจำเป็น ต้องใช้ซิมการ์ดจริงที่ใช้ในระหว่างสำรองข้อมูล)
- ข้อความ, Apple Messages for Business, ข้อความ (SMS) และข้อความ MMS (หากจำเป็น ต้องใช้ซิมการ์ดจริงที่ใช้ระหว่างสำรองข้อมูล)

ข้อมูลสำรอง iCloud ยังใช้เพื่อสำรองข้อมูลพวงกุญแจภายในอุปกรณ์ ซึ่งเข้ารหัสด้วยกุญแจที่ได้จากกุญแจการเข้ารหัสราก UID ของ Secure Enclave ของอุปกรณ์อีกด้วย กุญแจนี้เป็นกุญแจเฉพาะอุปกรณ์และ Apple จะไม่สามารถทราบได้ ซึ่งจะทำให้สามารถกู้คืนฐานข้อมูลไปยังอุปกรณ์เครื่องเดียวกับที่สร้างฐานข้อมูลขึ้นมาเท่านั้นได้ และหมายความว่าคนอื่นซึ่งรวมถึง Apple ไม่สามารถอ่านได้ โปรดดูที่ Secure Enclave สำหรับข้อมูลเพิ่มเติม

แอปข้อความบน iCloud

ข้อความบน iCloud ช่วยทำให้ประวัติข้อความทั้งหมดของผู้ใช้อัปเดตและมีให้ใช้งานบนอุปกรณ์ทั้งหมดเสมอ

ด้วยการปกป้องข้อมูลมาตรฐาน ข้อความบน iCloud มีการเข้ารหัสแบบต้นทางถึงปลายทางเมื่อปิดใช้ข้อมูลสำรอง iCloud เมื่อเปิดใช้ข้อมูลสำรอง iCloud ข้อมูลสำรองจะมีสำเนากุญแจการเข้ารหัสของข้อความบน iCloud ดังนั้น Apple จึงสามารถช่วยผู้ใช้กู้คืนข้อความได้แม้ว่าผู้ใช้จะสูญเสียการเข้าถึงพวงกุญแจ iCloud และอุปกรณ์ที่เชื่อถือแล้วของตน ถ้าผู้ใช้ปิดใช้ข้อมูลสำรอง iCloud กุญแจใหม่จะถูกสร้างขึ้นบนอุปกรณ์ของผู้ใช้เพื่อปกป้องข้อความบน iCloud ในอนาคต กุญแจใหม่จะถูกจัดเก็บในพวงกุญแจ iCloud เท่านั้น ซึ่งผู้ใช้สามารถเข้าถึงได้เฉพาะบนอุปกรณ์ที่เชื่อถือแล้วของตน และข้อมูลใหม่ที่เขียนไปยังตัวบรรจุจะไม่สามารถถอดรหัสได้ด้วยกุญแจตัวบรรจุเก่า

ด้วยการปกป้องข้อมูลขั้นสูง ข้อความบน iCloud จะเข้ารหัสแบบต้นทางถึงปลายทางเสมอ เมื่อเปิดใช้ข้อมูลสำรอง iCloud ทุกอย่างที่อยู่ภายในจะเข้ารหัสแบบต้นทางถึงปลายทาง ซึ่งรวมถึงกุญแจการเข้ารหัสข้อความบน iCloud กุญแจบริการข้อมูลสำรอง iCloud รวมถึงกุญแจตัวบรรจุข้อความบน iCloud จะถูกสร้างขึ้นทั้งสองรายการเมื่อผู้ใช้เปิดใช้การปกป้องข้อมูลขั้นสูง โปรดดูบทความบริการช่วยเหลือของ Apple ภาพรวมความปลอดภัยของข้อมูล iCloud สำหรับข้อมูลเพิ่มเติม

ความปลอดภัยของผู้ติดต่อการกู้คืนบัญชี

ผู้ใช้สามารถเพิ่มผู้คนที่พวกเขาไว้วางใจได้สูงสุดห้าคนเป็นผู้ติดต่อการกู้คืนบัญชี เพื่อช่วยพวกเขากู้คืนบัญชีและข้อมูล iCloud รวมถึงข้อมูลทั้งหมดที่เข้ารหัสแบบต้นทางถึงปลายทาง ไม่ว่าผู้ใช้จะเปิดใช้การปกป้องข้อมูลขั้นสูงไว้หรือไม่ก็ตาม ทั้ง Apple และผู้ติดต่อการกู้คืนบัญชีจะไม่มีข้อมูลที่จำเป็นส่วนบุคคลที่ใช้ในการกู้คืนข้อมูล iCloud ที่เข้ารหัสแบบต้นทางถึงปลายทางของผู้ใช้

ผู้ติดต่อการกู้คืนได้รับการออกแบบโดยคำนึงถึงความเป็นส่วนตัวของผู้ใช้ Apple จะไม่ทราบผู้ติดต่อการกู้คืนที่เลือกไว้ของผู้ใช้ เซิร์ฟเวอร์ของ Apple จะเรียนรู้ข้อมูลเกี่ยวกับผู้ติดต่อการกู้คืนในช่วงท้ายของความพยายามในการกู้คืนเท่านั้น หลังจากที่ผู้ใช้ขอความช่วยเหลือจากผู้ติดต่อและผู้ติดต่อได้เริ่มให้ความช่วยเหลือเกี่ยวกับการกู้คืนจริงๆ ข้อมูลนั้นจะไม่ถูกเก็บรักษาไว้หลังจากที่การกู้คืนเสร็จสิ้น

กระบวนการด้านความปลอดภัยของผู้ติดต่อการกู้คืนบัญชี

เมื่อผู้ใช้ตั้งค่าผู้ติดต่อการกู้คืนบัญชี กุญแจที่เข้าถึงข้อมูล iCloud ของผู้ใช้ ซึ่งรวมถึงข้อมูล CloudKit ที่เข้ารหัสแบบต้นทางถึงปลายทาง จะถูกเข้ารหัสด้วยกุญแจแบบสุ่มที่ปลอดภัยสูง จากนั้นกุญแจแบบสุ่มนี้จะถูกแยกระหว่างผู้ติดต่อการกู้คืนและ Apple เมื่อถึงเวลากู้คืน การกู้คืนกุญแจดั้งเดิมและการเข้าถึงข้อมูล iCloud ของผู้ใช้จะทำได้ก็ต่อเมื่อส่วนของกุญแจทั้งสองถูกรวมเข้าด้วยกันอีกครั้ง

ในการตั้งค่าผู้ติดต่อการกู้คืนบัญชี อุปกรณ์ของผู้ใช้จะสื่อสารกับเซิร์ฟเวอร์ของ Apple เพื่ออัปโหลดส่วนของข้อมูลกุญแจที่ Apple จะถือ จากนั้นอุปกรณ์จะสร้างตัวบรรจุ CloudKit ที่เข้ารหัสแบบต้นทางถึงปลายทางกับผู้ติดต่อการกู้คืนเพื่อแชร์ส่วนที่ผู้ติดต่อการกู้คืนต้องใช้ ทั้ง Apple และผู้ติดต่อการกู้คืนยังได้รับความลับการอนุญาตเดียวกันจากผู้ใช้ ซึ่งจะต้องใช้ในภายหลังสำหรับการกู้คืนอีกด้วย การสื่อสารเพื่อเชิญและยอมรับผู้ติดต่อการกู้คืนจะเกิดขึ้นผ่านช่องทาง IDS ที่มีการตรวจสอบสิทธิ์ร่วมกัน ผู้ติดต่อการกู้คืนจะจัดเก็บข้อมูลที่ได้รับไว้ในพวงกุญแจ iCloud โดยอัตโนมัติ Apple ไม่สามารถเข้าถึงได้ทั้งเนื้อหาของตัวบรรจุ CloudKit หรือพวงกุญแจ iCloud ที่จัดเก็บข้อมูลนี้ เมื่อดำเนินการแชร์ เซิร์ฟเวอร์ของ Apple จะดูเฉพาะ ID ที่ไม่ระบุตัวตนสำหรับผู้ติดต่อการกู้คืน

หลังจากนั้น เมื่อผู้ใช้ต้องการกู้คืนบัญชีและข้อมูล iCloud พวกเขาสามารถขอความช่วยเหลือจากผู้ติดต่อการกู้คืนได้ ในเวลานั้น รหัสการกู้คืนจะถูกสร้างขึ้นโดยอุปกรณ์ของผู้ติดต่อการกู้คืน ซึ่งผู้ติดต่อการกู้คืนจะมอบให้กับผู้ใช้โดยไม่ผ่านย่านความถี่ (ตัวอย่างเช่น มอบให้ตัวต่อตัว หรือบอกทางโทรศัพท์) จากนั้นผู้ใช้จะป้อนรหัสการกู้คืนบนอุปกรณ์ของตนเพื่อสร้างการเชื่อมต่อที่ปลอดภัยระหว่างอุปกรณ์ต่างๆ โดยใช้โปรโตคอล SPAKE2+ ซึ่งมีเนื้อหาที่ Apple ไม่สามารถเข้าถึงได้ การโต้ตอบนี้จัดทำโดยเซิร์ฟเวอร์ของ Apple แต่ Apple จะไม่สามารถเริ่มกระบวนการกู้คืนได้

หลังจากสร้างการเชื่อมต่อที่ปลอดภัยและทำการตรวจสอบความปลอดภัยที่จำเป็นทั้งหมดเสร็จสิ้นแล้ว อุปกรณ์ของผู้ติดต่อการกู้คืนจะส่งคืนส่วนของข้อมูลกุญแจของตัวเองและความลับการอนุญาตที่สร้างไว้ก่อนหน้านี้กลับไปยังผู้ใช้ที่ร้องขอการกู้คืน ผู้ใช้จะแสดงความลับการอนุญาตนี้กับเซิร์ฟเวอร์ของ Apple ซึ่งจะอนุญาตการเข้าถึงข้อมูลกุญแจที่ Apple เก็บไว้อยู่ การมอบความลับการอนุญาตยังเป็นการอนุญาตให้รีเซ็ตรหัสผ่านบัญชีเพื่อกู้คืนการเข้าถึงบัญชีอีกด้วย

สุดท้าย อุปกรณ์ของผู้ใช้จะรวมข้อมูลกุญแจที่ได้รับจาก Apple และผู้ติดต่อการกู้คืนบัญชีเข้าด้วยกันอีกครั้ง จากนั้นจะใช้ข้อมูลกุญแจนี้เพื่อถอดรหัสและกู้คืนข้อมูล iCloud

กระบวนการนี้มีมาตรการที่ป้องกันไม่ให้ผู้ติดต่อการกู้คืนเริ่มต้นการกู้คืนโดยไม่ได้รับความยินยอมจากผู้ใช้ ซึ่งรวมถึงการพิสูจน์ความเป็นบุคคลกับบัญชีของผู้ใช้ ถ้าบัญชีมีการใช้งานอยู่ การกู้คืนโดยใช้ผู้ติดต่อการกู้คืนยังต้องทราบรหัสอุปกรณ์ล่าสุดหรือรหัสความปลอดภัย iCloud อีกด้วย

ความปลอดภัยของผู้ติดต่อรับมรดก

ถ้าผู้ใช้ต้องการให้ผู้รับผลประโยชน์ที่กำหนดไว้สามารถเข้าถึงข้อมูล iCloud ของตนได้หลังจากที่ผู้ใช้ถึงแก่กรรมแล้ว ผู้ใช้สามารถตั้งค่าผู้ติดต่อรับมรดกในบัญชีของตนได้ ผู้รับผลประโยชน์ที่เป็นผู้ติดต่อรับมรดกจะได้รับสิทธิ์การเข้าถึงข้อมูล iCloud ทั้งหมดของผู้ถึงแก่กรรม ซึ่งรวมถึงข้อมูลที่เข้ารหัสแบบต้นทางถึงปลายทางเกือบทั้งหมด ยกเว้นข้อมูลพวงกุญแจ iCloud อย่างรหัสผ่านบัญชี เทคโนโลยีที่เป็นพื้นฐานของผู้ติดต่อรับมรดกนั้นคล้ายคลึงกับวิธีการทำงานของผู้ติดต่อการกู้คืน โดยประกอบด้วยกุญแจแบบสุ่มที่ปลอดภัยสูงซึ่งถูกแยกระหว่าง Apple และผู้ติดต่อรับมรดก ดังนั้นจึงไม่มีฝ่ายใดสามารถถอดรหัสข้อมูลใดๆ ได้ด้วยตัวเอง ผู้รับผลประโยชน์จะได้รับข้อมูลคลาสเดียวกันไม่ว่าผู้ใช้จะเปิดใช้การปกป้องข้อมูลขั้นสูงไว้หรือไม่ก็ตาม

ข้อมูลกุญแจที่ผู้รับผลประโยชน์จะได้รับนั้นเรียกว่ากุญแจการเข้าถึงในเอกสารประกอบสำหรับผู้ใช้ปลายทาง และจะถูกบันทึกโดยอัตโนมัติบนอุปกรณ์ที่รองรับ แต่ยังสามารถพิมพ์และจัดเก็บแบบออฟไลน์เพื่อใช้งานได้อีกด้วย โปรดดูบทความบริการช่วยเหลือของ Apple วิธีเพิ่มผู้ติดต่อรับมรดกสำหรับ Apple ID ของคุณสำหรับข้อมูลเพิ่มเติม

หลังจากผู้ใช้ถึงแก่กรรมแล้ว ผู้ติดต่อรับมรดกจะลงชื่อเข้าเว็บไซต์การอ้างสิทธิ์ของ Apple เพื่อเริ่มการเข้าถึง กระบวนการนี้ต้องใช้ใบมรณบัตรและมีการอนุญาตบางส่วนด้วยความลับการอนุญาตที่กล่าวถึงในส่วนที่แล้ว หลังจากที่การตรวจสอบความปลอดภัยทั้งหมดเสร็จสิ้นแล้ว Apple จะออกชื่อผู้ใช้และรหัสผ่านสำหรับบัญชีใหม่และเปิดเผยข้อมูลกุญแจที่จำเป็นกับผู้ติดต่อรับมรดก

ในการป้อนกุญแจการเข้าถึงได้ง่ายขึ้นเมื่อจำเป็น กุญแจจะแสดงเป็นรหัสตัวเลขและตัวอักษรพร้อมคิวอาร์โค้ดที่เกี่ยวข้อง หลังจากป้อนกุญแจการเข้าถึงแล้ว การเข้าถึงข้อมูล iCloud ของผู้ถึงแก่กรรมจะถูกกู้คืน ซึ่งสามารถดำเนินการได้บนอุปกรณ์หรือสร้างการเข้าถึงผ่านออนไลน์ได้ โปรดดูบทความบริการช่วยเหลือของ Apple ขอรับสิทธิ์การเข้าถึงบัญชี Apple ในฐานะผู้ติดต่อรับมรดกสำหรับข้อมูลเพิ่มเติม

ความปลอดภัยของ iCloud Private Relay

iCloud Private Relay ช่วยปกป้องผู้ใช้เมื่อเรียกดูเว็บด้วย Safari เป็นหลัก แต่ยังมีคำขอแก้ไขชื่อ DNS ทั้งหมดอีกด้วย วิธีนี้ช่วยให้แน่ใจว่าจะไม่มีฝ่ายหนึ่งฝ่ายใดแม้แต่ Apple ที่สามารถเชื่อมโยงที่อยู่ IP และกิจกรรมการท่องเว็บของผู้ใช้ได้ ซึ่งทำได้โดยใช้พร็อกซี่ที่แตกต่างกัน นั่นคือ พร็อกซี่ขาเข้าที่จัดการโดย Apple และพร็อกซี่ขาออกที่จัดการโดยผู้ให้บริการเนื้อหา ในการใช้ iCloud Private Relay ผู้ใช้ต้องใช้งาน iOS 15, iPadOS 15 หรือ macOS 12.0.1 ขึ้นไป และลงชื่อเข้าบัญชี iCloud+ ด้วย Apple ID ของตน จากนั้นสามารถเปิดใช้ iCloud Private Relay ได้ใน การตั้งค่า > iCloud หรือ การตั้งค่าระบบ > iCloud

โปรดดูที่ภาพรวม iCloud Private Relay สำหรับข้อมูลเพิ่มเติม

การจัดการรหัสและรหัสผ่าน

ภาพรวมความปลอดภัยของรหัสผ่าน

iOS, iPadOS และ macOS ทำให้ผู้ใช้สามารถตรวจสอบสิทธิ์เพื่อเข้าใช้แอปของบริษัทอื่นและเข้าถึงเว็บไซต์ที่ใช้รหัสผ่านได้ง่ายขึ้น วิธีที่ดีที่สุดในการจัดการรหัสผ่านคือการไม่จำเป็นต้องใช้รหัสผ่าน คุณสมบัติลงชื่อเข้าด้วย Apple ช่วยให้ผู้ใช้ลงชื่อเข้าแอปของบริษัทอื่นและเว็บไซต์ต่างๆ ได้โดยไม่ต้องสร้างและจัดการบัญชีหรือรหัสผ่าน เพิ่มเติมในขณะที่ปกป้องการลงชื่อเข้าด้วยการตรวจสอบสิทธิ์สองปัจจัยสำหรับ Apple ID สำหรับไซต์ที่ไม่รองรับลงชื่อเข้าด้วย Apple คุณสมบัติรหัสผ่านที่ปลอดภัยสูงแบบอัตโนมัติจะทำให้อุปกรณ์ของผู้ใช้สามารถสร้าง เชื่อมข้อมูล และป้อนรหัสผ่านที่ปลอดภัยสูงแบบไม่ซ้ำกันสำหรับไซต์และแอปได้โดยอัตโนมัติ ใน iOS และ iPadOS รหัสผ่านจะถูกบันทึกไปยังพวงกุญแจการป้อนรหัสผ่านอัตโนมัติแบบพิเศษที่สามารถจัดการและควบคุมได้โดยไปที่การตั้งค่า > รหัสผ่าน

ใน macOS รหัสผ่านที่บันทึกไว้สามารถจัดการได้ในการตั้งค่ารหัสผ่านของ Safari ระบบเชื่อมข้อมูลนี้ยังสามารถใช้เชื่อมข้อมูลรหัสผ่านที่ผู้ใช้สร้างเองได้อีกด้วย

ความปลอดภัยของลงชื่อเข้าด้วย Apple ID

ลงชื่อเข้าด้วย Apple เป็นทางเลือกที่มีความเป็นส่วนตัวมากกว่าระบบการลงชื่อเข้าครั้งเดียวแบบอื่นๆ ซึ่งมอบความสะดวกสบายและประสิทธิภาพจากการลงชื่อเข้าด้วยการแตะเพียงครั้งเดียว ขณะเดียวกันก็ให้ความความโปร่งใสและความสามารถในการควบคุมข้อมูลส่วนบุคคลของผู้ใช้ที่มากขึ้น

ลงชื่อเข้าด้วย Apple ช่วยให้ผู้ใช้ตั้งค่าบัญชีและลงชื่อเข้าแอปและเว็บไซต์ได้โดยใช้ Apple ID ที่ผู้ใช้มีอยู่แล้ว และช่วยให้ผู้ใช้ควบคุมข้อมูลส่วนบุคคลของตนได้มากยิ่งขึ้น แอปสามารถถามแค่ชื่อและที่อยู่อีเมลของผู้ใช้เมื่อตั้งค่าบัญชีได้ และผู้ใช้สามารถเลือกได้เสมอว่า พวกเขาจะแชร์ที่อยู่อีเมลส่วนบุคคลของตัวเองกับแอป หรือเลือกที่จะไม่เปิดเผยที่อยู่อีเมลส่วนบุคคลของตน แล้วใช้บริการส่งต่ออีเมลส่วนตัวของ Apple ที่เป็นบริการใหม่แทน บริการส่งต่ออีเมลนี้จะแชร์ที่อยู่อีเมลที่ไม่ระบุชื่อและไม่ซ้ำกัน ซึ่งจะส่งต่อไปยังที่อยู่อีเมลส่วนบุคคลของผู้ใช้เพื่อให้ผู้ใช้ยังคงได้รับการติดต่อที่เป็นประโยชน์จากนักพัฒนา แต่ก็ยังรักษาระดับความเป็นส่วนตัวและการควบคุมเหนือข้อมูลส่วนบุคคลของตัวเอง

ลงชื่อเข้าด้วย Apple สร้างขึ้นเพื่อความปลอดภัย ผู้ใช้ทุกคนที่ใช้ลงชื่อเข้าด้วย Apple จะต้องเปิดใช้งานการตรวจสอบสิทธิ์สองปัจจัยไว้สำหรับ Apple ID ของตน การตรวจสอบสิทธิ์สองปัจจัยไม่เพียงช่วยรักษาความปลอดภัยของ Apple ID ของผู้ใช้ แต่ยังช่วยรักษาความปลอดภัยของบัญชีที่ผู้ใช้ตั้งค่าไว้กับแอปอีกด้วย นอกจากนี้ Apple ได้พัฒนาและรวมสัญญาณป้องกันการหลอกลวงที่รักษาความเป็นส่วนตัวเข้ากับลงชื่อเข้าด้วย Apple ด้วย สัญญาณนี้ช่วยให้นักพัฒนามั่นใจได้ว่าผู้ใช้รายใหม่ของพวกเขาเป็นคนจริงๆ ไม่ใช่บอตหรือบัญชีที่เขียนขึ้น

รหัสผ่านที่ปลอดภัยสูงแบบอัตโนมัติ

เมื่อเปิดใช้งานพวงกุญแจ iCloud แล้ว iOS, iPadOS และ macOS จะสร้างรหัสผ่านแบบสุ่มที่ปลอดภัยสูงและไม่ซ้ำกันเมื่อผู้ใช้ลงทะเบียนหรือเปลี่ยนรหัสผ่านของตนบนเว็บไซต์ใน Safari ใน iOS และ iPadOS การสร้างรหัสผ่านที่ปลอดภัยสูงแบบอัตโนมัติยังมีให้ใช้ในแอปอีกด้วย โดยผู้ใช้ต้องไม่ใช้รหัสผ่านที่ปลอดภัยสูง รหัสผ่านที่สร้างจะบันทึกอยู่ในพวงกุญแจและอัปเดตอยู่เสมอบนอุปกรณ์ทุกเครื่องด้วยพวงกุญแจ iCloud เมื่อเปิดใช้งานอยู่

ตามค่าเริ่มต้นแล้ว รหัสผ่านที่สร้างโดย iOS และ iPadOS จะมีอักขระ 20 ตัว ซึ่งประกอบไปด้วยตัวเลขหนึ่งตัว อักขระตัวพิมพ์ใหญ่หนึ่งตัว เครื่องหมายขีดสั้นสองขีด และอักขระตัวพิมพ์เล็ก 16 ตัว รหัสผ่านที่สร้างเหล่านี้มีความปลอดภัยสูง โดยประกอบด้วย Entropy 71 บิต

รหัสผ่านถูกสร้างขึ้นโดยอิงจากการตรวจจับที่พิจารณาว่าประสบการณ์ช่องรหัสผ่านใช้สำหรับการสร้างรหัสผ่านหรือไม่ ถ้าการตรวจจับไม่รู้จักรหัสผ่านเฉพาะบริบทที่ใช้ในระหว่างการสร้างรหัสผ่าน นักพัฒนาแอปสามารถตั้งค่า `UITextContentType.newPassword` บนช่องข้อความได้ และนักพัฒนาเว็บก็สามารถตั้งค่า `autocomplete= “new-password”` บนองค์ประกอบ <input> ได้

แอปและเว็บไซต์สามารถกำหนดกฎเกณฑ์เพื่อช่วยให้แน่ใจว่ารหัสผ่านที่สร้างสามารถใช้งานร่วมกับบริการที่เกี่ยวข้องได้ นักพัฒนากำหนดกฎเกณฑ์เหล่านี้โดยใช้ `UITextInputPasswordRules` หรือคุณลักษณะ `passwordrules` บนองค์ประกอบ input จากนั้นอุปกรณ์จะสร้างรหัสผ่านที่ปลอดภัยที่สุดเพื่อให้เป็นไปตามกฎเกณฑ์เหล่านี้อย่างสมบูรณ์

ความปลอดภัยของการป้อนรหัสผ่านอัตโนมัติ

การป้อนรหัสผ่านอัตโนมัติจะป้อนเอกสารสิทธิ์ที่จัดเก็บอยู่ในพวงกุญแจโดยอัตโนมัติ ตัวจัดการรหัสผ่านสำหรับพวงกุญแจ iCloud และการป้อนรหัสผ่านอัตโนมัติจะมีคุณสมบัติต่อไปนี้:

- การป้อนเอกสารสิทธิ์ในแอปและเว็บไซต์
- การสร้างรหัสผ่านที่ปลอดภัยสูง
- การบันทึกรหัสผ่านทั้งในแอปและเว็บไซต์ใน Safari
- การแชร์รหัสผ่านอย่างปลอดภัยกับรายชื่อติดต่อของผู้ใช้
- การให้รหัสผ่านกับ Apple TV ในบริเวณใกล้เคียงที่ร้องขอเอกสารสิทธิ์

การสร้างและการบันทึกรหัสผ่านภายในแอป รวมถึงการให้รหัสผ่านกับ Apple TV จะมีให้ใช้ใน iOS และ iPadOS เท่านั้น

การป้อนรหัสผ่านอัตโนมัติในแอป

iOS และ iPadOS ช่วยให้ผู้ใช้สามารถป้อนชื่อและรหัสผ่านผู้ใช้ที่บันทึกไว้ลงในช่องที่เกี่ยวกับเอกสารสิทธิ์ในแอปได้ ซึ่งคล้ายกับวิธีการทำงานของการป้อนรหัสผ่านอัตโนมัติใน Safari ใน iOS และ iPadOS ผู้ใช้จะแตะรูปกุญแจในแถบ QuickType ของแป้นพิมพ์ซอฟต์แวร์ ใน macOS สำหรับแอปที่สร้างด้วย Mac Catalyst เมนูรหัสผ่านแบบเลื่อนลงจะแสดงใต้ช่องที่เกี่ยวกับเอกสารสิทธิ์

เมื่อแอปมีการเชื่อมโยงอย่างเหนียวแน่นกับเว็บไซต์ที่ใช้กลไกการเชื่อมโยงระหว่างแอปกับเว็บไซต์แบบเดียวกัน และดำเนินการโดยไฟล์การเชื่อมโยงเว็บไซต์กับแอปของ Apple ไฟล์เดียวกัน แถบ QuickType ของ iOS และ iPadOS และเมนูแบบเลื่อนลงของ macOS จะแนะนำเอกสารสิทธิ์สำหรับแอปนั้นโดยตรงหากมีเอกสารสิทธิ์ใดๆ ที่ถูกบันทึกไปยังพวงกุญแจการป้อนรหัสผ่านอัตโนมัติ วิธีนี้ช่วยให้ผู้ใช้สามารถเลือกเปิดเผยเอกสารสิทธิ์ที่บันทึกโดย Safari ไปยังแอปที่ใช้คุณสมบัติความปลอดภัยแบบเดียวกันได้โดยที่แอปเหล่านั้นไม่ต้องใช้ API

การป้อนรหัสผ่านอัตโนมัติจะไม่เปิดเผยเอกสารสิทธิ์ให้กับแอปจนกว่าผู้ใช้จะยินยอมปล่อยเอกสารสิทธิ์ให้กับแอปนั้น รายการเอกสารสิทธิ์จะถูกเรียกใช้จากหรือแสดงภายนอกกระบวนการของแอป

เมื่อแอปและเว็บไซต์มีความสัมพันธ์ที่เชื่อถือแล้ว และผู้ใช้ส่งเอกสารสิทธิ์ภายในแอปแล้ว iOS และ iPadOS อาจจะแจ้งให้ผู้ใช้บันทึกเอกสารสิทธิ์เหล่านั้นไปยังพวงกุญแจการป้อนรหัสผ่านอัตโนมัติสำหรับใช้ในภายหลัง

การเข้าถึงของแอปไปยังรหัสผ่านที่บันทึกไว้

แอป iOS, iPadOS และ macOS สามารถขอความช่วยเหลือจากพวงกุญแจการป้อนรหัสผ่านอัตโนมัติในการลงชื่อเข้าได้โดยใช้ `ASAuthorizationPasswordProvider` และ `SecAddSharedWebCredential` ตัวกำหนดรหัสผ่านและคำขอของตัวกำหนดรหัสผ่านสามารถใช้ร่วมกับลงชื่อเข้าด้วย Apple ได้ เพื่อให้มีการเรียก API ตัวเดียวกันเพื่อช่วยเหลือผู้ใช้ลงชื่อเข้าแอปไม่ว่าบัญชีของผู้ใช้จะอิงรหัสผ่านหรือไม่ก็ตาม หรือไม่ว่าบัญชีนั้นจะสร้างโดยใช้ลงชื่อเข้าด้วย Apple หรือไม่ก็ตาม

แอปสามารถเข้าถึงรหัสผ่านที่บันทึกไว้ได้ต่อเมื่อนักพัฒนาแอปและผู้ดูแลระบบเว็บไซต์ได้ให้อนุญาตแล้ว และผู้ใช้ได้ให้ความยินยอมแล้ว นักพัฒนาแอปแสดงความตั้งใจเข้าใช้งานรหัสผ่าน Safari ที่บันทึกไว้โดยการใส่สิทธิ์ในแอปของตน สิทธิ์จะแสดงรายชื่อโดเมนของเว็บไซต์ที่เกี่ยวข้องที่มีคุณสมบัติอย่างครบถ้วน และเว็บไซต์จะต้องวางไฟล์บนเซิร์ฟเวอร์ของตัวเองที่แสดงข้อมูลจำเพาะที่ไม่ซ้ำกันของแอปที่ Apple อนุญาต

เมื่อติดตั้งแอปที่มีสิทธิ์ com.apple.developer.associated-domains ระบบ iOS และ iPadOS จะส่งคำขอ TLS ไปที่เว็บไซต์แต่ละเว็บในรายการ และร้องขอหนึ่งในไฟล์ต่อไปนี้:

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

ถ้าไฟล์ดังกล่าวแสดงรายการข้อมูลจำเพาะของแอปที่ติดตั้ง ระบบ iOS และ iPadOS จะทำเครื่องหมายเว็บไซต์และแอปว่ามีความสัมพันธ์ที่เชื่อถือแล้ว การเรียก API สองตัวนี้จากความสัมพันธ์ที่เชื่อถือแล้วเท่านั้นที่จะส่งผลให้มีการแจ้งไปยังผู้ใช้ ซึ่งจะต้องให้การยินยอมก่อนที่รหัสผ่านใดๆ จะถูกปล่อยไปยังแอป ถูกอัปเดต หรือถูกลบ

คำแนะนำสำหรับความปลอดภัยของรหัสผ่าน

รายการรหัสผ่านของการป้อนรหัสผ่านอัตโนมัติใน iOS, iPadOS และ macOS จะระบุว่ารหัสผ่านใดที่ผู้ใช้บันทึกไว้จะถูก**นำกลับมาใช้ซ้ำ**กับเว็บไซต์อื่น รหัสผ่านใดที่ถือว่า**ปลอดภัยต่ำ** และรหัสผ่านใดที่เกิด**การรั่วไหลของข้อมูล**

ภาพรวม

การใช้รหัสผ่านเดียวกันกับบริการมากกว่าหนึ่งบริการอาจจะทำให้บัญชีเหล่านั้นเสี่ยงต่อการโจมตีเอกสารสิทธิ์แบบ Stuffing ถ้าบริการถูกโจมตีและรหัสผ่านรั่วไหล ผู้โจมตีอาจจะลองใช้เอกสารสิทธิ์เดียวกันกับบริการอื่นๆ เพื่อสร้างความเสียหายต่อบัญชีอื่นๆ เพิ่มเติมได้

- รหัสผ่านจะถูกทำเครื่องหมายว่า**นำกลับมาใช้ซ้ำ**หากพบว่ามีการใช้รหัสผ่านเดียวกันสำหรับรหัสผ่านที่บันทึกไว้มากกว่าหนึ่งรหัสผ่านในโดเมนต่างๆ
- รหัสผ่านจะถูกทำเครื่องหมายว่า**ไม่ปลอดภัย**หากเป็นรหัสผ่านที่ผู้โจมตีสามารถคาดเดาได้ง่าย iOS, iPadOS และ macOS จะตรวจหารูปแบบที่ใช้บ่อยในการสร้างรหัสผ่านที่จดจำได้ง่าย เช่น การใช้คำที่พบในพจนานุกรม การเปลี่ยนแทนที่อักขระที่พบบ่อย (เช่น การใช้ “p4ssw0rd” แทน “password”), รูปแบบที่พบบนแป้นพิมพ์ (เช่น “q12we34r” จากแป้นพิมพ์ QWERTY) หรือรูปแบบการเรียงลำดับที่ซ้ำกัน (เช่น “123123”) รูปแบบเหล่านี้มักถูกใช้บ่อยเพื่อสร้างรหัสผ่านให้ตรงตามข้อกำหนดรหัสผ่านขั้นต่ำสำหรับบริการต่างๆ แต่ก็ยังเป็นรูปแบบที่ผู้โจมตีมักใช้เพื่อพยายามรับรหัสผ่านโดยใช้ แบบ Brute Force อีกด้วย

  เนื่องจากบริการจำนวนมากเจาะจงให้ใช้รหัส PIN สี่ถึงหกหลักโดยเฉพาะ รหัสสั้นๆ เหล่านี้จึงถูกประเมินด้วยกฎเกณฑ์ที่แตกต่างกัน รหัส PIN จะถือว่าไม่ปลอดภัยหากเป็นหนึ่งในรหัส PIN ที่ใช้บ่อยที่สุด หรือหากเป็นรูปแบบการเรียงลำดับจากน้อยไปหามากหรือจากมากไปหาน้อย เช่น “1234” หรือ “8765” หรือหากเป็นรูปแบบที่ซ้ำๆ กัน เช่น “123123” หรือ “123321”
- รหัสผ่านจะถูกทำเครื่องหมายว่า**รั่วไหล**หากคุณสมบัติการตรวจสอบรหัสผ่านสามารถระบุได้ว่ารหัสผ่านนั้นมีการรั่วไหลของข้อมูล โปรดดูที่ การตรวจสอบรหัสผ่าน สำหรับข้อมูลเพิ่มเติม

รหัสผ่านที่ไม่ปลอดภัย ใช้ซ้ำ และรั่วไหลจะระบุอยู่ในรายการของรหัสผ่าน (macOS) หรือมีอยู่ในอินเทอร์เฟซคำแนะนำด้านความปลอดภัยโดยเฉพาะ (iOS และ iPadOS) ถ้าผู้ใช้เข้าสู่ระบบเว็บไซต์ใน Safari โดยใช้รหัสผ่านที่บันทึกไว้ก่อนหน้านี้ซึ่งเป็นรหัสผ่านที่ไม่ปลอดภัยหรือถือว่าไม่ปลอดภัยเนื่องจากมีการรั่วไหลของข้อมูล ระบบจะแสดงการเตือนที่แนะนำให้ผู้ใช้อัปเกรดเป็นรหัสผ่านที่ปลอดภัยสูงแบบอัตโนมัติ

การอัปเกรดความปลอดภัยของการตรวจสอบสิทธิ์สำหรับบัญชีใน iOS และ iPadOS

แอปที่ใช้ส่วนขยายการแก้ไขการตรวจสอบสิทธิ์ของบัญชี (ในเฟรมเวิร์คของบริการตรวจสอบสิทธิ์) จะสามารถอัปเกรดบัญชีที่ใช้รหัสผ่านได้อย่างง่ายดายด้วยการแตะปุ่มเพียงปุ่มเดียว ตัวอย่างเช่น แอปเหล่านั้นสามารถสลับไปใช้การลงชื่อเข้าด้วย Apple หรือรหัสผ่านที่ปลอดภัยสูงแบบอัตโนมัติได้ ส่วนขยายนี้มีให้ใช้ใน iOS และ iPadOS

ถ้าแอปได้ใช้จุดขยายและติดตั้งไว้บนอุปกรณ์แล้ว ผู้ใช้จะเห็นตัวเลือกการอัปเกรดการขยายเมื่อดูคำแนะนำด้านความปลอดภัยของรหัสผ่านของเอกสารสิทธิ์ที่เกี่ยวข้องกับแอปในตัวจัดการรหัสผ่านพวงกุญแจ iCloud ในการตั้งค่า การอัปเกรดยังมีให้เมื่อผู้ใช้ลงชื่อเข้าแอปด้วยเอกสารสิทธิ์ที่มีความเสี่ยงด้วยเช่นกัน แอปมีความสามารถในการสั่งให้ระบบไม่แจ้งตัวเลือกการอัปเกรดให้ผู้ใช้ทราบหลังจากลงชื่อเข้า การใช้ AuthenticationServices API แบบใหม่ทำให้แอปสามารถใช้งานส่วนขยายและดำเนินการอัปเกรดได้ด้วยตัวเองจากการตั้งค่าบัญชีหรือหน้าจอการจัดการบัญชีในแอปได้ด้วย

แอปสามารถเลือกที่จะรองรับการอัปเกรดรหัสผ่านที่ปลอดภัย การอัปเกรดลงชื่อเข้าด้วย Apple หรือการอัปเกรดทั้งสองแบบได้ ในการอัปเกรดรหัสผ่านที่ปลอดภัยสูง ระบบจะสร้างรหัสผ่านที่ปลอดภัยสูงแบบอัตโนมัติให้ผู้ใช้ ถ้าจำเป็น แอปสามารถสร้างกฎสำหรับรหัสผ่านแบบกำหนดเองให้ปฏิบัติตามเมื่อสร้างรหัสผ่านใหม่ได้ เมื่อผู้ใช้สลับบัญชีจากการใช้รหัสผ่านเป็นการใช้ลงชื่อเข้าด้วย Apple ระบบจะมอบเอกสารสิทธิ์ลงชื่อเข้าด้วย Apple ฉบับใหม่กับส่วนขยายที่เชื่อมโยงกับบัญชีดังกล่าว ระบบจะไม่มอบอีเมล Apple ID ของผู้ใช้ให้เป็นส่วนหนึ่งของเอกสารสิทธิ์ หลังจากอัปเกรดลงชื่อเข้าด้วย Apple สำเร็จแล้ว ระบบจะลบเอกสารสิทธิ์ของรหัสผ่านที่ใช้ก่อนหน้านี้ออกจากพวงกุญแจของผู้ใช้หากมีการบันทึกเอกสารสิทธิ์ดังกล่าวไว้ในพวงกุญแจนั้น

ส่วนขยายการแก้ไขการตรวจสอบสิทธิ์บัญชีมีโอกาสในการดำเนินการตรวจสอบสิทธิ์ผู้ใช้เพิ่มเติมก่อนจะดำเนินการอัปเกรด สำหรับการอัปเกรดที่เริ่มต้นภายในตัวจัดการรหัสผ่านหรือหลังจากลงชื่อเข้าแอป ส่วนขยายจะมอบชื่อผู้ใช้และรหัสผ่านของบัญชีเพื่ออัปเกรด สำหรับการอัปเกรดในแอป ระบบจะให้ชื่อผู้ใช้เท่านั้น ถ้าส่วนขยายต้องใช้การตรวจสอบสิทธิ์เพิ่มเติม ส่วนขยายจะขอให้แสดงอินเทอร์เฟซผู้ใช้แบบกำหนดเองก่อนที่จะดำเนินการอัปเกรดต่อไป กรณีการใช้งานที่ตั้งไว้สำหรับแสดงอินเทอร์เฟซผู้ใช้นี้คือเพื่อให้ผู้ใช้ป้อนปัจจัยรองของการตรวจสอบสิทธิ์เพื่ออนุญาตการอัปเกรด

การตรวจสอบรหัสผ่าน

การตรวจสอบรหัสผ่านเป็นคุณสมบัติที่จับคู่รหัสผ่านที่จัดเก็บไว้ในพวงกุญแจการป้อนรหัสผ่านอัตโนมัติของผู้ใช้กับรายการที่อัปเดตและดูแลอย่างต่อเนื่องของรหัสผ่านที่ทราบว่ามีการรั่วไหลจากองค์กรออนไลน์ต่างๆ ถ้าเปิดใช้คุณสมบัตินี้อยู่ โปรโตคอลการตรวจสอบจะจับคู่รหัสผ่านพวงกุญแจการป้อนรหัสผ่านอัตโนมัติของผู้ใช้กับรายการที่ดูแลอย่างต่อเนื่อง

วิธีการทำงานของการตรวจสอบ

อุปกรณ์ของผู้ใช้จะทำการตรวจสอบรหัสผ่านของผู้ใช้แบบวนซ้ำอย่างต่อเนื่อง โดยค้นหาช่วงเวลาที่ไม่ขึ้นกับรหัสผ่านของผู้ใช้หรือรูปแบบการใช้ตัวจัดการรหัสผ่าน วิธีนี้จะช่วยให้มั่นใจว่าสถานะการตรวจสอบยืนยันอัปเดตตรงกันกับรายการที่ดูแลในปัจจุบันของรหัสผ่านที่มีการรั่วไหล ในการช่วยป้องกันการรั่วไหลของข้อมูลที่เกี่ยวข้องกับจำนวนรหัสผ่านจำนวนมากที่ไม่ซ้ำกันของผู้ใช้ คำขอจะถูกแบ่งเป็นกลุ่มแล้วดำเนินการแบบคู่ขนาน การตรวจสอบแต่ละครั้งจะมีการตรวจสอบยืนยันรหัสผ่านในจำนวนที่แน่นอนควบคู่กัน และหากผู้ใช้มีน้อยกว่าจำนวนนี้ รหัสผ่านแบบสุ่มจะถูกสร้างขึ้นและเพิ่มลงในข้อความค้นหาเพื่อสร้างความแตกต่าง

รหัสผ่านจับคู่กันได้อย่างไร

รหัสผ่านจะจับคู่กันโดยผ่านกระบวนการสองส่วน รหัสผ่านที่รั่วไหลที่พบบ่อยที่สุดจะอยู่ภายในรายการภายในเครื่องบนอุปกรณ์ของผู้ใช้ ถ้ารหัสผ่านของผู้ใช้อยู่ในรายการนี้ ผู้ใช้จะได้รับการแจ้งเตือนในทันทีโดยไม่มีการโต้ตอบภายนอกใดๆ สิ่งนี้ได้รับการออกแบบมาเพื่อให้แน่ใจว่าจะไม่มีข้อมูลอยู่รั่วไหลเกี่ยวกับรหัสผ่านของผู้ใช้ ซึ่งเป็นรหัสผ่านที่มีความเสี่ยงมากที่สุดเนื่องจากการละเมิดรหัสผ่าน

ถ้ารหัสผ่านไม่อยู่ในรายการที่ใช้บ่อยที่สุด ระบบจะจับคู่รหัสผ่านนั้นกับรหัสผ่านที่รั่วไหลน้อยที่สุด

การเปรียบเทียบรหัสผ่านของผู้ใช้กับรายการที่ดูแล

การตรวจสอบยืนยันว่าไม่มีรหัสผ่านในรายการภายในเครื่องเป็นการจับคู่รหัสผ่านที่เกี่ยวข้องกับการโต้ตอบบางส่วนกับเซิร์ฟเวอร์ Apple เพื่อช่วยให้แน่ใจว่ารหัสผ่านของผู้ใช้ที่ถูกต้องไม่ส่งไปที่ Apple รูปแบบของ **อินเทอร์เซกชั่นของชุดการเข้ารหัสแบบส่วนตัว**ถูกใช้งานโดยเปรียบเทียบรหัสผ่านของผู้ใช้กับชุดของรหัสผ่านที่รั่วไหลจำนวนมาก สิ่งนี้ได้รับการออกแบบมาเพื่อให้แน่ใจว่าสำหรับรหัสผ่านที่มีความเสี่ยงในการละเมิดน้อยลงจะมีการแชร์ข้อมูลเพียงเล็กน้อยกับ Apple สำหรับรหัสผ่านของผู้ใช้ ข้อมูลนี้จะจำกัดคำนำหน้า 15 บิตของแฮชการเข้ารหัส การเอารหัสผ่านที่รั่วไหลบ่อยที่สุดออกจากกระบวนการโต้ตอบโดยใช้รายการภายในเครื่องของรหัสผ่านที่รั่วไหลบ่อยที่สุดจะช่วยลดส่วนที่แตกต่างที่สัมพันธ์กับความถี่ของรหัสผ่านในกลุ่มบริการเว็บ ซึ่งทำให้เป็นไปไม่ได้ในเชิงปฏิบัติที่จะอนุมานรหัสผ่านของผู้ใช้จากการค้นหาเหล่านี้

โปรโตคอลที่รองรับจะแบ่งพาร์ติชั่นรายการของรหัสผ่านที่เรียบเรียงซึ่งประกอบด้วยรหัสผ่านประมาณ 1.5 พันล้านรหัสในแต่ละครั้งที่มีการเขียนนี้ โดยแบ่งออกเป็นกลุ่มต่างๆ 215 กลุ่ม กลุ่มที่รหัสผ่านอยู่จะอิงตาม 15 บิตแรกของค่าแฮช SHA256 ของรหัสผ่าน นอกจากนี้ รหัสผ่านที่รั่วไหลแต่ละรายการจะมี pw ที่เชื่อมโยงกับจุดที่เป็นเส้นโค้งรูปไข่บนเส้นโค้ง NIST P256 ดังนี้: $P_{pw} = \alpha \cdot H_{SWU}(pw)$ โดย α คือกุญแจแบบสุ่มที่เป็นความลับที่มีเพียง Apple ที่ทราบ และ H_{SWU} คือฟังก์ชั่น Oracle แบบสุ่มที่เทียบผังรหัสผ่านกับจุดที่เป็นเส้นโค้งโดยอิงจากวิธีการ Shallue-van de Woestijne-Ulas การแปลงข้อมูลนี้ออกแบบมาเพื่อซ่อนค่าของรหัสผ่านในเชิงคำนวณและช่วยป้องกันไม่ให้เปิดเผยรหัสผ่านที่รั่วไหลใหม่ผ่านการตรวจสอบรหัสผ่าน

ในการคำนวณอินเตอร์เซกชั่นของชุดการเข้ารหัสแบบส่วนตัว อุปกรณ์ของผู้ใช้จะกำหนดกลุ่มที่รหัสผ่านอยู่โดยใช้ λ ซึ่งเป็นคำนำหน้า 15 บิตของ SHA256(upw) โดยที่ upw จะเป็นส่วนหนึ่งของรหัสผ่านของผู้ใช้ อุปกรณ์จะสร้างค่าคงที่แบบสุ่มของตัวเอง นั่นคือ β แล้วส่งจุด $P_c = \beta \cdot H_{SWU}(upw)$ ไปยังเซิร์ฟเวอร์พร้อมกับคำขอของกลุ่มที่สอดคล้องกันกับ λ ที่เซิร์ฟเวอร์นี้ β จะซ่อนข้อมูลเกี่ยวกับรหัสผ่านของผู้ใช้และจำกัด λ ในการเปิดเผยข้อมูลที่อยู่ในรหัสผ่านกับ Apple สุดท้าย เซิร์ฟเวอร์จะรับจุดที่ส่งจากอุปกรณ์ของผู้ใช้แล้วคำนวณ $\alpha P_c = \alpha\beta \cdot H_{SWU}(upw)$ จากนั้นส่งค่าคืนพร้อมกับกลุ่มของจุดที่เหมาะสม $B\lambda = \{ P_{pw} \mid SHA256(pw)$ ซึ่งขึ้นต้นด้วยคำนำหน้า $\lambda\}$ ไปยังอุปกรณ์

ข้อมูลที่ส่งคืนจะทำให้อุปกรณ์คำนวณ $B'_\lambda = \{\beta \cdot P_{pw} \mid P_{pw} \in B_\lambda\}$ แล้วตรวจสอบให้แน่ใจว่ารหัสผ่านของผู้ใช้รั่วไหลหาก $\alpha P_c \in B'_\lambda$

การส่งรหัสผ่านให้กับผู้ใช้อื่นหรืออุปกรณ์ Apple เครื่องอื่น

Apple ส่งรหัสผ่านอย่างปลอดภัยไปยังผู้ใช้หรืออุปกรณ์ Apple อื่นด้วย AirDrop และบน Apple TV

การบันทึกเอกสารสิทธิ์ไปยังอุปกรณ์อื่นด้วย AirDrop

เมื่อเปิดใช้งาน iCloud ผู้ใช้สามารถใช้ AirDrop เพื่อส่งข้อมูลประจำตัวที่บันทึกไว้ไปยังอุปกรณ์อื่น ข้อมูลประจำตัวประกอบด้วยชื่อผู้ใช้และรหัสผ่าน รวมถึงเว็บไซต์ที่บันทึกรหัสผ่านนั้นไว้ การส่งเอกสารสิทธิ์ด้วย AirDrop จะดำเนินการในโหมดเฉพาะรายชื่อเท่านั้นโดยไม่คำนึงถึงการตั้งค่าของผู้ใช้ หลังจากที่ผู้ใช้ให้ความยินยอมแล้ว ข้อมูลประจำตัวจะถูกจัดเก็บไว้ในพวงกุญแจการป้อนรหัสผ่านอัตโนมัติของผู้ใช้บนอุปกรณ์ที่เป็นเครื่องรับ

การป้อนเอกสารสิทธิ์ในแอปบน Apple TV

Apple TV มีการป้อนรหัสผ่านอัตโนมัติให้ใช้งานเพื่อป้อนเอกสารสิทธิ์ลงในแอปบนเครื่อง เมื่อผู้ใช้เน้นที่ช่องข้อความชื่อผู้ใช้หรือรหัสผ่านใน tvOS Apple TV จะเริ่มประกาศคำขอสำหรับการป้อนรหัสผ่านอัตโนมัติผ่านบลูทูธพลังงานต่ำ (BLE)

iPhone, iPad หรือ iPod touch ในบริเวณใกล้เคียงจะแสดงการแจ้งโดยเชิญให้ผู้ใช้แชร์เอกสารสิทธิ์กับ Apple TV นี่คือวิธีการสร้างวิธีการเข้ารหัส:

- ถ้าอุปกรณ์และ Apple TV ใช้บัญชี iCloud เดียวกัน การเข้ารหัสระหว่างอุปกรณ์จะเกิดขึ้นโดยอัตโนมัติ
- ถ้าอุปกรณ์ลงชื่อเข้าบัญชี iCloud นอกเหนือจากบัญชีที่ Apple TV ใช้ ผู้ใช้จะได้รับแจ้งให้สร้างการเชื่อมต่อที่เข้ารหัสผ่านการใช้รหัส PIN ในการรับการแจ้งนี้ iPhone ต้องปลดล็อคอยู่และอยู่ในระยะใกล้เคียงกับ Siri Remote ที่จับคู่กับ Apple TV เครื่องนั้น

หลังจากสร้างการเชื่อมต่อที่เข้ารหัสโดยใช้การเข้ารหัสลิงก์ BLE เอกสารสิทธิ์จะถูกส่งไปที่ Apple TV แล้วป้อนอัตโนมัติลงในช่องข้อความที่เกี่ยวข้องบนแอป

ส่วนขยายผู้ให้บริการเอกสารสิทธิ์

ใน iOS, iPadOS และ macOS ผู้ใช้สามารถกำหนดการเข้าร่วมแอปของบริษัทอื่นเป็นผู้ให้บริการเอกสารสิทธิ์สำหรับการป้อนรหัสผ่านอัตโนมัติในการตั้งค่ารหัสผ่าน (iOS และ iPadOS) หรือในการตั้งค่าส่วนขยายในการตั้งค่าระบบ (macOS) ได้ กลไกนี้จะสร้างอยู่บนส่วนขยายของแอป ส่วนขยายผู้ให้บริการเอกสารสิทธิ์ต้องมีมุมมองสำหรับการเลือกเอกสารสิทธิ์ และส่วนขยายอาจสามารถให้เมตาดาต้าเกี่ยวกับเอกสารสิทธิ์ที่บันทึกหรือไม่ก็ได้ เพื่อให้สามารถเสนอได้โดยตรงบนแถบ QuickType (iOS และ iPadOS) หรือในคำแนะนำโดยการเติมอัตโนมัติ (macOS) เมตาดาต้าประกอบด้วยเว็บไซต์ของเอกสารสิทธิ์และชื่อผู้ใช้ที่เกี่ยวข้อง แต่ไม่มีรหัสผ่าน โดย iOS, iPadOS และ macOS จะสื่อสารกับส่วนขยายเพื่อรับรหัสผ่านเมื่อผู้ใช้เลือกที่จะป้อนเอกสารสิทธิ์ลงในแอปหรือเว็บไซต์ใน Safari เมตาดาต้าเอกสารสิทธิ์ถูกจัดเก็บอยู่ภายในตัวบรรจุของแอปของผู้ให้บริการเอกสารสิทธิ์ และจะถูกเอาออกโดยอัตโนมัติเมื่อถอนการติดตั้งแอป

พวงกุญแจ iCloud

ภาพรวมความปลอดภัยของพวงกุญแจ iCloud

พวงกุญแจ iCloud ช่วยให้ผู้ใช้สามารถเชื่อมข้อมูลรหัสผ่านของตนเองระหว่างอุปกรณ์ iOS และ iPadOS และคอมพิวเตอร์ Mac ได้อย่างปลอดภัย โดยไม่เปิดเผยข้อมูลนั้นไปที่ Apple นอกเหนือจากความเป็นส่วนตัวและความปลอดภัยที่แน่นหนาแล้ว เป้าหมายอื่นที่ส่งผลกระทบต่อการออกแบบและสถาปัตยกรรมของพวงกุญแจ iCloud เป็นอย่างสูงคือความสะดวกในการใช้งาน และความสามารถในการกู้คืนพวงกุญแจ พวงกุญแจ iCloud ประกอบด้วยบริการสองอย่าง คือ การเชื่อมข้อมูลพวงกุญแจและการกู้คืนพวงกุญแจ

Apple ออกแบบพวงกุญแจ iCloud และการกู้คืนพวงกุญแจ เพื่อให้รหัสผ่านของผู้ใช้ยังคงได้รับการปกป้องภายในเงื่อนไขต่อไปนี้:

- บัญชี iCloud ของผู้ใช้ไม่ปลอดภัย
- iCloud ถูกบุกรุกจากผู้โจมตีภายนอกหรือพนักงาน
- บุคคลอื่นเข้าถึงบัญชีผู้ใช้

การรวมตัวจัดการรหัสผ่านกับพวงกุญแจ iCloud

iOS, iPadOS และ macOS สามารถสร้างสตริงแบบสุ่มที่ปลอดภัยสูงในเชิงการเข้ารหัสได้โดยอัตโนมัติเพื่อใช้เป็นรหัสผ่านบัญชีใน Safari นอกจากนี้ iOS และ iPadOS ยังสามารถสร้างรหัสผ่านที่ปลอดภัยสูงสำหรับแอปได้อีกด้วย รหัสผ่านที่สร้างแล้วจะถูกจัดเก็บในพวงกุญแจและเชื่อมข้อมูลกับอุปกรณ์อื่นๆ รายการพวงกุญแจจะถ่ายโอนจากอุปกรณ์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งโดยผ่านเซิร์ฟเวอร์ของ Apple แต่จะเข้ารหัสด้วยวิธีการที่ทำให้ Apple และอุปกรณ์เครื่องอื่นๆ อ่านเนื้อหาไม่ได้

การเชื่อมข้อมูลพวงกุญแจที่ปลอดภัย

เมื่อผู้ใช้เปิดใช้งานพวงกุญแจ iCloud เป็นครั้งแรก อุปกรณ์จะสร้างวงจรที่เชื่อถือได้ และสร้างข้อมูลประจำตัวการเชื่อมข้อมูลสำหรับตัวเอง ข้อมูลระบุตัวตนที่ใช้ในการเชื่อมข้อมูลประกอบด้วยกุญแจส่วนตัวและกุญแจสาธารณะ และจัดเก็บไว้ในพวงกุญแจของอุปกรณ์ กุญแจสาธารณะของข้อมูลระบุตัวตนที่ใช้ในการเชื่อมข้อมูลจะอยู่ในวงจร และวงจรจะได้รับการลงชื่อสองครั้ง ครั้งแรกโดยใช้กุญแจส่วนตัวของข้อมูลระบุตัวตนที่ใช้ในการเชื่อมข้อมูล จากนั้นอีกครั้งด้วยกุญแจรูปไข่แบบอสมมาตร (โดยใช้ P-256) ที่ได้รับจากรหัสผ่านบัญชี iCloud ของผู้ใช้ พารามิเตอร์ (ค่า salt และการทำซ้ำแบบสุ่ม) ที่จัดเก็บไว้กับวงจรนั้นใช้เพื่อสร้างกุญแจที่อิงตามรหัสผ่าน iCloud ของผู้ใช้

สำหรับบัญชีการตรวจสอบสิทธิ์สองปัจจัย วงจรการเชื่อมข้อมูลเพิ่มเติมที่คล้ายกันจะถูกสร้างขึ้นและจัดเก็บไว้ใน CloudKit ข้อมูลระบุตัวตนของอุปกรณ์ในระบบนี้ประกอบด้วยกุญแจรูปไข่แบบไม่สมมาตรสองคู่ (โดยใช้ P-384) ซึ่งจัดเก็บไว้ในพวงกุญแจด้วย อุปกรณ์แต่ละเครื่องมีรายการข้อมูลระบุตัวตนที่เชื่อถือโดยอุปกรณ์นั้น และมีการลงชื่อในรายการนี้โดยใช้กุญแจข้อมูลระบุตัวตนอันใดอันหนึ่ง

พื้นที่จัดเก็บข้อมูล iCloud ของวงจรการเชื่อมข้อมูล

วงจรการเชื่อมข้อมูลที่มีการลงชื่อจะถูกจัดเก็บไว้ในพื้นที่จัดเก็บข้อมูลค่ากุญแจ iCloud ของผู้ใช้ ซึ่งไม่สามารถอ่านได้โดยไม่ทราบรหัสผ่าน iCloud ของผู้ใช้ และไม่สามารถแก้ไขได้อย่างถูกต้องหากไม่มีกุญแจส่วนตัวของข้อมูลระบุตัวตนที่มีการเชื่อมข้อมูลของสมาชิก

สำหรับบัญชีการตรวจสอบสิทธิ์สองปัจจัย รายการการเชื่อมข้อมูลของแต่ละอุปกรณ์จะถูกจัดเก็บไว้ใน CloudKit รายการไม่สามารถอ่านได้โดยไม่ทราบรหัสผ่าน iCloud ของผู้ใช้ และไม่สามารถแก้ไขได้อย่างถูกต้องหากไม่มีกุญแจส่วนตัวของอุปกรณ์ที่เป็นเจ้าของ

วิธีเพิ่มอุปกรณ์เครื่องอื่นของผู้ใช้ไปยังวงจรการเชื่อมข้อมูล

เมื่อลงชื่อเข้า iCloud สำหรับอุปกรณ์ใหม่จะเข้าร่วมวงจรการเชื่อมข้อมูลพวงกุญแจ iCloud ด้วยวิธีใดวิธีหนึ่งจากสองวิธี: โดยการจับคู่และรับการสนับสนุนโดยอุปกรณ์พวงกุญแจ iCloud ที่มีอยู่ หรือโดยใช้การกู้คืนพวงกุญแจ iCloud

ในระหว่างขั้นตอนการจับคู่ อุปกรณ์ของผู้สมัครจะสร้างข้อมูลระบุตัวตนที่มีการเชื่อมข้อมูลใหม่สำหรับทั้งวงจรการเชื่อมข้อมูลและรายการการเชื่อมข้อมูล (สำหรับบัญชีการตรวจสอบสิทธิ์สองปัจจัย) และแสดงต่อผู้สนับสนุน ผู้สนับสนุนจะเพิ่มกุญแจสาธารณะของสมาชิกใหม่ลงในวงจรการเชื่อมข้อมูลและลงชื่อเข้าอีกครั้งด้วยข้อมูลระบุตัวตนที่มีการเชื่อมข้อมูลและรหัสที่ได้มาจากรหัสผ่าน iCloud ของผู้ใช้ วงจรเชื่อมข้อมูลใหม่จะอยู่บน iCloud ซึ่งจะลงชื่อในลักษณะเดียวกันโดยสมาชิกใหม่ของวงจร ในบัญชีการตรวจสอบสิทธิ์สองปัจจัย อุปกรณ์ของผู้สนับสนุนยังจัดเตรียม**บัตรกำนัล**ที่มีการลงชื่อด้วยรหัสระบุตัวตนของอุปกรณ์ที่เข้าร่วมด้วย ซึ่งเป็นการแสดงว่าอุปกรณ์ของผู้สมัครควรได้รับความเชื่อถือ จากนั้นจะอัปเดตรายการข้อมูลระบุตัวตนที่มีการเชื่อมข้อมูลที่เชื่อถือได้แต่ละรายการเพื่อให้ครอบคลุมผู้สมัคร

ตอนนี้จะมีสมาชิกของวงจรลงชื่อสองราย และแต่ละรายจะมีกุญแจสาธารณะของเพียร์ของตัวเอง ตอนนี้พวกเขาก็สามารถเริ่มแลกเปลี่ยนรายการพวงกุญแจแต่ละรายการผ่านพื้นที่จัดเก็บข้อมูลค่ากุญแจ iCloud หรือเก็บไว้ใน CloudKit ตามความเหมาะสมสำหรับสถานการณ์ ถ้าสมาชิกในวงจรทั้งสองมีการอัปเดตรายการเดียวกัน ระบบจะเลือกรายการใดรายการหนึ่งซึ่งส่งผลให้มีความสอดคล้องกันในที่สุด แต่ละรายการที่ถูกเชื่อมข้อมูลจะถูกเข้ารหัส จึงสามารถถอดรหัสได้โดยอุปกรณ์ที่อยู่ในวงจรที่เชื่อถือได้ของผู้ใช้เท่านั้น แต่จะไม่สามารถถอดรหัสโดยอุปกรณ์เครื่องอื่นใดหรือโดย Apple ได้

เมื่อมีอุปกรณ์ใหม่เข้าร่วมในวงจรการเชื่อมข้อมูล “กระบวนการเข้าร่วม” นี้จะเกิดขึ้นซ้ำๆ ตัวอย่างเช่น เมื่ออุปกรณ์ที่สามเข้าร่วม จะสามารถจับคู่กับอุปกรณ์ที่มีอยู่ได้ เมื่อเพิ่มเพียร์ใหม่ เพียร์ต่างๆ จะเชื่อมข้อมูลกับเพียร์ใหม่ วิธีนี้ได้รับการออกแบบมาเพื่อให้แน่ใจว่าสมาชิกทุกคนจะมีรายการพวงกุญแจเดียวกัน

ซึ่งจะเชื่อมข้อมูลเฉพาะบางรายการเท่านั้น

รายการพวงกุญแจบางรายการเป็นอุปกรณ์เฉพาะ เช่น กุญแจ iMessage และต้องอยู่เฉพาะในอุปกรณ์เท่านั้น ด้วยเหตุนี้ ทุกรายการที่จะเชื่อมข้อมูลต้องมีการทำเครื่องหมายด้วยคุณลักษณะ `kSecAttrSynchronizable` ไว้อย่างชัดเจน

Apple จะตั้งค่าคุณลักษณะนี้สำหรับข้อมูลผู้ใช้ Safari (รวมถึงชื่อผู้ใช้ รหัสผ่าน และหมายเลขบัตรเครดิต) เช่นเดียวกับรหัสผ่าน Wi-Fi, กุญแจการเข้ารหัส HomeKit และรายการพวงกุญแจอื่นๆ ที่รองรับการเข้ารหัส iCloud แบบต้นทางถึงปลายทาง

นอกจากนี้ รายการในพวงกุญแจที่เพิ่มโดยแอปของบุคคลหรือบริษัทอื่นก็จะมีค่าเริ่มต้นเป็นแบบไม่เชื่อมข้อมูลด้วยเช่นกัน นักพัฒนาต้องตั้งค่าคุณลักษณะ `kSecAttrSynchronizable` เมื่อเพิ่มรายการลงในพวงกุญแจ

การกู้คืนพวงกุญแจ iCloud ที่ปลอดภัย

พวงกุญแจ iCloud จะฝากข้อมูลพวงกุญแจของผู้ใช้ไว้กับ Apple โดยจะ**ไม่**อนุญาตให้ Apple อ่านรหัสผ่านและข้อมูลอื่นๆ ที่อยู่ในพวงกุญแจ ถึงแม้ว่าผู้ใช้จะมีอุปกรณ์เพียงแค่เครื่องเดียว การกู้คืนพวงกุญแจก็จะเป็นมาตรการขั้นสุดท้ายในการป้องกันข้อมูลสูญหาย ซึ่งเป็นเรื่องสำคัญอย่างยิ่งเมื่อใช้ Safari สร้างรหัสผ่านแบบสุ่มที่มีความปลอดภัยสูงสำหรับบัญชีบนเว็บ เนื่องจากรหัสผ่านเหล่านั้นจะบันทึกอยู่ในพวงกุญแจเพียงที่เดียวเท่านั้น

หลักสำคัญของการกู้คืนพวงกุญแจคือการตรวจสอบสิทธิ์ครั้งที่สองและบริการรับฝากที่ปลอดภัย ซึ่งสร้างขึ้นโดย Apple เพื่อรองรับคุณสมบัตินี้โดยเฉพาะ พวงกุญแจของผู้ใช้จะเข้ารหัสด้วยรหัสที่มีความปลอดภัยสูง และบริการรับฝากจะมอบสำเนาของพวงกุญแจให้เมื่อเกิดเหตุการณ์ที่ตรงตามเงื่อนไขอันเข้มงวดเท่านั้น

การใช้การตรวจสอบสิทธิ์ครั้งที่สอง

การสร้างรหัสที่มีความปลอดภัยสูงมีหลายวิธี:

- ถ้าการตรวจสอบสิทธิ์สองปัจจัยเปิดใช้งานอยู่สำหรับบัญชีของผู้ใช้ รหัสอุปกรณ์จะถูกใช้เพื่อกู้คืนพวงกุญแจที่ฝากไว้
- ถ้าไม่ได้ตั้งค่าการตรวจสอบสิทธิ์สองปัจจัยไว้ ระบบจะขอให้ผู้ใช้สร้างรหัสความปลอดภัย iCloud โดยมีรหัสหกหลัก นอกจากนี้ ผู้ใช้สามารถกำหนดรหัสของตัวเองให้ยาวขึ้น หรือพวกเขาสามารถให้อุปกรณ์สร้างรหัสลับแบบสุ่มซึ่งพวกเขาสามารถบันทึกและเก็บไว้เองได้โดยไม่ต้องใช้การตรวจสอบสิทธิ์สองปัจจัย

กระบวนการฝากพวงกุญแจ

หลังจากสร้างรหัสแล้ว พวงกุญแจจะถูกฝากไว้กับ Apple อันดับแรก อุปกรณ์ iOS, iPadOS หรือ macOS จะส่งออกสำเนาพวงกุญแจของผู้ใช้หนึ่งชุด จากนั้นจะเข้ารหัสห่อด้วยกุญแจในกระเป๋ากุญแจ (Keybag) แบบไม่สมมาตรและวางไว้ในพื้นที่จัดเก็บข้อมูลค่ากุญแจ iCloud ของผู้ใช้ กระเป๋ากุญแจ (Keybag) จะถูกห่อด้วยรหัสรักษาความปลอดภัย iCloud ของผู้ใช้และด้วยกุญแจสาธารณะของคลัสเตอร์โมดูลรักษาความปลอดภัยฮาร์ดแวร์ (HSM) ที่จะจัดเก็บข้อมูลที่ฝากไว้ สิ่งนี้จะกลายเป็น**บันทึกการโอน iCloud** ของผู้ใช้ สำหรับบัญชีการตรวจสอบสิทธิ์สองปัจจัย พวงกุญแจยังถูกจัดเก็บไว้ใน CloudKit และรวมเข้ากับกุญแจระดับกลางที่สามารถกู้คืนได้ด้วยเนื้อหาของบันทึกการโอน iCloud เท่านั้น จึงให้การป้องกันในระดับเดียวกัน

เนื้อหาของบันทึกการโอนยังอนุญาตให้อุปกรณ์ที่มีการกู้คืนสามารถเข้าร่วมพวงกุญแจ iCloud ได้อีกครั้ง ซึ่งเป็นการพิสูจน์กับอุปกรณ์ที่มีอยู่ว่าอุปกรณ์ที่มีการกู้คืนได้ดำเนินการตามขั้นตอนการโอนสำเร็จแล้ว และด้วยเหตุนี้จึงได้รับการยืนยันตัวตนจากเจ้าของบัญชีแล้ว

หมายเหตุ: ถ้าผู้ใช้ตัดสินใจใช้รหัสรักษาความปลอดภัยที่เข้ารหัสแบบสุ่มแทนที่จะกำหนดรหัสของตัวเองหรือใช้ค่าสี่หลัก ข้อมูลที่ฝากไว้ก็ไม่จำเป็นต้องใช้ แต่รหัสรักษาความปลอดภัย iCloud จะถูกใช้เพื่อห่อกุญแจแบบสุ่มโดยตรงแทน

นอกเหนือจากการสร้างโค้ดความปลอดภัยแล้ว ผู้ใช้จะต้องลงทะเบียนเบอร์โทรศัพท์อีกด้วย การทำเช่นนี้จะให้การตรวจสอบสิทธิ์ระดับรองในระหว่างการกู้คืนพวงกุญแจ ผู้ใช้จะได้รับข้อความ SMS ที่ต้องตอบกลับเพื่อดำเนินการกู้คืนต่อไป

ความปลอดภัยของข้อมูลที่ฝากสำหรับพวงกุญแจ iCloud

iCloud มอบโครงสร้างพื้นฐานที่ปลอดภัยสำหรับการฝากพวงกุญแจเพื่อช่วยให้มั่นใจได้ว่ามีเพียงผู้ใช้และอุปกรณ์ที่ได้รับอนุญาตเท่านั้นที่จะสามารถดำเนินการกู้คืนได้ สิ่งที่อยู่เบื้องหลัง iCloud คือคลัสเตอร์ของโมดูลรักษาความปลอดภัยฮาร์ดแวร์ (HSM) ที่จะปกป้องข้อมูลที่ฝากไว้ ตามที่ได้อธิบายไว้ก่อนหน้านี้ แต่ละคลัสเตอร์จะมีกุญแจที่ใช้เข้ารหัสข้อมูลที่ฝากไว้ภายใต้การดูแล

ในการกู้คืนพวงกุญแจ ผู้ใช้ต้องตรวจสอบสิทธิ์ด้วยบัญชีและรหัสผ่าน iCloud และตอบ SMS ที่ส่งไปที่เบอร์โทรศัพท์ที่ลงทะเบียนไว้ หลังจากเสร็จแล้ว ผู้ใช้จะต้องป้อนรหัสรักษาความปลอดภัย iCloud ของตัวเอง คลัสเตอร์ HSM จะตรวจสอบยืนยันว่าผู้ใช้ทราบรหัสรักษาความปลอดภัย iCloud หรือไม่โดยใช้โปรโตคอล Secure Remote Password (SRP) โดยจะไม่ส่งตัวรหัสผ่านไปที่ Apple คลัสเตอร์แต่ละส่วนจะตรวจสอบยืนยันว่าผู้ใช้พยายามขอรับข้อมูลของตัวเองจนครบจำนวนครั้งที่อนุญาตแล้วหรือไม่ ตามที่อธิบายไว้ด้านล่าง ถ้าส่วนใหญ่ยินยอม คลัสเตอร์จะแกะห่อข้อมูลที่ฝากไว้แล้วส่งไปที่อุปกรณ์ของผู้ใช้

จากนั้น อุปกรณ์จะใช้รหัสรักษาความปลอดภัย iCloud เพื่อแกะห่อกุญแจแบบสุ่มที่ใช้เข้ารหัสพวงกุญแจของผู้ใช้ด้วยกุญแจนั้น พวงกุญแจที่ได้รับจากพื้นที่จัดเก็บข้อมูลค่ากุญแจ iCloud และ CloudKit จะถูกถอดรหัสและกู้คืนไปที่อุปกรณ์ โดย iOS, iPadOS และ macOS จะอนุญาตให้ลองตรวจสอบสิทธิ์และดึงข้อมูลที่ฝากเพียง 10 ครั้งเท่านั้น หลังจากพยายามไม่สำเร็จหลายครั้ง ข้อมูลจะถูกล็อคและผู้ใช้จะต้องโทรหาฝ่ายบริการช่วยเหลือของ Apple เพื่อขอให้เพิ่มจำนวนครั้งในการลอง หลังจากพยายามไม่สำเร็จเป็นครั้งที่ 10 คลัสเตอร์ HSM จะทำลายข้อมูลที่ฝากไว้และพวงกุญแจจะสูญหายอย่างถาวร ซึ่งจะช่วยปกป้องจากการพยายามเจาะข้อมูลด้วย Brute Force โดยแลกกับการสูญเสียข้อมูลพวงกุญแจ

นโยบายเหล่านี้เขียนเป็นโค้ดไว้ในเฟิร์มแวร์ของ HSM การ์ดที่มีสิทธิ์เข้าถึงระดับผู้ดูแลที่อนุญาตให้ทำการเปลี่ยนแปลงกับเฟิร์มแวร์ได้ได้ถูกทำลายไปแล้ว ความพยายามใดๆ ในการดัดแปลงเฟิร์มแวร์หรือเข้าถึงกุญแจส่วนตัวจะทำให้คลัสเตอร์ HSM ลบกุญแจส่วนตัวนั้น ถ้าเกิดเหตุการณ์เช่นนี้ขึ้น เจ้าของพวงกุญแจแต่ละรายการที่ปกป้องด้วยคลัสเตอร์จะได้รับข้อความแจ้งว่าตนสูญเสียข้อมูลที่ฝากไว้แล้ว ซึ่งพวกเขาสามารถเลือกที่จะฝากใหม่ได้

Apple Pay

ภาพรวมความปลอดภัยของ Apple Pay

เมื่อใช้ Apple Pay ผู้ใช้สามารถใช้อุปกรณ์ iPhone, iPad, Mac และ Apple Watch ที่รองรับเพื่อชำระเงินด้วยวิธีที่ง่าย ปลอดภัย และเป็นส่วนตัวในร้าน แอป และบนเว็บใน Safari ได้ ผู้ใช้ยังสามารถเพิ่มบัตรโดยสาร บัตรประจำตัวนักเรียน และบัตรสำหรับสอดเปิดอุปกรณ์ที่รองรับ Apple Pay ไปยังกระเป๋าสตางค์ได้อีกด้วย ซึ่งเป็นวิธีที่ง่ายสำหรับผู้ใช้ และถูกสร้างให้มีความปลอดภัยทั้งในฮาร์ดแวร์และซอฟต์แวร์

Apple Pay ยังได้รับการออกแบบให้ปกป้องข้อมูลส่วนบุคคลของผู้ใช้ด้วย Apple Pay ไม่เก็บรวบรวมข้อมูลธุรกรรมใดๆ ที่สามารถโยงกลับไปยังตัวผู้ใช้ได้ ธุรกรรมการชำระเงินเกิดขึ้นระหว่างผู้ใช้ ผู้ขาย และผู้ออกบัตร

ความปลอดภัยของส่วนประกอบของ Apple Pay

Apple Pay ใช้คุณสมบัติด้านฮาร์ดแวร์และซอฟต์แวร์หลายประการเพื่อทำให้การซื้อสินค้าเป็นไปอย่างปลอดภัยและเชื่อถือได้

Secure Element

Secure Element คือชิปที่ได้รับการรับรองมาตรฐานอุตสาหกรรมที่ทำงานบนแพลตฟอร์ม Java Card ซึ่งเป็นไปตามข้อกำหนดอุตสาหกรรมการเงินสำหรับการชำระเงินอิเล็กทรอนิกส์ Secure Element IC และแพลตฟอร์ม Java Card ได้รับการรับรองตามกระบวนการประเมินความปลอดภัยของ EMVCo หลังจากผ่านการประเมินความปลอดภัย EMVCo จะออกใบรับรอง IC และแพลตฟอร์มที่ไม่ซ้ำกัน

Secure Element IC ได้รับการรับรองตามมาตรฐานเกณฑ์ทั่วไป โปรดดูที่การรับรองความปลอดภัยของหน่วยประมวลผล Secure Enclave ในการรับรองแพลตฟอร์ม Apple สำหรับข้อมูลเพิ่มเติม

ตัวควบคุม NFC

ตัวควบคุม NFC จะจัดการกับโปรโตคอล Near Field Communication และเปิดเส้นทางการสื่อสารระหว่างหน่วยประมวลผลแอปพลิเคชันกับ Secure Element และระหว่าง Secure Element กับเทอร์มินัลจุดจำหน่าย

กระเป๋าสตางค์

แอปกระเป๋าสตางค์ใช้เพื่อเพิ่มและจัดการบัตรเครดิต บัตรเดบิต และบัตรร้านค้า และเพื่อชำระเงินด้วย Apple Pay ผู้ใช้สามารถดูบัตรของตัวเองและอาจดูข้อมูลเพิ่มเติมที่ผู้ออกบัตรของผู้ใช้มีให้ได้ในกระเป๋าสตางค์ เช่น นโยบายความเป็นส่วนตัวของผู้ออกบัตร รายการธุรกรรมล่าสุด และอื่นๆ ผู้ใช้ยังสามารถเพิ่มบัตรไปยัง Apple Pay ได้อีกด้วยใน:

- ผู้ช่วยตั้งค่าและการตั้งค่าสำหรับ iOS และ iPadOS
- แอป Watch สำหรับ Apple Watch
- กระเป๋าสตางค์และ Apple Pay ในการตั้งค่าระบบสำหรับคอมพิวเตอร์ Mac ที่มี Touch ID

นอกจากนี้ กระเป๋าสตางค์ยังทำให้ผู้ใช้สามารถเพิ่มและจัดการบัตรโดยสาร บัตรรางวัล บัตรผ่านขึ้นเครื่อง ตั๋ว บัตรของขวัญ บัตรประจำตัวนักเรียน บัตรสำหรับสอดเปิดอุปกรณ์ และอื่นๆ ได้อีกด้วย

Secure Enclave

Secure Enclave จะจัดการกระบวนการตรวจสอบสิทธิ์และอนุญาตให้ทำธุรกรรมการชำระเงินต่อไปได้สำหรับ iPhone, iPad, Apple Watch, คอมพิวเตอร์ Mac ที่มี Touch ID และคอมพิวเตอร์ Mac ที่มี Apple Silicon ที่ใช้ Magic Keyboard ที่มี Touch ID

บน Apple Watch อุปกรณ์จะต้องได้รับการปลดล็อค และผู้ใช้จะต้องกดสองครั้งที่ปุ่มด้านข้าง การกดสองครั้งจะถูกตรวจพบและส่งต่อโดยตรงไปที่ Secure Element หรือ Secure Enclave หากมีให้ใช้งานได้ โดยไม่ผ่านหน่วยประมวลผลแอปพลิเคชัน

เซิร์ฟเวอร์ Apple Pay

เซิร์ฟเวอร์ Apple Pay จะจัดการการตั้งค่าและกำหนดสิทธิ์บัตรเครดิต บัตรเดบิต บัตรโดยสาร บัตรประจำตัวนักเรียน และบัตรสำหรับสอดเปิดอุปกรณ์ในกระเป๋าสตางค์ เซิร์ฟเวอร์เหล่านั้นยังจัดการหมายเลขบัญชีอุปกรณ์ที่จัดเก็บอยู่ใน Secure Element อีกด้วย เซิร์ฟเวอร์จะสื่อสารกับทั้งอุปกรณ์และกับเครือข่ายการชำระเงินหรือเซิร์ฟเวอร์ผู้ออกบัตร เซิร์ฟเวอร์ Apple Pay ยังรับผิดชอบการเข้ารหัสเอกสารสิทธิ์การชำระเงินอีกครั้งสำหรับการชำระเงินภายในแอปหรือบนเว็บอีกด้วย

Apple Pay ปกป้องการซื้อของผู้ใช้อย่างไร

Secure Element

Secure Element มีแอพเพล็ตที่ออกแบบมาเป็นพิเศษเพื่อจัดการ Apple Pay และยังมีแอพเพล็ตที่ได้รับการรับรองโดยเครือข่ายการชำระเงินหรือผู้ออกบัตรอีกด้วย ข้อมูลบัตรเครดิต บัตรเดบิต หรือบัตรเติมเงินจะถูกส่งแบบเข้ารหัสจากเครือข่ายการชำระเงินหรือผู้ออกบัตรไปยังแอพเพล็ตเหล่านี้โดยใช้กุญแจที่เครือข่ายการชำระเงินหรือผู้ออกบัตรและโดเมนความปลอดภัยของแอพเพล็ตรู้จักเท่านั้น ข้อมูลนี้จะมีการจัดเก็บภายในแอพเพล็ตและมีรหัสปกป้องโดยใช้คุณสมบัติความปลอดภัยของ Secure Element ระหว่างการทำธุรกรรม เทอร์มินัลจะติดต่อกับ Secure Element โดยตรงผ่านตัวควบคุม Near Field Communication (NFC) ผ่านบัสฮาร์ดแวร์สำหรับการใช้งานเฉพาะ

ตัวควบคุม NFC

ในฐานะเกตเวย์ของ Secure Element ตัวควบคุม NFC จะช่วยให้การรับรองว่ารายการธุรกรรมการชำระเงินแบบไร้การสัมผัสทั้งหมดจะมีการทำโดยใช้เทอร์มินัลจุดจำหน่ายที่อยู่ในระยะใกล้เคียงกับอุปกรณ์ เฉพาะคำขอชำระเงินที่มาจากเทอร์มินัลในพื้นที่เท่านั้นที่จะได้รับการทำเครื่องหมายโดยตัวควบคุม NFC เป็นธุรกรรมแบบไร้การสัมผัส

หลังจากการชำระเงินด้วยบัตรเครดิต บัตรเดบิต หรือบัตรเติมเงิน (รวมถึงบัตรร้านค้า) ได้รับการอนุมัติจากผู้ถือบัตรโดยใช้ Face ID, Touch ID หรือรหัสผ่าน หรือบน Apple Watch ที่ปลดล็อคโดยการกดสองครั้งที่ปุ่มด้านข้าง การตอบสนองแบบไร้การสัมผัสที่กำหนดสิทธิ์โดยแอพเพล็ตการชำระเงินภายในของ Secure Element จะได้รับการกำหนดเส้นทางโดยตัวควบคุมให้ไปยังช่องข้อมูล NFC เท่านั้น ผลลัพธ์คือ รายละเอียดสำหรับการอนุญาตการชำระเงินสำหรับรายการธุรกรรมการชำระเงินแบบไร้การสัมผัสจะอยู่ในคลื่น NFC ในเครื่องและไม่มีการเปิดเผยไปยังหน่วยประมวลผลแอปพลิเคชันไม่ว่ากรณีใดๆ ในทางตรงกันข้าม รายละเอียดการอนุญาตการชำระเงินสำหรับการชำระเงินภายในแอปและบนเว็บจะมีการส่งไปยังหน่วยประมวลผลแอปพลิเคชัน แต่จะส่งหลังจากที่เข้ารหัสโดย Secure Element ไปยังเซิร์ฟเวอร์ Apple Pay แล้วเท่านั้น

บัตรเครดิต บัตรเดบิต และบัตรเติมเงิน

ภาพรวมความปลอดภัยของการกำหนดสิทธิ์ของบัตร

เมื่อผู้ใช้เพิ่มบัตรเครดิต บัตรเดบิต หรือบัตรเติมเงิน (รวมถึงบัตรร้านค้า) ไปยังกระเป๋าสตางค์แล้ว Apple จะส่งข้อมูลบัตรอย่างปลอดภัยพร้อมกับข้อมูลอื่นๆ ที่เกี่ยวกับบัญชีและอุปกรณ์ของผู้ใช้ไปยังผู้ออกบัตรหรือผู้ให้บริการที่ได้รับอนุญาตจากผู้ออกบัตร ผู้ออกบัตรจะใช้ข้อมูลนี้เพื่อตัดสินใจว่าจะอนุญาตการเพิ่มบัตรไปยังกระเป๋าสตางค์หรือไม่ ในฐานะที่เป็นส่วนหนึ่งของกระบวนการการกำหนดสิทธิ์ของบัตร Apple Pay จะใช้การเรียกจากฝั่งเซิร์ฟเวอร์สามแบบเพื่อส่งและรับการติดต่อกับผู้ออกบัตรหรือเครือข่าย ได้แก่

- ช่องที่ต้องกรอกข้อมูล
- ตรวจสอบบัตร
- ลิงก์และการกำหนดสิทธิ์

ผู้ออกบัตรหรือเครือข่ายจะใช้การเรียกเหล่านี้เพื่อตรวจสอบยืนยัน อนุญาต และเพิ่มบัตรไปยังกระเป๋าสตางค์ เซสชั่นเซิร์ฟเวอร์ลูกข่ายเหล่านี้ใช้ TLS 1.2 ในการถ่ายโอนข้อมูล

หมายเลขบัตรแบบเต็มจะไม่ถูกจัดเก็บในอุปกรณ์หรือบนเซิร์ฟเวอร์ Apple Pay แต่หมายเลขบัญชีอุปกรณ์ที่ไม่ซ้ำจะถูกสร้าง เข้ารหัส และจัดเก็บใน Secure Element แทน หมายเลขบัญชีอุปกรณ์ที่ไม่ซ้ำนี้จะถูกเข้ารหัสแบบที่ Apple ไม่สามารถเข้าถึงได้ หมายเลขบัญชีอุปกรณ์เป็นหมายเลขที่ไม่ซ้ำกันและจะแตกต่างจากหมายเลขบัตรเครดิตหรือบัตรเดบิตส่วนใหญ่ ผู้ออกบัตรหรือเครือข่ายการชำระเงินสามารถป้องกันการใช้งานบัตรบนบัตรแถบแม่เหล็กผ่านทางโทรศัพท์ หรือบนเว็บไซต์ได้ หมายเลขบัญชีอุปกรณ์ใน Secure Element จะไม่ถูกจัดเก็บในเซิร์ฟเวอร์ Apple Pay หรือไม่ถูกสำรองข้อมูลไปยัง iCloud และจะแยกจากอุปกรณ์ iOS, iPadOS และ watchOS และจากคอมพิวเตอร์ Mac ที่มี Touch ID

บัตรสำหรับใช้งานกับ Apple Watch จะถูกกำหนดสิทธิ์สำหรับ Apple Pay โดยใช้แอป Apple Watch บน iPhone หรือภายในแอปสำหรับ iPhone ของผู้ออกบัตร การเพิ่มบัตรไปยัง Apple Watch ต้องให้นาฬิกาอยู่ภายในระยะการติดต่อของบลูทูธ บัตรจะได้รับการลงทะเบียนสำหรับใช้งานกับ Apple Watch โดยเฉพาะ และมีหมายเลขบัญชีอุปกรณ์ของตัวเอง ซึ่งจะถูกจัดเก็บภายใน Secure Element บน Apple Watch

เมื่อเพิ่มบัตรเครดิต บัตรเดบิต หรือบัตรเติมเงิน (รวมทั้งบัตรร้านค้า) บัตรเหล่านั้นจะแสดงในรายการของบัตรในระหว่างการตั้งค่าโดยผู้ช่วยตั้งค่าบนอุปกรณ์ที่ลงชื่อเข้าบัญชี iCloud เดียวกัน บัตรเหล่านี้จะยังคงอยู่ในรายการตราบเท่าที่ยังเปิดใช้งานบนอุปกรณ์อย่างน้อยหนึ่งเครื่อง บัตรจะถูกเอาออกจากรายการนี้หลังจากที่ถูกเอาออกจากอุปกรณ์ทุกเครื่องเป็นเวลา 7 วัน คุณสมบัตินี้จะต้องใช้การตรวจสอบสิทธิ์สองปัจจัยเพื่อให้เปิดใช้งานบนบัญชี iCloud ที่เกี่ยวข้อง

การเพิ่มบัตรเครดิตหรือบัตรเดบิตไปยัง Apple Pay

คุณสามารถเพิ่มบัตรเครดิตไปยัง Apple Pay บนอุปกรณ์ Apple ได้ด้วยตนเอง

การเพิ่มบัตรเครดิตหรือบัตรเดบิตด้วยตัวเอง

ในการเพิ่มบัตรด้วยตัวเอง ชื่อ หมายเลขบัตร วันหมดอายุ และ CVV จะถูกใช้เพื่อให้กระบวนการจัดเตรียมสะดวกขึ้น ผู้ใช้สามารถป้อนข้อมูลดังกล่าวจากภายในการตั้งค่า กระเป๋าสตางค์ หรือแอป Apple Watch ได้โดยการพิมพ์หรือใช้กล้องของอุปกรณ์ เมื่อกล้องจับภาพข้อมูลบัตรได้ Apple จะพยายามใส่ข้อมูลชื่อ หมายเลขบัตร และวันหมดอายุลงไป รูปภาพจะไม่ถูกบันทึกไปที่อุปกรณ์หรือจัดเก็บในคลังรูปภาพ หลังจากป้อนข้อมูลลงในช่องทั้งหมดแล้ว กระบวนการตรวจสอบบัตรจะตรวจสอบยืนยันช่องอื่นๆ นอกเหนือจาก CVV ด้วย จากนั้นข้อมูลจะถูกเข้ารหัสและส่งไปที่เซิร์ฟเวอร์ Apple Pay

ถ้า ID ข้อกำหนดและเงื่อนไขถูกส่งกลับมาพร้อมกับกระบวนการทำงานตรวจสอบบัตร Apple จะดาวน์โหลดและแสดงข้อกำหนดและเงื่อนไขของผู้ออกบัตรไปยังผู้ใช้ ถ้าผู้ใช้ยอมรับข้อกำหนดและเงื่อนไข Apple จะส่ง ID ของข้อกำหนดที่ได้รับการยอมรับ รวมถึง CVV ไปที่กระบวนการผูกบัตรและกำหนดสิทธิ์ นอกจากนี้ ในฐานะที่เป็นส่วนหนึ่งของกระบวนการลิงก์และการกำหนดสิทธิ์ Apple จะแชร์ข้อมูลจากอุปกรณ์กับผู้ออกบัตรหรือเครือข่าย ซึ่งรวมถึงข้อมูลเกี่ยวกับ (a) กิจกรรมของบัญชี iTunes และ App Store ของผู้ใช้ (เช่น ผู้ใช้มีประวัติการทำธุรกรรมใน iTunes มายาวนานหรือไม่) (b) อุปกรณ์ของผู้ใช้ (เช่น หมายเลขโทรศัพท์ ชื่อ และรุ่นของอุปกรณ์ของผู้ใช้รวมถึงอุปกรณ์ Apple อื่นๆ ที่จำเป็นในการตั้งค่า Apple Pay) และ (c) ตำแหน่งที่ตั้งโดยประมาณของผู้ใช้ ณ เวลาที่ผู้ใช้เพิ่มบัตร (หากผู้ใช้เปิดใช้บริการระบุตำแหน่งที่ตั้งไว้) ผู้ออกบัตรจะใช้ข้อมูลนี้เพื่อตัดสินใจว่าจะอนุญาตการเพิ่มบัตรไปยัง Apple Pay หรือไม่

สองสิ่งจะเกิดขึ้นเป็นผลจากกระบวนการผูกบัตรและเตรียมใช้งาน:

- อุปกรณ์จะเริ่มดาวน์โหลดไฟล์บัตรผ่านกระเป๋าสตางค์ที่แสดงบัตรเครดิตหรือเดบิต
- อุปกรณ์จะเริ่มต้นผูกบัตรเข้ากับ Secure Element

ไฟล์บัตรผ่านประกอบด้วย URL สำหรับดาวน์โหลดภาพบัตร เมตาดาต้าเกี่ยวกับบัตร เช่น ข้อมูลติดต่อ แอปของผู้ออกบัตรที่เกี่ยวข้อง และคุณสมบัติที่รองรับ นอกจากนี้ ไฟล์บัตรผ่านยังประกอบด้วยข้อมูลสถานะบัตรผ่านอีกด้วย ซึ่งรวมถึงข้อมูลต่างๆ เช่น การปรับแต่ง Secure Element เสร็จสมบูรณ์หรือไม่ บัตรถูกระงับอยู่ในตอนนี้โดยผู้ออกบัตรหรือไม่ หรือต้องมีการตรวจสอบยืนยันเพิ่มเติมก่อนที่บัตรจะสามารถใช้ชำระเงินได้ด้วย Apple Pay หรือไม่

การเพิ่มบัตรเครดิตหรือบัตรเดบิตจากบัญชี iTunes Store

สำหรับบัตรเครดิตหรือบัตรเดบิตที่อยู่ในระบบของ iTunes ผู้ใช้อาจต้องป้อนรหัสผ่าน Apple ID ของตัวเองอีกครั้ง หมายเลขบัตรจะถูกดึงมาจาก iTunes และกระบวนการตรวจสอบบัตรจะเริ่มต้นขึ้น ถ้าบัตรสามารถใช้ได้กับ Apple Pay อุปกรณ์จะดาวน์โหลดและแสดงข้อกำหนดและเงื่อนไข จากนั้นจะส่ง ID ของข้อกำหนดและรหัสความปลอดภัยของบัตรไปที่กระบวนการผูกบัตรและกำหนดสิทธิ์ การตรวจสอบยืนยันเพิ่มเติมอาจเกิดขึ้นสำหรับบัตรบัญชี iTunes ที่บันทึกอยู่ในระบบ

การเพิ่มบัตรเครดิตหรือเดบิตจากแอปของผู้ออกบัตร

เมื่อแอปได้รับการลงทะเบียนสำหรับใช้งานกับ Apple Pay กุญแจจะถูกสร้างขึ้นสำหรับแอปและเซิร์ฟเวอร์ของผู้ออกบัตร กุญแจเหล่านี้ใช้สำหรับเข้ารหัสข้อมูลบัตรที่ส่งไปยังผู้ออกบัตร วิธีนี้ได้รับการออกแบบมาเพื่อป้องกันไม่ให้อุปกรณ์ของ Apple อ่านข้อมูลได้ โฟลว์การเตรียมใช้งานคล้ายคลึงกับที่ใช้สำหรับบัตรที่เพิ่มด้วยตัวเองตามที่อธิบายด้านบน ยกเว้นรหัสผ่านแบบครั้งเดียวจะถูกใช้แทนที่ CVV

การเพิ่มบัตรเครดิตหรือเดบิตจากเว็บไซต์ของผู้ออกบัตร

ผู้ออกบัตรบางรายสามารถเริ่มต้นกระบวนการกำหนดสิทธิ์บัตรสำหรับกระเป๋าสตางค์ได้โดยตรงจากเว็บไซต์ของผู้ออกบัตร ในกรณีนี้ ผู้ใช้เริ่มต้นกระบวนการโดยเลือกบัตรที่จะกำหนดสิทธิ์บนเว็บไซต์ของผู้ออกบัตร จากนั้นผู้ใช้จะถูกนำไปยังประสบการณ์การลงชื่อเข้า Apple แบบครบวงจร (ซึ่งอยู่ภายในโดเมนของ Apple) และจะถูกขอให้ลงชื่อเข้าด้วย Apple ID ของผู้ใช้ เมื่อลงชื่อเข้าสำเร็จแล้ว ผู้ใช้จะเลือกอุปกรณ์อย่างน้อยหนึ่งเครื่องเพื่อกำหนดสิทธิ์บัตร และจำเป็นต้องยืนยันผลการกำหนดสิทธิ์ในอุปกรณ์เป้าหมายแต่ละเครื่อง

การเพิ่มการตรวจสอบยืนยันเพิ่มเติม

ผู้ออกบัตรสามารถตัดสินใจได้ว่าบัตรเครดิตหรือบัตรเดบิตต้องการการตรวจสอบยืนยันเพิ่มเติมหรือไม่ ผู้ใช้อาจจะเลือกตัวเลือกที่แตกต่างกันสำหรับการตรวจสอบยืนยันเพิ่มเติมได้ ขึ้นอยู่กับตัวเลือกที่ผู้ออกบัตรมีให้ เช่น ข้อความตัวอักษร อีเมล การโทรหาฝ่ายบริการลูกค้า หรือวิธีการในแอปของบริษัทอื่นที่ได้รับอนุญาตเพื่อตรวจสอบยืนยันให้เสร็จสมบูรณ์ สำหรับข้อความตัวอักษรหรืออีเมล ผู้ใช้จะเลือกจากข้อมูลติดต่อที่ผู้ออกบัตรบันทึกอยู่ในระบบ ระบบจะส่งรหัสซึ่งต้องป้อนลงในกระเป๋าสตางค์ การตั้งค่า หรือแอป Apple Watch สำหรับบริการลูกค้าหรือการตรวจสอบยืนยันโดยใช้แอป ผู้ออกบัตรจะต้องดำเนินกระบวนการติดต่อสื่อสารของตัวเอง

การอนุญาตการชำระเงินกับ Apple Pay

สำหรับอุปกรณ์ที่มี Secure Enclave การชำระเงินจะทำได้หลังจากที่ได้รับอนุญาตจาก Secure Enclave เท่านั้น วิธีนี้จะรวมไปถึงการยืนยันว่าผู้ใช้ได้ยืนยันตัวตนด้วย Face ID, Touch ID หรือรหัสผ่านอุปกรณ์บน iPhone หรือ iPad ถ้ามี Face ID หรือ Touch ID จะถือว่าเป็นวิธีตามค่าเริ่มต้น แต่สามารถใช้รหัสได้ทุกเมื่อ รหัสจะถูกเสนอให้ใช้โดยอัตโนมัติหลังจากพยายามจับคู่ลายนิ้วมือไม่สำเร็จสามครั้ง หรือการพยายามจับคู่ใบหน้าไม่สำเร็จสองครั้ง หลังจากจับคู่ไม่สำเร็จห้าครั้ง คุณต้องใช้รหัส ต้องใช้รหัสเมื่อไม่ได้กำหนดค่า Face ID หรือ Touch ID หรือไม่ได้เปิดใช้งานสำหรับ Apple Pay สำหรับการชำระเงินบน Apple Watch อุปกรณ์จะต้องปลดล็อคด้วยรหัสแล้วกดปุ่มด้านข้างสองครั้ง

การใช้กุญแจการจับคู่ที่แชร์

การติดต่อระหว่าง Secure Enclave และ Secure Element จะเกิดขึ้นบนอินเทอร์เฟซแบบอนุกรม ซึ่งมี Secure Element เชื่อมต่อกับตัวควบคุม NFC ซึ่งจะเชื่อมต่อกับหน่วยประมวลผลแอปพลิเคชันอีกต่อหนึ่ง แม้ว่าจะไม่ถูกเชื่อมต่อโดยตรง Secure Enclave และ Secure Element จะสามารถสื่อสารได้อย่างปลอดภัยโดยใช้กุญแจการจับคู่ที่แชร์ซึ่งได้รับการจัดเตรียมระหว่างกระบวนการผลิต การเข้ารหัสและการยืนยันตัวตนของการสื่อสารนั้นใช้ AES ด้วย Nonces ที่มีการเข้ารหัสซึ่งใช้โดยทั้งสองฝ่ายเพื่อป้องกันการโจมตีแบบส่งข้อมูลซ้ำ กุญแจการจับคู่จะถูกสร้างขึ้นภายใน Secure Enclave จากกุญแจ UID และข้อมูลจำเพาะที่ไม่ซ้ำกันของ Secure Element จากนั้นกุญแจการจับคู่จะถูกถ่ายโอนอย่างปลอดภัยจาก Secure Enclave ไปยังโมดูลรักษาความปลอดภัยฮาร์ดแวร์ (HSM) ในโรงงาน ซึ่งมีข้อมูลกุญแจที่จำเป็นในการส่งกุญแจการจับคู่เข้าไปยัง Secure Element

การอนุญาตการทำธุรกรรมอย่างปลอดภัย

เมื่อผู้ใช้อนุญาตธุรกรรม ซึ่งรวมถึงลักษณะท่าทางทางกายภาพที่สื่อสารโดยตรงกับ Secure Enclave จากนั้น Secure Enclave จะส่งข้อมูลที่เซ็นชื่อแล้วเกี่ยวกับประเภทของการตรวจสอบสิทธิ์และรายละเอียดเกี่ยวกับประเภทของธุรกรรม (แบบไร้การสัมผัสหรือภายในแอป) ไปที่ Secure Element ซึ่งผูกอยู่กับค่า Authorization Random (AR) ค่า AR ถูกสร้างขึ้นใน Secure Enclave เมื่อผู้ใช้กำหนดสิทธิ์ของบัตรเครดิตเป็นครั้งแรก และค่าจะยังคงอยู่ต่อไปขณะที่ Apple Pay เปิดใช้งาน โดยได้รับการปกป้องด้วยการเข้ารหัสและกลไกป้องกันการย้อนกลับของ Secure Enclave AR จะถูกส่งไปยัง Secure Element อย่างปลอดภัยโดยใช้กุญแจการจับคู่ เมื่อได้รับค่า AR ใหม่ Secure Element จะทำเครื่องหมายบัตรใดๆ ที่เพิ่มไว้ก่อนหน้านี้ว่าถูกลบ

การใช้รหัสลับการชำระเงินเพื่อความปลอดภัยที่เปลี่ยนทุกครั้ง

รายการธุรกรรมการชำระเงินที่มาจากแอพเพล็ตการชำระเงินประกอบด้วยรหัสลับการชำระเงินพร้อมหมายเลขบัญชีอุปกรณ์ รหัสลับนี้ซึ่งเป็นรหัสแบบครั้งเดียวจะมีการคำนวณโดยใช้ตัวนับธุรกรรมและกุญแจ ตัวนับธุรกรรมจะเพิ่มขึ้นทุกครั้งที่มีธุรกรรมรายการใหม่ กุญแจจะถูกกำหนดสิทธิ์ในแอพเพล็ตการชำระเงินระหว่างการตั้งค่าส่วนบุคคล และเป็นกุญแจที่เครือข่ายการชำระเงิน หรือผู้ออกบัตร หรือเครือข่ายการชำระเงินและผู้ออกบัตรรู้จัก ข้อมูลอื่นๆ อาจถูกใช้ในการคำนวณเช่นกัน ทั้งนี้ขึ้นอยู่กับแบบแผนการชำระเงิน ข้อมูลดังกล่าวรวมถึง:

- Terminal Unpredictable Number สำหรับธุรกรรมผ่าน Near Field Communication (NFC)
- ค่า Nonce จากเซิร์ฟเวอร์ Apple Pay สำหรับธุรกรรมภายในแอป

รหัสความปลอดภัยเหล่านี้จะมีการส่งมอบให้กับเครือข่ายการชำระเงินและผู้ออกบัตร ซึ่งจะทำให้ผู้ออกบัตรสามารถตรวจสอบยืนยันรายการธุรกรรมแต่ละรายการได้ ความยาวของรหัสความปลอดภัยเหล่านี้อาจแตกต่างออกไปขึ้นอยู่กับประเภทของรายการธุรกรรม

การชำระเงินด้วยบัตรโดยใช้ Apple Pay

Apple Pay สามารถใช้เพื่อชำระเงินสำหรับสินค้าที่ซื้อในร้าน ภายในแอป และในเว็บไซต์ได้

การชำระเงินด้วยบัตรในร้าน

ถ้า iPhone หรือ Apple Watch เปิดอยู่และตรวจพบพื้นที่ NFC อุปกรณ์จะแสดงให้ผู้ใช้เห็นบัตรที่ร้องขอ (หากการเลือกอัตโนมัติเปิดใช้อยู่สำหรับบัตรนั้น) หรือบัตรเริ่มต้น ซึ่งจัดการได้ในการตั้งค่า ผู้ใช้ยังสามารถไปที่กระเป๋าสตางค์ แล้วเลือกบัตรได้ หรือเมื่ออุปกรณ์ล็อคอยู่ผู้ใช้ก็สามารถ:

- กดสองครั้งที่ปุ่มด้านข้างบนอุปกรณ์ที่มี Face ID
- กดสองครั้งที่ปุ่มโฮมบนอุปกรณ์ที่มี Touch ID
- การใช้คุณสมบัติการช่วยการเข้าถึงที่อนุญาตให้เข้าถึง Apple Pay จากหน้าจอที่ล็อคอยู่

ขั้นต่อไป ก่อนการส่งข้อมูล ผู้ใช้ต้องยืนยันตัวตนโดยใช้ Face ID, Touch ID หรือรหัส เมื่อ Apple Watch ปลดล็อคอยู่ การกดสองครั้งที่ปุ่มด้านข้างจะเป็นการเปิดใช้งานบัตรเริ่มต้นสำหรับการชำระเงิน ระบบจะไม่ส่งข้อมูลการชำระเงินใดๆ โดยไม่มีการตรวจสอบสิทธิ์ของผู้ใช้

หลังจากผู้ใช้ตรวจสอบสิทธิ์ หมายเลขบัญชีอุปกรณ์และรหัสความปลอดภัยสำหรับธุรกรรมรายการเฉพาะที่เปลี่ยนทุกครั้งจะถูกใช้เมื่อประมวลผลการชำระเงิน ทั้ง Apple และอุปกรณ์ของผู้ใช้จะไม่ส่งหมายเลขบัตรเครดิตหรือบัตรเดบิตแบบเต็มไปยังผู้ขาย Apple อาจจะได้รับข้อมูลรายการธุรกรรมที่ไม่ระบุชื่อ เช่น เวลาและตำแหน่งที่ตั้งโดยประมาณของรายการธุรกรรม ซึ่งจะช่วยปรับปรุง Apple Pay และผลิตภัณฑ์และบริการอื่นๆ ของ Apple

การชำระเงินด้วยบัตรภายในแอป

Apple Pay ยังสามารถใช้เพื่อชำระเงินบนแอป iPhone, iPad, Mac และ Apple Watch ได้อีกด้วย เมื่อผู้ใช้ชำระเงินในแอปโดยใช้ Apple Pay ทาง Apple จะได้รับข้อมูลธุรกรรมที่เข้ารหัส ก่อนที่ข้อมูลจะถูกส่งไปยังนักพัฒนาหรือผู้ขาย Apple จะเข้ารหัสรายการธุรกรรมนั้นอีกครั้งด้วยกุญแจที่ใช้สำหรับนักพัฒนาโดยเฉพาะ Apple Pay จะเก็บข้อมูลรายการธุรกรรมที่ไม่ระบุชื่อ เช่น ยอดซื้อโดยประมาณ ข้อมูลนี้ไม่สามารถผูกกับผู้ใช้ได้ และไม่รวมข้อมูลรายการที่ผู้ใช้ซื้อ

เมื่อแอปเริ่มต้นธุรกรรมการชำระเงิน Apple Pay เซิร์ฟเวอร์ Apple Pay จะได้รับรายการธุรกรรมที่เข้ารหัสจากอุปกรณ์ก่อนที่ผู้ขายจะได้รับ จากนั้นเซิร์ฟเวอร์ Apple Pay จะเข้ารหัสรายการธุรกรรมอีกครั้งโดยใช้กุญแจสำหรับผู้ขายโดยเฉพาะก่อนที่จะส่งธุรกรรมต่อไปให้ผู้ขาย

เมื่อแอปร้องขอการชำระเงิน แอปจะเรียกไปยัง API เพื่อระบุว่าอุปกรณ์รองรับ Apple Pay หรือไม่ และผู้ใช้มีบัตรเครดิตหรือบัตรเดบิตที่สามารถชำระเงินบนเครือข่ายการชำระเงินที่ผู้ขายยอมรับหรือไม่ แอปจะร้องขอชิ้นส่วนของข้อมูลใดๆ ที่จำเป็นต้องใช้เพื่อประมวลผลและทำรายการธุรกรรมให้สมบูรณ์ เช่น ที่อยู่การเรียกเก็บเงินและที่อยู่จัดส่ง และข้อมูลติดต่อ จากนั้นแอปจะขอให้ iOS, iPadOS หรือ watchOS แสดงหน้า Apple Pay ซึ่งจะร้องขอข้อมูลสำหรับแอป รวมถึงข้อมูลที่จำเป็นอื่นๆ เช่น บัตรที่ต้องใช้

ในตอนนี้ แอปจะได้รับข้อมูลเมือง รัฐ และรหัสไปรษณีย์เพื่อคำนวณค่าจัดส่งสุดท้าย แอปจะไม่ให้ข้อมูลที่ร้องขอแบบครบชุดจนกว่าผู้ใช้จะอนุมัติการชำระเงินด้วย Face ID, Touch ID, หรือรหัสของอุปกรณ์ หลังจากการชำระเงินได้รับอนุญาตแล้ว ข้อมูลที่แสดงในหน้า Apple Pay จะถูกถ่ายโอนไปยังผู้ขาย

การอนุญาตการชำระเงินในแอป

เมื่อผู้ใช้อนุมัติการชำระเงิน จะมีการเรียกไปยังเซิร์ฟเวอร์ Apple Pay เพื่อรับ Nonce แบบเข้ารหัสซึ่งคล้ายกับค่าที่ส่งกลับมาโดยเทอร์มินัล NFC ที่ใช้สำหรับการทำธุรกรรมในร้านค้า ค่า Nonce พร้อมกับข้อมูลธุรกรรมอื่นๆ จะถูกส่งต่อไปยัง Secure Element เพื่อคำนวณข้อมูลประจำตัวการชำระเงินที่เข้ารหัสด้วยกุญแจของ Apple ข้อมูลประจำตัวการชำระเงินที่เข้ารหัสจะถูกส่งคืนไปยังเซิร์ฟเวอร์ Apple Pay ซึ่งจะถอดรหัสข้อมูลประจำตัว ตรวจสอบยืนยัน Nonce ในข้อมูลประจำตัวกับ Nonce ที่ส่งมาจากเซิร์ฟเวอร์ Apple Pay เดิม และเข้ารหัสข้อมูลประจำตัวการชำระเงินอีกครั้งด้วยรหัสผู้ขายที่เชื่อมโยงกับ ID ผู้ขาย จากนั้นการชำระเงินจะถูกส่งกลับไปยังอุปกรณ์ ซึ่งจะส่งข้อมูลกลับไปยังแอปผ่าน API และจากนั้นแอปจะส่งข้อมูลไปยังระบบของผู้ค้าเพื่อประมวลผล ผู้ค้าสามารถถอดรหัสเอกสารสิทธิ์การชำระเงินด้วยกุญแจส่วนตัวสำหรับการประมวลผล กระบวนการนี้พร้อมกับลายเซ็นจากเซิร์ฟเวอร์ของ Apple ช่วยให้ผู้ขายสามารถตรวจสอบยืนยันได้ว่ารายการธุรกรรมนั้นเป็นไปเพื่อผู้ขายรายนี้โดยเฉพาะ

API ต้องใช้สิทธิ์ที่ระบุ ID ผู้ขายที่รองรับ แอปยังสามารถรวมข้อมูลเพิ่มเติม (เช่น หมายเลขคำสั่งซื้อหรือข้อมูลประจำตัวลูกค้า) เพื่อส่งไปที่ Secure Element ให้ลงชื่อ ทั้งนี้เพื่อให้แน่ใจว่าธุรกรรมไม่สามารถเบี่ยงเบนไปที่ลูกค้ารายอื่นได้ สิ่งนี้สามารถดำเนินการให้สำเร็จได้โดยนักพัฒนาแอป ซึ่งสามารถระบุ applicationData บน PKPaymentRequest ได้ แฮชของข้อมูลนี้จะถูกรวมอยู่ในข้อมูลการชำระเงินที่เข้ารหัส จากนั้นผู้ขายจะเป็นผู้รับผิดชอบในการตรวจสอบยืนยันว่าแฮช applicationData ของตนตรงกับข้อมูลที่รวมอยู่ในข้อมูลการชำระเงิน

การชำระเงินด้วยบัตรในเว็บไซต์

Apple Pay สามารถใช้เพื่อชำระเงินในเว็บไซต์ได้บน iPhone, iPad, Apple Watch และคอมพิวเตอร์ Mac ที่มี Touch ID ธุรกรรม Apple Pay ยังสามารถเริ่มต้นได้บน Mac แล้วทำให้เสร็จสมบูรณ์บน iPhone หรือ Apple Watch ที่สามารถใช้งาน Apple Pay ได้ ซึ่งใช้บัญชี iCloud เดียวกันได้อีกด้วย

Apple Pay บนเว็บกำหนดให้เว็บไซต์ที่เข้าร่วมทั้งหมดลงทะเบียนกับ Apple หลังจากลงทะเบียนโดเมนแล้ว การตรวจสอบความถูกต้องของชื่อโดเมนจะดำเนินการหลังจากที่ Apple ออกใบรับรองสำหรับลูกข่าย TLS แล้วเท่านั้น เว็บไซต์ที่รองรับ Apple Pay จะต้องแสดงเนื้อหาผ่าน HTTPS สำหรับธุรกรรมการชำระเงินในแต่ละรายการ เว็บไซต์จะต้องเก็บเซสชั่นรักษาความปลอดภัยที่ไม่ซ้ำกันของผู้ค้ากับเซิร์ฟเวอร์ Apple ที่ใช้ใบรับรองสำหรับลูกข่าย TLS ที่ออกโดย Apple ข้อมูลเซสชั่นของผู้ค้าจะลงชื่อโดย Apple หลังจากลายเซ็นเซสชั่นของผู้ขายได้รับการตรวจสอบยืนยันแล้ว เว็บไซต์อาจสอบถามว่าผู้ใช้มีอุปกรณ์ที่สามารถใช้ Apple Pay ได้หรือไม่ และอุปกรณ์ของผู้ใช้มีบัตรเครดิต บัตรเดบิต หรือบัตรเติมเงินที่เปิดใช้งานบนอุปกรณ์นั้นอยู่หรือไม่ รายละเอียดอื่นจะไม่ถูกแชร์ ถ้าผู้ใช้ไม่ต้องการแชร์ข้อมูลนี้ ผู้ใช้สามารถปิดใช้งานคำขอ Apple Pay ในการตั้งค่าความเป็นส่วนตัวของ Safari บนอุปกรณ์ iPhone, iPad และ Mac ได้

หลังจากตรวจสอบความถูกต้องของเซสชั่นผู้ขายแล้ว มาตรการความเป็นส่วนตัวและความปลอดภัยทั้งหมดจะเหมือนกับกรณีที่ผู้ใช้ชำระเงินภายในแอป

ถ้าผู้ใช้จะส่งต่อข้อมูลที่เกี่ยวข้องกับการชำระเงินจาก Mac ไปยัง iPhone หรือ Apple Watch คุณสมบัติ Handoff สำหรับ Apple Pay จะใช้โปรโตคอลบริการข้อมูลประจำตัว (IDS) ของ Apple ที่เข้ารหัสแบบต้นทางถึงปลายทางเพื่อส่งข้อมูลเกี่ยวกับการชำระเงินระหว่าง Mac ของผู้ใช้และอุปกรณ์ที่ให้อนุญาต ลูกข่าย IDS บน Mac ใช้กุญแจอุปกรณ์ของผู้ใช้ในการเข้ารหัส เพื่อทำให้อุปกรณ์อื่นๆ ไม่สามารถถอดรหัสข้อมูลนี้ได้ และกุญแจดังกล่าวจะไม่มีให้ Apple ใช้งาน การค้นหาอุปกรณ์สำหรับ Handoff สำหรับ Apple Pay จะมีประเภทและข้อมูลจำเพาะที่ไม่ซ้ำกันของบัตรเครดิตของผู้ใช้ รวมไปถึงเมตาดาต้าบางส่วน หมายเลขบัญชีเฉพาะอุปกรณ์ของบัตรของผู้ใช้จะไม่ถูกแชร์ และจะยังคงถูกจัดเก็บอย่างปลอดภัยต่อไปบน iPhone หรือ Apple Watch ของผู้ใช้ Apple ยังถ่ายโอนที่อยู่สำหรับติดต่อ ที่อยู่จัดส่ง และที่อยู่เรียกเก็บเงินที่ใช้ล่าสุดของผู้ใช้อย่างปลอดภัยผ่านพวงกุญแจ iCloud อีกด้วย

หลังจากที่ผู้ใช้อนุมัติการชำระเงินโดยใช้ Face ID, Touch ID, รหัส หรือกดสองครั้งที่ปุ่มด้านข้างของ Apple Watch โทเค็นการชำระเงินที่เข้ารหัสไปยังสำหรับใบรับรองผู้ขายของแต่ละเว็บไซต์โดยเฉพาะจะถูกส่งอย่างปลอดภัยจาก iPhone หรือ Apple Watch ของผู้ใช้ไปยัง Mac จากนั้นจึงส่งไปยังเว็บไซต์ของร้านค้า

เฉพาะอุปกรณ์ที่อยู่ในระยะใกล้เคียงกันเท่านั้นที่สามารถกำหนดให้การชำระเงินเสร็จสมบูรณ์ได้ ระยะใกล้เคียงจะกำหนดโดยประกาศผ่านบลูทูธพลังงานต่ำ (BLE)

บัตรผ่านแบบไร้การสัมผัสใน Apple Pay

ในการส่งข้อมูลจากบัตรผ่านที่รองรับไปยังเทอร์มินัล NFC ที่ใช้งานร่วมกันได้ Apple จะใช้โปรโตคอล Apple Value Added Service (Apple VAS) โปรโตคอล VAS สามารถใช้ได้บนเทอร์มินัลแบบไร้สัมผัสหรือในแอปของ iPhone และใช้ NFC เพื่อสื่อสารกับอุปกรณ์ Apple ที่รองรับ โปรโตคอล VAS ทำงานได้ในระยะทางสั้นๆ และสามารถใช้เพื่อแสดงบัตรผ่านแบบไร้การสัมผัสเพียงอย่างเดียว หรือใช้เป็นส่วนหนึ่งของธุรกรรม Apple Pay ได้

เมื่อถืออุปกรณ์ใกล้กับเทอร์มินัล NFC เทอร์มินัลจะเริ่มรับข้อมูลบัตรผ่านโดยการส่งคำขอสำหรับบัตรผ่าน ถ้าผู้ใช้มีบัตรผ่านที่มีข้อมูลจำเพาะของผู้ให้บริการบัตร ผู้ใช้จะถูกขอให้อนุมัติการใช้งานโดยใช้ Face ID, Touch ID หรือรหัส ข้อมูลบัตรผ่าน ตราประทับเวลา และกุญแจ ECDH P-256 แบบสุ่มใช้ครั้งเดียวจะถูกใช้ร่วมกับกุญแจสาธารณะของผู้ให้บริการบัตรผ่านเพื่อรับกุญแจการเข้ารหัสสำหรับข้อมูลบัตรผ่าน ซึ่งจะถูกส่งไปยังเทอร์มินัล

ตั้งแต่ iOS 12.0.1 จนถึงและรวมถึง iOS 13 ผู้ใช้อาจเลือกบัตรผ่านด้วยตนเองก่อนที่จะแสดงต่อเครื่องอ่านบัตร NFC ของผู้ขาย ใน iOS 13.1 ขึ้นไป ผู้ให้บริการบัตรผ่านสามารถกำหนดค่าบัตรผ่านที่เลือกเองว่าจะให้มีการตรวจสอบสิทธิ์จากผู้ใช้หรือใช้งานโดยไม่ต้องตรวจสอบสิทธิ์ได้

การทำให้บัตรใช้งานไม่ได้ด้วย Apple Pay

บัตรเครดิต บัตรเดบิต และบัตรเติมเงินที่ถูกเพิ่มไปที่ Secure Element จะสามารถใช้งานได้ก็ต่อเมื่อมีการแสดงการอนุญาตไปยัง Secure Element โดยใช้กุญแจการจับคู่และค่า Authorization Random (AR) เดียวกันกับตอนที่เพิ่มบัตร เมื่อได้รับค่า AR ใหม่ Secure Element จะทำเครื่องหมายบัตรใดๆ ที่เพิ่มไว้ก่อนหน้านี้ว่าถูกลบ การทำเช่นนี้จะทำให้ระบบปฏิบัติการสั่งให้ Secure Enclave ระบุว่าบัตรไม่สามารถใช้ได้โดยทำเครื่องหมายสำเนาของค่า AR ว่าไม่ถูกต้องภายใต้สถานการณ์ต่อไปนี้:

วิธีการ	อุปกรณ์
รหัสถูกปิดใช้งาน	iPhone, iPad, Apple Watch
รหัสผ่านถูกปิดใช้งาน	Mac
ผู้ใช้ลงชื่อออกจาก iCloud	iPhone, iPad, Mac, Apple Watch
ผู้ใช้เลือกลบข้อมูลเนื้อหาและการตั้งค่าทั้งหมด	iPhone, iPad, Mac, Apple Watch
อุปกรณ์ถูกกู้คืนจากโหมดการกู้คืน	iPhone, iPad, Mac, Apple Watch
การเลิกจับคู่	Apple Watch

การระงับบัตร การเอาบัตรออก และการลบบัตร

ผู้ใช้สามารถระงับ Apple Pay บน iPhone, iPad และ Apple Watch ได้โดยตั้งค่าอุปกรณ์ให้อยู่ในโหมดสูญหายโดยใช้ “ค้นหาของฉัน” ผู้ใช้ยังสามารถเอาบัตรออกและลบบัตรออกจาก Apple Pay ได้โดยใช้ “ค้นหาของฉัน”, iCloud.com หรือบนอุปกรณ์ของผู้ใช้ได้โดยตรงผ่านกระเป๋าสตางค์ บน Apple Watch คุณสามารถเอาบัตรออกได้โดยใช้การตั้งค่า iCloud, แอป Apple Watch บน iPhone หรือเอาออกจากนาฬิกาได้โดยตรง ความสามารถในการชำระเงินโดยใช้บัตรบนอุปกรณ์จะถูกระงับหรือเอาออกจาก Apple Pay โดยผู้ออกบัตรหรือเครือข่ายการชำระเงินที่เกี่ยวข้อง แม้ว่าอุปกรณ์จะออฟไลน์อยู่และไม่ได้เชื่อมต่อกับเครือข่ายเซลลูลาร์หรือ Wi-Fi ก็ตาม ผู้ใช้ยังสามารถโทรหาผู้ออกบัตรเพื่อให้ระงับหรือเอาบัตรออกจาก Apple Pay ได้อีกด้วย

เมื่อผู้ใช้ลบข้อมูลทั้งอุปกรณ์โดยใช้การลบข้อมูลเนื้อหาและการตั้งค่าทั้งหมด หรือโดยใช้ “ค้นหาของฉัน” หรือกู้คืนอุปกรณ์ของตัวเอง iPhone, iPad, iPod touch, Mac และ Apple Watch จะสั่งให้ Secure Element ทำเครื่องหมายบัตรทั้งหมดว่าถูกลบ วิธีนี้จะมีผลเหมือนกับการเปลี่ยนบัตรเป็นสถานะไม่สามารถใช้งานได้โดยทันที จนกว่าจะสามารถติดต่อเซิร์ฟเวอร์ Apple Pay เพื่อให้ลบบัตรทั้งหมดออกจาก Secure Element อย่างสมบูรณ์ได้ Secure Enclave จะทำเครื่องหมาย AR ว่าไม่ถูกต้องโดยเป็นอิสระจากกัน ดังนั้นการอนุญาตการชำระเงินเพิ่มเติมสำหรับบัตรที่ลงทะเบียนไว้ก่อนหน้านี้จึงไม่สามารถทำได้ เมื่ออุปกรณ์ออนไลน์ อุปกรณ์จะพยายามติดต่อเซิร์ฟเวอร์ Apple Pay เพื่อช่วยให้แน่ใจว่าบัตรทั้งหมดใน Secure Element จะถูกลบ

ความปลอดภัยของ Apple Card

สำหรับ iPhone และ Mac รุ่นที่รองรับ ผู้ใช้สามารถสมัคร Apple Card ได้อย่างปลอดภัย

การสมัคร Apple Card

ใน iOS 12.4 ขึ้นไป macOS 10.14.6 ขึ้นไป และ watchOS 5.3 ขึ้นไป Apple Card สามารถใช้กับ Apple Pay เพื่อชำระเงินในร้าน ในแอป และบนเว็บได้

ในการสมัครใช้ Apple Card ผู้ใช้จะต้องลงชื่อเข้าบัญชี iCloud ของตัวเองบนอุปกรณ์ iOS หรือ iPadOS ที่สามารถใช้งานร่วมกับ Apple Pay ได้ จากนั้นตั้งค่าการตรวจสอบสิทธิ์สองปัจจัยบนบัญชี iCloud เมื่อการสมัครได้รับการอนุมัติ Apple Card จะพร้อมใช้งานในกระเป๋าสตางค์ หรือในการตั้งค่า > กระเป๋าสตางค์และ Apple Pay ในอุปกรณ์ที่เข้าเกณฑ์ใดๆ ที่ผู้ใช้ลงชื่อเข้าด้วย Apple ID ของตน

เมื่อผู้ใช้สมัครใช้ Apple Card ข้อมูลประจำตัวของผู้ใช้จะได้รับการตรวจสอบยืนยันอย่างปลอดภัยโดยคู่ค้าผู้ให้บริการข้อมูลประจำตัวของ Apple แล้วข้อมูลจะถูกแชร์กับ Goldman Sachs Bank USA เพื่อวัตถุประสงค์ด้านการประเมินข้อมูลประจำตัวและเครดิต

ข้อมูลอย่างเช่นหมายเลขประกันสังคมหรือภาพของเอกสารประจำตัวที่ให้ระหว่างการสมัครจะได้รับการส่งอย่างปลอดภัยไปที่คู่ค้าผู้ให้บริการข้อมูลประจำตัวของ Apple และ/หรือ Goldman Sachs Bank USA โดยเข้ารหัสด้วยกุญแจที่เกี่ยวข้องของผู้ใช้ Apple ไม่สามารถถอดรหัสข้อมูลนี้ได้

ข้อมูลรายได้ที่ให้ระหว่างการสมัครและข้อมูลบัญชีธนาคารที่ใช้ในการชำระบิลจะถูกส่งอย่างปลอดภัยไปยัง Goldman Sachs Bank USA โดยเข้ารหัสด้วยกุญแจของผู้ใช้ ข้อมูลบัญชีธนาคารจะถูกบันทึกในพวงกุญแจ Apple ไม่สามารถถอดรหัสข้อมูลนี้ได้

เมื่อมีการเพิ่ม Apple Card ลงในกระเป๋าสตางค์ อาจมีการแชร์ข้อมูลเดียวกันกับที่มีการแชร์เมื่อผู้ใช้เพิ่มบัตรเครดิตหรือบัตรเดบิตกับ Goldman Sachs Bank USA ซึ่งเป็นธนาคารคู่ค้าของ Apple และกับ Apple Payments Inc. ข้อมูลนี้ใช้สำหรับการแก้ไขปัญหา การป้องกันการฉ้อโกง และวัตถุประสงค์ด้านระเบียบข้อบังคับเท่านั้น

สำหรับ iOS 14.6 ขึ้นไป, iPadOS 14.6 ขึ้นไป และ watchOS 7.5 ขึ้นไป ผู้จัดการประจำครอบครัว iCloud ที่มี Apple Card จะสามารถแชร์บัตรของตนกับสมาชิกครอบครัว iCloud ที่มีอายุมากกว่า 13 ปีได้ ต้องมีการตรวจสอบสิทธิ์ผู้ใช้เพื่อยืนยันคำเชิญ กระเป๋าสตางค์ใช้กุญแจใน Secure Enclave เพื่อประมวลผลลายเซ็นที่ผูกมัดกับเจ้าของและผู้รับเชิญ ลายเซ็นนั้นจะได้รับการตรวจสอบบนเซิร์ฟเวอร์ของ Apple

หรือผู้จัดการสามารถกำหนดวงเงินการทำธุรกรรมสำหรับผู้เข้าร่วมได้ บัตรผู้เข้าร่วมยังสามารถถูกล็อคเพื่อหยุดการใช้จ่ายผ่านกระเป๋าสตางค์ได้ทุกเมื่ออีกด้วย เมื่อเจ้าของร่วมหรือผู้เข้าร่วมที่มีอายุเกิน 18 ปีตอบรับคำเชิญและทำการสมัคร พวกเขาจะต้องผ่านขั้นตอนการสมัครเดียวกับที่กำหนดไว้ในส่วนการสมัครของ Apple Card ในกระเป๋าสตางค์

การใช้ Apple Card

บัตรจริงสามารถสั่งซื้อได้จาก Apple Card ในกระเป๋าสตางค์ หลังจากที่ผู้ใช้ได้รับบัตรจริงแล้ว บัตรจะเปิดใช้งานโดยใช้แท็ก NFC ที่อยู่ในซองแบบพับสองทบของบัตรจริง แท็กของบัตรจะไม่ซ้ำกัน และไม่สามารถใช้เปิดใช้งานบัตรของผู้ใช้รายอื่นได้ หรือสามารถเปิดใช้งานบัตรด้วยตนเองได้ในการตั้งค่ากระเป๋าสตางค์ นอกจากนี้ผู้ใช้ยังสามารถเลือกที่จะล็อคหรือปลดล็อคบัตรจริงได้ตลอดเวลาจากกระเป๋าสตางค์

การชำระเงินด้วยบัตร Apple Card และรายละเอียดบัตรผ่านในกระเป๋าสตางค์

การชำระเงินที่ครบกำหนดชำระในบัญชี Apple Card สามารถดำเนินการได้จากกระเป๋าสตางค์ใน iOS ด้วย Apple Cash และบัญชีธนาคาร การชำระบิลสามารถกำหนดให้เป็นการชำระประจำหรือการชำระเพียงครั้งเดียวในวันที่ระบุได้ด้วย Apple Cash และบัญชีธนาคาร เมื่อผู้ใช้ชำระเงิน จะมีการเรียกไปยังเซิร์ฟเวอร์ Apple Pay เพื่อขอรับ Nonce ที่มีการเข้ารหัสคล้ายกับ Apple Cash Nonce พร้อมด้วยรายละเอียดการตั้งค่าการชำระเงิน จะถูกส่งต่อไปยัง Secure Element เพื่อประมวลผลลายเซ็น ลายเซ็นจะถูกส่งกลับไปยังเซิร์ฟเวอร์ Apple Pay การตรวจสอบสิทธิ์ ความสมบูรณ์ และความถูกต้องของการชำระเงินจะได้รับการตรวจสอบยืนยันผ่านลายเซ็นและค่า Nonce โดยเซิร์ฟเวอร์ Apple Pay และคำสั่งจะถูกส่งผ่านต่อไปยัง Goldman Sachs Bank USA เพื่อประมวลผล

กระเป๋าสตางค์จะดึงข้อมูลหมายเลข Apple Card โดยแสดงใบรับรอง เซิร์ฟเวอร์ Apple Pay จะตรวจสอบใบรับรองเพื่อยืนยันว่ากุญแจถูกสร้างขึ้นใน Secure Enclave จากนั้นใช้กุญแจนี้เพื่อเข้ารหัสหมายเลข Apple Card ก่อนส่งคืนไปยังกระเป๋าสตางค์เพื่อให้เฉพาะ iPhone ที่ขอหมายเลข Apple Card เท่านั้นที่สามารถถอดรหัสได้ หลังจากการถอดรหัส หมายเลข Apple Card จะถูกบันทึกไว้ในพวงกุญแจ iCloud

การแสดงรายละเอียดหมายเลข Apple Card ในบัตรผ่านโดยใช้กระเป๋าสตางค์ต้องมีการตรวจสอบสิทธิ์ผู้ใช้ด้วย Face ID, Touch ID หรือรหัส ผู้ใช้สามารถแทนที่สิ่งนี้ได้ในส่วนข้อมูลบัตร และปิดใช้งานของเก่า

การป้องกันการฉ้อโกงขั้นสูง

สำหรับ iOS 15 ขึ้นไป และ iPadOS 15 ขึ้นไป ผู้ใช้ Apple Card จะสามารถเปิดใช้งานการป้องกันการฉ้อโกงขั้นสูงในกระเป๋าสตางค์ได้ เมื่อเปิดใช้งานการป้องกันการฉ้อโกงขั้นสูงแล้ว รหัสความปลอดภัยของบัตรจะมีการดึงข้อมูลใหม่ทุกสองสามวัน

ความปลอดภัยของ Apple Cash

ใน iOS 11.2 ขึ้นไป, iPadOS 13.1 ขึ้นไป และ watchOS 4.2 ขึ้นไป คุณสามารถใช้ Apple Pay บน iPhone, iPad หรือ Apple Watch เพื่อส่ง รับ และเรียกขอเงินจากผู้ใช้รายอื่นได้ เมื่อผู้ใช้ได้รับเงิน เงินจะถูกเพิ่มในบัญชี Apple Cash ที่สามารถเข้าถึงได้ในกระเป๋าสตางค์หรือภายในการตั้งค่า > กระเป๋าสตางค์และ Apple Pay ในอุปกรณ์ที่เข้าเกณฑ์ใดๆ ที่ผู้ใช้ลงชื่อเข้าด้วย Apple ID ของตน

ใน iOS 14, iPadOS 14 และ watchOS 7 ผู้จัดการประจำครอบครัว iCloud ที่ยืนยันตัวตนด้วย Apple Cash จะสามารถเปิดใช้งาน Apple Cash ให้กับสมาชิกในครอบครัวที่มีอายุต่ำกว่า 18 ปีได้ ผู้จัดการสามารถจำกัดความสามารถในการส่งเงินของผู้ใช้เหล่านี้ให้เฉพาะสมาชิกครอบครัวหรือเฉพาะรายชื่อได้ ถ้ามีสมาชิกในครอบครัวที่อายุต่ำกว่า 18 ปีที่ผ่านการกู้คืนบัญชี Apple ID ผู้จัดการประจำครอบครัวจะต้องเปิดใช้งานบัตร Apple Cash อีกครั้งด้วยตนเองสำหรับผู้ใช้รายนั้น ถ้าสมาชิกครอบครัวที่มีอายุต่ำกว่า 18 ปีไม่ได้เป็นส่วนหนึ่งของครอบครัว iCloud แล้ว ยอดเงิน Apple Cash ของพวกเขาจะถ่ายโอนไปยังบัญชีของผู้จัดการโดยอัตโนมัติ

เมื่อคุณตั้งค่า Apple Cash ข้อมูลเดียวกันกับตอนที่คุณเพิ่มบัตรเครดิตหรือบัตรเดบิตอาจจะถูกแชร์กับธนาคารคู่ค้าของเรา Green Dot Bank และกับ Apple Payments Inc. ซึ่งเป็นบริษัทย่อยที่ Apple เป็นเจ้าของทั้งหมด บริษัทนี้สร้างขึ้นเพื่อปกป้องความเป็นส่วนตัวของผู้ใช้โดยจะจัดเก็บและประมวลผลข้อมูลแยกต่างหากจากส่วนที่เหลือของ Apple และด้วยวิธีที่ส่วนที่เหลือของ Apple ไม่ทราบ ข้อมูลนี้จะใช้เพื่อจุดประสงค์ด้านการแก้ไขปัญหา การป้องกันการฉ้อโกง และระเบียบข้อบังคับเท่านั้น

การใช้ Apple Cash ใน iMessage

ในการใช้การชำระเงินแบบคนสู่คนและใช้ Apple Cash ผู้ใช้จะต้องลงชื่อเข้าบัญชี iCloud ของตัวเองบนอุปกรณ์ที่สามารถใช้งานร่วมกับ Apple Cash ได้ จากนั้นตั้งค่าการตรวจสอบสิทธิ์สองปัจจัยบนบัญชี iCloud คำขอและการถ่ายโอนข้อมูลทางการเงินระหว่างผู้ใช้เริ่มต้นจากภายในแอปข้อความหรือโดยการถาม Siri เมื่อผู้ใช้พยายามส่งเงิน iMessage จะแสดงหน้า Apple Pay ยอดเงิน Apple Cash จะถูกใช้ก่อนเสมอ ถ้ามีความจำเป็น ระบบจะดึงเงินเพิ่มเติมจากบัตรเครดิตหรือบัตรเดบิตใบที่สองที่ผู้ใช้เพิ่มไว้ในกระเป๋าสตางค์

การใช้ Apple Cash ในร้าน แอป และบนเว็บ

สามารถใช้บัตร Apple Cash ในกระเป๋าสตางค์กับ Apple Pay เพื่อชำระเงินในร้านค้า ในแอป และบนเว็บได้ เงินในบัญชี Apple Cash ยังสามารถโอนไปที่บัญชีธนาคารได้อีกด้วย นอกจากการได้รับเงินจากผู้ใช้รายอื่นแล้ว ผู้ใช้ยังสามารถเติมเงินเข้าบัญชี Apple Cash จากบัตรเดบิตหรือบัตรเติมเงินในกระเป๋าสตางค์ได้อีกด้วย

Apple Payments Inc. จะจัดเก็บและอาจจะใช้ข้อมูลธุรกรรมของผู้ใช้สำหรับการแก้ไขปัญหา การป้องกันการฉ้อโกง และสำหรับจุดประสงค์ตามระเบียบข้อบังคับเมื่อดำเนินการธุรกรรมเสร็จแล้ว ส่วนอื่นๆ ของ Apple จะไม่ทราบว่าผู้ใช้ส่งเงินให้ใคร รับเงินจากใคร หรือซื้อสินค้าด้วยบัตร Apple Cash ที่ใด

เมื่อผู้ใช้ส่งเงินด้วย Apple Pay หรือเพิ่มเงินเข้าบัญชี Apple Cash หรือโอนเงินเข้าบัญชีธนาคาร จะมีการเรียกไปยังเซิร์ฟเวอร์ Apple Pay เพื่อขอรับ nonce ที่มีการเข้ารหัส ซึ่งคล้ายกับกับค่าที่ส่งกลับมาสำหรับภายในแอป Apple Pay Nonce พร้อมกับข้อมูลธุรกรรมอื่นๆ จะถูกส่งไปยัง Secure Element เพื่อประมวลผลลายเซ็นสำหรับการชำระเงิน ลายเซ็นจะส่งคืนไปยังเซิร์ฟเวอร์ Apple Pay การตรวจสอบสิทธิ์ ความสมบูรณ์ และความถูกต้องของธุรกรรมจะได้รับการตรวจสอบยืนยันผ่านลายเซ็นการชำระเงินและค่า Nonce โดยเซิร์ฟเวอร์ Apple Pay จากนั้นการโอนเงินจะเริ่มต้น และผู้ใช้จะได้รับแจ้งเมื่อธุรกรรมเสร็จสมบูรณ์แล้ว

ถ้าธุรกรรมเกี่ยวข้องกับรายการต่อไปนี้:

- บัตรเดบิตสำหรับเพิ่มเงิน Apple Cash
- การให้เงินเพิ่มเติมหากยอดเงินใน Apple Cash ไม่เพียงพอ

เอกสารสิทธิ์การชำระเงินที่เข้ารหัสยังมีการสร้างและส่งข้อมูลไปยังเซิร์ฟเวอร์ Apple Pay อีกด้วย ซึ่งจะคล้ายกับการทำงานของ Apple Pay ภายในแอปและเว็บไซต์

หลังจากยอดเงินของบัญชี Apple Cash เกินจำนวนที่กำหนด หรือถ้าตรวจพบกิจกรรมที่ผิดปกติ ผู้ใช้จะได้รับแจ้งให้ตรวจสอบยืนยันข้อมูลประจำตัว ข้อมูลที่ให้สำหรับตรวจสอบยืนยันข้อมูลประจำตัวของผู้ใช้ เช่น หมายเลขประกันสังคม หรือคำตอบสำหรับคำถามต่างๆ (เช่น ยืนยันชื่อถนนที่ผู้ใช้เคยอาศัยก่อนหน้านี้) จะถูกส่งอย่างปลอดภัยไปยังคู่ค้าของ Apple และเข้ารหัสโดยใช้กุญแจของผู้ใช้ Apple ไม่สามารถถอดรหัสข้อมูลนี้ได้ ผู้ใช้จะได้รับการแจ้งให้ตรวจสอบยืนยันข้อมูลประจำตัวของตนเองอีกครั้งหากกู้คืนบัญชี Apple ID ก่อนที่จะได้รับสิทธิ์เข้าถึงยอดเงิน Apple Cash ของตนเอง

Tap to Pay on iPhone อย่างปลอดภัย

Tap to Pay on iPhone มีให้ใช้งานใน iOS 15.4 ซึ่งทำให้ร้านค้าในสหรัฐอเมริกายอมรับการชำระเงินผ่าน Apple Pay และการชำระเงินแบบไร้การสัมผัสอื่นๆ โดยใช้ iPhone และแอป iOS ที่เปิดใช้งานโดยคู่ค้า ด้วยบริการนี้ ผู้ใช้ที่มีอุปกรณ์ iPhone ที่รองรับสามารถรับการชำระเงินแบบไร้การสัมผัส รวมถึงบัตรผ่าน **Apple Pay** ที่รองรับ NFC ได้อย่างปลอดภัย เมื่อใช้ Tap to Pay on iPhone ผู้ขายไม่จำเป็นต้องใช้ฮาร์ดแวร์เพิ่มเติมเพื่อรับการชำระเงินแบบไร้การสัมผัส

Tap to Pay on iPhone ได้รับการออกแบบมาเพื่อปกป้องข้อมูลส่วนบุคคลของผู้ชำระเงิน บริการนี้จะไม่รวบรวมข้อมูลการทำธุรกรรมที่สามารถผูกโยงกับผู้ชำระเงินได้ ข้อมูลบัตรชำระเงิน เช่น หมายเลขบัตรเครดิต/เดบิต (PAN) ได้รับการรักษาความปลอดภัยโดย Secure Element และไม่มีการส่งข้อมูลนี้ให้ร้านค้า ข้อมูลบัตรชำระเงินจะอยู่ระหว่างผู้ให้บริการชำระเงินของร้านค้า ผู้ชำระเงิน และผู้ออกบัตร นอกจากนี้ บริการ Tap to Pay จะไม่เก็บชื่อ ที่อยู่ หรือเบอร์โทรศัพท์ของผู้ชำระเงิน

Tap to Pay on iPhone ได้รับการประเมินจากภายนอกโดยห้องปฏิบัติการด้านความปลอดภัยที่ได้รับการรับรอง และได้รับการอนุมัติโดย American Express, Discover, Mastercard และ Visa

ความปลอดภัยขององค์ประกอบการชำระเงินแบบไร้การสัมผัส

- **Secure Element:** Secure Element [ลิงก์ไปยังส่วน Secure Element ของ Apple Pay] ซึ่งโฮสต์เคอร์เนลการชำระเงินที่อ่านและรักษาความปลอดภัยข้อมูลบัตรชำระเงินแบบไร้การสัมผัส
- **ตัวควบคุม NFC:** ตัวควบคุม NFC จะจัดการโปรโตคอล Near Field Communication และกำหนดเส้นทางการสื่อสารระหว่างหน่วยประมวลผลแอปพลิเคชันและ Secure Element และระหว่าง Secure Element กับบัตรชำระเงินแบบไร้การสัมผัส
- **เซิร์ฟเวอร์ของ Tap to Pay on iPhone:** เซิร์ฟเวอร์ Tap to Pay on iPhone จะจัดการการตั้งค่าและการกำหนดสิทธิ์เคอร์เนลการชำระเงินในอุปกรณ์ เซิร์ฟเวอร์ยังตรวจสอบความปลอดภัยของ Tap to Pay on iPhone ในลักษณะที่เข้ากันได้กับมาตรฐานของการชำระเงินแบบไร้การสัมผัสบน COTS (CPoC) จาก Payment Card Industry Security Standards Council (PCI SSC) และเป็นไปตามมาตรฐานของ PCI DSS

วิธีที่ Tap to Pay อ่านบัตรเครดิต บัตรเดบิต และบัตรเติมเงิน

ภาพรวมการรักษาความปลอดภัยการกำหนดสิทธิ์

เมื่อใช้ Tap to Pay on iPhone ครั้งแรกโดยใช้แอปที่มีสิทธิ์เพียงพอ เซิร์ฟเวอร์ Tap to Pay on iPhone จะตรวจสอบว่าอุปกรณ์ตรงตามเกณฑ์คุณสมบัติหรือไม่ เช่น รุ่นของอุปกรณ์ เวอร์ชั่น iOS และมีการกำหนดรหัสหรือไม่ หลังจากการตรวจสอบเสร็จสิ้น แอพเพล็ตการยอมรับการชำระเงินจะถูกดาวน์โหลดจากเซิร์ฟเวอร์ Tap to Pay on iPhone และติดตั้งบน Secure Element พร้อมกับการกำหนดค่าเคอร์เนลการชำระเงินที่เกี่ยวข้อง การดำเนินการนี้จะดำเนินการอย่างปลอดภัยระหว่างเซิร์ฟเวอร์ Tap to Pay on iPhone และ Secure Element Secure Element จะตรวจสอบความสมบูรณ์และความถูกต้องของข้อมูลนี้ก่อนการติดตั้ง

ภาพรวมความปลอดภัยของการอ่านบัตร

เมื่อแอป Tap to Pay on iPhone ร้องขอการอ่านบัตรจากเฟรมเวิร์ค ProximityReader แผ่นงานที่ควบคุมโดย iOS จะแสดงขึ้นและแจ้งให้ผู้ใช้แตะบัตรชำระเงิน จากนั้น iOS จะเริ่มต้นการทำงานของเครื่องอ่านบัตรชำระเงินแล้วขอเคอร์เนลการชำระเงินใน Secure Element เพื่อเริ่มต้นการอ่านบัตร

ในขั้นตอนนี้ Secure Element จะเข้าควบคุมตัวควบคุม NFC ในโหมดตัวอ่าน โหมดนี้อนุมัติให้แลกเปลี่ยนข้อมูลบัตรระหว่างบัตรชำระเงินและ Secure Element ผ่านตัวควบคุม NFC เท่านั้น บัตรชำระเงินสามารถอ่านได้เฉพาะในโหมดนี้

หลังจากที่แอพเพล็ตการยอมรับการชำระเงินบน Secure Element ได้อ่านบัตรเสร็จแล้ว แอพเพล็ตจะเข้ารหัสและลงชื่อข้อมูลของบัตร ข้อมูลบัตรยังคงเข้ารหัสและได้รับการตรวจสอบสิทธิ์จนกว่าจะส่งถึงผู้ให้บริการชำระเงิน เฉพาะผู้ให้บริการชำระเงินที่แอปใช้ในการร้องขอการอ่านบัตรเท่านั้นที่สามารถถอดรหัสข้อมูลบัตรได้ ผู้ให้บริการชำระเงินต้องขอกุญแจถอดรหัสข้อมูลบัตรจากเซิร์ฟเวอร์ Tap to Pay on iPhone เซิร์ฟเวอร์ Tap to Pay on iPhone จะปล่อยกุญแจถอดรหัสไปยังผู้ให้บริการชำระเงินหลังจากตรวจสอบยืนยันความสมบูรณ์และความถูกต้องของข้อมูล และหลังจากตรวจสอบยืนยันว่าบัตรจะอ่านได้ภายใน 60 วินาทีนับจากที่อ่านบัตรบนอุปกรณ์

โมเดลนี้ช่วยให้แน่ใจว่าข้อมูลบัตรไม่สามารถถอดรหัสได้โดยบุคคลอื่นที่ไม่ใช่ผู้ให้บริการชำระเงิน ซึ่งดำเนินการธุรกรรมนี้แทนร้านค้า

การใช้กระเป๋าสตางค์

การเข้าถึงโดยใช้กระเป๋าสตางค์

ผู้ใช้สามารถเก็บกุญแจบ้าน กุญแจรถ และกุญแจสำหรับห้องพักในโรงแรมไว้ในกระเป๋าสตางค์บนอุปกรณ์ iPhone และ Apple Watch ที่รองรับได้ ผู้ใช้ยังสามารถจัดเก็บป้ายชื่อที่ใช้ในองค์กรและบัตรประจำตัวนักเรียนได้อีกด้วย เมื่อผู้ใช้มาถึงประตู ระบบจะแสดงกุญแจที่ถูกต้องโดยอัตโนมัติ ทำให้ผู้ใช้สามารถผ่านเข้าไปได้ด้วยการแตะเพียงครั้งเดียวโดยใช้ Near Field Communication (NFC)

ความสะดวกของผู้ใช้

เมื่อมีการเพิ่มกุญแจ บัตรผ่าน บัตรประจำตัวนักเรียน หรือป้ายชื่อที่ใช้ในองค์กรในกระเป๋าสตางค์ โหมดเร่งด่วนจะเปิดใช้ตามค่าเริ่มต้น บัตรในโหมดเร่งด่วนจะโต้ตอบกับเครื่องปลายทางที่รับสัญญาณโดยไม่ต้องใช้ Face ID, Touch ID, การตรวจสอบสิทธิ์ด้วยรหัส หรือการกดสองครั้งที่ปุ่มด้านข้างของ Apple Watch ในการปิดใช้งานคุณสมบัตินี้ ผู้ใช้สามารถปิดใช้โหมดเร่งด่วนได้โดยแตะปุ่มเพิ่มเติมที่ด้านหน้าของบัตรในกระเป๋าสตางค์ ในการเปิดใช้โหมดเร่งด่วนอีกครั้ง ผู้ใช้ต้องใช้ Face ID, Touch ID หรือรหัส

ความเป็นส่วนตัวและความปลอดภัย

กุญแจในกระเป๋าสตางค์ใช้ประโยชน์จากความเป็นส่วนตัวและความปลอดภัยที่มีอยู่ใน iPhone และ Apple Watch อย่างเต็มที่ Apple จะไม่ได้รับการแชร์ข้อมูลว่าบุคคลใช้กุญแจในกระเป๋าสตางค์เมื่อใดหรือที่ไหน และจะไม่มีการเก็บข้อมูลไว้ในเซิร์ฟเวอร์ของ Apple รวมถึงข้อมูลประจำตัวจะถูกเก็บไว้อย่างปลอดภัยภายใน Secure Element (SE) ของอุปกรณ์ที่รองรับ โฮสต์ SE ออกแบบแอพเพล็ตเป็นพิเศษเพื่อจัดการและจัดเก็บกุญแจการเข้าถึงอย่างปลอดภัย ทำให้มั่นใจได้ว่ากุญแจไม่สามารถถูกดึงข้อมูลออกมาได้

ก่อนกำหนดสิทธิ์กุญแจการเข้าถึงใดๆ ผู้ใช้จะต้องลงชื่อเข้าบัญชี iCloud ของตนบน iPhone ที่ใช้งานร่วมกันได้ และเปิดใช้การตรวจสอบสิทธิ์สองปัจจัยสำหรับบัญชี iCloud ของตน ยกเว้นบัตรประจำตัวนักเรียนซึ่งไม่ต้องเปิดใช้การตรวจสอบสิทธิ์สองปัจจัย

เมื่อผู้ใช้เริ่มกระบวนการกำหนดสิทธิ์ จะมีขั้นตอนที่คล้ายกับขั้นตอนที่เกี่ยวข้องกับการกำหนดสิทธิ์บัตรเครดิตและเดบิต เช่น ลิงก์และการกำหนดสิทธิ์ ระหว่างการทำธุรกรรม ตัวอ่านจะสื่อสารกับ Secure Element ผ่านตัวควบคุม Near-field-communication (NFC) โดยใช้ช่องทางที่ปลอดภัยที่กำหนดไว้

จำนวนอุปกรณ์ ซึ่งรวมถึง iPhone และ Apple Watch ที่สามารถกำหนดสิทธิ์ด้วยกุญแจการเข้าถึงได้จะถูกกำหนดและควบคุมโดยคู่ค้าแต่ละราย และอาจแตกต่างกันไปสำหรับแต่ละคู่ค้า วิธีการดังกล่าวช่วยให้คู่ค้าแต่ละรายสามารถควบคุมจำนวนกุญแจการเข้าถึงที่กำหนดสิทธิ์ไว้สูงสุดต่อประเภทอุปกรณ์เพื่อให้เหมาะกับความต้องการเฉพาะได้ เพื่อจุดประสงค์นี้ Apple จะจัดหาประเภทอุปกรณ์และข้อมูลจำเพาะอุปกรณ์ที่ไม่ระบุชื่อให้กับคู่ค้า ข้อมูลจำเพาะจะแตกต่างกันไปสำหรับคู่ค้าทุกรายเนื่องจากเหตุผลด้านความเป็นส่วนตัวและความปลอดภัย

สามารถปิดใช้งานหรือเอากุญแจออกได้โดย:

- การลบอุปกรณ์จากระยะไกลด้วย “ค้นหาของฉัน”
- การเปิดใช้งานโหมดสูญหายด้วย “ค้นหาของฉัน”
- การรับคำสั่งล้างข้อมูลระยะไกลสำหรับการจัดการอุปกรณ์เคลื่อนที่ (MDM)
- การเอาบัตรทั้งหมดออกจากหน้าบัญชี Apple ID ของผู้ใช้
- การเอาบัตรทั้งหมดออกจาก iCloud.com
- การนำบัตรทั้งหมดออกจากกระเป๋าสตางค์
- การเอาบัตรออกในแอปของผู้ออกบัตร

สำหรับ iOS 15.4 ขึ้นไป เมื่อผู้ใช้กดสองครั้งที่ปุ่มด้านข้างบน iPhone ที่มี Face ID หรือกดสองครั้งที่ปุ่มโฮมบน iPhone ที่มี Touch ID บัตรผ่านและรายละเอียดกุญแจการเข้าถึงจะไม่แสดงจนกว่าพวกเขาจะยืนยันตัวตนกับอุปกรณ์ จำเป็นต้องมี Face ID, Touch ID หรือการตรวจสอบสิทธิ์ด้วยรหัสก่อนที่ข้อมูลเฉพาะของบัตรผ่าน ซึ่งรวมถึงรายละเอียดการจองโรงแรมจะแสดงในกระเป๋าสตางค์

การเข้าถึงประเภทข้อมูลประจำตัว

การเข้าถึงจากกระเป๋าสตางค์มีหลายประเภท เช่น ธุรกิจบริการ ป้ายชื่อที่ใช้ในองค์กร บัตรประจำตัวนักเรียน กุญแจบ้าน และกุญแจรถ

ธุรกิจบริการ

กุญแจห้องพักโรงแรมในกระเป๋าสตางค์ช่วยมอบประสบการณ์ที่ง่ายดายและไร้การสัมผัสตั้งแต่เช็คอินจนถึงเช็คเอาต์ ในขณะเดียวกันก็มอบความเป็นส่วนตัวและความปลอดภัยสำหรับแขกที่เพิ่มขึ้นมาจากการใช้กุญแจการ์ดโรงแรมที่ทำจากพลาสติกแบบดั้งเดิม แขกของโรงแรมสามารถแตะเพื่อปลดล็อคสถานที่ที่รองรับด้วยกุญแจห้องในกระเป๋าสตางค์บน iPhone และ Apple Watch Series 4 ขึ้นไปที่ใช้งานร่วมกันได้

ความสามารถของกระเป๋าสตางค์ได้รับการออกแบบมาโดยเฉพาะเพื่อลดความยุ่งยากสำหรับลูกค้า:

- การกำหนดสิทธิ์ก่อนเดินทางมาถึงจากแอปของโรงแรม เพื่อเพิ่มบัตรผ่านไปยังกระเป๋าสตางค์ก่อนการเข้าพัก
- ไทล์บัตรผ่านเช็คอิน เพื่อเริ่มการเช็คอินและการกำหนดห้องได้จากกระเป๋าสตางค์
- การอัปเดตกุญแจหลังการกำหนดสิทธิ์ เพื่อรองรับการขยายหรือแก้ไขการเข้าพักปัจจุบัน
- การรองรับกุญแจหลายห้องสำหรับบัตรผ่านแบบใช้ครั้งเดียวในกระเป๋าสตางค์
- การจัดเก็บกุญแจที่หมดอายุโดยอัตโนมัติในกระเป๋าสตางค์

ป้ายชื่อที่ใช้ในองค์กร

คุณสามารถเพิ่มป้ายพนักงานของคู่ค้าที่รองรับในกระเป๋าสตางค์บน iPhone และ Apple Watch ได้ ซึ่งช่วยให้พนักงานทั่วโลกเข้าถึงที่ทำงานได้แบบไร้การสัมผัส ในการเพิ่มป้าย พนักงานต้องเปิดใช้งานการตรวจสอบสิทธิ์หลายปัจจัยสำหรับบัญชีที่ใช้ในการลงชื่อเข้าแอปที่นายจ้างจัดหาให้

ป้ายพนักงานใช้ประโยชน์จากความสามารถในการเข้าถึงของ Apple ทำให้ผู้ใช้สามารถ:

- เพิ่มป้ายพนักงานไปยัง Apple Watch ที่จับคู่ไว้โดยอัตโนมัติผ่านการกำหนดสิทธิ์แบบผลักข้อมูลที่ไม่ต้องติดตั้งแอปของคู่ค้า
- เข้าถึงสิ่งอำนวยความสะดวกในสำนักงานได้อย่างราบรื่นโดยใช้โหมดเร่งด่วน
- เข้าถึงที่ทำงานแม้แบตเตอรี่ iPhone ของพวกเขาจะหมด

บัตรนักเรียน

สำหรับ iOS 12 ขึ้นไป นักศึกษา คณาจารย์ และเจ้าหน้าที่ในวิทยาเขตที่เข้าร่วมสามารถเพิ่มบัตรประจำตัวนักศึกษาไปยังกระเป๋าสตางค์บน iPhone และ Apple Watch รุ่นที่รองรับเพื่อเข้าถึงสถานที่ต่างๆ และชำระเงินได้ทุกที่ที่รับการชำระผ่านบัตร

ผู้ใช้จะเพิ่มบัตรประจำตัวนักศึกษาลงในกระเป๋าสตางค์ผ่านแอปที่ผู้ออกบัตรหรือโรงเรียนที่เข้าร่วมจัดหาให้ กระบวนการทางเทคนิคที่เกิดขึ้นจะเหมือนกับกระบวนการที่อธิบายใน การเพิ่มบัตรเครดิตหรือบัตรเดบิตจากแอปของผู้ออกบัตร นอกจากนี้ แอปที่ออกบัตรจะต้องรองรับการตรวจสอบสิทธิ์สองปัจจัยบนบัญชีที่ป้องกันการเข้าถึงข้อมูลประจำตัวนักเรียนด้วย บัตรอาจจะถูกตั้งค่าได้พร้อมกันบนอุปกรณ์ Apple ที่รองรับสูงสุดสองเครื่องซึ่งได้ลงชื่อเข้าด้วย Apple ID เดียวกันไว้

บ้านที่อยู่ร่วมกันหลายครอบครัว

ผู้เช่าและพนักงานหน่วยงานบริการของคู่ค้าที่รองรับสามารถใช้กุญแจบ้านที่อยู่ในกระเป๋าสตางค์เพื่อเข้าถึงอาคาร หน่วยงาน และพื้นที่ส่วนกลางได้ สามารถกำหนดสิทธิ์กุญแจบ้านได้จากแอปที่คู่ค้าจัดหาให้ สำหรับคู่ค้าที่รองรับการกำหนดสิทธิ์แบบไร้ความยุ่งยาก ผู้บริหารอสังหาริมทรัพย์สามารถส่งลิงก์ไปยังผู้เช่าเพื่อเริ่มต้นการกำหนดสิทธิ์โดยใช้ช่องทางการส่งข้อความที่ต้องการ (เช่น อีเมลหรือ SMS) ผู้เช่าเพียงกดลิงก์ก็สามารถที่จะแลกใช้กุญแจได้แล้ว แอปคลิปยังมอบประสบการณ์ที่ปลอดภัยและราบรื่น ทำให้สามารถกำหนดสิทธิ์กุญแจได้โดยไม่ต้องติดตั้งแอปของคู่ค้า โปรดดูบทความบริการช่วยเหลือของ Apple การใช้แอปคลิปบน iPhone สำหรับข้อมูลเพิ่มเติม

กุญแจบ้าน

สามารถใช้กุญแจบ้านในกระเป๋าสตางค์กับล็อคประตูที่รองรับ NFC ได้เพียงแค่แตะด้วย iPhone หรือ Apple Watch โปรดดูบทความบริการช่วยเหลือของ Apple ปลดล็อคประตูของคุณด้วยกุญแจบ้านบน iPhone สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีที่ผู้ใช้สามารถตั้งค่าและใช้กุญแจบ้าน

เมื่อผู้ใช้ตั้งค่ากุญแจบ้าน ผู้อยู่อาศัยทุกคนในบ้านจะได้รับกุญแจบ้านโดยอัตโนมัติด้วย ในการแชร์กุญแจบ้านเพิ่มเติมหรือเอาสมาชิกของบ้านที่แชร์ออก เจ้าของบ้านสามารถใช้แอปบ้านเพื่อจัดการคำเชิญและสมาชิกได้ เมื่อผู้ใช้เลือกยอมรับคำเชิญให้เข้าร่วมบ้านด้วยกุญแจบ้านแล้ว การดำเนินการนี้จะเริ่มต้นการกำหนดสิทธิ์กุญแจบ้านในกระเป๋าสตางค์บนอุปกรณ์ของผู้ใช้ ถ้าผู้ใช้เลือกที่จะออกจากบ้านหรือหากเจ้าของบ้านยกเลิกการเข้าถึง การดำเนินการเหล่านี้จะเอากุญแจบ้านออกจากกระเป๋าสตางค์ด้วย

กุญแจรถ

การจัดเก็บกุญแจรถแบบดิจิตอลในกระเป๋าสตางค์ได้รับการรองรับดั้งเดิมในอุปกรณ์ iPhone ที่รองรับและอุปกรณ์ Apple Watch ที่จับคู่อยู่ กุญแจรถจะแสดงเป็นบัตรผ่าน (สร้างโดย Apple ในนามของผู้ผลิตยานยนต์) ในกระเป๋าสตางค์และรองรับวงจรชีวิตบัตร Apple Pay อย่างเต็มรูปแบบ (โหมดสูญหาย iCloud, การล้างข้อมูลระยะไกล, การลบบัตรผ่านภายในเครื่อง และการลบข้อมูลเนื้อหาและการตั้งค่าทั้งหมด) นอกจากการจัดการบัตร Apple Pay ตามมาตรฐานแล้ว กุญแจรถที่แชร์สามารถลบได้จาก iPhone, Apple Watch ของเจ้าของกุญแจ และใน Human Machine Interface (HMI) ของยานพาหนะด้วย

กุญแจรถสามารถใช้เพื่อปลดล็อคและล็อคยานพาหนะ รวมถึงเพื่อสตาร์ทเครื่องยนต์หรือตั้งค่ายานพาหนะให้อยู่ในโหมดขับขี่ได้ "ธุรกรรมมาตรฐาน" มีการตรวจสอบสิทธิ์ร่วมกันและเป็นสิ่งจำเป็นสำหรับการสตาร์ทเครื่องยนต์ ธุรกรรมการปลดล็อคและการล็อคอาจใช้ "ธุรกรรมที่รวดเร็ว" เมื่อต้องการเหตุผลของการดำเนินการ

กุญแจจะถูกสร้างผ่านการจับคู่ iPhone กับยานพาหนะที่เป็นเจ้าของและรองรับ กุญแจทั้งหมดจะถูกสร้างบน Secure Element แบบฝังในตามการสร้างกุญแจแบบออนบอร์ด (ECC-OBKG) ที่เป็นเส้นโค้งรูปไข่ (NIST P-256) และกุญแจส่วนตัวจะอยู่ใน Secure Element ตลอดเวลา การสื่อสารระหว่างอุปกรณ์และรถจะใช้ NFC หรือการผสมผสานระหว่าง บลูทูธ LE และ UWB ส่วนการจัดการกุญแจจะใช้ Apple เพื่อส่งไปยังเซิร์ฟเวอร์ API ของผู้ผลิตยานยนต์ที่มี TLS ซึ่งมีการตรวจสอบสิทธิ์ร่วมกัน หลังจากจับคู่กุญแจกับ iPhone แล้ว Apple Watch ที่จับคู่กับ iPhone เครื่องดังกล่าวจะได้รับกุญแจด้วยเช่นกัน เมื่อกุญแจถูกลบไม่ว่าในยานพาหนะหรือบนอุปกรณ์ คุณจะไม่สามารถกู้คืนได้ กุญแจบนอุปกรณ์ที่สูญหายหรือถูกขโมยสามารถถูกระงับและกลับไปใช้งานต่อได้ แต่การกำหนดสิทธิ์อีกครั้งบนอุปกรณ์เครื่องใหม่จำเป็นต้องมีการจับคู่หรือการแชร์ใหม่

ความปลอดภัยของกุญแจรถใน iOS

นักพัฒนาจะสามารถสนับสนุนวิธีการรักษาความปลอดภัยแบบไม่ใช้กุญแจเพื่อเข้าถึงยานพาหนะใน iPhone ที่รองรับและ Apple Watch ที่จับคู่อยู่ได้

การจับคู่กับเจ้าของ

เจ้าของจะต้องพิสูจน์ว่าเป็นผู้ครอบครองยานพาหนะ (วิธีขึ้นอยู่กับผู้ผลิตรถยนต์) และสามารถเริ่มกระบวนการจับคู่ได้ในแอปของผู้ผลิตรถยนต์ โดยใช้อีเมลลิงก์ที่ได้รับจากผู้ผลิตรถยนต์หรือจากเมนูของยานพาหนะ ในทุกกรณี เจ้าของจะต้องแสดงรหัสผ่านการจับคู่แบบครั้งเดียวที่เป็นข้อมูลลับกับ iPhone ซึ่งใช้เพื่อสร้างช่องทางการจับคู่ที่ปลอดภัยโดยใช้โปรโตคอล SPAKE2+ ด้วยเส้นโค้ง NIST P-256 เมื่อใช้แอปหรือลิงก์อีเมล รหัสผ่านจะถูกโอนไปยัง iPhone โดยอัตโนมัติ ซึ่งจะต้องป้อนด้วยตนเองเมื่อเริ่มต้นการจับคู่จากยานพาหนะ

การแชร์กุญแจ

iPhone ที่จับคู่ของเจ้าของสามารถแชร์กุญแจกับอุปกรณ์ iPhone (และอุปกรณ์ Apple Watch ที่จับคู่กันอยู่) ของสมาชิกครอบครัวและเพื่อนที่มีสิทธิ์ได้ โดยส่งคำเชิญเฉพาะอุปกรณ์โดยใช้ iMessage และบริการข้อมูลประจำตัว (IDS) ของ Apple คำสั่งการแชร์ทั้งหมดถูกแลกเปลี่ยนโดยใช้คุณสมบัติ IDS ที่เข้ารหัสแบบต้นทางถึงปลายทาง iPhone ที่จับคู่อยู่ของเจ้าของจะป้องกันไม่ให้ช่อง IDS เปลี่ยนระหว่างกระบวนการแชร์เพื่อป้องกันการส่งต่อคำเชิญ

เมื่อตอบรับคำเชิญแล้ว iPhone ของสมาชิกครอบครัวหรือเพื่อนจะสร้างกุญแจดิจิตอลแล้วส่งลำดับการรับรองการสร้างกุญแจกลับไปยัง iPhone เพื่อตรวจสอบยืนยันว่ากุญแจถูกสร้างบนอุปกรณ์ของแท้ของ Apple iPhone ที่จับคู่ของเจ้าของจะลงชื่อกุญแจสาธารณะ ECC ของ iPhone เครื่องอื่นของสมาชิกครอบครัวหรือเพื่อนแล้วส่งลายเซ็นกลับไปยัง iPhone ของสมาชิกครอบครัวหรือเพื่อน การดำเนินการลงชื่อในอุปกรณ์ของเจ้าของจะต้องมีการตรวจสอบสิทธิ์ผู้ใช้ (Face ID, Touch ID หรือการป้อนรหัส) รวมถึงเจตนาของผู้ใช้ที่ปลอดภัยที่อธิบายไว้ในการใช้งานสำหรับ Face ID และ Touch ID ระบบจะขออนุญาตเมื่อส่งคำเชิญและคำขอจะถูกจัดเก็บใน Secure Element สำหรับการใช้งานเมื่ออุปกรณ์ของเพื่อนส่งคำขอลงชื่อกลับมา การให้สิทธิ์กุญแจนั้นจะมอบให้กับยานพาหนะผ่านทางออนไลน์โดยเซิร์ฟเวอร์ OEM ของยานพาหนะหรือในระหว่างการใช้งานครั้งแรกของกุญแจที่ใช้ร่วมกันบนยานพาหนะ

การลบกุญแจ

กุญแจสามารถลบได้บนอุปกรณ์ผู้ถือกุญแจจากอุปกรณ์ของเจ้าของและในยานพาหนะ การลบผู้ถือกุญแจ iPhone จะมีผลทันที แม้ว่าผู้ถือกุญแจจะใช้กุญแจอยู่ก็ตาม ดังนั้นคำเตือนที่ชัดเจนจะแสดงขึ้นก่อนการลบ การลบกุญแจในยานพาหนะอาจทำได้ทุกเมื่อหรือทำได้เมื่อยานพาหนะออนไลน์เท่านั้น

ในทั้งสองกรณี การลบบนอุปกรณ์ผู้ถือกุญแจหรือยานพาหนะจะรายงานไปยังเซิร์ฟเวอร์คลังกุญแจ (KIS) ทางฝั่งผู้ผลิตรถยนต์ ซึ่งจะลงทะเบียนกุญแจที่ออกสำหรับยานพาหนะเพื่อจุดประสงค์ด้านการประกันภัย

เจ้าของสามารถขอลบได้จากด้านหลังของบัตรผ่านเจ้าของ อันดับแรก คำขอจะถูกส่งไปยังผู้ผลิตรถยนต์เพื่อเอากุญแจในยานพาหนะออก ผู้ผลิตรถยนต์เป็นผู้ระบุเงื่อนไขในการเอากุญแจออกจากยานพาหนะ เฉพาะเมื่อเอากุญแจออกในยานพาหนะ เซิร์ฟเวอร์ของผู้ผลิตรถยนต์จะส่งคำขอยุติระยะไกลไปยังอุปกรณ์ผู้ถือกุญแจ

เมื่อยุติกุญแจในอุปกรณ์แล้ว แอปขนาดเล็กที่จัดการกุญแจรถดิจิตอลจะสร้างการรับรองการยุติที่ลงชื่อแบบเข้ารหัส ซึ่งใช้เป็นหลักฐานการลบโดยผู้ผลิตรถยนต์และใช้เพื่อเอากุญแจออกจาก KIS

ธุรกรรมมาตรฐาน NFC

สำหรับยานยนต์ที่ใช้กุญแจ NFC ช่องสัญญาณที่ปลอดภัยระหว่างเครื่องอ่านและ iPhone จะเริ่มต้นโดยการสร้างคู่กุญแจชั่วคราวบนเครื่องอ่านและที่ฝั่ง iPhone เมื่อใช้วิธีข้อตกลงกุญแจ ทั้งสองฝั่งจะได้รับความลับที่แชร์และจะใช้ความลับที่แชร์เพื่อสร้างกุญแจแบบสมมาตรที่แชร์โดยใช้ Diffie-Hellman ซึ่งเป็นฟังก์ชั่นการรับกุญแจ และลายเซ็นจากกุญแจระยะยาวที่สร้างขึ้นระหว่างการจับคู่

กุญแจสาธารณะชั่วคราวที่สร้างจากฝั่งยานพาหนะจะได้รับการลงชื่อด้วยกุญแจส่วนตัวระยะยาวของเครื่องอ่าน ทำให้เกิดการตรวจสอบสิทธิ์ของเครื่องอ่านโดย iPhone จากมุมมองของ iPhone โปรโตคอลนี้ได้รับการออกแบบมาเพื่อป้องกันการเปิดเผยข้อมูลที่ละเอียดอ่อนแก่ศัตรูที่สกัดกั้นการสื่อสาร

สุดท้ายแล้ว iPhone จะใช้ช่องทางที่ปลอดภัยที่สร้างขึ้นเพื่อเข้ารหัสข้อมูลจำเพาะกุญแจสาธารณะ ร่วมกับลายเซ็นที่ประมวลผลบนคำตอบที่ได้รับข้อมูลของเครื่องอ่านและข้อมูลเฉพาะแอปบางส่วน การตรวจสอบยืนยันลายเซ็น iPhone โดยเครื่องอ่านจะอนุญาตให้เครื่องอ่านตรวจสอบสิทธิ์ของอุปกรณ์

ธุรกรรมที่รวดเร็ว

iPhone สร้างรหัสลับที่อิงจากความลับที่มีการแชร์ก่อนหน้านี้ในระหว่างธุรกรรมมาตรฐาน รหัสลับนี้ทำให้ยานพาหนะตรวจสอบสิทธิ์อุปกรณ์ได้อย่างรวดเร็วในสถานการณ์ที่ต้องใช้ความไว อีกทางเลือกหนึ่ง ช่องทางที่ปลอดภัยระหว่างยานพาหนะกับอุปกรณ์จะถูกสร้างขึ้นด้วยกุญแจเซสชั่นการรับจากความลับที่แชร์ก่อนหน้าระหว่างการทำธุรกรรมมาตรฐานและคู่กุญแจชั่วคราวใหม่ ความสามารถของยานพาหนะในการสร้างช่องทางที่ปลอดภัยจะตรวจสอบสิทธิ์ของยานพาหนะไปยัง iPhone

ธุรกรรมมาตรฐาน BLE/UWB

สำหรับยานพาหนะที่ใช้กุญแจ UWB จะมีการสร้างเซสชั่นบลูทูธ LE ระหว่างยานพาหนะกับ iPhone เช่นเดียวกับธุรกรรม NFC ความลับที่ใช้ร่วมกันจะได้รับจากทั้งสองฝ่ายและใช้สำหรับสร้างเซสชั่นที่ปลอดภัย เซสชั่นนี้ใช้เพื่อการได้รับและยอมรับ UWB Ranging Secret Key (URSK) ในภายหลัง URSK จะมีให้สำหรับวิทยุ UWB ในอุปกรณ์ของผู้ใช้และบนยานพาหนะ เพื่อให้อุปกรณ์ของผู้ใช้มีการแปลเป็นภาษาท้องถิ่นไปยังตำแหน่งเฉพาะที่อยู่ใกล้หรือภายในยานพาหนะได้อย่างแม่นยำ จากนั้นยานพาหนะจะใช้ตำแหน่งอุปกรณ์เพื่อตัดสินใจเกี่ยวกับการอนุญาตให้ปลดล็อคหรือสตาร์ทยานพาหนะ URSK มี TTL ที่กำหนดไว้ล่วงหน้า ในการหลีกเลี่ยงการหยุดชะงักของช่วงเมื่อ TTL หมดอายุ สามารถรับ URSK มาล่วงหน้าสำหรับอุปกรณ์ SE และ HSM/SE ของยานพาหนะในขณะที่ช่วงปลอดภัยไม่ทำงาน แต่มีการเชื่อมต่อ BLE ซึ่งช่วยหลีกเลี่ยงความจำเป็นในการทำธุรกรรมมาตรฐานเพื่อให้ได้มาซึ่ง URSK ใหม่ในสถานการณ์ที่วิกฤติด้านเวลา URSK ที่ได้รับมาก่อนหน้านี้สามารถถ่ายโอนอย่างรวดเร็วไปยังวิทยุ UWB ของรถยนต์และอุปกรณ์เพื่อหลีกเลี่ยงการหยุดชะงักของช่วง UWB ได้

ความเป็นส่วนตัว

เซิร์ฟเวอร์สินค้าคงคลังหลักของผู้ผลิตยานยนต์ (KIS) จะไม่มีการจัดเก็บ ID อุปกรณ์, SEID หรือ Apple ID โดยจะจัดเก็บเฉพาะข้อมูลจำเพาะที่เปลี่ยนแปลงได้ ตัวอย่างเช่น ข้อมูลจำเพาะ CA ข้อมูลจำเพาะนี้ไม่ผูกกับข้อมูลส่วนตัวใดๆ ในอุปกรณ์หรือโดยเซิร์ฟเวอร์ และจะถูกลบเมื่อผู้ใช้ลบข้อมูลอุปกรณ์โดยสมบูรณ์ (โดยใช้ลบข้อมูลทั้งหมดและการตั้งค่า)

การเพิ่มบัตรโดยสารและบัตร eMoney ไปยังกระเป๋าสตางค์

สำหรับตลาดหลายแห่งทั่วโลก ผู้ใช้จะสามารถเพิ่มบัตรโดยสารและบัตร eMoney ที่รองรับไปยังกระเป๋าสตางค์บน iPhone และ Apple Watch รุ่นที่รองรับได้ ซึ่งขึ้นอยู่กับผู้ให้บริการ อาจทำได้โดยการโอนมูลค่าหรือบัตรโดยสาร (หรือทั้งสองอย่าง) จากบัตรจริงเป็นรูปแบบดิจิตอลไปยังกระเป๋าสตางค์หรือโดยการกำหนดสิทธิ์บัตรโดยสารใหม่หรือบัตร eMoney จากกระเป๋าสตางค์หรือแอปของผู้ออกบัตร หลังจากเพิ่มบัตรโดยสารลงในกระเป๋าสตางค์แล้ว ผู้ใช้สามารถโดยสารการขนส่งสาธารณะได้ง่ายๆ โดยแสดง iPhone หรือ Apple Watch ใกล้กับเครื่องอ่านบัตรโดยสาร บัตรโดยสารบางประเภทยังสามารถใช้ชำระเงินได้อีกด้วย

วิธีการทำงานของบัตรโดยสารและบัตร eMoney

บัตรโดยสารและบัตร eMoney ที่เพิ่มเข้ามาจะเชื่อมโยงกับบัญชี iCloud ของผู้ใช้ ถ้าผู้ใช้เพิ่มบัตรมากกว่าหนึ่งใบไปยังกระเป๋าสตางค์ Apple หรือผู้ออกบัตรอาจสามารถเชื่อมโยงข้อมูลส่วนบุคคลของผู้ใช้กับข้อมูลบัญชีที่เกี่ยวข้องระหว่างบัตรต่างๆ ได้ บัตรโดยสาร บัตร eMoney และการทำธุรกรรมจะได้รับการคุ้มครองโดยชุดกุญแจที่เข้ารหัสแบบลำดับชั้น

ในระหว่างขั้นตอนการโอนยอดคงเหลือจากบัตรจริงไปยังกระเป๋าสตางค์ ผู้ใช้จะต้องป้อนข้อมูลเฉพาะของบัตร ผู้ใช้ยังอาจจะต้องระบุข้อมูลส่วนบุคคลเพื่อเป็นหลักฐานว่าเป็นผู้ครอบครองบัตรอีกด้วย เมื่อถ่ายโอนบัตรผ่านจาก iPhone ไปยัง Apple Watch อุปกรณ์ทั้งสองต้องออนไลน์อยู่

สามารถเติมเงินไปยังยอดคงเหลือได้ด้วยเงินจากบัตรเครดิต บัตรเดบิต และบัตรเติมเงินผ่านกระเป๋าสตางค์หรือจากแอปผู้ออกบัตรโดยสารหรือ eMoney ในการทำความเข้าใจเกี่ยวกับความปลอดภัยของการโหลดยอดเงินอีกครั้งเมื่อใช้ Apple Pay ให้ดูที่ การชำระเงินด้วยบัตรภายในแอป ในการเรียนรู้วิธีกำหนดสิทธิ์บัตรจากภายในแอปของผู้ออกบัตร โปรดดู การเพิ่มบัตรเครดิตหรือเดบิตจากแอปของผู้ออกบัตร

ถ้ารองรับการกำหนดสิทธิ์จากบัตรจริง ผู้ออกบัตรโดยสารหรือ eMoney จะมีกุญแจการเข้ารหัสที่จำเป็นในการตรวจสอบสิทธิ์ของบัตรจริงและตรวจสอบยืนยันข้อมูลที่ผู้ใช้ป้อน หลังจากตรวจสอบยืนยันข้อมูล ระบบจะสามารถสร้างหมายเลขบัญชีอุปกรณ์สำหรับ Secure Element และเปิดใช้งานบัตรผ่านที่เพิ่มใหม่ในกระเป๋าสตางค์ด้วยยอดคงเหลือที่โอน สำหรับบัตรบางใบ หลังจากที่กำหนดสิทธิ์จากบัตรจริงเสร็จสิ้นแล้ว บัตรจริงจะถูกปิดใช้งาน

เมื่อสิ้นสุดการกำหนดสิทธิ์ประเภทใดประเภทหนึ่ง หากยอดคงเหลือในบัตรถูกจัดเก็บไว้ในอุปกรณ์ จะถูกเข้ารหัสและจัดเก็บไว้ในแอพเพล็ตที่กำหนดใน Secure Element ผู้ดำเนินการจะมีกุญแจในการดำเนินการเข้ารหัสข้อมูลบัตรสำหรับการทำธุรกรรมที่เกี่ยวข้องกับยอดคงเหลือ

ตามค่าเริ่มต้น ผู้ใช้บัตรโดยสารจะได้รับประโยชน์จากประสบการณ์การโดยสารด่วนที่ราบรื่น ซึ่งช่วยให้พวกเขาชำระเงินและโดยสารได้โดยไม่ต้องใช้ Face ID, Touch ID หรือรหัส ข้อมูลต่างๆ เช่น สถานีที่ไปล่าสุด ประวัติธุรกรรม และตั๋วอื่นๆ อาจจะเข้าถึงได้โดยเครื่องอ่านบัตรแบบไร้การสัมผัสที่อยู่ใกล้ๆ ที่โหมดเร่งด่วนเปิดใช้งานอยู่ ผู้ใช้สามารถเปิดใช้ข้อกำหนดการยืนยันตัวตนสำหรับ Face ID, Touch ID หรือรหัสในการตั้งค่ากระเป๋าสตางค์และ Apple Pay ได้โดยการปิดใช้งานการโดยสารด่วน บัตร eMoney ไม่รองรับโหมดเร่งด่วน

เช่นเดียวกับบัตร Apple Pay อื่นๆ ผู้ใช้สามารถระงับหรือเอาบัตร eMoney ออกได้โดย:

- การลบอุปกรณ์จากระยะไกลด้วย “ค้นหาของฉัน”
- การเปิดใช้งานโหมดสูญหายด้วย “ค้นหาของฉัน”
- การป้อนคำสั่งการล้างข้อมูลระยะไกลของการจัดการอุปกรณ์เคลื่อนที่ (MDM)
- การเอาบัตรทั้งหมดออกจากหน้าบัญชี Apple ID ของผู้ใช้
- การเอาบัตรทั้งหมดออกจาก iCloud.com
- การนำบัตรทั้งหมดออกจากกระเป๋าสตางค์
- การเอาบัตรออกในแอปของผู้ออกบัตร

เซิร์ฟเวอร์ Apple Pay จะแจ้งผู้ให้บริการบัตรเพื่อระงับหรือปิดใช้งานบัตรเหล่านั้น ถ้าผู้ใช้เอาบัตรโดยสารหรือบัตร eMoney ออกจากอุปกรณ์ออนไลน์ จะสามารถกู้คืนยอดคงเหลือได้โดยเพิ่มบัตรกลับไปยังอุปกรณ์ที่ลงชื่อเข้าด้วย Apple ID เดียวกัน ถ้าอุปกรณ์ออฟไลน์ ปิดเครื่อง หรือใช้งานไม่ได้ การกู้คืนอาจจะไม่สามารถทำได้

การเพิ่มบัตรโดยสารและบัตร eMoney ไปยัง Apple Watch ของสมาชิกครอบครัว

สำหรับ iOS 15 และ watchOS 8 ผู้จัดการประจำครอบครัว iCloud สามารถเพิ่มบัตรโดยสารและบัตร eMoney ให้กับอุปกรณ์ Apple Watch ของสมาชิกในครอบครัวผ่านแอป Watch ของ iPhone ได้ เมื่อทำการกำหนดสิทธิ์บัตรเหล่านี้ให้กับ Apple Watch ของสมาชิกในครอบครัว นาฬิกาจะต้องอยู่ใกล้ๆ และเชื่อมต่อกับ iPhone ของผู้จัดการโดยใช้ Wi-Fi หรือบลูทูธ สมาชิกในครอบครัวจะต้องเปิดใช้งานการตรวจสอบสิทธิ์สองปัจจัยสำหรับ Apple ID ของพวกเขาจึงจะดำเนินการตามขั้นตอนนี้ได้

สมาชิกในครอบครัวสามารถส่งคำขอเพื่อเพิ่มเงินไปยังบัตรโดยสารหรือบัตร eMoney จาก Apple Watch ได้โดยใช้ iMessage เนื้อหาของข้อความได้รับการปกป้องโดยการเข้ารหัสแบบต้นทางถึงปลายทาง ตามที่อธิบายไว้ใน ภาพรวมความปลอดภัยของ iMessage การเพิ่มเงินลงในบัตรบน Apple Watch ของสมาชิกครอบครัวสามารถทำได้จากระยะไกลโดยใช้ Wi-Fi หรือการเชื่อมต่อเซลลูลาร์ ไม่จำเป็นต้องอยู่ในระยะที่ใกล้ชิดกัน

หมายเหตุ: คุณสมบัตินี้อาจไม่สามารถใช้ได้ในบางประเทศหรือภูมิภาค

บัตรเครดิตและบัตรเดบิต

ในบางเมือง เครื่องอ่านบัตรโดยสารจะยอมรับ (สมาร์ท) การ์ด EMV ในการชำระค่าโดยสาร เมื่อผู้ใช้แสดงบัตรเครดิตหรือบัตรเดบิต EMV กับเครื่องอ่านบัตร ผู้ใช้จะต้องตรวจสอบสิทธิ์ในลักษณะเดียวกันกับ “ชำระเงินด้วยบัตรเครดิตและบัตรเดบิตในร้านค้า”

สำหรับ iOS 12.3 ขึ้นไป สามารถเปิดใช้งานบัตรเครดิต/เดบิต EMV บางบัตรในกระเป๋าสตางค์สำหรับการโดยสารด่วนได้ การโดยสารด่วนอนุญาตให้ผู้ใช้ชำระค่าเดินทางสำหรับผู้ให้บริการขนส่งที่รองรับโดยไม่ต้องใช้ Face ID, Touch ID หรือรหัส เมื่อผู้ใช้กำหนดสิทธิ์บัตรเครดิตหรือบัตรเดบิต EMV บัตรใบแรกที่มีการกำหนดสิทธิ์ไปยังกระเป๋าสตางค์จะถูกเปิดใช้งานสำหรับการโดยสารด่วน ผู้ใช้สามารถแตะปุ่มเพิ่มเติมที่ด้านหน้าของบัตรในกระเป๋าสตางค์และปิดใช้งานการโดยสารด่วนสำหรับบัตรนั้นโดยตั้งการตั้งค่าการโดยสารด่วนเป็นไม่มี ผู้ใช้ยังสามารถเลือกบัตรเครดิตหรือบัตรเดบิตใบอื่นเป็นบัตรโดยสารด่วนโดยใช้กระเป๋าสตางค์ได้อีกด้วย ต้องใช้ Face ID, Touch ID หรือรหัสเพื่อเปิดใช้งานใหม่อีกครั้ง หรือเลือกบัตรอื่นสำหรับการโดยสารด่วน

Apple Card และ Apple Cash สามารถใช้ได้กับการโดยสารด่วน

บัตรประจำตัวในกระเป๋าสตางค์

สำหรับ iPhone 8 ขึ้นไปที่ใช้ iOS 15.4 ขึ้นไป และ Apple Watch Series 4 ขึ้นไปที่ใช้ watchOS 8.4 ขึ้นไป ผู้ใช้สามารถเพิ่มบัตรประจำตัวประชาชนมลรัฐหรือใบขับขี่ในกระเป๋าสตางค์ แล้วแตะ iPhone หรือ Apple Watch เพื่อแสดงบัตรได้อย่างราบรื่นและปลอดภัยในสถานที่ที่เข้าร่วม

หมายเหตุ: คุณสมบัตินี้ใช้ได้เฉพาะกับรัฐในสหรัฐอเมริกาที่เข้าร่วมเท่านั้น

บัตรประจำตัวในกระเป๋าสตางค์จะใช้คุณสมบัติความปลอดภัยที่มีอยู่ในฮาร์ดแวร์และซอฟต์แวร์ของอุปกรณ์ของผู้ใช้เพื่อช่วยปกป้องข้อมูลระบุตัวตนและช่วยรักษาข้อมูลส่วนบุคคลให้ปลอดภัย

การเพิ่มใบขับขี่หรือบัตรประจำตัวประชาชนมลรัฐไปยังกระเป๋าสตางค์

บน iPhone ผู้ใช้สามารถแตะปุ่มเพิ่ม (+) ที่ด้านบนสุดของหน้าจอในกระเป๋าสตางค์เพื่อเริ่มการเพิ่มใบอนุญาตหรือบัตรประจำตัวได้ ถ้าผู้ใช้มีการจับคู่ Apple Watch ในขณะที่ตั้งค่า ผู้ใช้จะได้รับแจ้งให้เพิ่มใบขับขี่หรือบัตรประจำตัวไปยังกระเป๋าสตางค์บน Apple Watch

ขั้นแรกให้ผู้ใช้ใช้ iPhone สแกนใบขับขี่หรือบัตรประจำตัวประชาชนมลรัฐทั้งด้านหน้าและด้านหลัง iPhone จะประเมินคุณภาพและประเภทของภาพเพื่อช่วยให้มั่นใจว่าภาพที่ให้มานั้นเป็นที่ยอมรับโดยหน่วยงานที่ออกบัตรของรัฐ ภาพบัตรประจำตัวเหล่านี้ได้รับการเข้ารหัสไปยังกุญแจของผู้มีอำนาจที่แต่งตั้งโดยรัฐบนอุปกรณ์แล้วส่งไปยังผู้มีอำนาจที่แต่งตั้งโดยรัฐ

ขั้นตอนต่อไป ผู้ใช้จะถูกขอให้ทำตามชุดการเคลื่อนไหวใบหน้าและศีรษะ การเคลื่อนไหวเหล่านี้จะได้รับการประเมินโดยอุปกรณ์ของผู้ใช้และโดย Apple เพื่อช่วยลดความเสี่ยงของบุคคลที่ใช้รูปถ่าย วิดีโอ หรือหน้ากากเพื่อพยายามเพิ่มบัตรประจำตัวของผู้อื่นในกระเป๋าสตางค์ ผลลัพธ์จากการวิเคราะห์การเคลื่อนไหวเหล่านี้จะถูกส่งไปยังหน่วยงานที่ออกบัตรของรัฐ แต่ไม่ใช่วิดีโอของการเคลื่อนไหว

ในการช่วยให้มั่นใจว่าผู้ที่เพิ่มบัตรประจำตัวในกระเป๋าสตางค์นั้นเป็นบุคคลเดียวกันกับที่อยู่ในบัตรประจำตัว ผู้ใช้จะถูกขอให้ถ่ายรูปเซลฟี่ ก่อนที่ภาพถ่ายของผู้ใช้จะถูกส่งไปยังหน่วยงานที่ออกบัตรของรัฐ เซิร์ฟเวอร์ของ Apple และอุปกรณ์ของผู้ใช้จะเปรียบเทียบภาพถ่ายกับความคล้ายคลึงกันของบุคคลที่ทำตามชุดการเคลื่อนไหวใบหน้าและศีรษะ เพื่อช่วยให้มั่นใจว่าภาพถ่ายที่ส่งมาเป็นภาพถ่ายจริง ที่มีความคล้ายคลึงกับที่อยู่ในบัตรประจำตัว หลังจากทำการเปรียบเทียบแล้ว ภาพถ่ายจะถูกเข้ารหัสบนอุปกรณ์แล้วส่งไปยังหน่วยงานที่ออกบัตรของรัฐเพื่อเปรียบเทียบกับภาพในไฟล์บัตรประจำตัว

สุดท้าย ผู้ใช้จะถูกขอให้ดำเนินการตรวจสอบสิทธิ์ด้วย Face ID หรือ Touch ID อุปกรณ์ของผู้ใช้จะเชื่อมโยงการจับคู่นี้กับชีวมิติของ Face ID หรือ Touch ID ที่ตรงกันกับบัตรประจำตัวประชาชนมลรัฐเพื่อให้แน่ใจว่ามีเพียงบุคคลที่เพิ่มบัตรประจำตัวลงใน iPhone เครื่องนี้เท่านั้นที่สามารถแสดงบัตรได้ จะไม่สามารถใช้ข้อมูลชีวมิติที่ลงทะเบียนอื่นเพื่ออนุมัติการแสดงบัตรประจำตัวได้ กระบวนการนี้จะเกิดขึ้นในอุปกรณ์เท่านั้นและจะไม่ถูกส่งไปยังหน่วยงานที่ออกบัตรของรัฐ

หน่วยงานที่ออกบัตรของรัฐจะได้รับข้อมูลที่จำเป็นในการตั้งค่าบัตรประจำตัวลงดิจิตอล ซึ่งรวมถึงภาพด้านหน้าและด้านหลังของบัตรประจำตัวของผู้ใช้ ข้อมูลที่อ่านจากบาร์โค้ด PDF417 รวมถึงภาพเซลฟี่ที่ผู้ใช้ถ่ายซึ่งเป็นส่วนหนึ่งของกระบวนการตรวจสอบยืนยันบัตรประจำตัว สถานะการออกจะได้รับค่าตัวเลขหลักเดียว ซึ่งใช้เพื่อช่วยป้องกันการฉ้อโกง ซึ่งขึ้นอยู่กับรูปแบบการใช้อุปกรณ์ของผู้ใช้ ข้อมูลการตั้งค่า และข้อมูลเกี่ยวกับ Apple ID ส่วนบุคคล การตัดสินใจโดยหน่วยงานที่ออกบัตรของรัฐในการอนุมัติหรือปฏิเสธบัตรประจำตัวที่ถูกเพิ่มในกระเป๋าสตางค์ถือเป็นที่สิ้นสุด

หลังจากที่หน่วยงานที่ออกบัตรของรัฐอนุญาตให้เพิ่มบัตรประจำตัวประชาชนมลรัฐหรือใบขับขี่ไปยังกระเป๋าสตางค์แล้ว คู่กุญแจจะถูกสร้างขึ้นใน Secure Element โดย iPhone ซึ่งผูกบัตรประจำตัวของผู้ใช้กับอุปกรณ์เฉพาะนั้น ถ้าเพิ่มใน Apple Watch คู่กุญแจจะถูกสร้างขึ้นใน Secure Element โดย Apple Watch

หลังจากที่บัตรประจำตัวอยู่บน iPhone แล้ว ข้อมูลที่สะท้อนถึงบัตรประจำตัวของผู้ใช้ในกระเป๋าสตางค์จะถูกจัดเก็บในรูปแบบที่เข้ารหัสซึ่งปกป้องโดย Secure Enclave

การใช้ใบขับขี่หรือบัตรประจำตัวประชาชนมลรัฐในกระเป๋าสตางค์

ในการใช้บัตรประจำตัวของตนในกระเป๋าสตางค์ ผู้ใช้จำเป็นต้องตรวจสอบสิทธิ์ด้วยอุปกรณ์ Face ID หรือ Touch ID ที่เชื่อมโยงกับบัตรประจำตัวในกระเป๋าสตางค์ก่อนที่ iPhone จะนำเสนอข้อมูลต่อเครื่องอ่านข้อมูลประจำตัว

ในการใช้บัตรประจำตัวของตนในกระเป๋าสตางค์บน Apple Watch ผู้ใช้จำเป็นต้องปลดล็อค iPhone โดยใช้ Face ID หรือลายนิ้วมือ Touch ID ที่เกี่ยวข้องทุกครั้งที่ใส่ Apple Watch จากนั้น พวกเขาสามารถใช้บัตรประจำตัวของตนในกระเป๋าสตางค์ได้โดยไม่ต้องตรวจสอบสิทธิ์จนกว่าจะถอด Apple Watch ออกอีกครั้ง ความสามารถนี้ใช้ประโยชน์จากความสามารถพื้นฐานในการปลดล็อคอัตโนมัติซึ่งมีรายละเอียดอยู่ในความปลอดภัยของระบบสำหรับ watchOS

เมื่อผู้ใช้แสดง iPhone หรือ Apple Watch ของตนใกล้กับตัวอ่านข้อมูลประจำตัว ผู้ใช้จะเห็นข้อความแจ้งบนอุปกรณ์ที่แสดงว่ามีการร้องขอข้อมูลใด โดยใคร และแสดงว่าพวกเขาต้องการจะจัดเก็บข้อมูลนั้นหรือไม่ หลังจากการยืนยันตัวตนด้วย Face ID หรือ Touch ID ที่เกี่ยวข้องแล้ว ข้อมูลระบุตัวตนที่ร้องขอจะถูกปล่อยออกจากอุปกรณ์

สิ่งสำคัญ: ผู้ใช้ไม่จำเป็นต้องปลดล็อค แสดง หรือมอบอุปกรณ์เพื่อแสดงบัตรประจำตัว

ถ้าผู้ใช้เปิดใช้งานคุณสมบัติการช่วยการเข้าถึง เช่น การสั่งการด้วยเสียง การควบคุมสวิตช์ หรือ Assistive Touch แทนที่จะเป็น Face ID หรือ Touch ID พวกเขาสามารถใช้รหัสเพื่อเข้าถึงและแสดงข้อมูลได้

การส่งข้อมูลระบุตัวตนไปยังตัวอ่านข้อมูลประจำตัวเป็นไปตามมาตรฐาน ISO/IEC 18013-5 ซึ่งมีกลไกความปลอดภัยหลายแบบที่สามารถตรวจจับ ยับยั้ง และลดความเสี่ยงด้านความปลอดภัยได้ ซึ่งประกอบด้วยความสมบูรณ์ของข้อมูลประจำตัวและการต่อต้านการปลอมแปลง การผูกมัดอุปกรณ์ การรับทราบและยินยอม และการรักษาความลับของข้อมูลผู้ใช้ผ่านลิงก์วิทยุ

ความสมบูรณ์ของข้อมูลประจำตัวและการป้องกันการปลอมแปลง

บัตรประจำตัวในกระเป๋าสตางค์ใช้ลายเซ็นที่ผู้ออกจัดหาให้เพื่ออนุญาตให้ตัวอ่านที่ปฏิบัติตามมาตรฐาน ISO/IEC 18013-5 สามารถตรวจสอบยืนยันบัตรประจำตัวของผู้ใช้ในกระเป๋าสตางค์ได้ นอกจากนี้ องค์ประกอบข้อมูลทั้งหมดในบัตรประจำตัวในกระเป๋าสตางค์ยังได้รับการป้องกันการปลอมแปลงรายบุคคลอีกด้วย ซึ่งจะช่วยให้ตัวอ่านข้อมูลระบุตัวตนสามารถขอชุดย่อยเฉพาะขององค์ประกอบข้อมูลที่มีอยู่ในบัตรประจำตัวในกระเป๋าสตางค์ และเพื่อให้บัตรประจำตัวในกระเป๋าสตางค์ตอบสนองด้วยชุดย่อยเดียวกันนั้นได้ จึงมีการแชร์เฉพาะข้อมูลที่ร้องขอและเพิ่มความเป็นส่วนตัวสูงสุดให้กับผู้ใช้

การผูกอุปกรณ์

บัตรประจำตัวในการตรวจสอบสิทธิ์ของกระเป๋าสตางค์จะใช้ลายเซ็นอุปกรณ์เพื่อป้องกันการโคลนบัตรประจำตัวและการเล่นซ้ำของธุรกรรมการระบุตัวตน โดยการจัดเก็บรหัสส่วนตัวสำหรับการตรวจสอบสิทธิ์บัตรประจำตัวใน Secure Element ของอุปกรณ์ iPhone บัตรประจำตัวจะถูกผูกไว้กับอุปกรณ์เดียวกันกับที่หน่วยงานที่ออกบัตรของรัฐสร้างบัตรประจำตัวให้

การแสดงความยินยอม

บัตรประจำตัวในการตรวจสอบสิทธิ์ของตัวอ่านกระเป๋าสตางค์จะตรวจสอบสิทธิ์ของตัวอ่านข้อมูลประจำตัวโดยใช้โปรโตคอลที่กำหนดไว้ในมาตรฐาน ISO/IEC 18013-5 ในระหว่างการแสดง ไอคอนที่ได้รับจากใบรับรองของตัวอ่านจะแสดงให้ผู้ใช้เห็น เพื่อให้ผู้ใช้มั่นใจได้ว่าพวกเขากำลังโต้ตอบกับบุคคลที่ถูกต้อง

การรักษาความลับของข้อมูลผู้ใช้ผ่านลิงก์วิทยุ

การเข้ารหัสเซสชั่นช่วยให้มั่นใจได้ว่าข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ (PII) ทั้งหมดที่มีการแลกเปลี่ยนระหว่างบัตรประจำตัวในกระเป๋าสตางค์และตัวอ่านข้อมูลประจำตัวจะได้รับการเข้ารหัส การเข้ารหัสจะดำเนินการโดยชั้นแอปพลิเคชัน ความปลอดภัยของการเข้ารหัสเซสชั่นจึงไม่ได้ขึ้นอยู่กับการรักษาความปลอดภัยที่ชั้นการรับส่ง (เช่น NFC, บลูทูธ และ Wi-Fi)

บัตรประจำตัวในกระเป๋าสตางค์ช่วยรักษาความเป็นส่วนตัวของข้อมูลของผู้ใช้

บัตรประจำตัวในกระเป๋าสตางค์จะเป็นไปตามกระบวนการ “ดึงข้อมูลอุปกรณ์” ที่ระบุไว้ใน ISO/IEC 18013-5 การดึงข้อมูลอุปกรณ์ช่วยขจัดความจำเป็นในการเรียกไปยังเซิร์ฟเวอร์ในระหว่างการแสดง ดังนั้นจึงปกป้องผู้ใช้จากการถูกติดตามโดย Apple และผู้ออกบัตรได้

iMessage

ภาพรวมความปลอดภัยของ iMessage

Apple iMessage คือบริการรับส่งข้อความสำหรับอุปกรณ์ iOS และ iPadOS, Apple Watch และคอมพิวเตอร์ Mac โดย iMessage รองรับข้อความและไฟล์แนบ เช่น รูปภาพ รายชื่อ ตำแหน่งที่ตั้ง ลิงก์ และไฟล์แนบบนข้อความโดยตรง เช่น ไอคอนยกนิ้วโป้ง ข้อความจะแสดงบนอุปกรณ์ทุกเครื่องที่จดทะเบียนไว้ของผู้ใช้ เพื่อให้สามารถสนทนาต่อได้จากอุปกรณ์ทุกเครื่องของผู้ใช้ iMessage ใช้บริการการแจ้งผลักข้อมูลของ Apple (APNs) ในปริมาณมาก Apple ไม่เก็บบันทึกการใช้งานเนื้อหาของข้อความหรือไฟล์แนบ ซึ่งรายการเหล่านี้จะถูกปกป้องด้วยการเข้ารหัสแบบต้นทางถึงปลายทาง ดังนั้นเฉพาะผู้ส่งและผู้รับเท่านั้นที่จะสามารถเข้าถึงข้อมูลได้ Apple ไม่สามารถถอดรหัสข้อมูลได้

เมื่อผู้ใช้เปิดใช้ iMessage บนอุปกรณ์ อุปกรณ์จะสร้างกุญแจการเข้ารหัสและกุญแจการเซ็นชื่อแบบเป็นคู่เพื่อใช้กับบริการ สำหรับการเข้ารหัส จะมีกุญแจการเข้ารหัส RSA 1280 บิต และกุญแจการเข้ารหัส EC 256 บิตบนเส้นโค้ง NIST P-256 สำหรับลายเซ็น จะมีการใช้กุญแจการลงชื่อ 256 บิตที่ใช้อัลกอริทึมลายเซ็นดิจิตอลแบบเส้นโค้งรูปไข่ (ECDSA) กุญแจส่วนตัวจะถูกบันทึกลงในพวงกุญแจของอุปกรณ์และจะใช้งานได้หลังจากปลดล็อคครั้งแรกเท่านั้น กุญแจสาธารณะจะถูกส่งไปยังบริการข้อมูลประจำตัว (IDS) ของ Apple ซึ่งกุญแจเหล่านี้จะถูกเชื่อมโยงกับเบอร์โทรศัพท์หรือที่อยู่อีเมลของผู้ใช้พร้อมกับที่อยู่ APNs ของอุปกรณ์

เมื่อผู้ใช้เปิดใช้งานอุปกรณ์เพิ่มเติมสำหรับใช้งานกับ iMessage กุญแจสาธารณะการเข้ารหัสและการลงชื่อ ที่อยู่ APNs และเบอร์โทรศัพท์ที่ถูกเชื่อมโยงของผู้ใช้จะถูกเพิ่มไปยังบริการไดเรกทอรี ผู้ใช้ยังสามารถเพิ่มที่อยู่อีเมลเพิ่มเติม ซึ่งได้รับการตรวจสอบยืนยันโดยการส่งลิงก์ยืนยัน เบอร์โทรศัพท์จะได้รับการตรวจสอบยืนยันโดยเครือข่ายผู้ให้บริการและ SIM ในบางเครือข่าย การตรวจสอบยืนยันนี้จะต้องใช้ SMS (ระบบจะแสดงหน้าต่างโต้ตอบการยืนยันให้ผู้ใช้เห็นหาก SMS ไม่อยู่ในระดับศูนย์) การตรวจสอบยืนยันเบอร์โทรศัพท์อาจต้องใช้สำหรับบริการระบบหลายๆ อย่างนอกเหนือจาก iMessage เช่น FaceTime และ iCloud อุปกรณ์ที่จดทะเบียนทุกเครื่องของผู้ใช้จะแสดงข้อความเตือนเมื่ออุปกรณ์ เบอร์โทรศัพท์ หรือที่อยู่อีเมลใหม่ถูกเพิ่ม

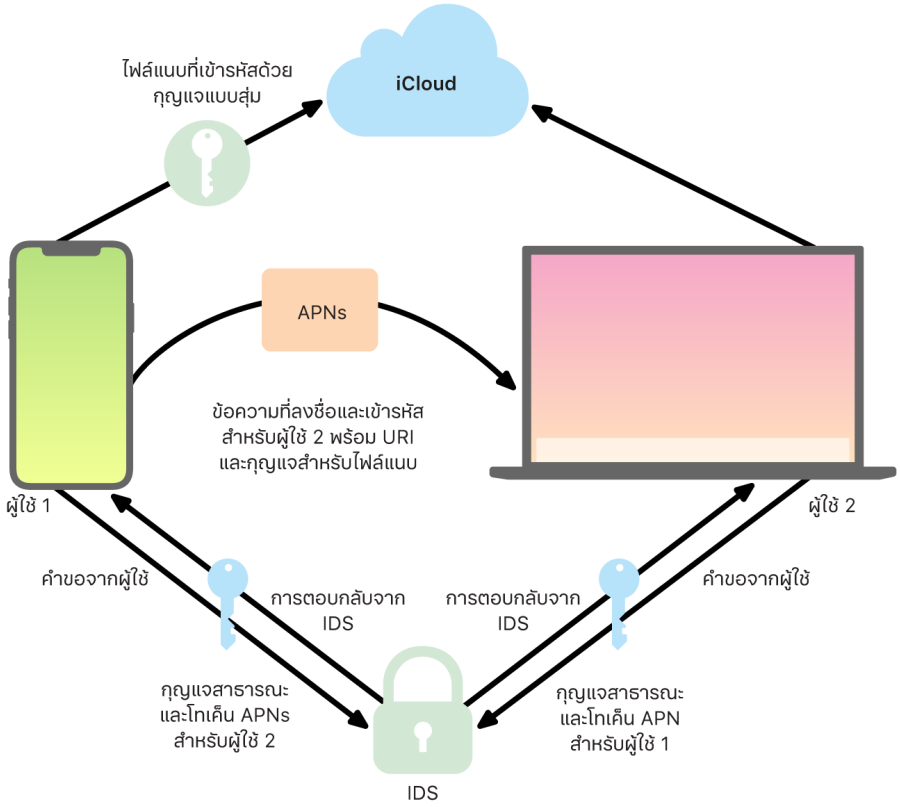
วิธีการที่ iMessage ส่งและรับข้อความอย่างปลอดภัย

ผู้ใช้เริ่มต้นบทสนทนา iMessage ใหม่โดยการป้อนที่อยู่หรือชื่อ ถ้าผู้ใช้ป้อนเบอร์โทรศัพท์หรือที่อยู่อีเมล อุปกรณ์จะติดต่อบริการข้อมูลประจำตัว (IDS) ของ Apple เพื่อเรียกใช้กุญแจสาธารณะและที่อยู่ APNs สำหรับอุปกรณ์ทั้งหมดที่เชื่อมโยงกับผู้รับนั้น ถ้าผู้ใช้ป้อนชื่อ อันดับแรกอุปกรณ์จะใช้แอปรายชื่อของผู้ใช้เพื่อรวบรวมเบอร์โทรศัพท์และที่อยู่อีเมลที่เชื่อมโยงกับชื่อนั้น จากนั้นรับกุญแจสาธารณะและที่อยู่ APNs จาก IDS

ข้อความที่ส่งออกของผู้ใช้แต่ละอันจะถูกเข้ารหัสสำหรับอุปกรณ์ของผู้รับแต่ละเครื่อง กุญแจการเข้ารหัสสาธารณะและกุญแจการเซ็นชื่อของอุปกรณ์ที่รับจะดึงข้อมูลจาก IDS สำหรับอุปกรณ์ที่รับแต่ละเครื่อง อุปกรณ์ที่ส่งจะสร้างค่า 88 บิต แบบสุ่ม และใช้ค่าดังกล่าวเป็นกุญแจ HMAC-SHA256 เพื่อสร้างค่า 40 บิตที่ได้รับจากกุญแจสาธารณะและข้อความธรรมดาของผู้ส่งและผู้รับ การแปรผันของค่า 88 บิต และ 40 บิต จะเป็นการสร้างกุญแจ 128 บิต ที่เข้ารหัสข้อความโดยใช้ AES ในโหมดตัวนับ (CTR) ค่า 40 บิต จะใช้ในฝั่งผู้รับเพื่อตรวจสอบยืนยันความสมบูรณ์ของข้อความธรรมดาที่ถอดรหัสแล้ว กุญแจ AES รายข้อความนี้จะถูกเข้ารหัสโดยใช้ RSA-OAEP ไปที่กุญแจสาธารณะของอุปกรณ์ที่รับ ชุดของข้อความตัวอักษรที่เข้ารหัสและกุญแจข้อความที่เข้ารหัสจะถูกแฮชด้วย SHA-1 และแฮชจะได้รับการลงชื่อด้วยอัลกอริทึมลายเซ็นดิจิตอลแบบเส้นโค้งรูปไข่ (ECDSA) โดยใช้กุญแจการลงชื่อส่วนตัวของอุปกรณ์ที่ส่ง ใน iOS 13 ขึ้นไป และ iPadOS 13.1 ขึ้นไป อุปกรณ์อาจใช้การเข้ารหัส Elliptic Curve Integrated Encryption Scheme (ECIES) แทนการเข้ารหัส RSA

ข้อความผลลัพธ์ที่ได้ ซึ่งแต่ละอันสำหรับอุปกรณ์ที่รับแต่ละเครื่อง จะประกอบด้วยข้อความตัวอักษรที่เข้ารหัส กุญแจข้อความที่เข้ารหัส และลายมือชื่อดิจิตอลของผู้ส่ง ข้อความจะถูกส่งไปยัง APNs สำหรับการส่งต่อ เมตาดาต้า เช่น ตราประทับเวลาและข้อมูลเส้นทาง APNs จะไม่ถูกเข้ารหัส การติดต่อกับ APNs จะถูกเข้ารหัสโดยใช้ช่องทาง forward-secret TLS

APNs สามารถส่งต่อข้อความขนาดสูงสุด 4 หรือ 16 KB เท่านั้น ทั้งนี้ขึ้นอยู่กับเวอร์ชั่นของ iOS หรือ iPadOS ถ้าข้อความตัวอักษรยาวเกินไป หรือถ้าไฟล์แนบ เช่น รูปภาพ รวมอยู่ด้วย ไฟล์แนบจะถูกเข้ารหัสโดยใช้ AES ในโหมด CTR พร้อมกับกุญแจ 256 บิตที่สร้างแบบสุ่ม และมีการอัปโหลดไปยัง iCloud กุญแจ AES สำหรับไฟล์แนบ ตัวระบุแหล่งทรัพยากรสากล (URI) ของกุญแจ และแฮช SHA-1 ของกุญแจในรูปแบบที่เข้ารหัสแล้วจะถูกส่งไปยังผู้รับเป็นเนื้อหาของ iMessage โดยได้รับการปกป้องความลับและความสมบูรณ์ของข้อมูลผ่านการเข้ารหัส iMessage แบบปกติ ตามที่แสดงในไดอะแกรมต่อไปนี้



สำหรับบทสนทนากลุ่ม กระบวนการทำงานนี้จะมีการทำซ้ำสำหรับผู้รับแต่ละรายและอุปกรณ์ของผู้รับ

สำหรับฝั่งรับ อุปกรณ์แต่ละเครื่องจะได้รับสำเนาของข้อความจาก APNs และหากจำเป็น จะได้รับไฟล์แนบจาก iCloud เบอร์โทรศัพท์ที่โทรเข้าหรือที่อยู่อีเมลของผู้ส่งจะถูกจับคู่กับรายชื่อของผู้รับเพื่อให้แสดงชื่อเมื่อเป็นไปได้

เช่นเดียวกับการแจ้งเตือนแบบผลักข้อมูลทั้งหมด ข้อความจะถูกลบออกจาก APNs เมื่อส่งเรียบร้อยแล้ว อย่างไรก็ตาม ข้อความ iMessage จะถูกจัดเข้าคิวเพื่อการส่งไปยังอุปกรณ์ออฟไลน์ ซึ่งแตกต่างจากการแจ้งเตือน APNs อื่น ข้อความจะถูกจัดเก็บไว้บนเซิร์ฟเวอร์ของ Apple สูงสุด 30 วัน

การแชร์ชื่อและรูปภาพสำหรับ iMessage ที่ปลอดภัย

การแชร์ชื่อและรูปภาพสำหรับ iMessage ช่วยให้ผู้ใช้สามารถแชร์ชื่อและรูปภาพโดยใช้ iMessage ได้ ผู้ใช้สามารถเลือกข้อมูลบัตรของฉันหรือปรับแต่งชื่อและใส่ภาพที่ผู้ใช้เลือกได้ การแชร์ชื่อและรูปภาพของ iMessage จะใช้ระบบสองขั้นตอนในการเผยแพร่ชื่อและรูปภาพ

ข้อมูลจะถูกแบ่งแยกย่อยเป็นช่อง แต่ละช่องจะถูกเข้ารหัสและตรวจสอบสิทธิ์แยกจากกัน และด้วยกัน โดยใช้กระบวนการด้านล่าง ข้อมูลจะมีสามช่อง:

- ชื่อ
- รูปภาพ
- ชื่อไฟล์รูปภาพ

ขั้นตอนแรกในการสร้างคือการสุ่มสร้างกุญแจบันทึก 128 บิตบนอุปกรณ์ จากนั้นกุญแจบันทึกนี้จะถูกรับมาพร้อมกับ HKDF-HMAC-SHA256 เพื่อสร้างกุญแจย่อยสามรายการ: กุญแจ 1:กุญแจ 2:กุญแจ 3 = HKDF(กุญแจบันทึก, "ชื่อเล่น") ในแต่ละช่อง เวกเตอร์การเริ่มต้นทำงาน (IV) 96 บิตจะถูกสร้างขึ้นแบบสุ่มและข้อมูลจะถูกเข้ารหัสโดยใช้ AES-CTR และกุญแจ 1 จากนั้นจะมีการคำนวณรหัสการตรวจสอบสิทธิ์ข้อความ (MAC) ด้วย HMAC-SHA256 โดยใช้กุญแจ 2 และจะครอบคลุมชื่อของช่อง, IV ของช่อง และข้อความที่เข้ารหัสของช่อง ขั้นสุดท้าย ชุดค่า MAC ของช่องแต่ละช่องจะถูกนำมาต่อกันและ MAC ของค่าเหล่านั้นจะถูกคำนวณด้วย HMAC-SHA256 โดยใช้กุญแจ 3 MAC 256 บิตจะถูกจัดเก็บไว้กับข้อมูลที่เข้ารหัส 128 บิตแรกของ MAC นี้จะถูกใช้เป็น RecordID

จากนั้นข้อมูลบันทึกที่เข้ารหัสนี้จะถูกจัดเก็บไว้ในฐานข้อมูลสาธารณะ CloudKit ภายใต้ RecordID ข้อมูลบันทึกนี้จะไม่เปลี่ยนแปลงและเมื่อผู้ใช้เลือกที่จะเปลี่ยนชื่อและรูปภาพของตน ข้อมูลบันทึกที่เข้ารหัสรายการใหม่จะถูกสร้างขึ้นทุกครั้ง เมื่อผู้ใช้ 1 เลือกที่จะแชร์ชื่อและรูปภาพของตัวเองกับผู้ใช้ 2 พวกเขาจะส่งกุญแจบันทึกไปพร้อมกับ recordID ภายในเพย์โหลด iMessage ของพวกเขา ซึ่งจะถูกเข้ารหัส

เมื่ออุปกรณ์ของผู้ใช้ 2 ได้รับเพย์โหลด iMessage นี้ อุปกรณ์จะสังเกตเห็นว่าเพย์โหลดประกอบด้วย recordID และกุญแจของชื่อเล่นและรูปภาพ จากนั้นอุปกรณ์ของผู้ใช้ 2 จะออกไปที่ฐานข้อมูล CloudKit สาธารณะเพื่อดึงข้อมูลชื่อและรูปภาพที่เข้ารหัสที่ ID ของข้อมูลบันทึกแล้วส่งข้อมูลนั้นไปให้อีกฝ่ายโดยใช้ iMessage

หลังจากที่ดึงข้อความมาแล้ว อุปกรณ์ของผู้ใช้ 2 จะถอดรหัสเพย์โหลดและตรวจสอบยืนยันลายเซ็นโดยใช้ตัว recordID เอง ถ้าผ่าน ผู้ใช้ 2 จะได้รับชื่อและรูปภาพ และพวกเขาสามารถเลือกเพิ่มข้อมูลนี้ไปยังรายชื่อของตนหรือใช้ข้อมูลนี้กับแอปข้อความได้

Apple Messages for Business ที่ปลอดภัย

Apple Messages for Business คือบริการรับส่งข้อความที่ช่วยให้ผู้ใช้สามารถสื่อสารกับธุรกิจต่างๆ โดยใช้แอปข้อความได้ ด้วย Apple Messages for Business ผู้ใช้จะเป็นผู้ควบคุมการสนทนาเสมอ อีกทั้งยังสามารถลบการสนทนาและปิดกั้นไม่ให้ธุรกิจส่งข้อความถึงพวกเขาในอนาคตได้อีกด้วย เพื่อความเป็นส่วนตัว ธุรกิจจะไม่ได้รับข้อมูลเบอร์โทรศัพท์ ที่อยู่อีเมล หรือบัญชี iCloud ของผู้ใช้ แต่ข้อมูลจำเพาะที่ไม่ซ้ำกันของลูกค้าที่เรียก **Opaque ID** จะถูกสร้างขึ้นโดยบริการข้อมูลประจำตัว(IDS) ของ Apple และแชร์กับธุรกิจ Opaque ID มีลักษณะเฉพาะสำหรับความสัมพันธ์ระหว่าง Apple ID ของผู้ใช้และ Business ID ของธุรกิจ ผู้ใช้จะมี Opaque ID ที่แตกต่างกันสำหรับทุกๆ ธุรกิจที่ติดต่อโดยใช้ Apple Messages for Business ผู้ใช้ตัดสินใจว่าจะแชร์ข้อมูลระบุตัวตนส่วนบุคคลกับธุรกิจหรือไม่และเมื่อใด และบริการ Apple Messages for Business จะไม่มีการเก็บประวัติการสนทนา

Apple Messages for Business รองรับ Apple ID ที่มีการจัดการจาก Apple Business Manager และกำหนดว่าจะเปิดใช้งานสำหรับ iMessage และ FaceTime ใน Apple School Manager หรือไม่

ข้อความที่ส่งไปยังธุรกิจจะถูกเข้ารหัสระหว่างอุปกรณ์ของผู้ใช้และเซิร์ฟเวอร์การส่งข้อความของ Apple โดยใช้ความปลอดภัยระดับเดียวกันและเซิร์ฟเวอร์การส่งข้อความของ Apple ในรูปแบบ iMessages เซิร์ฟเวอร์การส่งข้อความของ Apple จะถอดรหัสข้อความเหล่านี้ใน RAM แล้วส่งต่อข้อความไปยังธุรกิจผ่านลิงก์ที่เข้ารหัสโดยใช้ TLS 1.2 ข้อความจะไม่ถูกจัดเก็บในรูปแบบที่ไม่ได้เข้ารหัสในขณะที่ส่งผ่านบริการ Apple Messages for Business การตอบกลับของธุรกิจจะส่งโดยใช้ TLS 1.2 ไปยังเซิร์ฟเวอร์การส่งข้อความของ Apple ซึ่งเป็นที่ที่การตอบกลับได้รับการเข้ารหัสโดยใช้กุญแจสาธารณะเฉพาะตัวของอุปกรณ์ของผู้รับแต่ละเครื่อง

ถ้าอุปกรณ์ของผู้ใช้ออนไลน์อยู่ ข้อความจะถูกส่งทันทีและไม่ถูกแคชบนเซิร์ฟเวอร์การส่งข้อความของ Apple ถ้าอุปกรณ์ของผู้ใช้ไม่ได้ออนไลน์อยู่ ข้อความที่เข้ารหัสจะถูกแคชไว้เป็นระยะเวลาสูงสุด 30 วันเพื่อให้ผู้ใช้สามารถรับข้อความนั้นได้เมื่ออุปกรณ์กลับมาออนไลน์อีกครั้ง ทันทีที่อุปกรณ์กลับมาออนไลน์อีกครั้ง ข้อความจะถูกส่งแล้วลบออกจากการแคช หลังจาก 30 วัน ข้อความที่ถูกแคชและไม่ได้ส่งจะหมดอายุและถูกลบอย่างถาวร

ความปลอดภัยของ FaceTime

FaceTime คือบริการโทรแบบวิดีโอและเสียงของ Apple การโทร FaceTime จะใช้บริการการแจ้งเตือนแบบผลักข้อมูลของ Apple (APNs) เพื่อสร้างการเชื่อมต่อเริ่มต้นไปยังอุปกรณ์ที่จดทะเบียนของผู้ใช้ ซึ่งคล้ายคลึงกับ iMessage เนื้อหาแบบเสียง/วิดีโอของการโทร FaceTime จะถูกปกป้องด้วยการเข้ารหัสแบบต้นทางถึงปลายทาง ดังนั้นเฉพาะผู้ส่งและผู้รับเท่านั้นที่จะสามารถเข้าถึงข้อมูลได้ Apple ไม่สามารถถอดรหัสข้อมูลได้

การเชื่อมต่อ FaceTime เริ่มต้นสร้างขึ้นผ่านโครงสร้างพื้นฐานของเซิร์ฟเวอร์ Apple ที่ส่งต่อแพ็คเกตข้อมูลระหว่างอุปกรณ์ที่จดทะเบียนของผู้ใช้ อุปกรณ์จะใช้การแจ้งเตือนแบบ APNs และข้อความแบบ Session Traversal Utilities for NAT (STUN) ผ่านการเชื่อมต่อแบบส่งต่อข้อมูลเพื่อตรวจสอบยืนยันใบรับรองข้อมูลประจำตัวของอุปกรณ์และสร้างข้อมูลลับที่แชร์สำหรับแต่ละเซสชั่น ข้อมูลลับที่แชร์จะถูกใช้เพื่อรับกุญแจเซสชั่นสำหรับช่องทางสื่อที่สตรีมผ่าน Secure Real-time Transport Protocol (SRTP) แพ็คเกต SRTP ถูกเข้ารหัสโดยใช้ AES256 ในโหมด Counter และการยืนยันตัวตนด้วย HMAC-SHA1 หลังจากตั้งค่าการเชื่อมต่อเริ่มต้นและความปลอดภัยแล้ว FaceTime จะใช้ STUN และ Internet Connectivity Establishment (ICE) เพื่อสร้างการเชื่อมต่อแบบเพียร์ทูเพียร์ระหว่างอุปกรณ์ หากสามารถทำได้

FaceTime แบบกลุ่มทำให้ FaceTime สามารถรองรับผู้เข้าร่วมได้พร้อมกันสูงสุด 33 คน เช่นเดียวกับ FaceTime แบบคลาสสิกที่เป็นแบบหนึ่งต่อหนึ่ง สายโทรจะถูกเข้ารหัสแบบต้นทางถึงปลายทางบนอุปกรณ์ของผู้เข้าร่วมที่ได้รับเชิญ แม้ว่า FaceTime แบบกลุ่มจะนำโครงสร้างพื้นฐานและรูปแบบส่วนใหญ่ของ FaceTime แบบตัวต่อตัวมาใช้ซ้ำ การโทรแบบกลุ่มเหล่านี้มีกลไกการสร้างกุญแจที่สร้างขึ้นจากการยืนยันตัวตนโดย Apple Identity Service (IDS) โปรโตคอลนี้มีกระบวนการรักษาความลับในการส่งต่อ ซึ่งหมายความว่าช่องโหว่ของอุปกรณ์ของผู้ใช้จะไม่ทำให้เนื้อหาของการโทรที่ผ่านมารั่วไหล กุญแจเซสชั่นจะถูกหุ้มด้วย AES-SIV และแจกจ่ายระหว่างผู้เข้าร่วมโดยใช้โครงสร้าง ECIES ที่มีกุญแจ ECDH P-256 แบบชั่วคราว

เมื่อเบอร์โทรศัพท์หรือที่อยู่อีเมลใหม่ถูกเพิ่มไปยังการโทร FaceTime แบบกลุ่มที่กำลังดำเนินอยู่ อุปกรณ์ที่ใช้งานอยู่จะกำหนดกุญแจสื่อรายการใหม่และไม่แชร์กุญแจที่ใช้ก่อนหน้านี้กับอุปกรณ์ที่เพิ่งเชิญเข้ามา

ค้นหาของฉัน

ความปลอดภัยของ “ค้นหาของฉัน”

แอป “ค้นหาของฉัน” สำหรับอุปกรณ์ Apple ถูกสร้างขึ้นบนรากฐานการเข้ารหัสกุญแจสาธารณะขั้นสูง

ภาพรวม

แอป “ค้นหาของฉัน” เป็นการรวม “ค้นหา iPhone ของฉัน” และ “ค้นหาเพื่อนๆ ของฉัน” เข้าด้วยกันเป็นแอปเดียวใน iOS, iPadOS และ macOS “ค้นหาของฉัน” สามารถช่วยผู้ใช้ค้นหาอุปกรณ์ที่สูญหายได้ แม้ว่า Mac จะออฟไลน์อยู่ อุปกรณ์ที่ออนไลน์อยู่เพียงแจ้งตำแหน่งที่ตั้งของอุปกรณ์ให้แก่ผู้ใช้ผ่าน iCloud “ค้นหาของฉัน” ทำงานแบบออฟไลน์โดยการส่งสัญญาณบลูทูธระยะสั้นจากอุปกรณ์ที่สูญหายซึ่งสามารถตรวจพบได้โดยอุปกรณ์ Apple เครื่องอื่นๆ ที่ใช้งานอยู่ในบริเวณใกล้เคียง จากนั้นอุปกรณ์ที่อยู่ใกล้เคียงเหล่านั้นจะส่งต่อตำแหน่งที่ตั้งที่ตรวจพบอุปกรณ์ที่สูญหายไปยัง iCloud เพื่อให้ผู้ใช้สามารถระบุตำแหน่งที่ตั้งของอุปกรณ์ได้ในแอป “ค้นหาของฉัน” และในขณะเดียวกันก็ปกป้องความเป็นส่วนตัวและความปลอดภัยของผู้ใช้ทุกคนที่เกี่ยวข้อง “ค้นหาของฉัน” ทำงานแม้กระทั่งกับ Mac ที่ออฟไลน์อยู่และอยู่ในโหมดพัก

ด้วยการใช้บลูทูธและอุปกรณ์ iOS, iPadOS และ macOS หลายร้อยล้านเครื่องที่ใช้งานทั่วโลก ผู้ใช้สามารถระบุตำแหน่งอุปกรณ์ที่หายไปได้แม้ว่าอุปกรณ์จะไม่ได้เชื่อมต่อกับ Wi-Fi หรือเครือข่ายเซลลูลาร์ อุปกรณ์ iOS, iPadOS หรือ macOS เครื่องใดก็ตามที่เปิดใช้งาน "การค้นหาแบบออฟไลน์" ไว้ในการตั้งค่า "ค้นหาของฉัน" จะสามารถทำหน้าที่เป็น "อุปกรณ์ค้นหา" ได้ ซึ่งหมายความว่า อุปกรณ์ตรวจพบการมีอยู่ของอุปกรณ์อีกเครื่องที่สูญหายในขณะที่ออฟไลน์อยู่โดยใช้บลูทูธ จากนั้นอุปกรณ์จะใช้การเชื่อมต่อกับเครือข่ายเพื่อแจ้งตำแหน่งที่ตั้งโดยประมาณไปยังเจ้าของ เมื่ออุปกรณ์เปิดใช้งานการค้นหาแบบออฟไลน์ นั่นหมายความว่าผู้เข้าร่วมคนอื่นๆ จะสามารถค้นหาอุปกรณ์เครื่องนั้นได้ด้วยวิธีเดียวกัน การโต้ตอบทั้งหมดนี้ได้รับการเข้ารหัสแบบต้นทางถึงปลายทาง ไม่ระบุตัวตน และได้รับการออกแบบมาให้ใช้แบตเตอรี่และข้อมูลอย่างมีประสิทธิภาพ มีผลกระทบต่ออายุการใช้งานแบตเตอรี่และการใช้แผนบริการข้อมูลเซลลูลาร์เพียงเล็กน้อย รวมถึงผู้ใช้จะได้รับการปกป้องความเป็นส่วนตัวที่ดีขึ้น

หมายเหตุ: "ค้นหาของฉัน" อาจไม่มีให้ใช้ได้ครบทุกประเทศหรือภูมิภาค

การเข้ารหัสแบบต้นทางถึงปลายทาง

"ค้นหาของฉัน" ถูกสร้างขึ้นบนรากฐานการเข้ารหัสกุญแจสาธารณะขั้นสูง เมื่อการค้นหาแบบออฟไลน์เปิดใช้งานอยู่ในการตั้งค่า "ค้นหาของฉัน" คู่กุญแจการเข้ารหัสแบบส่วนตัว P-224 แบบเส้นโค้งรูปไข่ (EC) ที่ระบุเป็น {d,P} จะถูกสร้างขึ้นโดยตรงบนอุปกรณ์ โดยที่ **d** เป็นกุญแจส่วนตัวและ **P** เป็นกุญแจสาธารณะ นอกจากนี้ SK0 ลับ 256 บิต และตัวนับ $_i$ ก็จะเริ่มต้นที่ศูนย์ กุญแจส่วนตัวและข้อมูลลับนี้จะไม่ถูกส่งไปที่ Apple และจะเชื่อมข้อมูลกับอุปกรณ์เครื่องอื่นๆ ของผู้ใช้เท่านั้น โดยจะเชื่อมในรูปแบบการเข้ารหัสแบบต้นทางถึงปลายทางโดยใช้พวงกุญแจ iCloud ข้อมูลลับและตัวนับจะใช้เพื่อรับกุญแจสมมาตรปัจจุบัน SK_i ด้วยโครงสร้างแบบเรียกซ้ำต่อไปนี้: $SK_i = KDF(SK_{i-}1, \text{“update”})$

อิงจากกุญแจ SK_i จำนวนเต็มสองจำนวนที่มีค่ามาก u_i และ v_i จะถูกคำนวณด้วย $(u_i,v_i) = KDF(SK_i, \text{“diversify”})$ ทั้งกุญแจส่วนตัว P-224 ที่แสดงด้วย **d** และกุญแจสาธารณะที่สัมพันธ์กันที่แสดงด้วย **P** จะมีการรับมาโดยใช้ความสัมพันธ์แบบสัมพรรคที่ประกอบด้วยจำนวนเต็มสองจำนวนเพื่อคำนวณคู่กุญแจระยะสั้น: กุญแจส่วนตัวที่ได้รับคือ d_i, โดยที่ $d_i = u_i * d + v_i$ (โมดูโลลำดับของเส้นโค้ง P-224) และส่วนสาธารณะที่สัมพันธ์กันคือ P_i และตรวจสอบยืนยันว่า $P_i = u_i*P + v_i*G$

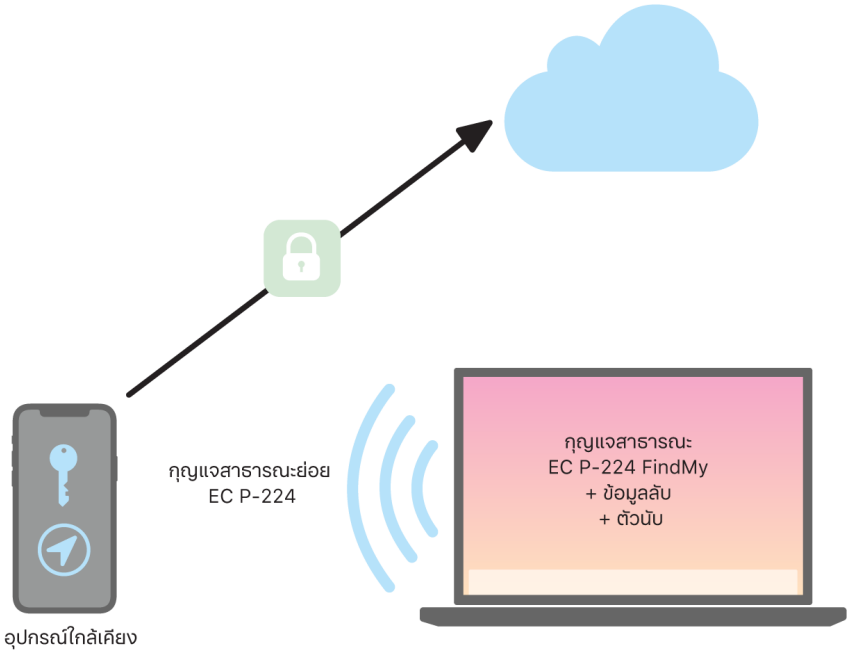
เมื่ออุปกรณ์สูญหายและไม่สามารถเชื่อมต่อกับ Wi-Fi หรือเซลลูลาร์ได้ เช่น MacBook Pro ถูกทิ้งไว้บนม้านั่งในสวนสาธารณะ อุปกรณ์นั้นจะเริ่มกระจายสัญญาณกุญแจสาธารณะ P_i ที่รับมาเป็นระยะๆ เป็นเวลาจำกัดในเพย์โหลดบลูทูธ เมื่อใช้ P-224 ตัวแทนกุญแจสาธารณะจะสามารถใส่ลงในเพย์โหลดบลูทูธรายการเดียวได้พอดี จากนั้นอุปกรณ์ที่อยู่รอบๆ จะสามารถช่วยค้นหาอุปกรณ์ที่ออฟไลน์ได้โดยเข้ารหัสตำแหน่งที่ตั้งของตัวเองไปยังกุญแจสาธารณะ ทุกๆ 15 นาทีโดยประมาณ กุญแจสาธารณะจะถูกแทนที่ด้วยกุญแจใหม่โดยใช้ค่าที่เพิ่มขึ้นของตัวนับและกระบวนการด้านบนเพื่อให้ผู้ใช้ไม่โดนติดตามโดยข้อมูลจำเพาะแบบต่อเนื่อง กลไกการดึงได้รับการออกแบบมาเพื่อป้องกันไม่ให้กุญแจสาธารณะ P_i ที่มีอยู่หลากหลายเชื่อมโยงกับอุปกรณ์เดียวกัน

การไม่เปิดเผยผู้ใช้และอุปกรณ์

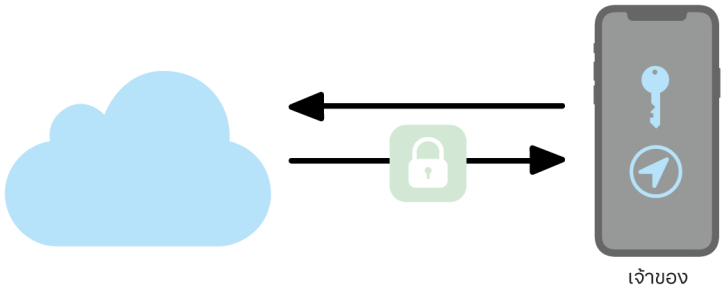
นอกเหนือจากการทำให้แน่ใจว่าข้อมูลตำแหน่งที่ตั้งและข้อมูลอื่นๆ จะถูกเข้ารหัสอย่างสมบูรณ์แล้ว ข้อมูลประจำตัวของผู้เข้าร่วมยังถูกเก็บเป็นความลับจากกันและกัน และจาก Apple อีกด้วย ข้อมูลที่ส่งไปที่ Apple โดยอุปกรณ์ค้นหาจะไม่มีข้อมูลการตรวจสอบสิทธิ์ในเนื้อหาหรือส่วนหัว ด้วยเหตุนี้ Apple จึงไม่ทราบว่าตัวค้นหาคือใคร หรือว่าอุปกรณ์ที่พบคืออุปกรณ์ของผู้ใด นอกจากนี้ Apple ยังไม่เก็บบันทึกข้อมูลที่เปิดเผยตัวตนของตัวค้นหา และไม่เก็บข้อมูลที่ทำให้คนอื่นทราบความสัมพันธ์ระหว่างตัวค้นหาและเจ้าของได้ เจ้าของอุปกรณ์จะได้รับเพียงข้อมูลตำแหน่งที่ตั้งที่เข้ารหัสเท่านั้น ซึ่งจะถูกถอดรหัสและแสดงในแอป "ค้นหาของฉัน" โดยไม่ระบุว่าใครเป็นคนพบอุปกรณ์

การใช้ “ค้นหาของฉัน” เพื่อค้นหาอุปกรณ์ Apple ที่สูญหาย

อุปกรณ์ใดๆ ของ Apple ที่อยู่ภายในระยะสัญญาณบลูทูธและเปิดใช้งานการค้นหาแบบออฟไลน์ไว้จะสามารถตรวจพบสัญญาณจากอุปกรณ์ Apple อีกเครื่องที่กำหนดค่าให้อนุญาต “ค้นหาของฉัน” ไว้และอ่านกุญแจกระจายสัญญาณ P_i รายการปัจจุบันได้ เมื่อใช้โครงสร้าง ECIES และกุญแจสาธารณะ P_i จากการกระจายสัญญาณ อุปกรณ์ค้นหาจะเข้ารหัสตำแหน่งที่ตั้งปัจจุบันของตัวเองและส่งต่อไปที่ Apple ตำแหน่งที่ตั้งที่เข้ารหัสจะเชื่อมโยงกับดัชนีเซิร์ฟเวอร์ ซึ่งคำนวณได้เป็นแฮช SHA256 ของกุญแจสาธารณะ P-224 P_i ที่ได้รับจากเพย์โหลดบลูทูธ Apple ไม่มีกุญแจถอดรหัสใดๆ ดังนั้น Apple จะไม่สามารถอ่านตำแหน่งที่ตั้งที่เข้ารหัสโดยตัวค้นหาได้ เจ้าของอุปกรณ์ที่สูญหายสามารถสร้างดัชนีอีกครั้งและถอดรหัสตำแหน่งที่ตั้งที่เข้ารหัสไว้ได้



เมื่อพยายามระบุตำแหน่งที่ตั้งของอุปกรณ์ที่สูญหาย ระบบจะประมาณการช่วงของค่าตัวนับที่คาดหวังสำหรับระยะเวลาในการค้นหาตำแหน่งที่ตั้ง เมื่อทราบกุญแจส่วนตัวดั้งเดิม P-224 **d** และค่าลับ SK_i ในช่วงค่าตัวนับของระยะเวลาการค้นหาแล้ว เจ้าของจะสามารถสร้างชุดค่า $\{d_i, SHA256(P_i)\}$ ขึ้นใหม่อีกครั้งตลอดระยะเวลาการค้นหาได้ จากนั้นอุปกรณ์ของเจ้าของที่ใช้ระบุตำแหน่งที่ตั้งของอุปกรณ์ที่สูญหายจะสามารถส่งคำขอไปยังเซิร์ฟเวอร์โดยใช้ชุดค่าดัชนี $SHA256(P_i)$ แล้วดาวน์โหลดตำแหน่งที่ตั้งที่เข้ารหัสจากเซิร์ฟเวอร์ได้ จากนั้นแอป “ค้นหาของฉัน” จะดำเนินการถอดรหัสภายในเครื่องกับตำแหน่งที่ตั้งที่ถูกเข้ารหัส โดยจะใช้กุญแจส่วนตัวที่ตรงกัน d_i และแสดงตำแหน่งที่ตั้งโดยประมาณของอุปกรณ์ที่สูญหายในแอป การแจ้งตำแหน่งที่ตั้งจากอุปกรณ์ค้นหาหลายๆ เครื่องจะถูกรวมเข้าด้วยกันโดยแอปของเจ้าของเพื่อสร้างตำแหน่งที่ตั้งที่แม่นยำยิ่งขึ้น



การค้นหาอุปกรณ์ที่ออฟไลน์อยู่

ถ้าผู้ใช้เปิดใช้งาน “ค้นหา iPhone ของฉัน” ไว้บนอุปกรณ์ของตัวเอง การค้นหาแบบออฟไลน์จะเปิดใช้งานตามค่าเริ่มต้นเมื่อผู้ใช้อัปเกรดอุปกรณ์เป็น iOS 13 ขึ้นไป, iPadOS 13.1 ขึ้นไป และ macOS 10.15 ขึ้นไป สิ่งนี้ได้รับการออกแบบมาเพื่อให้แน่ใจว่าผู้ใช้ทุกรายจะมีโอกาสค้นพบอุปกรณ์ของตนมากที่สุดเท่าที่จะเป็นไปได้หากอุปกรณ์สูญหาย อย่างไรก็ตาม ถ้าเมื่อใดก็ตามที่ผู้ใช้ไม่ต้องการเข้าร่วม ผู้ใช้สามารถปิดใช้งานการค้นหาแบบออฟไลน์ได้ในการตั้งค่า “ค้นหาของฉัน” บนอุปกรณ์ของพวกเขา เมื่อการค้นหาแบบออฟไลน์ถูกปิดใช้งาน อุปกรณ์จะไม่สามารถทำหน้าที่เป็นตัวค้นหาได้อีกต่อไปและไม่สามารถตรวจพบได้จากอุปกรณ์ค้นหาเครื่องอื่นๆ อย่างไรก็ตาม ผู้ใช้จะยังคงระบุตำแหน่งที่ตั้งของอุปกรณ์ได้ตราบใดที่ยังสามารถเชื่อมต่อกับเครือข่าย Wi-Fi หรือเซลลูลาร์ได้

เมื่อระบุตำแหน่งที่ตั้งของอุปกรณ์ที่สูญหายและออฟไลน์ได้แล้ว ผู้ใช้จะได้รับการแจ้งเตือนและข้อความอีเมลเพื่อแจ้งให้ผู้ใช้ทราบว่าอุปกรณ์ถูกพบแล้ว ในการดูตำแหน่งที่ตั้งของอุปกรณ์ที่สูญหาย ผู้ใช้จะต้องเปิดแอป “ค้นหาของฉัน” แล้วเลือกแถบอุปกรณ์ แทนที่จะแสดงอุปกรณ์บนแผนที่ที่ว่างเปล่า ซึ่งจะเกิดขึ้นก่อนที่จะระบุตำแหน่งที่ตั้งของอุปกรณ์ได้ แอป “ค้นหาของฉัน” จะแสดงตำแหน่งที่ตั้งบนแผนที่ โดยแสดงที่อยู่โดยประมาณและระยะเวลาที่ผ่านไปก่อนจะตรวจพบอุปกรณ์ ถ้ามีการแจ้งตำแหน่งที่ตั้งเข้ามาเพิ่ม ตำแหน่งที่ตั้งปัจจุบันและตราประทับเวลาจะอัปเดตโดยอัตโนมัติ แม้ว่าผู้ใช้จะไม่สามารถเล่นเสียงบนอุปกรณ์ที่ออฟไลน์หรือลบอุปกรณ์จากระยะไกลได้ ผู้ใช้สามารถใช้ข้อมูลตำแหน่งที่ตั้งเพื่อย้อนกลับไปยังจุดเริ่มต้นหรือดำเนินการอื่นๆ เพื่อช่วยกู้คืนอุปกรณ์กลับมาได้

ความต่อเนื่อง

ภาพรวมความปลอดภัยของคุณสมบัติความต่อเนื่อง

คุณสมบัติความต่อเนื่องใช้ประโยชน์จากเทคโนโลยีต่างๆ เช่น iCloud, บลูทูธ และ Wi-Fi เพื่อทำให้ผู้ใช้สามารถทำกิจกรรมจากอุปกรณ์เครื่องหนึ่งต่อในอุปกรณ์อีกเครื่องหนึ่ง โทรออกและรับสาย ส่งและรับข้อความตัวอักษร และแชร์การเชื่อมต่อกับอินเทอร์เน็ตแบบเซลลูลาร์ได้

ความปลอดภัยของ Handoff

Apple จัดการ Handoff อย่างปลอดภัย ไม่ว่าจะเป็นจากอุปกรณ์หนึ่งถึงอุปกรณ์อื่น ระหว่างแอปดั้งเดิมกับเว็บไซต์ หรือแม้แต่ Handoff ข้อมูลขนาดใหญ่

Handoff ทำงานอย่างปลอดภัยได้อย่างไร

ด้วย Handoff ผู้ใช้จะสามารถส่งสิ่งที่กำลังทำอยู่จากอุปกรณ์เครื่องหนึ่งไปยังอุปกรณ์อีกเครื่องหนึ่งได้โดยอัตโนมัติเมื่ออุปกรณ์ iOS, iPadOS และ macOS ของผู้ใช้อยู่ใกล้กัน Handoff ทำให้ผู้ใช้สามารถสลับอุปกรณ์แล้วทำงานต่อได้ทันที

เมื่อผู้ใช้ลงชื่อเข้า iCloud บนอุปกรณ์ที่สามารถใช้ Handoff ได้เครื่องที่สอง อุปกรณ์สองเครื่องนั้นจะสร้างการจับคู่แบบนอกช่วงความถี่สื่อสารปกติด้วยบลูทูธพลังงานต่ำ (BLE) 4.2 โดยใช้ APNs ระบบจะเข้ารหัสข้อความทีละข้อความคล้ายกับการเข้ารหัสข้อความใน iMessage หลังจากที่อุปกรณ์จับคู่กันแล้ว อุปกรณ์แต่ละเครื่องจะสร้างกุญแจ AES 256 บิตแบบสมมาตร ซึ่งจะจัดเก็บไว้ในพวงกุญแจของอุปกรณ์ กุญแจนี้ใช้เพื่อเข้ารหัสและตรวจสอบสิทธิ์ของการประกาศ BLE ที่จะส่งข้อมูลกิจกรรมปัจจุบันของอุปกรณ์ไปยังอุปกรณ์ที่จับคู่ผ่าน iCloud เครื่องอื่นๆ โดยใช้ AES256 ในโหมด GCM พร้อมมาตรการปกป้องการเล่นซ้ำ

เมื่ออุปกรณ์ได้รับการประกาศจากกุญแจใหม่เป็นครั้งแรก อุปกรณ์เครื่องนั้นจะสร้างการเชื่อมต่อ BLE กับอุปกรณ์เครื่องแรกแล้วแลกเปลี่ยนกุญแจการเข้ารหัสการประกาศ การเชื่อมต่อนี้มีการรักษาความปลอดภัยด้วยการเข้ารหัส BLE 4.2 แบบมาตรฐาน และการเข้ารหัสของข้อความแต่ละข้อความ ซึ่งมีลักษณะคล้ายกันกับการเข้ารหัส iMessage ในบางสถานการณ์ ข้อความเหล่านี้จะถูกส่งโดยใช้ APNs แทนที่จะเป็น BLE เพย์โหลดของกิจกรรมจะได้รับการปกป้องและถ่ายโอนในลักษณะเดียวกันกับ iMessage

Handoff ระหว่างแอปดั้งเดิมกับเว็บไซต์

Handoff ทำให้แอปดั้งเดิมของ iOS, iPadOS หรือ macOS สามารถทำกิจกรรมผู้ใช้ต่อได้บนหน้าเว็บในโดเมนที่นักพัฒนาแอปเป็นผู้ควบคุมอย่างถูกต้อง และยังทำให้สามารถทำกิจกรรมผู้ใช้ของแอปดั้งเดิมต่อในเว็บเบราว์เซอร์ได้อีกด้วย

ในการช่วยป้องกันไม่ให้แอปดั้งเดิมเปิดเว็บไซต์ที่ไม่ได้ควบคุมโดยนักพัฒนาต่อจากที่ค้างไว้ แอปจะต้องแสดงให้เห็นว่าแอปมีสิทธิ์อย่างถูกต้องในการควบคุมโดเมนเว็บที่ต้องการเปิดต่อ การควบคุมโดเมนเว็บไซต์จะสร้างโดยใช้กลไกสำหรับเอกสารสิทธิ์ของเว็บที่แชร์ สำหรับรายละเอียด ให้ดูที่ การเข้าถึงของแอปไปยังรหัสผ่านที่บันทึกไว้ ระบบจะต้องตรวจสอบความถูกต้องการควบคุมชื่อโดเมนของแอปก่อนที่แอปนั้นจะได้รับอนุญาตให้ยอมรับ Handoff กิจกรรมของผู้ใช้

แหล่งที่มาของการ Handoff หน้าเว็บสามารถเป็นเบราว์เซอร์ใดก็ได้ที่ใช้ API ของ Handoff เมื่อผู้ใช้ดูหน้าเว็บ ระบบจะประกาศชื่อโดเมนของหน้าเว็บเป็นไบต์การประกาศ Handoff ที่เข้ารหัส เฉพาะอุปกรณ์เครื่องอื่นของผู้ใช้เท่านั้นที่สามารถถอดรหัสไบต์การประกาศได้

ระบบของอุปกรณ์ที่เป็นฝ่ายรับจะตรวจสอบว่าแอปดั้งเดิมที่ติดตั้งอยู่ยอมรับ Handoff จากชื่อโดเมนที่ประกาศหรือไม่ แล้วแสดงไอคอนของแอปดั้งเดิมนั้นเป็นตัวเลือก Handoff เมื่อเปิดทำงาน แอปดั้งเดิมจะได้รับ URL แบบเต็มและชื่อของหน้าเว็บ โดยจะไม่มีการส่งข้อมูลอื่นจากเบราว์เซอร์ไปที่แอปดั้งเดิม

และในทางกลับกัน แอปดั้งเดิมสามารถระบุ URL สำรองเมื่ออุปกรณ์ที่เป็นฝ่ายรับ Handoff ไม่ได้ติดตั้งแอปดั้งเดิมเดียวกันได้ ในกรณีนี้ ระบบจะแสดงเบราว์เซอร์เริ่มต้นของผู้ใช้เป็นตัวเลือกแอป Handoff (หากเบราว์เซอร์นั้นใช้ API ของ Handoff) เมื่อมีการร้องขอ Handoff เบราว์เซอร์จะถูกเปิดใช้และมอบ URL สำรองที่แอปต้นทางให้มา โดย URL สำรองไม่จำเป็นต้องจำกัดอยู่เพียงชื่อโดเมนที่นักพัฒนาแอปดั้งเดิมเป็นผู้ควบคุม

Handoff ข้อมูลขนาดใหญ่

นอกจากการใช้คุณสมบัติพื้นฐานของ Handoff แล้ว แอปบางแอปอาจเลือกใช้ API ที่รองรับการส่งข้อมูลขนาดใหญ่ขึ้นผ่านทางเทคโนโลยี Wi-Fi แบบเพียร์ทูเพียร์ที่ Apple สร้างขึ้น (ในลักษณะคล้ายกันกับ AirDrop) ตัวอย่าง เช่น แอปเมลจะใช้ API เหล่านี้เพื่อรองรับ Handoff ของเมลฉบับร่าง ซึ่งอาจมีไฟล์แนบขนาดใหญ่

เมื่อแอปใช้คุณสมบัตินี้ การแลกเปลี่ยนระหว่างอุปกรณ์สองเครื่องจะเริ่มต้นเหมือนกับใน Handoff แต่หลังจากได้รับเพย์โหลดเริ่มต้นโดยใช้บลูทูธพลังงานต่ำ (BLE) แล้ว อุปกรณ์ที่เป็นเครื่องรับจะเริ่มการเชื่อมต่อใหม่ผ่าน Wi-Fi การเชื่อมต่อนี้ได้รับการเข้ารหัส (ด้วย TLS) และได้รับความเชื่อถือผ่านข้อมูลระบุตัวตนที่แชร์ผ่านพวงกุญแจ iCloud ข้อมูลประจำตัวในใบรับรองจะได้รับการตรวจสอบยืนยันเทียบกับตัวตนของผู้ใช้ ข้อมูลเพย์โหลดนอกเหนือจากนี้จะส่งผ่านการเชื่อมต่อแบบเข้ารหัสนี้จนกว่าจะถ่ายโอนเสร็จ

คลิปบอร์ดกลาง

คลิปบอร์ดกลางจะใช้ประโยชน์จาก Handoff เพื่อถ่ายโอนเนื้อหาในคลิปบอร์ดของผู้ใช้ไปยังอุปกรณ์ทุกเครื่องได้อย่างปลอดภัย เพื่อที่ผู้ใช้สามารถคัดลอกในอุปกรณ์เครื่องหนึ่งแล้ววางในอุปกรณ์อีกเครื่องหนึ่งได้ เนื้อหาจะได้รับการปกป้องด้วยวิธีการเดียวกันกับข้อมูล Handoff อื่นๆ และจะถูกแชร์ตามค่าเริ่มต้นผ่านคลิปบอร์ดกลาง นอกจากว่านักพัฒนาแอปเลือกไม่อนุญาตการแชร์

แอปสามารถเข้าถึงข้อมูลคลิปบอร์ดได้ไม่ว่าผู้ใช้จะวางคลิปบอร์ดลงในแอปแล้วหรือไม่ ด้วยคลิปบอร์ดกลาง การเข้าถึงข้อมูลนี้จะขยายรวมไปถึงแอปบนอุปกรณ์เครื่องอื่นๆ ของผู้ใช้ (ซึ่งสร้างโดยการลงชื่อเข้า iCloud)

ความปลอดภัยของการส่งต่อสายโทรเซลลูลาร์ของ iPhone

เมื่อ Mac, iPad, iPod touch หรือ HomePod ของผู้ใช้อยู่บนเครือข่าย Wi-Fi เดียวกับ iPhone ของผู้ใช้ อุปกรณ์จะสามารถโทรออกและรับสายได้โดยใช้การเชื่อมต่อกับเซลลูลาร์บน iPhone การกำหนดค่าจำเป็นต้องให้อุปกรณ์ต่างๆ ลงชื่อเข้าทั้ง iCloud และ FaceTime โดยใช้บัญชี Apple ID เดียวกัน

เมื่อมีสายเรียกเข้า อุปกรณ์ที่กำหนดค่าไว้ทุกเครื่องจะได้รับการแจ้งเตือนโดยใช้บริการการแจ้งผลักข้อมูลของ Apple (APNs) โดยการแจ้งเตือนแต่ละรายการจะใช้การเข้ารหัสแบบต้นทางถึงปลายทางเหมือนกับ iMessage อุปกรณ์ที่อยู่บนเครือข่ายเดียวกันจะแสดงอินเทอร์เฟซผู้ใช้สำหรับการแจ้งเตือนสายเรียกเข้า เมื่อผู้ใช้รับสาย เสียงจะถูกส่งจาก iPhone ของผู้ใช้อย่างราบรื่นโดยใช้การเชื่อมต่อแบบเพียร์ทูเพียร์ที่ปลอดภัยระหว่างอุปกรณ์สองเครื่อง

เมื่อรับสายบนอุปกรณ์เครื่องหนึ่ง เสียงเรียกเข้าของอุปกรณ์ที่จับคู่ผ่าน iCloud ที่อยู่ใกล้เคียงจะหยุดลงโดยการประกาศสั้นๆ โดยใช้บลูทูธพลังงานต่ำ (BLE) ไบต์ของการประกาศจะถูกเข้ารหัสโดยใช้วิธีการเดียวกับการแจ้งของ Handoff

สายโทรออกจะส่งต่อไปที่ iPhone โดยใช้ APNs ด้วยเช่นกัน และเสียงจะถูกส่งผ่านลิงก์เพียร์ทูเพียร์ที่ปลอดภัยระหว่างอุปกรณ์ในลักษณะเดียวกัน ผู้ใช้สามารถปิดใช้งานการส่งต่อสายโทรบนอุปกรณ์ได้โดยการปิดใช้สายโทรเซลลูลาร์ iPhone ในการตั้งค่า FaceTime

ความปลอดภัยของการส่งต่อข้อความตัวอักษร iPhone

การส่งต่อข้อความจะส่งข้อความตัวอักษร SMS ที่ได้รับบน iPhone ไปยัง iPad, iPod touch หรือ Mac ที่ลงทะเบียนไว้ของผู้ใช้โดยอัตโนมัติ อุปกรณ์แต่ละเครื่องต้องลงชื่อเข้าบริการ iMessage โดยใช้บัญชี Apple ID เดียวกัน เมื่อเปิดใช้การส่งต่อข้อความ การลงทะเบียนจะเกิดขึ้นโดยอัตโนมัติบนอุปกรณ์ที่อยู่ภายในวงจรที่เชื่อถือได้ของผู้ใช้หากการตรวจสอบสิทธิ์สองปัจจัยเปิดใช้อยู่ ถ้าไม่เป็นเช่นนั้น การลงทะเบียนจะได้รับการตรวจสอบยืนยันบนอุปกรณ์แต่ละเครื่องโดยการป้อนรหัสตัวเลขแบบสุ่มหกหลักที่ iPhone สร้างขึ้น

หลังจากเชื่อมโยงอุปกรณ์แล้ว iPhone จะเข้ารหัสและส่งต่อข้อความตัวอักษร SMS ที่ได้รับไปยังอุปกรณ์แต่ละเครื่อง โดยใช้วิธีการที่อธิบายไว้ในภาพรวมความปลอดภัยของ iMessage การตอบกลับจะถูกส่งกลับไปยัง iPhone โดยใช้วิธีการเดียวกัน จากนั้น iPhone จะส่งการตอบกลับเป็นข้อความตัวอักษรโดยใช้กลไกการส่ง SMS ของผู้ให้บริการ ผู้ใช้สามารถเปิดใช้หรือปิดใช้การส่งต่อข้อความได้ในการตั้งค่าข้อความ

ความปลอดภัยของ Instant Hotspot

Instant Hotspot จะเชื่อมต่ออุปกรณ์ Apple เครื่องอื่นกับฮอตสปอตส่วนบุคคลของ iOS หรือ iPadOS โดยอุปกรณ์ iOS และ iPadOS ที่รองรับ Instant Hotspot จะใช้บลูทูธพลังงานต่ำ (BLE) เพื่อค้นหาและสื่อสารกับอุปกรณ์ทุกเครื่องที่ลงชื่อเข้าบัญชี iCloud เดียวกันแต่ละบัญชีหรือบัญชีที่ใช้กับการแชร์กันในครอบครัว (ใน iOS 13 และ iPadOS) คอมพิวเตอร์ Mac ที่ใช้งานร่วมกันได้ซึ่งใช้ OS X 10.10 ขึ้นไปจะใช้เทคโนโลยีเดียวกันเพื่อค้นหาและสื่อสารกับอุปกรณ์ iOS และ iPadOS ที่ใช้ Instant Hotspot

เมื่อผู้ใช้ป้อนการตั้งค่า Wi-Fi บนอุปกรณ์หนึ่งในครั้งแรก อุปกรณ์นั้นจะส่งการประกาศ BLE ที่มีข้อมูลจำเพาะที่อุปกรณ์ทุกเครื่องที่ลงชื่อเข้าบัญชี iCloud เดียวกันตกลงยอมรับ ข้อมูลจำเพาะนั้นสร้างจาก DSID (Destination Signaling Identifier) ที่ผูกอยู่กับบัญชี iCloud และจะสับเปลี่ยนเป็นระยะๆ เมื่ออุปกรณ์อื่นที่ลงชื่อเข้าบัญชี iCloud เดียวกันอยู่ในระยะใกล้และรองรับฮอตสปอตส่วนบุคคล โดยอุปกรณ์เหล่านั้นจะตรวจหาสัญญาณแล้วตอบสนองเพื่อบ่งบอกความพร้อมใช้งานเพื่อใช้ Instant Hotspot

เมื่อผู้ใช้ที่ไม่ได้เป็นส่วนหนึ่งของการแชร์กันในครอบครัวเลือก iPhone หรือ iPad สำหรับฮอตสปอตส่วนบุคคล จะมีการส่งคำขอให้เปิดใช้ฮอตสปอตส่วนบุคคลไปยังอุปกรณ์เครื่องนั้น คำขอจะถูกส่งผ่านลิงก์ที่เข้ารหัสโดยใช้การเข้ารหัส BLE และคำขอจะถูกเข้ารหัสในลักษณะคล้ายกับการเข้ารหัส iMessage จากนั้นอุปกรณ์จะตอบสนองต่อลิงก์ BLE เดียวกันโดยใช้การเข้ารหัสรายข้อความเดียวกันกับข้อมูลการเชื่อมต่อกับฮอตสปอตส่วนบุคคล

สำหรับผู้ใช้ที่เป็นส่วนหนึ่งของการแชร์กันในครอบครัว ข้อมูลการเชื่อมต่อกับฮอตสปอตส่วนบุคคลจะถูกแชร์อย่างปลอดภัยโดยใช้กลไกที่คล้ายกับที่ใช้โดยอุปกรณ์ HomeKit เพื่อเชื่อมข้อมูล การเชื่อมต่อที่แชร์ข้อมูลฮอตสปอตระหว่างผู้ใช้จะได้รับการรักษาความปลอดภัยโดยเฉพาะด้วยกุญแจชั่วคราว ECDH (Curve25519) ที่ถูกตรวจสอบสิทธิ์ด้วยกุญแจสาธารณะ Ed25519 เฉพาะอุปกรณ์ที่เกี่ยวข้องของผู้ใช้ กุญแจสาธารณะที่ใช้จะเป็นกุญแจที่เคยเชื่อมข้อมูลระหว่างสมาชิกของการแชร์กันในครอบครัวโดยใช้ IDS เมื่อมีการสร้างการแชร์กันในครอบครัว

ความปลอดภัยของเครือข่าย

ภาพรวมความปลอดภัยของเครือข่าย

นอกเหนือจากความปลอดภัยในตัวที่ Apple ใช้เพื่อปกป้องข้อมูลที่จัดเก็บในอุปกรณ์ Apple แล้ว ก็ยังมีอีกหลายมาตรการที่องค์กรสามารถใช้เพื่อรักษาข้อมูลให้ปลอดภัย เมื่อมีการส่งต่อข้อมูลไปมาในอุปกรณ์ได้ ความปลอดภัยและมาตรการเหล่านี้ทั้งหมดจะอยู่ภายใต้ความปลอดภัยของเครือข่าย

เนื่องจากผู้ใช้จะต้องสามารถเข้าถึงเครือข่ายองค์กรได้จากทุกแห่งในโลก ดังนั้นจึงเป็นเรื่องสำคัญที่ต้องช่วยทำให้แน่ใจว่าผู้ใช้ได้รับการอนุญาตและข้อมูลของผู้ใช้ได้รับการปกป้องระหว่างส่งข้อมูล ในการบรรลุวัตถุประสงค์ด้านความปลอดภัยเหล่านี้ iOS, iPadOS และ macOS ผสานเทคโนโลยีที่ได้รับการรับรองและมาตรฐานล่าสุดสำหรับการเชื่อมต่อเครือข่ายทั้ง Wi-Fi และข้อมูลเซลลูลาร์ นี่จึงเป็นเหตุผลที่ระบบปฏิบัติการของเราใช้โปรโตคอลเครือข่ายมาตรฐานสำหรับการติดต่อสื่อสารที่ได้รับการตรวจสอบสิทธิ์ ที่ได้รับอนุญาต และที่เข้ารหัส และมอบการเข้าถึงแบบเดียวกันนี้ให้กับนักพัฒนาด้วย

ความปลอดภัยของ TLS

iOS, iPadOS และ macOS รองรับความปลอดภัยชั้นขนส่ง (TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3) และความปลอดภัยชั้นขนส่งดาต้าแกรม (DTLS) โปรโตคอล TLS รองรับทั้ง AES128 และ AES256 และเหมาะกับกระบวนการรักษาความปลอดภัยในอนาคต แอปอินเทอร์เน็ตต่างๆ เช่น Safari, ปฏิทิน และเมล จะใช้โปรโตคอลนี้โดยอัตโนมัติเพื่อเปิดใช้งานช่องทางการสื่อสารระหว่างอุปกรณ์และบริการเครือข่าย API ระดับสูง (เช่น CFNetwork) ทำให้นักพัฒนาใช้งาน TLS ในแอปของตนได้อย่างง่ายดาย ในขณะที่ API ระดับต่ำ (เช่น Network.framework) ให้การควบคุมในระดับที่ละเอียด CFNetwork จะไม่อนุญาต SSL 3 และแอปที่ใช้งาน WebKit (เช่น Safari) จะถูกห้ามสร้างการเชื่อมต่อ SSL 3

ใน iOS 11 ขึ้นไป และ macOS 10.13 ขึ้นไป ใบรับรอง SHA-1 จะไม่ได้รับอนุญาตสำหรับการเชื่อมต่อ TLS อีกต่อไปยกเว้นว่าจะเชื่อถือแล้วจากผู้ใช้ ใบอนุญาตที่มีกุญแจ RSA ที่สั้นกว่า 2048 บิตก็จะไม่ได้รับอนุญาตอีกด้วย ชุดรหัสสมมาตร RC4 เลิกใช้แล้วใน iOS 10 และ macOS 10.12 ตามค่าเริ่มต้น ไคลเอ็นต์หรือเซิร์ฟเวอร์ TLS ที่ปรับใช้กับ API การส่งข้อมูลที่ปลอดภัยจะไม่เปิดใช้งานชุดรหัส RC4 และไม่สามารถเชื่อมต่อเมื่อ RC4 เป็นชุดรหัสเพียงชุดเดียวที่พร้อมใช้งานได้เท่านั้น ในการทำให้ปลอดภัยยิ่งขึ้น ควรอัปเกรดบริการหรือแอปที่ต้องใช้ RC4 เพื่อให้ใช้งานชุดรหัสที่ปลอดภัยได้ ใน iOS 12.1 ใบรับรองที่ออกหลังวันที่ 15 ตุลาคม 2018 จากใบรับรองรากที่ระบบเชื่อถือแล้วจะต้องมีการเก็บบันทึกการใช้งานไว้ในบันทึกการใช้งานความโปร่งใสของใบรับรองที่เชื่อถือได้เพื่อให้ได้รับอนุญาตสำหรับการเชื่อมต่อกับ TLS ใน iOS 12.2 ระบบจะเปิดใช้งาน TLS 1.3 ตามค่าเริ่มต้นสำหรับ API ที่ชื่อ Network.framework และ NSURLSession ไคลเอ็นต์ TLS ที่ใช้ API การส่งข้อมูลที่ปลอดภัยไม่สามารถใช้ TLS 1.3

ความปลอดภัยของการส่งข้อมูลแอป

ความปลอดภัยของการส่งข้อมูลแอประบุข้อกำหนดการเชื่อมต่อตามค่าเริ่มต้นเพื่อให้แอปปฏิบัติตามแนวปฏิบัติเพื่อให้เชื่อมต่อได้อย่างปลอดภัยที่สุดเมื่อใช้งาน API ที่ชื่อ NSURLConnection, CFURL หรือ NSURLSession ตามค่าเริ่มต้น ความปลอดภัยของการส่งข้อมูลแอปจำกัดการเลือกรหัสที่จะรวมอยู่ในชุดที่มีกระบวนการรักษาความปลอดภัยในอนาคตเท่านั้น โดยเฉพาะ:

- ECDHE_ECDSA_AES และ ECDHE_RSA_AES ใน Galois/Counter Mode (GCM)
- โหมด Cipher Block Chaining (CBC)

แอปสามารถปิดใช้งานข้อกำหนดกระบวนการรักษาความปลอดภัยในอนาคตต่อโดเมนได้ ในกรณีเพิ่ม RSA_AES ในชุดรหัสที่พร้อมใช้งาน

เซิร์ฟเวอร์จะต้องรองรับ TLS 1.2 รวมทั้งกระบวนการรักษาความปลอดภัยในอนาคต และใบรับรองจะต้องถูกต้องและลงชื่อโดยใช้ SHA256 ขึ้นไป โดยมีกุญแจ RSA 2048 บิต หรือกุญแจเส้นโค้งรูปไข่ 256 บิตเป็นอย่างต่ำ

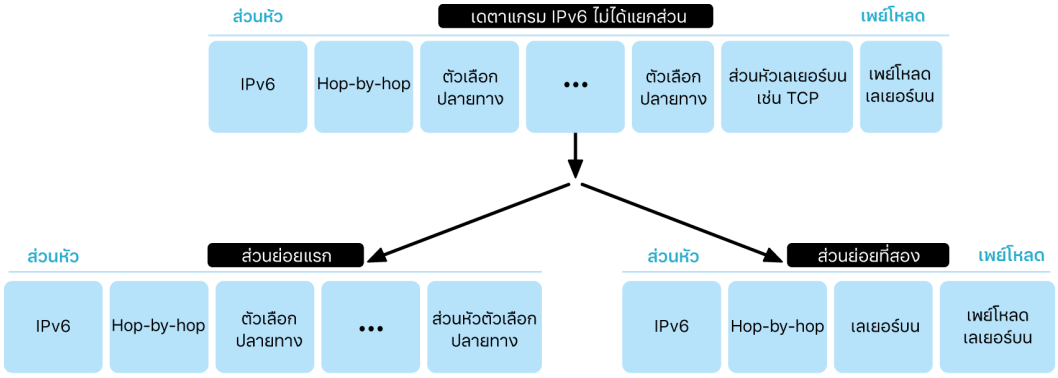
การเชื่อมต่อเครือข่ายที่ไม่ตรงตามข้อกำหนดเหล่านี้จะดำเนินการไม่สำเร็จ นอกเสียจากแอปนั้นจะแทนที่ความปลอดภัยของการส่งข้อมูลแอป ใบรับรองที่ไม่ถูกต้องจะทำให้เกิดความล้มเหลวและไม่มีการเชื่อมต่อ ความปลอดภัยของการส่งข้อมูลแอปจะปรับใช้โดยอัตโนมัติกับแอปทั้งหมดที่คอมไพล์มาสำหรับ iOS 9 ขึ้นไปและ macOS 10.11 ขึ้นไป

การตรวจสอบความถูกต้องของใบรับรอง

การประเมินสถานะที่เชื่อถือแล้วของใบรับรอง TLS จะดำเนินการโดยสอดคล้องกับมาตรฐานอุตสาหกรรมที่สร้างขึ้น ดังที่เริ่มต้นไว้ใน RFC 5280 และมาตรฐานรวมที่เกิดขึ้นใหม่ เช่น RFC 6962 (ความโปร่งใสของใบรับรอง) ใน iOS 11 ขึ้นไปและ macOS 10.13 ขึ้นไป อุปกรณ์ Apple จะอัปเดตรายการปัจจุบันของใบรับรองที่ถูกเพิกถอนและถูกจำกัดเป็นระยะๆ รายการนี้รวบรวมจากรายการการเพิกถอนใบรับรอง (CRL) ที่เผยแพร่โดยผู้ให้บริการออกใบรับรองลำดับชั้นบนสุดแบบในตัวที่ Apple เชื่อถือแล้วแต่ละราย รวมถึงโดยผู้ออกใบรับรอง CA ลำดับชั้นถัดลงมาด้วย รายการดังกล่าวอาจรวมถึงการจำกัดอื่นๆ โดยขึ้นอยู่กับดุลพินิจของ Apple ข้อมูลนี้จะใช้พิจารณาทุกครั้งที่มีการใช้ฟังก์ชั่นเครือข่าย API เพื่อทำการเชื่อมต่อที่ปลอดภัย ถ้ามีใบรับรองที่ถูกเพิกถอนจาก CA มากเกินกว่าที่จะแสดงแต่ละรายการได้ การประเมินความน่าเชื่อถืออาจจำเป็นต้องใช้การตอบสนองสถานะใบรับรองออนไลน์ (OCSP) แทน และถ้าไม่มีการตอบสนอง การประเมินความน่าเชื่อถือจะดำเนินการไม่สำเร็จ

ความปลอดภัยของ IPv6

ระบบปฏิบัติการทั้งหมดของ Apple รองรับ IPv6 โดยจะใช้งานกลไกจำนวนมากเพื่อปกป้องความเป็นส่วนตัวของผู้ใช้และความเสถียรของสแต็คเครือข่าย เมื่อใช้การกำหนดค่าที่อยู่ด้วยตัวเองอัตโนมัติ (SLAAC) ที่อยู่ IPv6 ของอินเทอร์เฟซทั้งหมดจะถูกสร้างขึ้นในลักษณะที่ช่วยป้องกันการติดตามข้ามไซต์ของอุปกรณ์บนเครือข่ายและในขณะเดียวกันก็ช่วยให้มีประสบการณ์ของผู้ใช้ที่ดีโดยการรับรองความเสถียรของที่อยู่เมื่อไม่มีการเปลี่ยนเครือข่ายเกิดขึ้น อัลกอริทึมการสร้างที่อยู่จะขึ้นอยู่กับที่อยู่ที่สร้างขึ้นโดยมีการเข้ารหัสของ RFC 3972 ซึ่งได้รับการปรับปรุงโดยตัวแก้ไขเฉพาะอินเทอร์เฟซเพื่อรับประกันว่าแม้กระทั่งอินเทอร์เฟซที่แตกต่างกันที่อยู่บนเครือข่ายเดียวกันจะมีที่อยู่ที่ต่างกันในท้ายที่สุด นอกจากนี้ ระบบจะสร้างที่อยู่ชั่วคราวที่มีอายุใช้งานที่ต้องการ 24 ชั่วโมงและจะใช้ที่อยู่นี้สำหรับการเชื่อมต่อใหม่ตามค่าเริ่มต้น เพื่อให้สอดคล้องกับคุณสมบัติที่อยู่ Wi-Fi แบบส่วนตัวที่นำมาใช้ใน iOS 14, iPadOS 14 และ watchOS 7 จะมีการสร้างที่อยู่ลิงก์ที่ไม่ซ้ำกันซึ่งอยู่ภายในสำหรับทุกเครือข่าย Wi-Fi ที่อุปกรณ์เข้าร่วมเครือข่าย จากนั้น SSID ของเครือข่ายจะถูกรวมเป็นองค์ประกอบเพิ่มเติมสำหรับการสร้างที่อยู่ซึ่งคล้ายกันกับพารามิเตอร์ Network_ID ของ RFC 7217 วิธีนี้ถูกใช้ใน iOS 14, iPadOS 14 และ watchOS 7 ในการปกป้องจากการโจมตีบนพื้นฐานของเฮดเดอร์และส่วนย่อยของส่วนขยาย IPv6 อุปกรณ์ Apple จะใช้มาตรการปกป้องที่ระบุใน RFC 6980, RFC 7112 และ RFC 8021 ต่างจากมาตรการอื่นๆ มาตรการเหล่านี้จะยับยั้งการโจมตีที่ส่วนหัวชั้นบนซึ่งจะพบได้เฉพาะในส่วนย่อยลำดับที่สอง (ดังที่แสดงด้านล่าง) ซึ่งอาจก่อให้เกิดความคลุมเครือของการควบคุมความปลอดภัย เช่น ฟิลเตอร์แพ็คเกตแบบสเตทเลส



นอกจากนี้ ในการช่วยให้การรับรองความน่าเชื่อถือของสแต็ค IPv6 ของระบบปฏิบัติการ Apple อุปกรณ์ของ Apple ยังบังคับใช้การจำกัดที่หลากหลายบนโครงสร้างข้อมูลที่เกี่ยวข้องกับ IPv6 เช่น คำนำหน้ารายอินเทอร์เฟซจำนวนมาก

ความปลอดภัยของเครือข่ายส่วนตัวเสมือน (VPN)

บริการเครือข่ายที่ปลอดภัยเช่นเครือข่ายส่วนตัวเสมือนโดยทั่วไปจะต้องใช้การตั้งค่าและกำหนดค่าขั้นต่ำเพื่อให้ทำงานได้กับอุปกรณ์ iOS, iPadOS และ macOS

โปรโตคอลที่รองรับ

อุปกรณ์เหล่านี้ทำงานได้กับเซิร์ฟเวอร์ VPN ที่รองรับโปรโตคอลและวิธีการตรวจสอบสิทธิ์ต่อไปนี้:

- IKEv2/IPsec ที่มีการตรวจสอบสิทธิ์โดยความลับที่แชร์, ใบรับรอง RSA, ใบรับรองอัลกอริทึมลายเซ็นดิจิตอลแบบเส้นโค้งรูปไข่ (ECDSA), EAP-MSCHAPv2 หรือ EAP-TLS
- SSL-VPN ที่ใช้แอปไคลเอ็นต์ที่เหมาะสมจาก App Store
- L2TP/IPsec ที่มีการตรวจสอบสิทธิ์ของผู้ใช้โดยรหัสผ่าน MS-CHAPV2 และการตรวจสอบสิทธิ์เครื่องโดยความลับที่แชร์ (iOS, iPadOS และ macOS) และ RSA SecurID หรือ CRYPTOCard (macOS เท่านั้น)
- Cisco IPsec ที่มีการตรวจสอบสิทธิ์ของผู้ใช้โดยรหัสผ่าน RSA SecurID หรือ CRYPTOCard และการตรวจสอบสิทธิ์เครื่องโดยความลับและใบรับรองที่แชร์ (macOS เท่านั้น)

การปรับใช้ VPN ที่รองรับ

iOS, iPadOS และ macOS รองรับรายการต่อไปนี้:

- **VPN ตามคำสั่ง:** สำหรับเครือข่ายที่ใช้การตรวจสอบสิทธิ์โดยใบรับรอง นโยบาย IT ระบุว่าโดเมนใดที่ต้องเชื่อมต่อกับ VPN โดยใช้โปรไฟล์การกำหนดค่า VPN
- **VPN สำหรับแต่ละแอป:** สำหรับทำให้การเชื่อมต่อ VPN ง่ายขึ้นและใช้งานได้ละเอียดยิ่งขึ้น โซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) สามารถระบุการเชื่อมต่อสำหรับแอปที่ได้รับการจัดการแต่ละแอป และโดเมนเฉพาะรายการใน Safari ได้ สิ่งนี้ช่วยรับรองว่าข้อมูลที่ปลอดภัยจะส่งไปยังและส่งจากเครือข่ายองค์กรเสมอ และข้อมูลส่วนตัวของผู้ใช้จะไม่ถูกส่งไป

iOS และ iPadOS รองรับรายการต่อไปนี้:

- **VPN แบบเปิดตลอดเวลา:** สำหรับอุปกรณ์ที่จัดการผ่านโซลูชั่น MDM และควบคุมดูแลโดยใช้ Apple Configurator สำหรับ Mac, Apple School Manager หรือ Apple Business Manager VPN แบบเปิดตลอดเวลาจะช่วยให้ผู้ใช้ไม่ต้องเปิดใช้ VPN เพื่อเปิดใช้การปกป้องเมื่อเชื่อมต่อกับเครือข่ายเซลลูลาร์และเครือข่าย Wi-Fi นอกจากนี้ยังช่วยให้องค์กรควบคุมการรับส่งข้อมูลของอุปกรณ์ได้อย่างสมบูรณ์โดยเชื่อมต่อการรับส่งข้อมูล IP ทั้งหมดกลับไปยังองค์กร การแลกเปลี่ยนเริ่มต้นของพารามิเตอร์และกุญแจสำหรับการเข้ารหัสในภายหลัง IKEv2 จะรักษาความปลอดภัยของการส่งข้อมูลด้วยการเข้ารหัสข้อมูล องค์กรสามารถตรวจสอบและกรองการส่งข้อมูลไปยังและจากอุปกรณ์ รักษาความปลอดภัยของข้อมูลภายในเครือข่าย และจำกัดการเข้าใช้งานอินเทอร์เน็ตของอุปกรณ์ได้

ความปลอดภัยของ Wi-Fi

การเข้าถึงเครือข่ายไร้สายอย่างปลอดภัย

แพลตฟอร์ม Apple ทั้งหมดรองรับการตรวจสอบสิทธิ์ Wi-Fi และโปรโตคอลการเข้ารหัสมาตรฐานอุตสาหกรรมเพื่อให้การเข้าถึงที่มีการตรวจสอบสิทธิ์และการรักษาความลับเมื่อเชื่อมต่อกับเครือข่ายไร้สายที่ปลอดภัยดังต่อไปนี้:

- WPA2 Personal
- WPA2 Enterprise
- WPA2/WPA3 Transitional
- WPA3 Personal
- WPA3 Enterprise
- WPA3 Enterprise ที่มีความปลอดภัย 192 บิต

WPA2 และ WPA3 ตรวจสอบสิทธิ์การเชื่อมต่อแต่ละครั้ง และมอบการเข้ารหัส AES แบบ 128 บิตเพื่อช่วยทำให้แน่ใจว่าข้อมูลที่ส่งผ่านทางอากาศจะเป็นความลับ ซึ่งให้ระดับการรับรองสูงสุดกับผู้ใช้ว่าข้อมูลจะได้รับการปกป้องเมื่อผู้ใช้ส่งและรับการสื่อสารผ่านการเชื่อมต่อกับเครือข่าย Wi-Fi

การรองรับ WPA3

WPA3 รองรับบนอุปกรณ์ Apple ต่อไปนี้:

- iPhone 7 ขึ้นไป
- iPad รุ่นที่ 5 ขึ้นไป
- Apple TV 4K ขึ้นไป
- Apple Watch Series 3 ขึ้นไป
- คอมพิวเตอร์ Mac (ปลายปี 2013 ขึ้นไป ที่มี 802.11ac ขึ้นไป)

อุปกรณ์ที่ใหม่กว่ารองรับการตรวจสอบสิทธิ์ด้วย WPA3 Enterprise ที่มีความปลอดภัย 192 บิต รวมถึงรองรับการเข้ารหัส AES แบบ 256 บิตเมื่อเชื่อมต่อกับจุดเชื่อมต่อ (APs) แบบไร้สายที่ใช้งานร่วมกันได้ ซึ่งจะมอบการปกป้องความลับที่แข็งแกร่งยิ่งขึ้นสำหรับการส่งข้อมูลที่ส่งผ่านทางอากาศ WPA3 Enterprise ที่มีความปลอดภัย 192 บิตรองรับบน iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max และอุปกรณ์ iOS และ iPadOS รุ่นต่อไป

การรองรับ PMF

นอกจากการปกป้องข้อมูลที่ส่งผ่านทางอากาศแล้ว แพลตฟอร์ม Apple ยังขยายระดับการปกป้อง WPA2 และ WPA3 เป็นกรอบการจัดการยูนิคาสต์และมัลติคาสต์ผ่านบริการกรอบการจัดการที่ปกป้อง (PMF) ซึ่งอ้างอิงใน 802.11w การรองรับ PMF จะมีให้ใช้งานบนอุปกรณ์ Apple ต่อไปนี้:

- iPhone 6 ขึ้นไป
- iPad Air 2 ขึ้นไป
- Apple TV HD ขึ้นไป
- Apple Watch Series 3 ขึ้นไป
- คอมพิวเตอร์ Mac (ปลายปี 2013 ขึ้นไป ที่มี 802.11ac ขึ้นไป)

ด้วยการรองรับ 802.1X อุปกรณ์ Apple สามารถผสานเข้าด้วยกันกับสภาพแวดล้อมการตรวจสอบสิทธิ์ RADIUS ที่กว้างขวางได้ วิธีการตรวจสอบสิทธิ์ไร้สาย 802.1X ที่รองรับจะรวมถึง EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0 และ PEAPv1

การปกป้องแพลตฟอร์ม

ระบบปฏิบัติการของ Apple ปกป้องอุปกรณ์จากช่องโหว่ในเฟิร์มแวร์ของหน่วยประมวลผลเครือข่าย ซึ่งหมายความว่าตัวควบคุมเครือข่ายที่มี Wi-Fi สามารถเข้าถึงหน่วยความจำของหน่วยประมวลผลแอปพลิเคชันได้อย่างจำกัด

- เมื่อ USB หรือ SDIO (Secure Digital Input Output) ถูกใช้เป็นอินเทอร์เฟซกับหน่วยประมวลผลของเครือข่าย หน่วยประมวลผลของเครือข่ายจะไม่สามารถเริ่มต้นธุรกรรมการเข้าถึงหน่วยความจำโดยตรง (DMA) ไปยังหน่วยประมวลผลแอปพลิเคชันได้
- เมื่อใช้ PCIe หน่วยประมวลผลเครือข่ายแต่ละรายการจะจำกัดอยู่ที่บัส PCIe ตัวเอง หน่วยการจัดการหน่วยความจำข้อมูลเข้า/ข้อมูลออก (IOMMU) บนบัส PCIe แต่ละรายการจะจำกัดการเข้าถึง DMA ของหน่วยประมวลผลเครือข่ายมากขึ้น โดยจำกัดไปที่หน่วยความจำและทรัพยากรที่ประกอบด้วยแพ็คเกตเครือข่ายและโครงสร้างการควบคุมเท่านั้น

โปรโตคอลที่เลิกใช้แล้ว

ผลิตภัณฑ์ของ Apple รองรับการตรวจสอบสิทธิ์ Wi-Fi และการเข้ารหัสที่เลิกใช้แล้วต่อไปนี้:

- WEP Open ที่มีทั้งกุญแจ 40 บิตและกุญแจ 104 บิต
- WEP Shared ที่มีทั้งกุญแจ 40 บิตและกุญแจ 104 บิต
- Dynamic WEP
- โปรโตคอลความสมบูรณ์ของกุญแจชั่วคราว (TKIP)
- WPA
- WPA/WPA2 Transitional

โปรโตคอลเหล่านี้ไม่ถือว่าปลอดภัยอีกต่อไป และการใช้งานของโปรโตคอลก็ไม่ได้รับการสนับสนุนเป็นอย่างมาก เนื่องจากเหตุผลด้านความเข้ากันได้ ความเชื่อถือได้ ประสิทธิภาพการทำงาน และความปลอดภัย โปรโตคอลเหล่านี้ถูกรองรับเพื่อจุดประสงค์ความเข้ากันได้แบบย้อนกลับเท่านั้น และอาจเอาออกในเวอร์ชั่นของซอฟต์แวร์ในอนาคต

ขอแนะนำให้โยกย้ายการใช้ Wi-Fi ไปยัง WPA3 Personal หรือ WPA3 Enterprise เพื่อให้มีการเชื่อมต่อ Wi-Fi ที่สมบูรณ์ ปลอดภัย และใช้งานร่วมกันได้มากที่สุดที่เป็นไปได้

ความเป็นส่วนตัวของ Wi-Fi

การสุ่มที่อยู่ MAC

แพลตฟอร์ม Apple ใช้ที่อยู่การควบคุมการเข้าถึงสื่อ (ที่อยู่ MAC) แบบสุ่มเมื่อสแกน Wi-Fi ในขณะที่ไม่ได้เชื่อมโยงกับเครือข่าย Wi-Fi การสแกนเหล่านี้สามารถดำเนินการเพื่อค้นหาและเชื่อมต่อกับเครือข่าย Wi-Fi ที่รู้จัก หรือเพื่อช่วยเหลือบริการหาตำแหน่งที่ตั้งสำหรับแอปที่ใช้กรอบภูมิศาสตร์ได้ เช่น การเตือนความจำที่อิงตามตำแหน่งที่ตั้งหรือการแก้ไขตำแหน่งที่ตั้งในแอปแผนที่ของ Apple โปรดทราบว่าการสแกน Wi-Fi ที่เกิดขึ้นในขณะที่พยายามเชื่อมต่อกับเครือข่าย Wi-Fi ที่ต้องการนั้นไม่ได้เป็นแบบสุ่ม มีการรองรับการสุ่มที่อยู่ MAC ของ Wi-Fi บน iPhone 5 ขึ้นไป

แพลตฟอร์ม Apple ใช้ที่อยู่ MAC แบบสุ่มเมื่อสแกน Preferred Network Offload ที่มีการปรับปรุง (ePNO) เมื่ออุปกรณ์ไม่ได้เชื่อมโยงกับเครือข่าย Wi-Fi หรือหน่วยประมวลผลอยู่ระหว่างการพัก การสแกน ePNO จะทำงานเมื่ออุปกรณ์ใช้บริการหาตำแหน่งที่ตั้งสำหรับแอปที่ใช้กรอบภูมิศาสตร์ เช่น การเตือนความจำที่อิงตามตำแหน่งที่ตั้ง ที่ระบุว่าอุปกรณ์อยู่ใกล้ตำแหน่งที่ตั้งเฉพาะหรือไม่

เนื่องจากที่อยู่ MAC ของอุปกรณ์จะเปลี่ยนเมื่อเลิกเชื่อมต่อกับเครือข่าย Wi-Fi ที่อยู่นี้จึงไม่สามารถใช้เพื่อติดตามอุปกรณ์อย่างต่อเนื่องโดยผู้ติดตามการส่งข้อมูล Wi-Fi แบบเชิงรับ แม้ว่าอุปกรณ์จะเชื่อมต่อกับเครือข่ายเซลลูลาร์อยู่ก็ตาม Apple แจ้งให้ผู้ผลิต Wi-Fi ทราบว่าการสแกน Wi-Fi ของ iOS และ iPadOS ใช้ที่อยู่ MAC แบบสุ่ม และทั้ง Apple หรือผู้ผลิตไม่สามารถทำนายที่อยู่ MAC แบบสุ่มเหล่านี้ได้

สำหรับ iOS 14 ขึ้นไป, iPadOS 14 ขึ้นไป และ watchOS 7 ขึ้นไป เมื่อ iPhone, iPad, iPod touch หรือ Apple Watch เชื่อมต่อกับเครือข่าย Wi-Fi อุปกรณ์จะระบุตัวเองด้วยที่อยู่ MAC ที่ไม่ซ้ำกัน (แบบสุ่ม) ต่อหนึ่งเครือข่าย คุณสมบัตินี้สามารถปิดใช้งานได้โดยผู้ใช้หรือโดยใช้ตัวเลือกใหม่ในเพย์โหลด Wi-Fi ในบางสถานการณ์อุปกรณ์จะย้อนกลับไปเป็นที่อยู่ MAC จริง

โปรดดูบทความบริการช่วยเหลือของ Apple ใช้ที่อยู่ Wi-Fi แบบส่วนตัวบน iPhone, iPad, iPod touch และ Apple Watch สำหรับข้อมูลเพิ่มเติม

การสุ่มหมายเลขลำดับเฟรม Wi-Fi

เฟรม Wi-Fi มีหมายเลขลำดับที่จะใช้โดยโปรโตคอล 802.11 ระดับต่ำเพื่อเปิดใช้งานการสื่อสาร Wi-Fi ที่มีประสิทธิภาพและเชื่อถือได้ เนื่องจากหมายเลขลำดับเหล่านี้เพิ่มขึ้นในแต่ละเฟรมที่ส่ง หมายเลขลำดับอาจถูกใช้เพื่อให้สัมพันธ์กับข้อมูลที่ส่งระหว่างการสแกน Wi-Fi พร้อมกับเฟรมอื่นๆ ที่ส่งโดยอุปกรณ์เดียวกัน

ในการป้องกันสิ่งนี้ อุปกรณ์ Apple จะสุ่มหมายเลขลำดับเมื่อใดก็ตามที่ที่อยู่ MAC เปลี่ยนไปยังที่อยู่แบบสุ่มใหม่ ซึ่งรวมถึงการสุ่มหมายเลขลำดับสำหรับการร้องขอการสแกนแต่ละครั้งที่เริ่มต้นขึ้นเมื่ออุปกรณ์ไม่ได้เชื่อมโยงอยู่ การสุ่มนี้รองรับบนอุปกรณ์ต่อไปนี้:

- iPhone 7 ขึ้นไป
- iPad รุ่นที่ 5 ขึ้นไป
- Apple TV 4K ขึ้นไป
- Apple Watch Series 3 ขึ้นไป
- iMac Pro (Retina 5K 27 นิ้ว ปี 2017) ขึ้นไป
- MacBook Pro (13 นิ้ว ปี 2018) ขึ้นไป
- MacBook Pro (15 นิ้ว ปี 2018) ขึ้นไป
- MacBook Air (Retina 13 นิ้ว ปี 2018) ขึ้นไป
- Mac mini (ปี 2018) ขึ้นไป
- iMac (Retina 4K 21.5 นิ้ว ปี 2019) ขึ้นไป
- iMac (Retina 5K 27 นิ้ว ปี 2019) ขึ้นไป
- Mac Pro (ปี 2019) ขึ้นไป

การเชื่อมต่อกับ Wi-Fi

Apple จะสร้างที่อยู่ MAC แบบสุ่มสำหรับการเชื่อมต่อ Wi-Fi แบบเพียร์ทูเพียร์ ที่ใช้สำหรับ AirDrop และ AirPlay ที่อยู่แบบสุ่มยังใช้สำหรับฮอตสปอตส่วนบุคคลใน iOS และ iPadOS (ที่มีซิมการ์ด) และการแชร์อินเทอร์เน็ตใน macOS อีกด้วย

ที่อยู่แบบสุ่มใหม่ถูกสร้างเมื่อใดก็ตามที่อินเทอร์เฟซเครือข่ายเริ่มต้นขึ้น และที่อยู่เฉพาะจะถูกสร้างขึ้นสำหรับแต่ละอินเทอร์เฟซตามความจำเป็นโดยเป็นอิสระจากกัน

เครือข่ายที่ซ่อนอยู่

เครือข่าย Wi-Fi จะถูกระบุโดยชื่อเครือข่ายของตัวเอง เป็นที่รู้จักกันว่าคือ**ชื่อเครือข่าย (SSID)** เครือข่าย Wi-Fi บางเครือข่ายถูกกำหนดค่าให้ซ่อน SSID ซึ่งส่งผลให้จุดเชื่อมต่อแบบไร้สายไม่แสดงชื่อของเครือข่าย เครือข่ายเหล่านี้เรียกว่า**เครือข่ายที่ซ่อนอยู่** iPhone 6s ขึ้นไป อุปกรณ์จะตรวจจับโดยอัตโนมัติเมื่อเครือข่ายซ่อนอยู่ ถ้าเครือข่ายไม่ได้ซ่อนอยู่ อุปกรณ์ iOS หรือ iPadOS จะส่งการตรวจสอบที่มี SSID รวมอยู่ในคำขอ แต่หากไม่ได้ซ่อน ก็จะไม่ส่ง การกำหนดค่านี้จะช่วยป้องกันไม่ให้อุปกรณ์แสดงชื่อของเครือข่ายที่ซ่อนอยู่ก่อนหน้านี้ซึ่งผู้ใช้เคยเชื่อมต่อไว้ ส่งผลให้มั่นใจในความเป็นส่วนตัวได้มากยิ่งขึ้น

ความปลอดภัยของบลูทูธ

มีบลูทูธสองประเภทในอุปกรณ์ Apple คือบลูทูธแบบคลาสสิกและบลูทูธพลังงานต่ำ (BLE) โมเดลความปลอดภัยของบลูทูธสำหรับทั้งสองเวอร์ชั่นรวมถึงคุณสมบัติเด่นด้านความปลอดภัยต่อไปนี้:

- **การจับคู่:** กระบวนการสำหรับการสร้างกุญแจความลับที่แชร์อย่างน้อยหนึ่งดอก
- **การเชื่อมต่อ:** การกระทำของการจัดเก็บกุญแจที่สร้างระหว่างการจับคู่เพื่อใช้ในการเชื่อมต่อที่เกิดขึ้นในภายหลังเพื่อสร้างคู่อุปกรณ์ที่เชื่อถือแล้ว
- **การตรวจสอบสิทธิ์:** การตรวจสอบยืนยันว่าอุปกรณ์สองอุปกรณ์มีกุญแจเดียวกัน
- **การเข้ารหัส:** การรักษาความลับข้อความ
- **ความสมบูรณ์ของข้อความ:** การป้องกันการปลอมข้อความ
- **การจับคู่แบบง่ายที่ปลอดภัย:** การป้องกันการแอบฟังเชิงรับและการป้องกันการโจมตีแบบแทรกกลางการสื่อสาร

บลูทูธเวอร์ชั่น 4.1 เพิ่มคุณสมบัติการเชื่อมต่อที่ปลอดภัยไปยังการส่งข้อมูลทางกายภาพของบลูทูธแบบคลาสสิก (BR/EDR)

คุณสมบัติด้านความปลอดภัยสำหรับบลูทูธแต่ละประเภทแสดงในรายการด้านล่าง

รองรับ	บลูทูธแบบคลาสสิก	บลูทูธพลังงานต่ำ
การจับคู่	เส้นโค้งรูปไข่ P-256	อัลกอริทึมที่ได้รับการอนุญาตจาก FIPS (AES-CMAC และเส้นโค้งรูปไข่ P-256)
การเชื่อมต่อ	ข้อมูลการจับคู่ที่จัดเก็บในตำแหน่งที่ปลอดภัยในอุปกรณ์ iOS, iPadOS, macOS, tvOS และ watchOS	ข้อมูลการจับคู่ที่จัดเก็บในตำแหน่งที่ปลอดภัยในอุปกรณ์ iOS, iPadOS, macOS, tvOS และ watchOS
การตรวจสอบสิทธิ์	อัลกอริทึมที่ได้รับการอนุญาตจาก FIPS (HMAC-SHA256 และ AES-CTR)	อัลกอริทึมที่ได้รับการอนุญาตจาก FIPS
การเข้ารหัส	การเข้ารหัส AES-CCM, ดำเนินการในตัวควบคุม	การเข้ารหัส AES-CCM, ดำเนินการในตัวควบคุม
ความสมบูรณ์ของข้อความ	AES-CCM, ใช้สำหรับความสมบูรณ์ของข้อความ	AES-CCM, ใช้สำหรับความสมบูรณ์ของข้อความ

รองรับ	บลูทูธแบบคลาสสิก	บลูทูธพลังงานต่ำ
การจับคู่แบบง่ายที่ปลอดภัย: การป้องกันการแอบฟังเชิงรับ	Elliptic Curve Diffie-Hellman Exchange Ephemeral (ECDHE)	Elliptic Curve Diffie-Hellman Exchange (ECDHE)
การจับคู่แบบง่ายที่ปลอดภัย: การป้องกันการโจมตีแบบแทรกกลางการสื่อสาร (MITM)	วิธีการเชิงตัวเลขที่ช่วยเหลือผู้ใช้สองวิธี: การเปรียบเทียบตัวเลขหรือการป้อน Passkey	วิธีการเชิงตัวเลขที่ช่วยเหลือผู้ใช้สองวิธี: การเปรียบเทียบตัวเลขหรือการป้อน Passkey การจับคู่ต้องใช้การตอบสนองจากผู้ใช้ ซึ่งรวมถึงโหมดการจับคู่ที่ไม่ใช่ MITM ทั้งหมด
Bluetooth 4.1 ขึ้นไป	iMac ปลายปี 2015 ขึ้นไป MacBook Pro ต้นปี 2015 ขึ้นไป	iOS 9 ขึ้นไป iPadOS 13.1 ขึ้นไป macOS 10.12 ขึ้นไป tvOS 9 ขึ้นไป watchOS 2.0 ขึ้นไป
Bluetooth 4.2 ขึ้นไป	iPhone 6 ขึ้นไป	iOS 9 ขึ้นไป iPadOS 13.1 ขึ้นไป macOS 10.12 ขึ้นไป tvOS 9 ขึ้นไป watchOS 2.0 ขึ้นไป

ความเป็นส่วนตัวของบลูทูธพลังงานต่ำ

ในการช่วยรักษาความปลอดภัยความเป็นส่วนตัวของผู้ใช้ BLE มีคุณสมบัติสองประการต่อไปนี้ ได้แก่ การสุ่มที่อยู่และการรับกุญแจแบบส่งข้าม

การสุ่มที่อยู่คือคุณสมบัติที่ลดความสามารถในการติดตามอุปกรณ์ BLE ในระยะเวลาหนึ่ง โดยการเปลี่ยนที่อยู่อุปกรณ์บลูทูธเป็นประจำ สำหรับอุปกรณ์ที่ใช้คุณสมบัติด้านความเป็นส่วนตัวในการเชื่อมต่อกับอุปกรณ์ที่รู้จักอีกครั้ง ที่อยู่ของอุปกรณ์ หรือที่เรียกว่า**ที่อยู่ส่วนตัว** จะต้องแก้ปัญหาโดยอุปกรณ์อื่นๆ ได้ ที่อยู่ส่วนตัวจะสร้างโดยใช้กุญแจการแก้ไขข้อมูลประจำตัวของอุปกรณ์ที่แลกเปลี่ยนระหว่างกระบวนการการจับคู่

iOS 13 ขึ้นไปและ iPadOS 13.1 ขึ้นไปมีความสามารถในการรับกุญแจลิงก์ข้ามการขนส่ง ซึ่งเป็นคุณสมบัติที่รู้จักกันในชื่อ**การรับกุญแจแบบส่งข้าม** ตัวอย่างเช่น กุญแจลิงก์ที่สร้างด้วย BLE สามารถใช้เพื่อรับกุญแจลิงก์บลูทูธแบบคลาสสิกได้ นอกจากนี้ Apple ยังเพิ่มการรองรับบลูทูธแบบคลาสสิกเป็น BLE ที่รองรับคุณสมบัติการเชื่อมต่อที่ปลอดภัย ซึ่งแนะนำใน Bluetooth Core Specification 4.1 (ให้ดูที่ Bluetooth Core Specification 5.1)

ความปลอดภัยของแถบความถี่กว้างยิ่งยวดใน iOS

ชิป U1 ใหม่ที่ออกแบบโดย Apple ใช้เทคโนโลยีแถบความถี่กว้างยิ่งยวดสำหรับการรับรู้ตำแหน่ง ซึ่งทำให้ iPhone 11, iPhone 11 Pro และ iPhone 11 Pro Max หรือ iPhone รุ่นใหม่กว่าสามารถค้นหาอุปกรณ์ Apple อื่นๆ ที่ติดตั้ง U1 ได้อย่างแม่นยำ เทคโนโลยีแบบแถบความถี่กว้างยิ่งยวดใช้เทคโนโลยีเดียวกันในการสุ่มข้อมูลที่พบในอุปกรณ์ Apple ที่รองรับอื่นๆ:

- การสุ่มที่อยู่ MAC
- การสุ่มหมายเลขลำดับเฟรม Wi-Fi

การลงชื่อเข้าครั้งเดียว

ความปลอดภัยของการลงชื่อเข้าครั้งเดียว

การลงชื่อเข้าครั้งเดียว

iOS และ iPadOS รองรับการตรวจสอบสิทธิ์ของเครือข่ายองค์กรผ่านการลงชื่อเข้าครั้งเดียว (SSO) SSO ทำงานกับเครือข่ายที่ใช้ Kerberos เพื่อตรวจสอบสิทธิ์ผู้ใช้กับบริการที่พวกเขาได้รับอนุญาตให้เข้าถึง SSO สามารถใช้ได้สำหรับกิจกรรมเครือข่ายจำนวนมาก ตั้งแต่เซสชั่น Safari ที่ปลอดภัยไปจนถึงแอปของบุคคลหรือบริษัทอื่น การตรวจสอบสิทธิ์ที่ใช้ใบรับรอง เช่น PKINIT ก็ได้รับการรองรับด้วยเช่นกัน

macOS รองรับการตรวจสอบสิทธิ์ของเครือข่ายองค์กรโดยใช้ Kerberos แอปสามารถใช้ Kerberos เพื่อตรวจสอบสิทธิ์ผู้ใช้กับบริการที่พวกเขาได้รับอนุญาตให้เข้าถึง Kerberos ยังสามารถใช้ได้สำหรับกิจกรรมเครือข่ายจำนวนมาก ตั้งแต่เซสชั่น Safari และการตรวจสอบสิทธิ์ระบบไฟล์เครือข่ายที่ปลอดภัย ไปจนถึงแอปของบุคคลหรือบริษัทอื่น การตรวจสอบสิทธิ์โดยใบรับรองได้รับการรองรับ อย่างไรก็ตาม แอปจะต้องนำ API ของนักพัฒนามาใช้

iOS, iPadOS และ macOS SSO ใช้โทเค็น SPNEGO และโปรโตคอล HTTP Negotiate เพื่อทำงานร่วมกับเกตเวย์การตรวจสอบสิทธิ์ที่ใช้ Kerberos และระบบการตรวจสอบสิทธิ์แบบผสานกับ Windows ที่รองรับตั๋ว Kerberos การรองรับ SSO ใช้โปรเจ็กต์โอเพนซอร์ซ Heimdal

ประเภทการเข้ารหัสต่อไปนี้ได้รับการรองรับใน iOS, iPadOS และ macOS:

- AES-128-CTS-HMAC-SHA1-96
- AES-256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari รองรับ SSO และแอปของบุคคลหรือบริษัทอื่นที่ใช้ API เครือข่าย iOS และ iPadOS มาตรฐานก็สามารถได้รับการกำหนดค่าเพื่อใช้งานด้วยเช่นกัน ในการกำหนดค่า SSO นั้น iOS และ iPadOS รองรับเพย์โหลดโปรไฟล์การกำหนดค่าที่อนุญาตให้โซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) เรียกใช้การตั้งค่าที่จำเป็น ซึ่งรวมถึงการตั้งค่าชื่อหลักของผู้ใช้ (ซึ่งก็คือบัญชีผู้ใช้ Active Directory) และการตั้งค่าบริเวณ Kerberos เช่นเดียวกับการกำหนดค่าว่าแอปและ URL เว็บ Safari ใดที่ควรได้รับอนุญาตให้ใช้ SSO

ในการกำหนดค่า Kerberos ใน macOS ให้รับตั๋วด้วย Ticket Viewer, เข้าสู่ระบบโดเมน Windows Active Directory หรือใช้เครื่องมือบรรทัดคำสั่ง `kinit`

การลงชื่อเข้าครั้งเดียวแบบขยายได้

นักพัฒนาแอปสามารถมอบการใช้การลงชื่อเข้าครั้งเดียวของตนเองโดยใช้ส่วนขยาย SSO ได้ ส่วนขยาย SSO ใช้งานเมื่อแอปเว็บหรือแอปดั้งเดิมต้องการใช้การให้ข้อมูลประจำตัวสำหรับการตรวจสอบสิทธิ์ของผู้ใช้ นักพัฒนาสามารถมอบส่วนขยายได้สองประเภท: ส่วนขยายที่เปลี่ยนเส้นทางไปยัง HTTPS และส่วนขยายที่ใช้กลไกการร้องถามและตอบกลับ เช่น Kerberos ซึ่งช่วยให้การลงชื่อเข้าครั้งเดียวแบบขยายได้รองรับแบบแผนการตรวจสอบสิทธิ์ OpenID, OAuth, SAML2 และ Kerberos

ในการใช้ส่วนขยายการลงชื่อเข้าครั้งเดียว แอปสามารถใช้ API AuthenticationServices หรือพึ่งพากลไกการสกัดกั้น URL ที่ระบบปฏิบัติการมีให้ได้ WebKit และ CFNetwork มีชั้นการสกัดกั้นทำให้สามารถรองรับการลงชื่อเข้าแบบครั้งเดียวได้อย่างราบรื่นสำหรับแอปดั้งเดิมหรือแอป WebKit ใดๆ สำหรับการใช้งานส่วนขยายการลงชื่อเข้าครั้งเดียว ต้องมีการติดตั้งการกำหนดค่าโดยผู้ดูแลระบบผ่านโปรไฟล์การจัดการอุปกรณ์เคลื่อนที่ (MDM) นอกจากนี้ ส่วนขยายแบบเปลี่ยนเส้นทางต้องใช้เพย์โหลดโดเมนที่เกี่ยวข้องเพื่อพิสูจน์ว่าเซิร์ฟเวอร์ข้อมูลประจำตัวที่รองรับรับรู้ถึงการมีอยู่ของส่วนขยาย

ส่วนขยายเดียวที่มาพร้อมระบบปฏิบัติการคือส่วนขยาย Kerberos SSO

ความปลอดภัยของ AirDrop

อุปกรณ์ Apple ที่รองรับ AirDrop จะใช้บลูทูธพลังงานต่ำ (BLE) และเทคโนโลยี Wi-Fi แบบเพียร์ทูเพียร์ที่สร้างโดย Apple เพื่อส่งไฟล์และข้อมูลไปยังอุปกรณ์ใกล้เคียง รวมถึงอุปกรณ์ iOS ที่รองรับ AirDrop และอุปกรณ์ iPad ที่ใช้ iOS 7 ขึ้นไปและคอมพิวเตอร์ Mac ที่ใช้ OS X 10.11 ขึ้นไป วิทยุ Wi-Fi ใช้เพื่อติดต่อโดยตรงระหว่างอุปกรณ์โดยไม่ใช้การเชื่อมต่อกับอินเทอร์เน็ตหรือจุดเชื่อมต่อ (AP) แบบไร้สายใดๆ การเชื่อมต่อนี้ได้รับการเข้ารหัสด้วย TLS

AirDrop ได้รับการตั้งค่าให้แชร์กับเฉพาะรายชื่อเป็นค่าเริ่มต้น ผู้ใช้ยังสามารถเลือกที่จะใช้งาน AirDrop เพื่อแชร์กับทุกคนหรือปิดใช้คุณสมบัตินี้โดยสิ้นเชิงได้ องค์กรสามารถจำกัดการใช้งาน AirDrop สำหรับอุปกรณ์หรือแอปที่ได้รับการจัดการโดยใช้โซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) ได้

การทำงานของ AirDrop

AirDrop ใช้บริการ iCloud เพื่อช่วยผู้ใช้ตรวจสอบสิทธิ์ เมื่อผู้ใช้ลงชื่อเข้า iCloud ข้อมูลประจำตัวของ RSA แบบ 2048 บิตจะถูกเก็บไว้ในอุปกรณ์ และเมื่อผู้ใช้เปิดใช้ AirDrop แฮชข้อมูลประจำตัวแบบสั้นของ AirDrop จะถูกสร้างขึ้นตามที่อยู่อีเมลและเบอร์โทรศัพท์ที่เชื่อมโยงกับ Apple ID ของผู้ใช้

เมื่อผู้ใช้เลือก AirDrop เป็นวิธีการแชร์รายการ อุปกรณ์ที่ส่งจะส่งสัญญาณ AirDrop ผ่าน BLE ที่มีแฮชข้อมูลประจำตัว AirDrop แบบสั้นของผู้ใช้ อุปกรณ์ Apple เครื่องอื่นที่เปิดอยู่ในระยะใกล้เคียงและเปิดใช้ AirDrop อยู่จะตรวจพบสัญญาณและตอบสนองโดยใช้ Wi-Fi แบบเพียร์ทูเพียร์ เพื่อให้อุปกรณ์ที่ส่งสามารถค้นพบข้อมูลจำเพาะของอุปกรณ์เครื่องใดๆ ที่มีการตอบสนอง

ในโหมดเฉพาะรายชื่อ แฮชข้อมูลประจำตัว AirDrop แบบสั้นที่ได้รับจะถูกเปรียบเทียบกับแฮชของผู้คนในแอปรายชื่อของอุปกรณ์ที่รับ ถ้าพบรายการที่ตรงกัน อุปกรณ์ที่ส่งจะตอบสนองผ่าน Wi-Fi แบบเพียร์ทูเพียร์พร้อมข้อมูลประจำตัวของอุปกรณ์นั้น ถ้าไม่มีการจับคู่ อุปกรณ์จะไม่ตอบสนอง

ในโหมดทุกคน จะใช้กระบวนการโดยรวมแบบเดียวกัน อย่างไรก็ตาม อุปกรณ์ที่รับจะตอบสนองแม้จะไม่มีการจับคู่ในแอปรายชื่อของอุปกรณ์

อุปกรณ์ที่ส่งจะเริ่มต้นการเชื่อมต่อกับ AirDrop โดยใช้ Wi-Fi แบบเพียร์ทูเพียร์ โดยใช้การเชื่อมต่อนี้เพื่อส่งแฮชข้อมูลประจำตัวแบบยาวไปยังอุปกรณ์ที่รับ ถ้าแฮชข้อมูลประจำตัวแบบยาวตรงกับแฮชของคนที่ทราบชื่อในแอปรายชื่อของผู้รับ ผู้รับจะตอบสนองกับแฮชข้อมูลประจำตัวแบบยาว

ถ้าแฮชได้รับการตรวจสอบยืนยัน ชื่อและรูปภาพของผู้รับ (ถ้ามีอยู่ในรายชื่อ) จะถูกแสดงในแผ่นงานการแชร์ AirDrop ของผู้ส่ง ใน iOS และ iPadOS แฮชจะแสดงในส่วน “ผู้คน” หรือ “อุปกรณ์” อุปกรณ์ที่ไม่ได้รับการตรวจสอบยืนยันหรือตรวจสอบสิทธิ์จะแสดงในแผ่นงานการแชร์ AirDrop ของผู้ส่ง โดยมีไอคอนเงาดำและชื่อของอุปกรณ์ ตามที่ระบุใน การตั้งค่า > ทั่วไป > เกี่ยวกับ > ชื่อ ใน iOS และ iPadOS อุปกรณ์จะแสดงในส่วน “คนอื่นๆ” ของแผ่นงานการแชร์ AirDrop

ผู้ใช้ที่ส่งสามารถเลือกได้ว่าต้องการแชร์กับใคร เมื่อมีการเลือกของผู้ใช้ อุปกรณ์ที่ส่งจะเริ่มต้นการเชื่อมต่อแบบเข้ารหัส (TLS) กับอุปกรณ์ที่รับ ซึ่งแลกเปลี่ยนใบรับรองข้อมูลประจำตัว iCloud กัน ข้อมูลประจำตัวในใบรับรองจะได้รับการตรวจสอบยืนยันเทียบกับแอปรายชื่อของผู้ใช้แต่ละราย

ถ้าใบรับรองได้รับการตรวจสอบยืนยัน ผู้ใช้ที่รับจะได้รับคำขอให้รับการถ่ายโอนข้อมูลเข้าจากผู้ใช้หรืออุปกรณ์ที่ระบุ ถ้าเลือกผู้รับหลายคน กระบวนการทำงานนี้จะมีการทำซ้ำสำหรับจุดหมายปลายทางแต่ละรายการ

ความปลอดภัยของการแชร์รหัสผ่าน Wi-Fi บน iPhone และ iPad

อุปกรณ์ iOS และ iPadOS ที่รองรับการแชร์รหัสผ่าน Wi-Fi จะใช้กลไกที่คล้ายคลึงกับ AirDrop ในการส่งรหัสผ่าน Wi-Fi จากอุปกรณ์เครื่องหนึ่งไปอีกเครื่องหนึ่ง

เมื่อผู้ใช้เลือกเครือข่าย Wi-Fi (ผู้เรียกขอ) และได้รับแจ้งขอรหัสผ่าน Wi-Fi อุปกรณ์ Apple จะเริ่มการแจ้งเกี่ยวกับบลูทูธพลังงานต่ำ (BLE) ซึ่งระบุว่าอุปกรณ์ต้องการรหัสผ่าน Wi-Fi อุปกรณ์ Apple อื่นๆ ที่เปิดอยู่ในระยะใกล้เคียง และมีรหัสผ่านสำหรับเครือข่าย Wi-Fi ที่เลือกจะเชื่อมต่อโดยใช้ BLE กับอุปกรณ์ที่เรียกขอ

อุปกรณ์ที่มีรหัสผ่าน Wi-Fi (ผู้ให้) ต้องมีข้อมูลรายชื่อของผู้เรียกขอ และผู้เรียกขอต้องพิสูจน์ข้อมูลประจำตัวของตัวเองโดยใช้กลไกที่คล้ายคลึงกับ AirDrop เมื่อข้อมูลประจำตัวได้รับการพิสูจน์แล้ว ผู้ให้จะส่งรหัสแก่ผู้เรียกขอ ซึ่งสามารถใช้เพื่อเข้าร่วมเครือข่ายได้

องค์กรสามารถจำกัดการใช้งานการแชร์รหัสผ่าน Wi-Fi สำหรับอุปกรณ์หรือแอปที่ได้รับการจัดการผ่านโซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) ได้

ความปลอดภัยของไฟร์วอลล์ใน macOS

macOS มีไฟร์วอลล์ในตัวเพื่อปกป้อง Mac จากการเข้าถึงเครือข่ายและการโจมตีโดยปฏิเสธการให้บริการ ไฟร์วอลล์สามารถกำหนดค่าได้ในบานหน้าต่างความปลอดภัยและความเป็นส่วนตัวของการตั้งค่าระบบ และรองรับการกำหนดค่าต่อไปนี้:

- ปิดกั้นการเชื่อมต่อที่เข้ามาทั้งหมดไม่ว่าจะเป็นแอปใด
- อนุญาตให้ซอฟต์แวร์ในตัวรับการเชื่อมต่อที่เข้ามาโดยอัตโนมัติ
- อนุญาตให้ซอฟต์แวร์ที่ดาวน์โหลดและลงชื่อรับการเชื่อมต่อที่เข้ามาโดยอัตโนมัติ
- เพิ่มหรือปฏิเสธการเข้าถึงโดยอิงตามแอปที่ระบุผู้ใช้
- ป้องกัน Mac จากการตอบสนองต่อคำขอการตรวจสอบ ICMP (Internet Control Message Protocol) และคำขอสแกนพอร์ต

ความปลอดภัยของชุดสินค้านักพัฒนา

ภาพรวมความปลอดภัยของชุดสินค้านักพัฒนา

Apple ให้บริการเฟรมเวิร์ค “ชุดสินค้า” จำนวนมากเพื่อช่วยให้นักพัฒนาของบริษัทอื่นสามารถขยายบริการของ Apple ได้ เฟรมเวิร์คเหล่านี้สร้างขึ้นมาโดยคำนึงถึงความเป็นส่วนตัวและความปลอดภัยของผู้ใช้เป็นหลัก:

- HomeKit
- CloudKit
- SiriKit
- DriverKit
- ReplayKit
- ARKit

ความปลอดภัยของ HomeKit

ความปลอดภัยของการสื่อสาร HomeKit

HomeKit ให้โครงสร้างการทำงานอัตโนมัติในบ้านที่ใช้งานความปลอดภัย iCloud และ iOS, iPadOS และ macOS เพื่อปกป้องและเชื่อมข้อมูลส่วนตัวโดยไม่เปิดเผยไปยัง Apple

ข้อมูลประจำตัวและความปลอดภัยของ HomeKit ใช้คู่กุญแจสาธารณะ-ส่วนตัว Ed25519 มีการสร้างคู่กุญแจ Ed25519 บนอุปกรณ์ iOS, iPadOS และ macOS สำหรับผู้ใช้แต่ละรายสำหรับ HomeKit ซึ่งจะกลายเป็นข้อมูลประจำตัว HomeKit ของผู้ใช้ คู่กุญแจจะใช้เพื่อตรวจสอบสิทธิ์ของการสื่อสารระหว่างอุปกรณ์ iOS, iPadOS และ macOS และระหว่างอุปกรณ์ iOS, iPadOS และ macOS และอุปกรณ์เสริม

กุญแจที่ถูกจัดเก็บอยู่ในพวงกุญแจและถูกรวมเฉพาะในข้อมูลสำรองพวงกุญแจที่เข้ารหัสจะอัปเดตให้ตรงกันอยู่เสมอระหว่างอุปกรณ์โดยใช้พวงกุญแจ iCloud ถ้ามีให้ใช้งานได้ HomePod และ Apple TV จะได้รับกุญแจโดยใช้การแตะเพื่อตั้งค่าหรือโหมดการตั้งค่า ตามที่อธิบายไว้ด้านล่าง กุญแจจะถูกแชร์จาก iPhone ไปยัง Apple Watch ที่จับคู่อยู่โดยใช้บริการข้อมูลประจำตัว (IDS) ของ Apple

การติดต่อระหว่างอุปกรณ์เสริม HomeKit

อุปกรณ์เสริม HomeKit จะสร้างคู่กุญแจ Ed25519 ของตัวเองสำหรับใช้งานในการติดต่อกับอุปกรณ์ iOS, iPadOS และ macOS ถ้าอุปกรณ์เสริมมีการกู้คืนกลับเป็นการตั้งค่าโรงงาน คู่กุญแจใหม่จะถูกสร้างขึ้น

ในการสร้างความสัมพันธ์ระหว่างอุปกรณ์ iOS, iPadOS และ macOS และอุปกรณ์เสริม HomeKit กุญแจจะถูกแลกเปลี่ยนโดยใช้โปรโตคอล Secure Remote Password (3072 บิต) ซึ่งใช้รหัสแปดหลักที่ผู้ผลิตอุปกรณ์เสริมให้มา และป้อนลงในอุปกรณ์ iOS และ iPadOS โดยผู้ใช้ จากนั้นเข้ารหัสโดยใช้ ChaCha20-Poly1305 AEAD ร่วมกับกุญแจที่ได้จาก HKDF-SHA512 ใบรับรอง MFi ของอุปกรณ์เสริมจะได้รับการตรวจสอบยืนยันในระหว่างการตั้งค่าด้วย อุปกรณ์เสริมที่ไม่มีชิป MFi สามารถสร้างการรองรับในตัวสำหรับการตรวจสอบสิทธิ์ซอฟต์แวร์ใน iOS 11.3 ขึ้นไปได้

เมื่ออุปกรณ์ iOS, iPadOS และ macOS และอุปกรณ์เสริม HomeKit สื่อสารระหว่างการใช้งาน แต่ละฝั่งจะตรวจสอบสิทธิ์ของอีกฝ่ายโดยใช้กุญแจที่แลกเปลี่ยนในกระบวนการทำงานเบื้องต้น เซสชั่นแต่ละเซสชั่นถูกสร้างโดยใช้โปรโตคอล Station-to-Station และมีการเข้ารหัสโดยใช้กุญแจที่ได้จาก HKDF-SHA512 โดยอิงตามกุญแจ Curve25519 แบบ per-session การทำงานนี้ปรับใช้กับทั้งอุปกรณ์เสริมที่ใช้งาน IP และบลูทูธพลังงานต่ำ (BLE)

สำหรับอุปกรณ์ BLE ที่รองรับการแจ้งเตือนด้านการกระจาย อุปกรณ์เสริมจะถูกกำหนดสิทธิ์ด้วยกุญแจการเข้ารหัสการกระจายผ่านทางเซสชั่นที่ปลอดภัยโดยอุปกรณ์ iOS, iPadOS และ macOS ที่จับคู่อยู่ กุญแจนี้ใช้สำหรับเข้ารหัสข้อมูลที่เกี่ยวกับการเปลี่ยนแปลงสถานะของอุปกรณ์เสริมซึ่งมีการแจ้งเตือนโดยใช้การประกาศ BLE กุญแจการเข้ารหัสการกระจายคือกุญแจที่ได้จาก HKDF-SHA512 และข้อมูลจะถูกเข้ารหัสโดยใช้อัลกอริทึม ChaCha20-Poly1305 AEAD กุญแจการเข้ารหัสการกระจายจะเปลี่ยนแปลงเป็นระยะๆ โดยอุปกรณ์ iOS, iPadOS และ macOS และอัปเดตกับอุปกรณ์อื่นโดยใช้ iCloud ตามที่ได้อธิบายไว้ในส่วนความปลอดภัยของข้อมูล

HomeKit และ Siri

Siri สามารถใช้เพื่อสอบถามและควบคุมอุปกรณ์เสริม และเปิดใช้งานบรรยากาศได้ ข้อมูลส่วนน้อยเกี่ยวกับการกำหนดค่าของบ้านจะมีการมอบให้ Siri แบบไม่ระบุชื่อ เพื่อให้ชื่อห้อง อุปกรณ์เสริม และบรรยากาศที่จำเป็นสำหรับการจดจำคำสั่ง เสียงที่ส่งไปที่ Siri อาจหมายถึงอุปกรณ์เสริมหรือคำสั่งเฉพาะ แต่ข้อมูล Siri ดังกล่าวจะไม่เชื่อมโยงกับคุณสมบัติอื่นๆ ของ Apple เช่น HomeKit

อุปกรณ์เสริม HomeKit ที่รองรับ Siri

ผู้ใช้สามารถเปิดใช้งานคุณสมบัติใหม่ๆ เช่น Siri และคุณสมบัติอื่นๆ ของ HomePod ได้ เช่น ตัวจับเวลา นาฬิกาปลุก อินเตอร์คอม และกริ่งประตู บนอุปกรณ์เสริมที่รองรับ Siri ได้โดยใช้แอปบ้าน เมื่อเปิดใช้งานคุณสมบัติเหล่านี้ อุปกรณ์เสริมจะทำงานร่วมกับ HomePod ที่จับคู่บนเครือข่ายในพื้นที่ซึ่งคุณสมบัติของ Apple เหล่านี้ทำงานอยู่ มีการแลกเปลี่ยนเสียงระหว่างอุปกรณ์ผ่านช่องสัญญาณที่เข้ารหัสโดยใช้ทั้งโปรโตคอล HomeKit และ AirPlay

เมื่อเปิดฟัง “หวัดดี Siri” อุปกรณ์เสริมจะฟังวลี “หวัดดี Siri” โดยใช้กลไกตรวจจับวลีทริกเกอร์ที่ทำงานอยู่ในเครื่อง ถ้ากลไกนี้ตรวจพบวลี กลไกจะส่งเฟรมเสียงไปยัง HomePod ที่จับคู่โดยตรงโดยใช้ HomeKit HomePod จะตรวจสอบเสียงครั้งที่สองและอาจยกเลิกเซสชั่นเสียงหากพบว่าวลีนั้นไม่มีวลีทริกเกอร์

เมื่อเปิดแตะเพื่อใช้งาน Siri ผู้ใช้สามารถกดปุ่มเฉพาะบนอุปกรณ์เสริมเพื่อเริ่มการสนทนากับ Siri ได้ เฟรมเสียงจะถูกส่งไปยัง HomePod ที่จับคู่โดยตรง

หลังจากตรวจพบการเรียกใช้งาน Siri ได้สำเร็จ HomePod จะส่งเสียงไปยังเซิร์ฟเวอร์ Siri และปฏิบัติตามเจตนาของผู้ใช้โดยใช้การรักษาความปลอดภัย ความเป็นส่วนตัว และการป้องกันการเข้ารหัสแบบเดียวกับที่ HomePod ปรับใช้กับการเรียกใช้งานของผู้ใช้ไปยัง HomePod เอง ถ้า Siri มีการตอบกลับด้วยเสียง การตอบสนองของ Siri จะถูกส่งผ่านช่องสัญญาณเสียงของ AirPlay ไปยังอุปกรณ์เสริม คำขอ Siri บางข้อต้องการข้อมูลเพิ่มเติมจากผู้ใช้ (เช่น การถามว่าผู้ใช้ต้องการฟังตัวเลือกเพิ่มเติมหรือไม่) ในกรณีดังกล่าว อุปกรณ์เสริมจะได้รับการระบุว่าผู้ใช้ควรได้รับแจ้ง และเสียงเพิ่มเติมจะสตรีมไปยัง HomePod

อุปกรณ์เสริมจำเป็นต้องมีตัวบ่งชี้ภาพเพื่อส่งสัญญาณไปยังผู้ใช้ในขณะที่กำลังฟังอยู่ (เช่น ไฟสถานะ LED) อุปกรณ์เสริมไม่มีความรู้เกี่ยวกับเจตนาของคำขอ Siri ยกเว้นการเข้าถึงสตรีมเสียง และไม่มีข้อมูลผู้ใช้จัดเก็บไว้ในอุปกรณ์เสริม

ความปลอดภัยของข้อมูล HomeKit

ข้อมูล HomeKit สามารถอัปเดตระหว่างอุปกรณ์ iOS, iPadOS และ macOS ของผู้ใช้ได้อย่างปลอดภัย โดยใช้พวงกุญแจ iCloud และ iCloud ระหว่างกระบวนการนี้ ข้อมูล HomeKit จะถูกเข้ารหัสโดยใช้กุญแจที่ได้มาจากข้อมูลประจำตัวของผู้ใช้ HomeKit และ nonce แบบสุ่ม และจะได้รับการจัดการในรูปแบบวัตถุไบนารีขนาดใหญ่แบบทึบแสง หรือ**บล็อบ (blob)** ข้อมูล blob ล่าสุดจะมีการจัดเก็บบน iCloud แต่จะไม่ถูกใช้เพื่อวัตถุประสงค์อื่นๆ เนื่องจากข้อมูลมีการเข้ารหัสโดยใช้กุญแจที่ใช้งานได้เฉพาะบนอุปกรณ์ iOS, iPadOS และ macOS ของผู้ใช้เท่านั้น เนื้อหาภายในจะไม่สามารถเข้าถึงได้ในระหว่างการส่งข้อมูลและพื้นที่จัดเก็บข้อมูล iCloud

ข้อมูล HomeKit ยังมีการเชื่อมข้อมูลระหว่างผู้ใช้หลายคนที่อยู่ภายในบ้านเดียวกันด้วย กระบวนการนี้ใช้การตรวจสอบสิทธิ์และการเข้ารหัสที่เหมือนกับที่ใช้ระหว่างอุปกรณ์ iOS, iPadOS และ macOS และอุปกรณ์เสริม HomeKit การตรวจสอบสิทธิ์ใช้งานกุญแจสาธารณะ Ed25519 ที่มีการแลกเปลี่ยนระหว่างอุปกรณ์เมื่อเพิ่มผู้ใช้ไปยังบ้าน หลังจากเพิ่มผู้ใช้ใหม่ไปที่บ้าน การสื่อสารเพิ่มเติมทุกครั้งจะได้รับการตรวจสอบสิทธิ์และเข้ารหัสโดยใช้โปรโตคอล Station-to-Station และกุญแจแบบ per-session

ผู้ใช้รายแรกที่เป็นผู้สร้างบ้านใน HomeKit หรือผู้ใช้รายอื่นที่มีสิทธิ์ในการแก้ไขสามารถเพิ่มผู้ใช้ใหม่ได้ อุปกรณ์ของเจ้าของจะกำหนดค่าอุปกรณ์เสริมด้วยกุญแจสาธารณะของผู้ใช้ใหม่ เพื่อให้อุปกรณ์เสริมสามารถตรวจสอบสิทธิ์และยอมรับคำสั่งจากผู้ใช้ใหม่ได้ เมื่อผู้ใช้ที่มีสิทธิ์ในการแก้ไขเพิ่มผู้ใช้ใหม่ กระบวนการจะมอบหมายให้ศูนย์กลางอุปกรณ์บ้านดำเนินการการทำงานให้เสร็จสมบูรณ์แทน

HomeKit และ Apple TV

กระบวนการเตรียมใช้งาน Apple TV สำหรับใช้กับ HomeKit จะดำเนินการโดยอัตโนมัติเมื่อผู้ใช้ลงชื่อเข้า iCloud บัญชี iCloud ต้องเปิดใช้งานการตรวจสอบสิทธิ์สองปัจจัย Apple TV และอุปกรณ์ของเจ้าของจะแลกเปลี่ยนกุญแจสาธารณะ Ed25519 ชั่วคราวผ่าน iCloud เมื่ออุปกรณ์ของเจ้าของและ Apple TV อยู่ในเครือข่ายในพื้นที่เดียวกัน ระบบจะใช้กุญแจชั่วคราวเพื่อทำให้การเชื่อมต่อผ่านเครือข่ายในพื้นที่ปลอดภัยโดยใช้โปรโตคอล Station-to-Station และกุญแจแบบ per-session กระบวนการนี้ใช้การตรวจสอบสิทธิ์และการเข้ารหัสที่เหมือนกับที่ใช้ระหว่างอุปกรณ์ iOS, iPadOS และ macOS และอุปกรณ์เสริม HomeKit ในการเชื่อมต่อภายในที่ปลอดภัยนี้ อุปกรณ์ของเจ้าของจะถ่ายโอนคู่กุญแจสาธารณะ-ส่วนตัว Ed25519 ของผู้ใช้ไปยัง Apple TV จากนั้นกุญแจเหล่านี้จะถูกใช้เพื่อทำให้การสื่อสารระหว่าง Apple TV และอุปกรณ์เสริม HomeKit และระหว่าง Apple TV และอุปกรณ์ iOS, iPadOS และ macOS เครื่องอื่นๆ ที่เป็นส่วนหนึ่งของบ้าน HomeKit ปลอดภัยอีกด้วย

ถ้าผู้ใช้ไม่มีอุปกรณ์หลายเครื่อง และไม่อนุญาตผู้ใช้เพิ่มเติมให้เข้าใช้ในบ้านของผู้ใช้ได้ ระบบจะไม่เชื่อมข้อมูล HomeKit ไปยัง iCloud

ข้อมูลในบ้านและแอป

การเข้าใช้งานข้อมูลในบ้านโดยแอปได้รับการควบคุมโดยการตั้งค่าความเป็นส่วนตัวของผู้ใช้ ระบบจะขอให้ผู้ใช้อนุญาตการเข้าถึงเมื่อแอปร้องขอข้อมูลในบ้าน คล้ายกับการขอใช้แอปรายชื่อ แอปรูปภาพ และทรัพยากร iOS, iPadOS และ macOS อื่นๆ ถ้าผู้ใช้อนุญาต แอปจะมีสิทธิ์เข้าถึงชื่อห้อง ชื่อของอุปกรณ์เสริม ห้องที่อุปกรณ์เสริมแต่ละชิ้นอยู่ และข้อมูลอื่นๆ ตามที่ระบุรายละเอียดในเอกสารประกอบสำหรับนักพัฒนา HomeKit ที่ https://developer.apple.com/homekit/

พื้นที่จัดเก็บข้อมูลภายใน

HomeKit จัดเก็บข้อมูลเกี่ยวกับบ้าน อุปกรณ์เสริม บรรยากาศ และผู้ใช้บนอุปกรณ์ iOS, iPadOS และ macOS ของผู้ใช้ ข้อมูลที่จัดเก็บนี้จะถูกเข้ารหัสโดยใช้กุญแจที่ได้จากกุญแจข้อมูลประจำตัว HomeKit ของผู้ใช้ ร่วมกับค่า Nonce แบบสุ่ม นอกจากนี้ ข้อมูล HomeKit ยังมีการจัดเก็บโดยใช้คลาสการปกป้องข้อมูลแบบปกป้องจนกว่าจะมีการตรวจสอบสิทธิ์ของผู้ใช้รายแรก ข้อมูล HomeKit มีการสำรองข้อมูลในรูปแบบข้อมูลสำรองที่เข้ารหัสเท่านั้น ดังนั้น ตัวอย่างเช่น การสำรองข้อมูลแบบไม่เข้ารหัสไปยัง Finder (ใน macOS 10.15 ขึ้นไป) หรือ iTunes (macOS 10.14 หรือก่อนหน้านี้) ผ่าน USB จะไม่มีข้อมูล HomeKit

การรักษาความปลอดภัยของเราท์เตอร์ด้วย HomeKit

เราท์เตอร์ที่รองรับ HomeKit ช่วยให้ผู้ใช้สามารถปรับปรุงความปลอดภัยของเครือข่ายภายในบ้านของพวกเขาได้ โดยการจัดการการเข้าถึง Wi-Fi ที่อุปกรณ์เสริม HomeKit ต้องใช้กับเครือข่ายในพื้นที่และอินเทอร์เน็ต เราท์เตอร์ยังรองรับการตรวจสอบสิทธิ์ PSK ส่วนตัว (PPSK) เพื่อให้สามารถเพิ่มอุปกรณ์เสริมไปยังเครือข่าย Wi-Fi ได้อีกด้วยโดยใช้กุญแจสำหรับอุปกรณ์เสริมนั้นโดยเฉพาะและสามารถเพิกถอนได้เมื่อจำเป็น การตรวจสอบสิทธิ์ PPSK จะปรับปรุงความปลอดภัยโดยไม่เปิดเผยรหัสผ่านหลักของ Wi-Fi ให้กับอุปกรณ์เสริม และโดยอนุญาตให้เราท์เตอร์ระบุอุปกรณ์เสริมได้อย่างปลอดภัยแม้ว่าจะต้องเปลี่ยนที่อยู่ MAC ก็ตาม

ในการใช้แอปบ้าน ผู้ใช้สามารถกำหนดค่าข้อจำกัดการเข้าถึงสำหรับกลุ่มอุปกรณ์เสริมได้ดังต่อไปนี้:

- **ไม่จำกัด:** อนุญาตการเข้าถึงอินเทอร์เน็ตและเครือข่ายในพื้นที่แบบไม่จำกัด
- **อัตโนมัติ:** การตั้งค่านี้เป็นค่าเริ่มต้น อนุญาตการเข้าถึงอินเทอร์เน็ตและเครือข่ายในพื้นที่โดยอิงตามรายการของไซต์อินเทอร์เน็ตและพอร์ตภายในที่ผู้ผลิตอุปกรณ์เสริมจัดหาให้กับ Apple รายการนี้รวมถึงไซต์และพอร์ตทั้งหมดที่อุปกรณ์เสริมจำเป็นต้องใช้เพื่อให้ทำงานได้อย่างถูกต้อง (ไม่จำกัด จะมีให้ใช้งานเมื่อมีรายการดังกล่าวเท่านั้น)
- **จำกัดเฉพาะบ้าน:** ไม่ต้องใช้การเข้าถึงอินเทอร์เน็ตหรือเครือข่ายในพื้นที่ ยกเว้นการเชื่อมต่อที่ HomeKit ต้องใช้ในการค้นหาและควบคุมอุปกรณ์เสริมจากเครือข่ายในพื้นที่ (รวมถึงจากศูนย์กลางอุปกรณ์บ้านเพื่อรองรับการควบคุมระยะไกล)

PPSK เป็นวลีรหัสผ่าน WPA2 ส่วนบุคคลที่มีความปลอดภัยสูงและใช้กับอุปกรณ์เสริมโดยเฉพาะ ซึ่งถูกสร้างขึ้นโดย HomeKit โดยอัตโนมัติ และถูกเพิกถอนเมื่ออุปกรณ์เสริมนั้นถูกเอาออกจากบ้านในภายหลัง PPSK จะใช้เมื่อ HomeKit เพิ่มอุปกรณ์เสริมไปยังเครือข่าย Wi-Fi ในบ้านที่ได้กำหนดค่าไว้ด้วยเราท์เตอร์ของ HomeKit การเพิ่มนี้จะแสดงในรูปแบบเอกสารสิทธิ์ Wi-Fi: HomeKit ที่ได้รับการจัดการบนหน้าจอการตั้งค่าสำหรับอุปกรณ์เสริมในแอปบ้าน อุปกรณ์เสริมที่เพิ่มไปยังเครือข่าย Wi-Fi ก่อนที่จะเพิ่มเราท์เตอร์จะได้รับการกำหนดค่าอีกครั้งเพื่อใช้ PPSK หากอุปกรณ์เสริมดังกล่าวรองรับ ไม่เช่นนั้น อุปกรณ์เสริมจะเก็บรักษาเอกสารสิทธิ์ที่มีอยู่

เพื่อเป็นมาตรการรักษาความปลอดภัยเพิ่มเติม ผู้ใช้จะต้องกำหนดค่าเราท์เตอร์ของ HomeKit โดยใช้แอปของผู้ผลิตเราท์เตอร์นั้นเพื่อให้แอปสามารถตรวจสอบความถูกต้องว่าผู้ใช้สามารถเข้าถึงเราท์เตอร์ได้และได้รับอนุญาตให้เพิ่มเราท์เตอร์ไปยังแอปบ้าน

ความปลอดภัยของกล้องใน HomeKit

กล้องที่มีที่อยู่โปรโตคอลอินเทอร์เน็ต (ที่อยู่ IP) ใน HomeKit จะส่งสตรีมวิดีโอและเสียงโดยตรงไปที่อุปกรณ์ iOS, iPadOS, tvOS และ macOS บนเครือข่ายในพื้นที่ที่เข้าถึงสตรีม สตรีมถูกเข้ารหัสโดยใช้กุญแจที่สร้างแบบสุ่มบนอุปกรณ์และกล้องโปรโตคอลอินเทอร์เน็ต (หรือกล้อง IP) และแลกเปลี่ยนระหว่างเซสชั่น HomeKit ที่ปลอดภัยกับกล้อง เมื่ออุปกรณ์ไม่ได้อยู่บนเครือข่ายในพื้นที่ สตรีมที่เข้ารหัสจะถูกส่งต่อผ่านศูนย์กลางอุปกรณ์บ้านไปยังอุปกรณ์ ศูนย์กลางอุปกรณ์บ้านไม่ได้ถอดรหัสสตรีมและทำหน้าที่เพียงส่งต่อระหว่างอุปกรณ์และกล้อง IP เมื่อแอปแสดงมุมมองวิดีโอกล้อง IP ใน HomeKit ไปที่ผู้ใช้ HomeKit จะทำให้เฟรมวิดีโอปลอดภัยจากกระบวนการระบบแยกต่างหาก ผลคือแอปไม่สามารถเข้าถึงหรือจัดเก็บสตรีมวิดีโอได้ นอกจากนี้ แอปจะไม่ได้รับอนุญาตให้ถ่ายภาพหน้าจอจากสตรีมนี้

วิดีโอ HomeKit ที่ปลอดภัย

HomeKit มีกลไกแบบต้นทางถึงปลายทางที่ปลอดภัยและเป็นส่วนตัวในการบันทึก วิเคราะห์ และแสดงคลิปจากกล้อง IP ใน HomeKit โดยไม่เปิดเผยเนื้อหาวิดีโอนั้นให้กับ Apple หรือบุคคลหรือบริษัทอื่นๆ เมื่อตรวจพบการเคลื่อนไหวโดยกล้อง IP คลิปวิดีโอจะถูกส่งโดยตรงไปยังอุปกรณ์ Apple ที่ทำหน้าที่เป็นศูนย์กลางอุปกรณ์บ้านโดยใช้การเชื่อมต่อกับเครือข่ายในพื้นที่แบบเฉพาะระหว่างศูนย์กลางอุปกรณ์บ้านนั้นกับกล้อง IP การเชื่อมต่อเครือข่ายในพื้นที่จะถูกเข้ารหัสด้วยคู่กุญแจแบบ per-session ที่ได้จาก HKDF-SHA512 ซึ่งมีการเจรจาบนเซสชั่น HomeKit ระหว่างศูนย์กลางอุปกรณ์บ้านและกล้อง IP โดย HomeKit จะถอดรหัสสตรีมเสียงและวิดีโอบนศูนย์กลางอุปกรณ์บ้านและวิเคราะห์เฟรมวิดีโอในเครื่องสำหรับกิจกรรมที่สำคัญใดๆ ถ้าตรวจพบกิจกรรมที่สำคัญ HomeKit จะเข้ารหัสคลิปวิดีโอโดยใช้ AES-256-GCM ที่มีกุญแจ AES256 ที่สร้างแบบสุ่ม HomeKit ยังสร้างเฟรมโปสเตอร์สำหรับแต่ละคลิปอีกด้วย และเฟรมโปสเตอร์เหล่านี้จะถูกเข้ารหัสโดยใช้กุญแจ AES256 เดียวกันเฟรมโปสเตอร์ที่เข้ารหัส รวมทั้งข้อมูลเสียงและวิดีโอจะถูกอัปโหลดไปยังเซิร์ฟเวอร์ iCloud เมตาดาต้าที่เกี่ยวข้องสำหรับแต่ละคลิปรวมถึงกุญแจการเข้ารหัสจะถูกอัปโหลดไปยัง CloudKit โดยใช้การเข้ารหัส iCloud แบบต้นทางถึงปลายทาง

สำหรับการจัดประเภทใบหน้า HomeKit จะจัดเก็บข้อมูลทั้งหมดที่ใช้เพื่อจัดประเภทใบหน้าของคนนั้นโดยเฉพาะใน CloudKit โดยใช้การเข้ารหัส iCloud แบบต้นทางถึงปลายทาง ข้อมูลที่จัดเก็บรวมถึงข้อมูลเกี่ยวกับแต่ละคน เช่น ชื่อและภาพที่แสดงใบหน้าของคนนั้น ภาพใบหน้าเหล่านี้สามารถเอามาจากแอปรูปภาพของคนนั้นได้หากได้เลือกไว้ หรือเก็บรวบรวมได้จากวิดีโอกล้อง IP ที่ได้รับการวิเคราะห์ก่อนหน้านี้ เซสชั่นการวิเคราะห์วิดีโอ HomeKit เพื่อความปลอดภัยจะใช้ข้อมูลการจัดประเภทนี้ในการระบุใบหน้าในการสตรีมวิดีโอเพื่อความปลอดภัยที่ได้รับโดยตรงจากกล้อง IP และรวมข้อมูลการระบุดังกล่าวในเมตาดาต้าคลิปที่กล่าวถึงก่อนหน้านี้

เมื่อใช้แอปบ้านในการดูคลิปจากกล้อง ข้อมูลจะถูกดาวน์โหลดจาก iCloud และกุญแจในการถอดรหัสสตรีมจะถูกแกะห่อออกภายในเครื่องโดยใช้การถอดรหัส iCloud แบบต้นทางถึงปลายทาง เนื้อหาวิดีโอที่เข้ารหัสจะถูกสตรีมจากเซิร์ฟเวอร์และถอดรหัสภายในเครื่องบนอุปกรณ์ iOS ก่อนแสดงในตัวแสดง คลิปวิดีโอแต่ละเซสชั่นอาจถูกแบ่งออกเป็นส่วนย่อยโดยที่ส่วนย่อยแต่ละส่วนมีการเข้ารหัสสตรีมเนื้อหาด้วยกุญแจเฉพาะของตนเอง

ความปลอดภัยของ HomeKit กับ Apple TV

HomeKit เชื่อมต่ออุปกรณ์เสริมระยะไกลของบริษัทอื่นบางรายการกับ Apple TV อย่างปลอดภัย และรองรับการเพิ่มโปรไฟล์ผู้ใช้ไปยัง Apple TV ของเจ้าของบ้าน

การใช้อุปกรณ์เสริมระยะไกลของบริษัทอื่นกับ Apple TV

บางอุปกรณ์เสริมจากระยะไกลของบริษัทอื่นจะส่งกิจกรรมการออกแบบอินเทอร์เฟซมนุษย์ (HID) และเสียง Siri ให้กับ Apple TV ที่เชื่อมโยงซึ่งถูกเพิ่มโดยใช้แอปบ้าน รีโมทจะส่งกิจกรรม HID ผ่านเซสชั่นที่ปลอดภัยไปยัง Apple TV รีโมททีวีที่สามารถใช้ Siri ได้จะส่งข้อมูลเสียงไปที่ Apple TV เมื่อผู้ใช้ตั้งใจเปิดใช้งานไมโครโฟนบนรีโมทโดยใช้ปุ่ม Siri ที่มีให้ใช้งานเฉพาะ รีโมทจะส่งเฟรมเสียงโดยตรงไปยัง Apple TV โดยใช้การเชื่อมต่อเครือข่ายในพื้นที่โดยเฉพาะ คู่กุญแจแบบ per-session ที่ได้จาก HKDF-SHA512 ซึ่งมีการต่อรองบนเซสชั่น HomeKit ระหว่าง Apple TV และรีโมททีวีจะถูกใช้เพื่อเข้ารหัสการเชื่อมต่อเครือข่ายในพื้นที่ HomeKit จะถอดรหัสเฟรมเสียงบน Apple TV แล้วส่งต่อเฟรมเสียงไปยังแอป Siri ซึ่งเฟรมเสียงเหล่านั้นจะได้รับการปกป้องความเป็นส่วนตัวแบบเดียวกันกับการสัญญาณเสียงเข้าทั้งหมดของ Siri

โปรไฟล์ Apple TV สำหรับบ้านของ HomeKit

เมื่อผู้ใช้บ้าน HomeKit เพิ่มโปรไฟล์ของตัวเองไปยังผู้ใช้ Apple TV ของบ้าน ระบบจะมอบการเข้าถึงรายการทีวี เพลง และพ็อดคาสท์แก่ผู้ใช้คนนั้น การตั้งค่าสำหรับผู้ใช้แต่ละคนที่อิงตามการใช้โปรไฟล์บน Apple TV จะถูกแชร์ไปยังบัญชี iCloud ของเจ้าของโดยใช้การเข้ารหัส iCloud แบบต้นทางถึงปลายทาง ข้อมูลดังกล่าวมีผู้ใช้แต่ละคนเป็นเจ้าของและจะถูกแชร์ให้กับเจ้าของเป็นแบบอ่านอย่างเดียว ผู้ใช้แต่ละคนในบ้านสามารถเปลี่ยนค่าเหล่านี้ได้ในแอปบ้านและ Apple TV ของเจ้าของจะใช้การตั้งค่าเหล่านี้

เมื่อการตั้งค่าเปิดใช้อยู่ บัญชี iTunes ของผู้ใช้จะมีให้ใช้งานได้บน Apple TV เมื่อการตั้งค่าปิด บัญชีและข้อมูลทั้งหมดที่เกี่ยวข้องกับผู้ใช้ดังกล่าวจะถูกลบออกบน Apple TV อุปกรณ์ของผู้ใช้จะเริ่มต้นการแชร์ CloudKit เริ่มต้นและโทเค็นสำหรับสร้างการแชร์ CloudKit อย่างปลอดภัยจะถูกส่งผ่านช่องสัญญาณเดียวกันอย่างปลอดภัยซึ่งใช้ในการเชื่อมข้อมูลระหว่างผู้ใช้ในบ้าน

ความปลอดภัยของ SiriKit สำหรับ iOS, iPadOS และ watchOS

Siri ใช้ระบบส่วนขยายของแอปเพื่อสื่อสารกับแอปของบุคคลหรือบริษัทอื่น โดย Siri บนอุปกรณ์สามารถเข้าถึงข้อมูลรายชื่อของผู้ใช้และตำแหน่งที่ตั้งปัจจุบันของอุปกรณ์ได้ แต่ก่อนที่ Siri จะมอบข้อมูลที่มีรหัสปกป้องให้แก่แอปใดแอปหนึ่ง Siri จะตรวจสอบสิทธิ์การเข้าถึงที่ควบคุมได้โดยผู้ใช้ของแอปนั้นก่อน Siri จะส่งเพียงข้อมูลบางส่วนที่เกี่ยวข้องของการพูดของผู้ใช้เดิมไปที่ส่วนขยายแอป โดยจะเป็นไปตามสิทธิ์เหล่านั้น ตัวอย่างเช่น ถ้าแอปไม่มีสิทธิ์เข้าถึงข้อมูลรายชื่อ Siri จะไม่แยกวิเคราะห์ความสัมพันธ์ในคำขอผู้ใช้ เช่น "จ่ายเงินให้แม่ของฉัน 10 ดอลลาร์โดยใช้แอปชำระเงิน" ในกรณีนี้ แอปจะเห็นเฉพาะความหมายตรงตัวของคำว่า "แม่ของฉัน" เท่านั้น

อย่างไรก็ตาม ถ้าผู้ใช้อนุญาตให้แอปเข้าถึงข้อมูลรายชื่อ แอปดังกล่าวก็จะได้รับข้อมูลที่แยกวิเคราะห์แล้วเกี่ยวกับแม่ของผู้ใช้ ถ้าความสัมพันธ์ถูกอ้างอิงในส่วนเนื้อหาของข้อความ ตัวอย่างเช่น "บอกแม่ทาง MessageApp ว่าพี่ชายเจ๋งมาก" Siri จะไม่แยกวิเคราะห์คำว่า "พี่ชายของฉัน" โดยไม่คำนึงถึงสิทธิ์ของแอป

แอปที่สามารถใช้งาน SiriKit ได้สามารถส่งคำศัพท์เฉพาะแอปหรือคำศัพท์เฉพาะผู้ใช้ไปยัง Siri ได้ เช่น ชื่อของรายชื่อของผู้ใช้ ข้อมูลนี้จะอนุญาตให้การจำเสียงพูดและการเข้าใจภาษาธรรมชาติของ Siri สามารถรู้จำคำศัพท์สำหรับแอปนั้นได้ และเกี่ยวข้องกับข้อมูลจำเพาะแบบสุ่ม ข้อมูลแบบกำหนดเองจะยังคงใช้งานได้ตราบเท่าที่ข้อมูลจำเพาะถูกใช้งานอยู่ หรือจนกว่าผู้ใช้จะปิดใช้งานการรวม Siri ของแอปในการตั้งค่า หรือจนกว่าแอปที่สามารถใช้งาน SiriKit ได้ถูกถอนการติดตั้ง

สำหรับการพูดอย่างเช่น "หาเส้นทางไปบ้านคุณแม่โดยใช้ RideShareApp" คำขอดังกล่าวจะต้องใช้ข้อมูลตำแหน่งที่ตั้งจากรายชื่อของผู้ใช้ Siri จะมอบข้อมูลที่ร้องขอไปยังส่วนขยายของแอปสำหรับคำขอดังกล่าวเท่านั้น โดยไม่อิงตามการตั้งค่าสิทธิ์ของผู้ใช้สำหรับตำแหน่งที่ตั้งหรือข้อมูลรายชื่อสำหรับแอปนั้น

ความปลอดภัยของ DriverKit สำหรับ macOS

DriverKit คือเฟรมเวิร์คที่อนุญาตให้นักพัฒนาสร้างไดรเวอร์อุปกรณ์ที่ผู้ใช้ติดตั้งบน Mac ของตนเอง ไดรเวอร์ที่สร้างด้วย DriverKit จะทำงานในพื้นที่ของผู้ใช้แทนที่จะเป็นส่วนขยายเคอร์เนลเพื่อความปลอดภัยและความเสถียรของระบบที่ได้รับการปรับปรุงให้ดียิ่งขึ้น วิธีการนี้ช่วยให้การติดตั้งง่ายขึ้นและเพิ่มความเสถียรและความปลอดภัยสำหรับ macOS

ผู้ใช้เพียงดาวน์โหลดแอป (ไม่จำเป็นต้องใช้ตัวติดตั้งเมื่อใช้ส่วนขยายระบบหรือ DriverKit) แล้วส่วนขยายจะถูกเปิดใช้งานเมื่อจำเป็นเท่านั้น วิธีการเหล่านี้จะแทนที่ kext สำหรับกรณีการใช้งานหลายกรณี ซึ่งต้องใช้สิทธิ์ผู้ดูแลระบบในการติดตั้งใน /System/Library หรือ /Library

สำหรับผู้ดูแลระบบ IT ที่ใช้ไดรเวอร์ของอุปกรณ์ ขอแนะนำให้เปลี่ยนไปใช้โซลูชั่นพื้นที่จัดเก็บข้อมูลคลาวด์ เครือข่ายและแอปความปลอดภัยที่ต้องใช้ส่วนขยายเคอร์เนลในเวอร์ชั่นที่ใหม่กว่าซึ่งสร้างขึ้นบนส่วนขยายระบบ เวอร์ชั่นใหม่เหล่านี้ช่วยลดโอกาสของของเคอร์เนลแพนิกบน Mac ได้เป็นอย่างมาก อีกทั้งยังลดช่องทางการโจมตีให้น้อยลงอีกด้วย ส่วนขยายใหม่เหล่านี้จะทำงานในพื้นที่ของผู้ใช้ ไม่ต้องใช้สิทธิ์พิเศษที่จำเป็นสำหรับการติดตั้ง และจะถูกเอาออกโดยอัตโนมัติเมื่อแอปแบบรวมถูกย้ายไปยังถังขยะ

เฟรมเวิร์ค DriverKit จะมอบคลาส C++ สำหรับบริการ I/O, การจับคู่อุปกรณ์, ตัวอธิบายความจำ และคิวการส่ง นอกจากนี้ เฟรมเวิร์คยังกำหนดประเภท I/O ที่เหมาะสมสำหรับหมายเลข คอลเลกชั่น สตริง และประเภททั่วไปอื่นๆ อีกด้วย ผู้ใช้จะใช้รายการเหล่านี้กับเฟรมเวิร์คไดรเวอร์เฉพาะรุ่น เช่น USBDriverKit และ HIDDriverKit ใช้เฟรมเวิร์คส่วนขยายระบบเพื่อติดตั้งและอัปเกรดไดรเวอร์

ความปลอดภัยของ ReplayKit ใน iOS และ iPadOS

ReplayKit เป็นเฟรมเวิร์คที่อนุญาตให้นักพัฒนาสามารถเพิ่มความสามารถในการบันทึกและการกระจายสัญญาณสดไปยังแอปได้ นอกจากนี้ ยังอนุญาตให้ผู้ใช้อธิบายเสียงบันทึกและการกระจายสัญญาณของผู้ใช้โดยใช้กล้องหน้าและไมโครโฟนของอุปกรณ์ได้อีกด้วย

การบันทึกภาพยนตร์

มีชั้นความปลอดภัยจำนวนมากที่สร้างลงในการบันทึกภาพยนตร์ดังนี้:

- **หน้าต่างโต้ตอบสิทธิ์:** ก่อนเริ่มการบันทึก ReplayKit จะแสดงคำขอการเตือนความยินยอมให้ผู้ใช้เพื่อให้ผู้ใช้รับทราบความตั้งใจในการบันทึกหน้าจอ ไมโครโฟน และกล้องหน้า การเตือนนี้จะแสดงหนึ่งครั้งต่อการทำงานแอปและจะแสดงอีกครั้งหากแอปถูกปล่อยให้ทำงานอยู่เบื้องหลังเป็นระยะเวลานานกว่า 8 นาที
- **การจับภาพหน้าจอและการบันทึกเสียง:** การจับภาพหน้าจอและการบันทึกเสียงจะเกิดขึ้นนอกกระบวนการของแอปในดีมอนของ ReplayKit replayd สิ่งนี้ได้รับการออกแบบมาเพื่อให้แน่ใจว่าเนื้อหาที่บันทึกจะไม่สามารถเข้าถึงกระบวนการแอปได้
- **การจับภาพหน้าจอและการบันทึกเสียงภายในแอป:** วิธีการนี้จะช่วยให้แอปรับวิดีโอและบัฟเฟอร์ตัวอย่างที่ได้รับการป้องกันโดยหน้าต่างโต้ตอบสิทธิ์ได้
- **การสร้างภาพยนตร์และพื้นที่จัดเก็บข้อมูล:** ไฟล์ภาพยนตร์จะเขียนลงในไดเรกทอรีที่สามารถเข้าถึงระบบย่อยของ ReplayKit ได้เท่านั้น และไม่สามารถเข้าถึงแอปใดๆ ได้ วิธีการนี้ช่วยป้องกันไม่ให้บุคคลอื่นใช้เสียงบันทึกโดยไม่ได้รับความยินยอมจากผู้ใช้
- **การแสดงตัวอย่างและการแชร์ของผู้ใช้ปลายทาง:** ผู้ใช้สามารถแสดงตัวอย่างและแชร์ภาพยนตร์ที่มีอินเทอร์เฟซผู้ใช้ที่ ReplayKit ขายได้ อินเทอร์เฟซผู้ใช้แสดงการทำงานอย่างอิสระผ่านโครงสร้างพื้นฐานส่วนขยาย iOS และมีสิทธิ์เข้าถึงไฟล์ภาพยนตร์ที่สร้างขึ้น

การกระจายสัญญาณด้วย ReplayKit

มีชั้นความปลอดภัยจำนวนมากที่สร้างลงในการกระจายสัญญาณภาพยนตร์ดังนี้:

- **การจับภาพหน้าจอและการบันทึกเสียง:** กลไกการจับภาพหน้าจอและการบันทึกเสียงในระหว่างการกระจายสัญญาณเหมือนกันกับการบันทึกภาพยนตร์และเกิดขึ้นใน `replayd`
- **ส่วนขยายการกระจายสัญญาณ:** สำหรับบริการของบริษัทอื่นๆ ในการเข้าร่วมการกระจายสัญญาณด้วย ReplayKit จะต้องสร้างส่วนขยายใหม่สองรายการที่กำหนดค่าโดยมีปลายทาง com.apple.broadcast-services ดังนี้:
  - ส่วนขยายอินเทอร์เฟซผู้ใช้ที่อนุญาตให้ผู้ใช้ตั้งค่าการกระจายสัญญาณของตน
  - ส่วนขยายการอัปโหลดที่จัดการการอัปโหลดข้อมูลวิดีโอและเสียงไปที่เซิร์ฟเวอร์ส่วนหลังของบริการต่างๆ

สถาปัตยกรรมช่วยให้แน่ใจว่าแอปที่โฮสต์ไม่มีสิทธิ์ในเนื้อหาของวิดีโอและเสียงที่มีการกระจายสัญญาณ เฉพาะ ReplayKit และส่วนขยายการกระจายสัญญาณของบริษัทอื่นที่มีสิทธิ์เข้าถึง

- **ตัวเลือกการกระจายสัญญาณ:** ด้วยตัวเลือกการกระจายสัญญาณ ผู้ใช้จะเริ่มต้นการกระจายสัญญาณระบบโดยตรงจากแอปโดยใช้อินเทอร์เฟซผู้ใช้ที่กำหนดด้วยระบบเดียวกันซึ่งสามารถเข้าถึงได้โดยใช้ศูนย์ควบคุม อินเทอร์เฟซผู้ใช้จะปรับใช้โดยใช้ API ส่วนตัวและเป็นส่วนขยายที่อยู่ภายในเฟรมเวิร์ค ReplayKit ตัวเลือกการแสดงระบบจะทำงานอย่างอิสระจากแอปที่โฮสต์
- **ส่วนขยายการอัปโหลด:** ส่วนขยายที่บริการการกระจายสัญญาณของบริษัทอื่นใช้เพื่อจัดการเนื้อหาวิดีโอและเสียงในระหว่างกระจายสัญญาณจะใช้บัฟเฟอร์ตัวอย่างที่ไม่เข้ารหัสแบบไฟล์ดิบ ในระหว่างโหมดของการจัดการนี้ ข้อมูลวิดีโอและเสียงจะถูกทำให้เป็นอนุกรม แล้วส่งไปที่ส่วนขยายการอัปโหลดของบุคคลหรือบริษัทอื่นในแบบเรียลไทม์ผ่านการเชื่อมต่อ XPC โดยตรง ข้อมูลวิดีโอจะเข้ารหัสโดยได้มาจากวัตถุ IOSurface จากบัฟเฟอร์ตัวอย่างวิดีโอ เข้ารหัสอย่างปลอดภัยเป็นวัตถุ XPC ส่งผ่าน XPC ไปยังส่วนขยายของบุคคลหรือบริษัทอื่น แล้วถอดรหัสอย่างปลอดภัยกลับเป็นวัตถุ IOSurface

ความปลอดภัยของ ARKit ใน iOS และ iPadOS

ARKit คือเฟรมเวิร์คที่ช่วยให้นักพัฒนาสร้างประสบการณ์ความจริงเสริมในแอปหรือเกมของตนเอง นักพัฒนาสามารถเพิ่มองค์ประกอบแบบ 2D หรือ 3D โดยใช้กล้องหน้าหรือกล้องหลังของอุปกรณ์ iOS หรือ iPadOS ได้

Apple ออกแบบกล้องต่างๆ โดยคำนึงถึงความเป็นส่วนตัว และแอปของบุคคลหรือบริษัทอื่นจะต้องได้รับการยินยอมจากผู้ใช้ก่อนเข้าถึงกล้อง ใน iOS และ iPadOS เมื่อผู้ใช้ให้สิทธิ์แอปในการเข้าถึงกล้องของตน แอปนั้นจะสามารถเข้าถึงภาพแบบเรียลไทม์ได้จากทั้งกล้องหน้าและกล้องหลัง แอปต่างๆ จะไม่ได้รับอนุญาตให้ใช้กล้องได้โดยปราศจากความโปร่งใสที่บ่งบอกว่ากล้องถูกใช้อยู่

รูปภาพและวิดีโอที่ถ่ายด้วยกล้องอาจมีข้อมูลอื่นๆ เช่น เวลาและสถานที่ที่รูปภาพหรือวิดีโอนั้นถูกบันทึก ระยะชัดลึก และ Overcapture ถ้าผู้ใช้ไม่ต้องการให้รูปภาพและวิดีโอที่ถ่ายด้วยแอปกล้องมีข้อมูลของตำแหน่งที่ตั้ง ผู้ใช้ก็สามารถควบคุมการตั้งค่านี้ได้ตลอดเวลาโดยไปที่ การตั้งค่า > ความเป็นส่วนตัว > บริการหาตำแหน่งที่ตั้ง > กล้อง ถ้าผู้ใช้ไม่ต้องการให้รูปภาพและวิดีโอมีข้อมูลตำแหน่งที่ตั้งเมื่อแชร์ ผู้ใช้สามารถปิดใช้ตำแหน่งที่ตั้งได้ในเมนูตัวเลือกในแผ่นงานการแชร์

ในการปรับประสบการณ์การใช้งาน AR ของผู้ใช้ให้ดียิ่งขึ้น แอปที่ใช้ ARKit สามารถใช้ข้อมูลการติดตามโลกหรือใบหน้าจากกล้องตัวอื่นได้ การติดตามโลกจะใช้อัลกอริทึมบนอุปกรณ์ของผู้ใช้เพื่อประมวลผลข้อมูลจากเซ็นเซอร์เหล่านี้เพื่อกำหนดตำแหน่งของการติดตามที่สัมพันธ์กับพื้นที่ทางกายภาพ การติดตามโลกจะเปิดใช้งานคุณสมบัติต่างๆ เช่น ทิศทางไปข้างหน้าโดยใช้ลำแสงในแอปแผนที่

การจัดการอุปกรณ์อย่างปลอดภัย

ภาพรวมการจัดการอุปกรณ์อย่างปลอดภัย

iOS, iPadOS, macOS และ tvOS รองรับนโยบายและการกำหนดค่าความปลอดภัยแบบยืดหยุ่นที่บังคับใช้และจัดการได้ง่าย ซึ่งจะทำให้องค์กรสามารถปกป้องข้อมูลขององค์กรและช่วยให้มั่นใจได้ว่าพนักงานปฏิบัติตามความต้องการขององค์กรผ่านอุปกรณ์เหล่านั้น ถึงแม้ว่าพวกเขาจะใช้อุปกรณ์ที่จัดหามาเอง ตัวอย่างเช่น เมื่อเข้าร่วมโปรแกรม “นำอุปกรณ์ของคุณมาเอง” (BYOD)

องค์กรสามารถใช้ทรัพยากรต่างๆ เช่น การปกป้องด้วยรหัสผ่าน โปรไฟล์การกำหนดค่า การลบข้อมูลระยะไกล และโซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) ของบริษัทอื่น เพื่อจัดการอุปกรณ์จำนวนมากและรักษาความปลอดภัยของข้อมูลบริษัท ถึงแม้ว่าพนักงานจะเข้าถึงข้อมูลนี้บนอุปกรณ์ของตัวเองก็ตาม

ใน iOS 13 ขึ้นไป, iPadOS 13.1 ขึ้นไป และ macOS 10.15 ขึ้นไป อุปกรณ์ Apple จะรองรับตัวเลือกการลงทะเบียนผู้ใช้แบบใหม่ที่ออกแบบมาเพื่อโปรแกรม BYOD โดยเฉพาะ การลงทะเบียนผู้ใช้มอบอิสระให้กับผู้ใช้เกี่ยวกับอุปกรณ์ของตนเองมากขึ้น ขณะเดียวกันก็เพิ่มเติมความปลอดภัยของข้อมูลขององค์กรโดยการจัดเก็บข้อมูลเหล่านั้นบนดิสก์โวลุ่ม APFS (Apple File System) ที่เข้ารหัสแบบแยกต่างหาก ซึ่งมอบความสมดุลด้านความปลอดภัย ความเป็นส่วนตัว และประสบการณ์ผู้ใช้สำหรับโปรแกรม BYOD ให้ดียิ่งขึ้น

ความปลอดภัยของโมเดลการจับคู่สำหรับ iPhone และ iPad

iOS และ iPadOS ใช้โมเดลการจับคู่เพื่อควบคุมการเข้าถึงอุปกรณ์จากคอมพิวเตอร์โฮสต์ การจับคู่จะสร้างความสัมพันธ์ที่เชื่อถือได้ระหว่างอุปกรณ์กับโฮสต์ที่อุปกรณ์เชื่อมต่ออยู่ซึ่งบ่งบอกโดยการแลกเปลี่ยนกุญแจสาธารณะ iOS และ iPadOS จะใช้สัญลักษณ์ความเชื่อถือนี้เพื่อเปิดใช้งานฟังก์ชั่นเพิ่มเติมกับโฮสต์ที่เชื่อมต่ออยู่เช่นกัน เช่น การเชื่อมข้อมูล ใน iOS 9 ขึ้นไป บริการต่างๆ:

- ที่ต้องใช้การจับคู่จะไม่สามารถเริ่มต้นได้จนกว่าผู้ใช้จะปลดล็อคอุปกรณ์
- จะไม่เริ่มต้นยกเว้นว่าอุปกรณ์จะเพิ่งถูกปลดล็อคมาไม่นาน
- อาจจะ (เช่น ด้วยการเชื่อมข้อมูลรูปภาพ) ต้องใช้อุปกรณ์ที่ปลดล็อคเพื่อเริ่มต้น

กระบวนการจับคู่จำเป็นต้องให้ผู้ใช้ปลดล็อคอุปกรณ์และยอมรับคำขอจับคู่จากโฮสต์ ใน iOS 9 ขึ้นไป ผู้ใช้ยังต้องป้อนรหัสของตัวเองอีกด้วย หลังจากนั้นโฮสต์และอุปกรณ์จะแลกเปลี่ยนและบันทึกกุญแจสาธารณะ RSA 2048 บิต จากนั้น โฮสต์จะได้รับกุญแจ 256 บิตที่สามารถปลดล็อคกระเป๋ากุญแจ (keybag) ของข้อมูลที่ฝาก ซึ่งจัดเก็บอยู่ในอุปกรณ์ได้ กุญแจที่แลกเปลี่ยนกันจะใช้เพื่อเริ่มเซสชั่น SSL แบบเข้ารหัส ซึ่งอุปกรณ์ต้องใช้ก่อนที่ส่งข้อมูลที่มีรหัสปกป้องไปที่โฮสต์หรือเริ่มบริการ (การเชื่อมข้อมูล iTunes หรือ Finder, การถ่ายโอนไฟล์, การพัฒนา Xcode เป็นต้น) ในการใช้เซสชั่นแบบเข้ารหัสนี้กับการสื่อสารทั้งหมด อุปกรณ์จะต้องเชื่อมต่อจากโฮสต์ผ่าน Wi-Fi ดังนั้นจึงต้องเคยจับคู่กันผ่าน USB มาก่อน การจับคู่ยังทำให้สามารถทำการวิเคราะห์หลายอย่างได้อีกด้วย ใน iOS 9 ถ้าไม่ได้ใช้บันทึกการจับคู่เป็นเวลานานกว่า 6 เดือน บันทึกนั้นจะหมดอายุ ใน iOS 11 ขึ้นไป กรอบเวลานี้จะสั้นลงเป็น 30 วัน

บริการการวินิจฉัยบางอย่าง รวมถึง com.apple.mobile.pcapd จะถูกจำกัดให้ทำงานผ่าน USB เท่านั้น นอกจากนี้ บริการ com.apple.file_relay ยังต้องใช้โปรไฟล์กำหนดค่าที่ Apple ลงชื่อรับรองเพื่อติดตั้งอีกด้วย ใน iOS 11 ขึ้นไป Apple TV สามารถใช้โปรโตคอล Secure Remote Password เพื่อสร้างความสัมพันธ์การจับคู่แบบไร้สายได้

ผู้ใช้สามารถล้างรายการโฮสต์ที่เชื่อถือได้ด้วยตัวเลือกรีเซ็ตการตั้งค่าเครือข่ายหรือตัวเลือกรีเซ็ตตำแหน่งที่ตั้งและความเป็นส่วนตัว

การจัดการอุปกรณ์เคลื่อนที่

ภาพรวมความปลอดภัยของการจัดการอุปกรณ์เคลื่อนที่

ระบบปฏิบัติการของ Apple รองรับการจัดการอุปกรณ์เคลื่อนที่ (MDM) ซึ่งทำให้องค์กรสามารถกำหนดค่าและจัดการนำอุปกรณ์ Apple ไปใช้ได้อย่างปลอดภัย

MDM ทำงานอย่างปลอดภัยได้อย่างไร

ความสามารถของ MDM สร้างขึ้นบนเทคโนโลยีระบบปฏิบัติการที่มีอยู่แล้ว เช่น โปรไฟล์การกำหนดค่า การลงทะเบียนผ่านทางอากาศ และบริการการแจ้งผลักข้อมูลของ Apple (APNs) ตัวอย่างเช่น จะใช้ APNs เพื่อปลุกอุปกรณ์เพื่อให้สามารถสื่อสารกับโซลูชั่น MDM ได้โดยตรงผ่านการเชื่อมต่อที่ปลอดภัย ด้วย APNs ข้อมูลลับหรือข้อมูลความเป็นเจ้าของจะไม่ส่งผ่าน

เมื่อใช้ MDM แผนก IT จะสามารถลงทะเบียนอุปกรณ์ Apple ในสภาพแวดล้อมองค์กร กำหนดค่าและอัปเดตการตั้งค่าแบบไร้สาย ตรวจสอบการปฏิบัติตามนโยบายองค์กร จัดการนโยบายรายการอัปเดตซอฟต์แวร์ แม้กระทั่งลบข้อมูลหรือล็อคอุปกรณ์ที่จัดการอยู่จากระยะไกลได้

นอกจากการลงทะเบียนอุปกรณ์แบบดั้งเดิมที่รองรับโดย iOS, iPadOS, macOS และ tvOS แล้ว ยังได้เพิ่มประเภทการลงทะเบียนลงใน iOS 13 ขึ้นไป, iPadOS 13.1 ขึ้นไป และ macOS 10.15 ขึ้นไปด้วย ซึ่งเรียกว่าการลงทะเบียนผู้ใช้ การลงทะเบียนผู้ใช้คือการลงทะเบียน MDM ที่มีเป้าหมายสำหรับการใช้โปรแกรม “การนำอุปกรณ์ของคุณมาเอง” (BYOD) โดยเฉพาะ ซึ่งอุปกรณ์นั้นเป็นอุปกรณ์ส่วนตัวของผู้ใช้แต่ใช้ในสภาพแวดล้อมที่ได้รับการจัดการ การลงทะเบียนผู้ใช้อนุญาตโซลูชั่น MDM ถึงสิทธิ์ที่จำกัดกว่าการลงทะเบียนอุปกรณ์ที่ไม่ได้รับการกำกับดูแล และให้การแยกการเข้ารหัสของข้อมูลผู้ใช้และองค์กร

ประเภทการลงทะเบียน

- **การลงทะเบียนอุปกรณ์แบบอัตโนมัติ:** การลงทะเบียนอุปกรณ์แบบอัตโนมัติช่วยให้องค์กรกำหนดค่าและจัดการอุปกรณ์ได้ทันทีที่อุปกรณ์ถูกแกะออกจากกล่อง (เรียกว่า**การปรับใช้แบบไม่ต้องสัมผัส**) อุปกรณ์เหล่านี้เรียกว่า**อุปกรณ์ที่ได้รับการกำกับดูแล** และผู้ใช้มีตัวเลือกในการป้องกันไม่ให้ผู้ใช้เอาโปรไฟล์ MDM ออก การลงทะเบียนอุปกรณ์แบบอัตโนมัติได้รับการออกแบบสำหรับอุปกรณ์ที่องค์กรเป็นเจ้าของ
- **การลงทะเบียนอุปกรณ์:** การลงทะเบียนอุปกรณ์ทำให้องค์กรสามารถให้ผู้ใช้ลงทะเบียนอุปกรณ์ แล้วจัดการการใช้งานอุปกรณ์ในลักษณะต่างๆ มากมายได้ด้วยตัวเอง รวมถึงความสามารถในการลบอุปกรณ์ การลงทะเบียนอุปกรณ์ยังมีชุดเพย์โหลดขนาดใหญ่ขึ้นและการจำกัดที่สามารถปรับใช้กับอุปกรณ์ได้อีกด้วย เมื่อผู้ใช้เอาโปรไฟล์การลงทะเบียนออก โปรไฟล์การกำหนดค่าทั้งหมด การตั้งค่า และแอปที่ได้รับการจัดการที่อิงตามโปรไฟล์การลงทะเบียนนั้นจะถูกเอาออกไปด้วยเช่นกัน
- **การลงทะเบียนผู้ใช้:** การลงทะเบียนผู้ใช้ได้รับการออกแบบสำหรับอุปกรณ์ที่ผู้ใช้เป็นเจ้าของและจะผสานรวมกับ Apple ID ที่ได้รับการจัดการเพื่อสร้างข้อมูลประจำตัวของผู้ใช้บนอุปกรณ์ Apple ID ที่ได้รับการจัดการเป็นส่วนหนึ่งของโปรไฟล์การลงทะเบียนผู้ใช้ และผู้ใช้ต้องตรวจสอบสิทธิ์ให้เสร็จเรียบร้อยเพื่อลงทะเบียนให้เสร็จสมบูรณ์ Apple ID ที่ได้รับการจัดการสามารถใช้พร้อมกับ Apple ID ส่วนบุคคลที่ผู้ใช้ได้ลงชื่อเข้าไว้อยู่แล้ว แอปและบัญชีที่ได้รับการจัดการใช้ Apple ID ที่ได้รับการจัดการ ส่วนแอปและบัญชีส่วนบุคคลใช้ Apple ID ส่วนบุคคล

การจำกัดอุปกรณ์

การจำกัดสามารถเปิดใช้งานได้ หรือในบางกรณีปิดใช้งานได้โดยผู้ดูแลระบบเพื่อช่วยป้องกันไม่ให้ผู้ใช้เข้าถึงแอป บริการ หรือฟังก์ชั่นของ iPhone, iPad, Mac หรือ Apple TV ที่ลงเบียนในโซลูชั่น MDM การจำกัดจะถูกส่งไปที่อุปกรณ์ในเพย์โหลดการจำกัดซึ่งเป็นส่วนหนึ่งของโปรไฟล์การกำหนดค่า การจำกัดบางอย่างบน iPhone ที่ได้รับการจัดการอาจจะสะท้อนหน้าจอบน Apple Watch ที่จับคู่อยู่

การจัดการการตั้งค่ารหัสและรหัสผ่าน

ตามค่าเริ่มต้นแล้ว จะสามารถกำหนดรหัสของผู้ใช้เป็น PIN ตัวเลขได้ ความยาวขั้นต่ำของรหัสสำหรับอุปกรณ์ iOS และ iPadOS ที่มี Face ID หรือ Touch ID คือสี่หลัก ขอแนะนำให้ใช้รหัสที่ยาวขึ้นและซับซ้อนขึ้นเนื่องจากจะทำให้เดาหรือโจมตีได้ยากขึ้น

ผู้ดูแลระบบสามารถบังคับให้ต้องใช้รหัสแบบซับซ้อนและนโยบายอื่นๆ ได้โดยใช้ MDM หรือ Microsoft Exchange ActiveSync หรือโดยการบังคับให้ผู้ใช้ต้องติดตั้งโปรไฟล์การกำหนดค่าด้วยตัวเอง จำเป็นต้องใช้รหัสผ่านผู้ดูแลระบบสำหรับการติดตั้งเพย์โหลดนโยบายเกี่ยวกับรหัส macOS นโยบายรหัสบางนโยบายสามารถกำหนดความยาว องค์ประกอบ หรือคุณลักษณะอื่นของรหัสได้

การบังคับใช้โปรไฟล์การกำหนดค่า

โปรไฟล์การกำหนดค่าเป็นวิธีหลักที่โซลูชั่น MDM ส่งและจัดการนโยบายและการจำกัดบนอุปกรณ์ที่ได้รับการจัดการ ถ้าองค์กรต้องการกำหนดค่าอุปกรณ์จำนวนมากหรือใส่การตั้งค่าอีเมลแบบกำหนดเอง การตั้งค่าเครือข่าย หรือใบรับรองให้กับอุปกรณ์จำนวนมาก โปรไฟล์การกำหนดค่าคือวิธีที่ปลอดภัยในการดำเนินการดังกล่าว

โปรไฟล์การกำหนดค่า

โปรไฟล์การกำหนดค่าคือไฟล์ XML (ลงท้ายด้วย .mobileconfig) ที่ประกอบด้วยเพย์โหลดที่โหลดการตั้งค่าและข้อมูลการอนุญาตลงบนอุปกรณ์ Apple โปรไฟล์การกำหนดค่าจะกำหนดค่าการตั้งค่า บัญชี การจำกัด และข้อมูลลับโดยอัตโนมัติ ไฟล์เหล่านี้สามารถสร้างได้โดยโซลูชั่น MDM หรือ Apple Configurator สำหรับ Mac หรือสามารถสร้างได้ด้วยตัวเอง ก่อนที่องค์กรจะส่งโปรไฟล์การกำหนดค่าไปยังอุปกรณ์ Apple องค์กรจะต้องลงทะเบียนอุปกรณ์ในโซลูชั่น MDM โดยใช้โปรไฟล์การลงทะเบียน

โปรไฟล์การลงทะเบียน

โปรไฟล์การลงทะเบียน คือโปรไฟล์การกำหนดค่าที่มีเพย์โหลด MDM ซึ่งลงทะเบียนอุปกรณ์ในโซลูชั่น MDM ที่ระบุสำหรับอุปกรณ์นั้น ซึ่งช่วยให้โซลูชั่น MDM สามารถส่งคำสั่งและโปรไฟล์การตั้งค่าไปยังอุปกรณ์และสอบถามลักษณะบางประการของอุปกรณ์ได้ เมื่อผู้ใช้เอาโปรไฟล์การลงทะเบียนออก โปรไฟล์การกำหนดค่าทั้งหมด การตั้งค่า และแอปที่ได้รับการจัดการที่อิงตามโปรไฟล์การลงทะเบียนนั้นจะถูกเอาออกไปด้วยเช่นกัน โปรไฟล์การลงทะเบียนสามารถมีได้เพียงครั้งละหนึ่งรายการบนอุปกรณ์

การตั้งค่าโปรไฟล์การกำหนดค่า

โปรไฟล์การกำหนดค่าจะมีการตั้งค่าจำนวนหนึ่งในเพย์โหลดเฉพาะที่สามารถระบุได้ รวมถึง (แต่ไม่จำกัดเพียง):

- นโยบายเกี่ยวกับรหัสและรหัสผ่าน
- การจำกัดคุณสมบัติของอุปกรณ์ (เช่น ปิดใช้งานกล้อง)
- การตั้งค่าเครือข่ายและ VPN
- การตั้งค่า Microsoft Exchange
- การตั้งค่าเมล
- การตั้งค่าบัญชี
- การตั้งค่าบริการไดเรกทอรี LDAP
- การตั้งค่าบริการปฏิทิน CalDAV
- เอกสารสิทธิ์และกุญแจ
- รายการอัปเดตซอฟต์แวร์

การลงชื่อเข้าและการเข้ารหัสโปรไฟล์

โปรไฟล์กำหนดค่าสามารถลงชื่อเพื่อยืนยันแหล่งที่มาแล้วเข้ารหัสเพื่อช่วยให้การรับรองความสมบูรณ์และปกป้องเนื้อหาได้ โปรไฟล์การกำหนดค่าสำหรับ iOS และ iPadOS ถูกเข้ารหัสโดยใช้ Cryptographic Message Syntax (CMS) ที่ระบุใน RFC 5652 ซึ่งรองรับ 3DES และ AES128

การติดตั้งโปรไฟล์

ผู้ใช้สามารถติดตั้งโปรไฟล์การกำหนดค่าบนอุปกรณ์ของตนได้โดยตรงโดยใช้ Apple Configurator สำหรับ Mac หรือสามารถดาวน์โหลดโดยใช้ Safari, ส่งแนบไปกับข้อความเมล, ถ่ายโอนโดยใช้ AirDrop หรือแอปไฟล์ใน iOS และ iPadOS หรือส่งทางอากาศโดยโซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) เมื่อผู้ใช้ตั้งค่าอุปกรณ์ใน Apple School Manager หรือ Apple Business Manager อุปกรณ์จะดาวน์โหลดและติดตั้งโปรไฟล์สำหรับการลงทะเบียน MDM สำหรับข้อมูลเกี่ยวกับวิธีการเอาโปรไฟล์ออก ให้ดูที่ข้อมูลเบื้องต้นเกี่ยวกับการจัดการอุปกรณ์เคลื่อนที่ใน Apple Platform Deployment

หมายเหตุ: บนอุปกรณ์ที่ได้รับการกำกับดูแล การกำหนดค่าโปรไฟล์ยังสามารถล็อคเข้ากับอุปกรณ์ได้อีกด้วย วิธีนี้ได้รับการออกแบบมาเพื่อป้องกันการเอาออกหรืออนุญาตให้เอาออกโดยใช้รหัสเท่านั้น เนื่องจากองค์กรจำนวนมากใช้อุปกรณ์ iOS และ iPadOS ของตัวเอง จึงสามารถเอาโปรไฟล์การกำหนดค่าที่ผูกมัดอุปกรณ์เข้ากับโซลูชั่น MDM ออกได้ แต่การทำเช่นนั้นจะเอาข้อมูลการกำหนดค่า ข้อมูล และแอปที่ได้รับการจัดการออกด้วยเช่นกัน

การลงทะเบียนอุปกรณ์แบบอัตโนมัติ

องค์กรสามารถลงทะเบียนอุปกรณ์ iOS, iPadOS, macOS และ tvOS ในการจัดการอุปกรณ์เคลื่อนที่ (MDM) โดยอัตโนมัติได้โดยไม่ต้องแตะหรือเตรียมอุปกรณ์ก่อนที่ผู้ใช้จะได้รับ หลังจากที่ลงทะเบียนในบริการใดบริการหนึ่งแล้ว ให้ผู้ดูแลระบบลงชื่อเข้าเว็บไซต์ของบริการ จากนั้นเชื่อมโปรแกรมเข้ากับโซลูชั่น MDM จากนั้นจะสามารถกำหนดอุปกรณ์ที่ซื้อให้กับผู้ใช้ผ่าน MDM ได้ ระหว่างกระบวนการกำหนดค่าอุปกรณ์ การจัดเตรียมมาตรการด้านความปลอดภัยที่เหมาะสมจะสามารถเพิ่มความปลอดภัยให้กับข้อมูลที่สำคัญได้ ตัวอย่างเช่น:

- กำหนดให้ผู้ใช้ตรวจสอบสิทธิ์ในการตั้งค่าครั้งแรกผ่านผู้ช่วยตั้งค่าของอุปกรณ์ Apple ระหว่างการเปิดใช้งาน
- สร้างการกำหนดค่าเบื้องต้นซึ่งให้สิทธิ์การเข้าถึงแบบจำกัด แล้วร้องขอให้มีการกำหนดค่าอุปกรณ์เพิ่มเติมเพื่อเข้าถึงข้อมูลสำคัญ

หลังจากกำหนดผู้ใช้แล้ว จะติดตั้งการกำหนดค่า การจำกัด หรือการควบคุมทั้งหมดที่ MDM ระบุโดยอัตโนมัติ การสื่อสารทั้งหมดระหว่างอุปกรณ์กับเซิร์ฟเวอร์ของ Apple จะถูกเข้ารหัสในระหว่างที่ส่งผ่าน HTTPS (TLS)

และสามารถทำให้กระบวนการตั้งค่าสำหรับผู้ใช้ง่ายขึ้นไปอีกได้ด้วยการเอาขั้นตอนบางอย่างในผู้ช่วยตั้งค่าสำหรับอุปกรณ์ออก เพื่อให้ผู้ใช้สามารถเริ่มต้นใช้งานได้อย่างรวดเร็ว ผู้ดูแลระบบยังสามารถควบคุมว่าผู้ใช้จะสามารถเอาโปรไฟล์ MDM ออกจากอุปกรณ์ได้หรือไม่ ซึ่งจะช่วยให้มั่นใจได้ว่าการจำกัดของอุปกรณ์จะอยู่ในเครื่องตลอดอายุของอุปกรณ์เครื่องนั้น หลังจากแกะกล่องและเปิดใช้งานอุปกรณ์แล้ว อุปกรณ์สามารถลงทะเบียนในโซลูชั่น MDM ขององค์กร และการตั้งค่าการจัดการ แอป และหนังสือทั้งหมดจะถูกติดตั้งตามที่ผู้ดูแลระบบ MDM ระบุไว้

Apple School Manager, Apple Business Manager และ Apple Business Essentials

Apple School Manager, Apple Business Manager และ Apple Business Essentials เป็นบริการสำหรับผู้ดูแลระบบไอทีในการปรับใช้อุปกรณ์ Apple ที่องค์กรซื้อโดยตรงจาก Apple หรือผ่านตัวแทนจำหน่ายและผู้ให้บริการเครือข่ายที่เข้าร่วมที่ได้รับอนุญาตจาก Apple

เมื่อใช้ร่วมกับโซลูชั่น MDM ผู้ดูแลระบบจะสามารถลดความซับซ้อนของขั้นตอนการตั้งค่าสำหรับผู้ใช้ กำหนดการตั้งค่าอุปกรณ์ และสามารถแจกจ่ายแอป รวมถึงหนังสือที่ซื้อในบริการทั้งสามนี้ได้ Apple School Manager ยังผสานรวมกับระบบข้อมูลนักเรียน (SIS) โดยตรงหรือใช้ SFTP และบริการทั้งสามบริการสามารถใช้ System for Cross-domain Identity Management (SCIM) หรือการตรวจสอบสิทธิ์แบบรวมศูนย์ด้วย Microsoft Azure Active Directory (Azure AD) เพื่อให้ผู้ดูแลระบบสามารถสร้างบัญชีได้อย่างรวดเร็ว

Apple ยังคงดำเนินการรับรองตามมาตรฐาน ISO/IEC 27001 และ 27018 เพื่อให้ลูกค้าของ Apple สามารถจัดการกับข้อผูกพันตามระเบียบข้อบังคับและตามสัญญาของตนได้ ใบรับรองเหล่านี้ให้การตรวจสอบอิสระแก่ลูกค้าของเราสำหรับข้อมูลเกี่ยวกับหลักปฏิบัติด้านความเป็นส่วนตัวและความปลอดภัยของ Apple สำหรับระบบที่อยู่ในขอบเขต โปรดดูที่การรับรองความปลอดภัยของบริการอินเทอร์เน็ตของ Apple ในการรับรองแพลตฟอร์ม Apple สำหรับข้อมูลเพิ่มเติม

หมายเหตุ: ในการเรียนรู้ว่ามีโปรแกรมของ Apple ให้บริการในบางประเทศหรือภูมิภาคหรือไม่ ให้ดูที่บทความบริการช่วยเหลือของ Apple ความพร้อมในการให้บริการและวิธีการชำระเงินโปรแกรมของ Apple สำหรับการศึกษาและธุรกิจ

การกำกับดูแลอุปกรณ์

โดยทั่วไป **การกำกับดูแล**หมายถึงอุปกรณ์นั้นจะเป็นขององค์กร ซึ่งจะมอบการควบคุมเพิ่มเติมเกี่ยวกับการกำหนดค่าและการจำกัดของอุปกรณ์ให้กับองค์กร โปรดดูที่เกี่ยวกับการควบคุมดูแลอุปกรณ์ Apple ใน Apple Platform Deployment สำหรับข้อมูลเพิ่มเติม

ความปลอดภัยของการล็อคการเข้าใช้เครื่อง

วิธีที่ Apple บังคับใช้การล็อคการเข้าใช้เครื่องจะแตกต่างกันไป โดยขึ้นอยู่กับว่าอุปกรณ์นั้นเป็น iPhone หรือ iPad, Mac ที่ใช้ Apple Silicon หรือ Mac ที่ใช้ Intel ที่มีชิป Apple T2 Security

ลักษณะการทำงานบน iPhone และ iPad

บนอุปกรณ์ iPhone และ iPad การล็อคการเข้าใช้เครื่องจะถูกบังคับใช้ผ่านกระบวนการเปิดใช้งานหลังจากหน้าจอการเลือก Wi-Fi ในผู้ช่วยตั้งค่าของ iOS และ iPadOS เมื่ออุปกรณ์ระบุว่าเปิดใช้งานอยู่ อุปกรณ์จะส่งคำขอไปยังเซิร์ฟเวอร์ Apple เพื่อรับใบรับรองการเปิดใช้งาน อุปกรณ์ที่ถูกล็อคการเข้าใช้งานจะขอให้ผู้ใช้ใส่เอกสารสิทธิ์ iCloud ของผู้ใช้ที่เปิดใช้งานการล็อคการเข้าใช้เครื่องอยู่ในขณะนั้น ผู้ช่วยตั้งค่า iOS และ iPadOS จะไม่ดำเนินการจนกว่าจะได้รับเอกสารสิทธิ์ที่ถูกต้อง

ลักษณะการทำงานบน Mac ที่ใช้ Apple Silicon

ใน Mac ที่มี Apple Silicon LLB จะตรวจสอบว่ามี LocalPolicy ที่ถูกต้องสำหรับอุปกรณ์นั้น และค่า nonce ของนโยบาย LocalPolicy ตรงกับค่าที่จัดเก็บไว้ในส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัย LLB จะบูตไปยัง recoveryOS หาก:

- ไม่มี LocalPolicy สำหรับ macOS เวอร์ชั่นปัจจุบัน
- LocalPolicy ไม่ถูกต้องสำหรับ macOS เวอร์ชั่นนั้น
- ค่าแฮช Nonce ของ LocalPolicy ไม่ตรงกับแฮชของค่าที่จัดเก็บอยู่ในส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัย

recoveryOS ตรวจพบว่าคอมพิวเตอร์ Mac ไม่ได้เปิดใช้งานอยู่และติดต่อเซิร์ฟเวอร์การเปิดใช้งานเพื่อรับใบรับรองการเปิดใช้งาน ถ้าอุปกรณ์ถูกล็อคการเข้าใช้เครื่อง recoveryOS จะขอให้ผู้ใช้ใส่เอกสารสิทธิ์ iCloud ของผู้ใช้ที่เปิดใช้งานการล็อคการเข้าใช้เครื่องอยู่ในขณะนั้น หลังจากได้รับใบรับรองการเปิดใช้งานที่ถูกต้อง กุญแจใบรับรองการเปิดใช้งานจะถูกใช้เพื่อรับใบรับรอง RemotePolicy คอมพิวเตอร์ Mac ใช้กุญแจ LocalPolicy และใบรับรอง RemotePolicy เพื่อสร้าง LocalPolicy ที่ถูกต้อง LLB จะไม่อนุญาตการบูตของ macOS หากไม่มี LocalPolicy ที่ถูกต้อง

ลักษณะการทำงานบนคอมพิวเตอร์ Mac ที่ใช้ Intel

ใน Mac ที่ใช้ Intel ที่มีชิป T2 เฟิร์มแวร์ของชิป T2 จะตรวจสอบยืนยันว่ามีใบรับรองการเปิดใช้งานที่ถูกต้องก่อนจะอนุญาตให้คอมพิวเตอร์บูตไปยัง macOS เฟิร์มแวร์ UEFI ที่โหลดโดยชิป T2 จะทำหน้าที่สอบถามสถานะการเปิดใช้งานของอุปกรณ์จากชิป T2 และบูตไปยัง recoveryOS แทนที่จะบูตไปยัง macOS หากไม่มีใบรับรองการเปิดใช้งานที่ถูกต้อง recoveryOS ตรวจพบว่า Mac ไม่ได้เปิดใช้งานอยู่และติดต่อเซิร์ฟเวอร์การเปิดใช้งานเพื่อรับใบรับรองการเปิดใช้งาน ถ้าอุปกรณ์ถูกล็อคการเข้าใช้เครื่อง recoveryOS จะขอให้ผู้ใช้ใส่เอกสารสิทธิ์ iCloud ของผู้ใช้ที่เปิดใช้งานการล็อคการเข้าใช้เครื่องอยู่ในขณะนั้น เฟิร์มแวร์ UEFI จะไม่อนุญาตการบูตของ macOS หากไม่มีใบรับรองการเปิดใช้งานที่ถูกต้อง

โหมดสูญหายที่ได้รับการจัดการและการล้างข้อมูลระยะไกล

โหมดสูญหายที่ได้รับการจัดการถูกใช้เพื่อค้นหาอุปกรณ์ที่ได้รับการกำกับดูแลเมื่ออุปกรณ์ดังกล่าวถูกขโมย หลังจากค้นหาพบแล้ว จะสามารถล็อคหรือลบข้อมูลอุปกรณ์จากระยะไกลได้

ภาพรวมโหมดสูญหายที่ได้รับการจัดการ

ถ้าอุปกรณ์ iOS หรือ iPadOS ที่ได้รับการกำกับดูแลที่มี iOS 9 ขึ้นไปสูญหายหรือถูกขโมย ผู้ดูแลระบบการจัดการอุปกรณ์เคลื่อนที่ (MDM) สามารถเปิดใช้งานโหมดสูญหายจากระยะไกลบนอุปกรณ์เครื่องนั้นได้ เมื่อเปิดใช้งานโหมดสูญหายที่ได้รับการจัดการ ผู้ใช้ปัจจุบันจะออกจากระบบและจะปลดล็อคอุปกรณ์ไม่ได้ หน้าจอจะแสดงข้อความที่ผู้ดูแลระบบสามารถกำหนดเองได้ เช่น แสดงเบอร์โทรศัพท์ให้โทรติดต่อเมื่อมีคนพบอุปกรณ์ ผู้ดูแลระบบยังสามารถร้องขอให้อุปกรณ์ส่งตำแหน่งที่ตั้งปัจจุบัน (แม้จะปิดใช้บริการหาตำแหน่งที่ตั้ง) และเลือกส่งเสียงได้อีกด้วย เมื่อผู้ดูแลระบบปิดใช้โหมดสูญหายที่จัดการอยู่ ซึ่งเป็นวิธีเดียวที่จะออกจากโหมดนี้ ผู้ใช้จะได้รับแจ้งการดำเนินการนี้ผ่านข้อความบนหน้าจอล็อคหรือการแจ้งเตือนบนหน้าจอโฮม

การล้างข้อมูลระยะไกล

ผู้ดูแลระบบและผู้ใช้สามารถลบข้อมูลอุปกรณ์ iOS, iPadOS และ macOS จากระยะไกลได้ (การลบข้อมูลระยะไกลโดยอัตโนมัติมีให้ใช้หาก Mac เปิดใช้งาน FileVault อยู่) สามารถทำการลบข้อมูลระยะไกลโดยอัตโนมัติได้โดยการทิ้งกุญแจสื่อออกจากพื้นที่จัดเก็บข้อมูลที่ลบได้ ซึ่งจะทำให้อ่านข้อมูลทั้งหมดไม่ได้ สำหรับการล้างข้อมูลระยะไกลผ่าน Microsoft Exchange ActiveSync อุปกรณ์จะเช็คอินกับเซิร์ฟเวอร์ Microsoft Exchange ก่อนที่จะลบข้อมูล

เมื่อ MDM หรือ iCloud ใช้คำสั่งลบข้อมูลระยะไกล อุปกรณ์ iPhone, iPad, iPod touch หรือ Mac จะส่งข้อมูลการรับรู้กลับไปยังโซลูชั่น MDM แล้วดำเนินการลบข้อมูล

ไม่สามารถลบข้อมูลระยะไกลได้ในสถานการณ์ดังนี้:

- ด้วยการลงทะเบียนผู้ใช้
- ใช้ Microsoft Exchange ActiveSync เมื่อติดตั้งบัญชีด้วยการลงทะเบียนผู้ใช้
- ใช้ Microsoft Exchange ActiveSync หากอุปกรณ์มีการกำกับดูแล

ผู้ใช้ยังสามารถลบข้อมูลในอุปกรณ์ iOS และ iPadOS ที่ครอบครองอยู่ได้โดยใช้แอปการตั้งค่าอีกด้วย และตามที่ได้กล่าวไปแล้ว คุณสามารถตั้งค่าให้อุปกรณ์ iOS และ iPadOS ดำเนินการลบข้อมูลโดยอัตโนมัติหลังจากที่ป้อนรหัสผิดหลายครั้งติดต่อกัน

ความปลอดภัยของ iPad ที่แชร์ใน iPadOS

iPad ที่แชร์คือโหมดหลายผู้ใช้สำหรับใช้ในการใช้งาน iPad โหมดนี้ทำให้ผู้ใช้สามารถแชร์ iPad ในขณะที่ยังคงแยกเอกสารและข้อมูลสำหรับผู้ใช้แต่ละคนได้ ผู้ใช้แต่ละคนจะได้รับจะตำแหน่งจัดเก็บข้อมูลที่สำรองไว้ของตัวเอง ซึ่งถูกใช้เป็นดิสก์โวลุ่ม APFS (Apple File System) ที่ปกป้องด้วยเอกสารสิทธิ์ของผู้ใช้ iPad ที่แชร์ต้องใช้ Apple ID ที่มีการจัดการซึ่งออกและเป็นเจ้าของโดยองค์กร

เมื่อใช้ iPad ที่แชร์ ผู้ใช้สามารถลงชื่อเข้าอุปกรณ์ที่เป็นขององค์กรซึ่งได้รับการกำหนดค่าให้ใช้งานโดยผู้ใช้หลายคนได้ ข้อมูลของผู้ใช้จะถูกแบ่งเป็นไดเรกทอรีที่แยกจากกัน โดยแต่ละไดเรกทอรีจะอยู่ในโดเมนการปกป้องข้อมูลของตัวเอง และจะถูกปกป้องด้วยทั้งสิทธิ์ของ UNIX และ Sandbox ใน iPadOS 13.4 ขึ้นไป ผู้ใช้ยังสามารถลงชื่อเข้าเซสชั่นชั่วคราวได้อีกด้วย เมื่อผู้ใช้ลงชื่อออกจากเซสชั่นชั่วคราว ดิสก์โวลุ่ม APFS ของพวกเขาจะถูกลบ และพื้นที่ที่สำรองไว้จะถูกส่งกลับคืนสู่ระบบ

การลงชื่อเข้า iPad ที่แชร์

จะรองรับทั้ง Apple ID ที่ได้รับการจัดการเดิมและรวมเมื่อลงชื่อเข้า iPad ที่แชร์ ขณะใช้บัญชีร่วมกันเป็นครั้งแรก ระบบจะเปลี่ยนเส้นทางผู้ใช้ไปยังพอร์ทัลการลงชื่อเข้าของผู้ให้บริการข้อมูลจำเพาะ (IdP) หลังจากที่ตรวจสอบสิทธิ์แล้ว จะมีการออกโทเค็นการเข้าถึงระยะสั้นสำหรับสำรองข้อมูล Apple ID ที่ได้รับการจัดการ และกระบวนการเข้าสู่ระบบจะดำเนินการคล้ายกับกระบวนการลงชื่อเข้า Apple ID ที่ได้รับการจัดการ เมื่อลงชื่อเข้าแล้ว ผู้ช่วยตั้งค่าบน iPad ที่แชร์จะแจ้งให้ผู้ใช้สร้างรหัส (เอกสารสิทธิ์) ที่ใช้เพื่อรักษาข้อมูลภายในบนอุปกรณ์ให้ปลอดภัยและตรวจสอบสิทธิ์เพื่อไปยังหน้าจอเข้าสู่ระบบในอนาคต เช่นเดียวกับอุปกรณ์สำหรับผู้ใช้คนเดียว ซึ่งผู้ใช้จะลงชื่อเข้า Apple ID ที่ได้รับการจัดการเพียงครั้งเดียวโดยใช้บัญชีรวม แล้วปลดล็อคอุปกรณ์ด้วยรหัสบน iPad ที่แชร์ ผู้ใช้จะลงชื่อเข้าเพียงครั้งเดียวโดยใช้บัญชีรวม จากนั้นจะใช้รหัสที่สร้างในครั้งต่อๆ ไป

เมื่อผู้ใช้ลงชื่อเข้าโดยไม่มีการตรวจสอบสิทธิ์ร่วมกัน Apple ID ที่ได้รับการจัดการจะถูกตรวจสอบสิทธิ์กับบริการข้อมูลประจำตัว (IDS) ของ Apple โดยใช้โปรโตคอล SRP ถ้าตรวจสอบสิทธิ์สำเร็จ จะได้รับโทเค็นการเข้าถึงระยะสั้นเฉพาะอุปกรณ์ ถ้าผู้ใช้เคยใช้อุปกรณ์มาก่อน ผู้ใช้จะมีบัญชีผู้ใช้ในเครื่องอยู่แล้ว ซึ่งจะปลดล็อคโดยใช้เอกสารสิทธิ์เดียวกัน

ถ้าผู้ใช้ไม่เคยใช้อุปกรณ์มาก่อน หรือกำลังใช้คุณสมบัติเซสชั่นชั่วคราว iPad ที่แชร์จะจัดเตรียม ID ผู้ใช้ใหม่ของ UNIX, ดิสก์โวลุ่ม APFS เพื่อจัดเก็บข้อมูลส่วนบุคคลของผู้ใช้ และพวงกุญแจภายใน เนื่องจากพื้นที่จัดเก็บข้อมูลถูกจัดสรร (สำรอง) ไว้สำหรับผู้ใช้ตอนที่มีการสร้างดิสก์โวลุ่ม APFS พื้นที่ที่เหลืออยู่จึงอาจไม่เพียงพอต่อการสร้างดิสก์โวลุ่มใหม่ ในกรณีดังกล่าว ระบบจะระบุผู้ใช้ที่มีอยู่แล้วเพื่อระบุว่าผู้ใช้คนใดที่เชื่อมข้อมูลไปยังคลาวด์เสร็จสิ้นแล้ว และปลดผู้ใช้คนนั้นออกจากอุปกรณ์เพื่อให้ผู้ใช้คนใหม่ลงชื่อเข้าได้ ในกรณีที่ผู้ใช้ที่มีอยู่ทั้งหมดยังอัปโหลดข้อมูลไปยังคลาวด์ของตนไม่เสร็จสิ้น ซึ่งเกิดขึ้นได้ยาก ผู้ใช้คนใหม่จะไม่สามารถลงชื่อเข้าได้ ในการลงชื่อเข้า ผู้ใช้คนใหม่จะต้องรอให้ข้อมูลของผู้ใช้คนหนึ่งเชื่อมข้อมูลเสร็จสิ้นก่อน หรือจะต้องขอให้ผู้ดูแลระบบบังคับลบบัญชีผู้ใช้ที่มีอยู่แล้ว ซึ่งเสี่ยงต่อการทำให้ข้อมูลสูญหาย

ถ้าอุปกรณ์ไม่ได้เชื่อมต่อกับอินเทอร์เน็ต (เช่น ถ้าผู้ใช้ไม่มีจุดเชื่อมต่อ Wi-Fi) อาจเกิดการตรวจสอบสิทธิ์ขึ้นกับบัญชีในเครื่องในช่วงระยะเวลาที่จำกัด ในสถานการณ์เช่นนั้น เฉพาะผู้ใช้ที่มีบัญชีในเครื่องอยู่ก่อนหน้านี้หรือผู้ใช้ที่มีเซสชั่นชั่วคราวเท่านั้นที่จะสามารถลงชื่อเข้าได้ หลังจากการจำกัดเวลาหมดอายุ ผู้ใช้จะต้องตรวจสอบสิทธิ์ออนไลน์แม้ว่าจะมีบัญชีในเครื่องอยู่แล้วก็ตาม

หลังจากที่บัญชีในเครื่องของผู้ใช้ถูกปลดล็อคหรือถูกสร้างแล้ว ถ้าบัญชีนั้นได้รับการตรวจสอบสิทธิ์จากระยะไกล โทเค็นระยะสั้นที่ออกโดยเซิร์ฟเวอร์ของ Apple จะถูกแปลงเป็นโทเค็น iCloud ที่อนุญาตให้ลงชื่อเข้า iCloud จากนั้นการตั้งค่าของผู้ใช้จะถูกกู้คืนและเอกสารและข้อมูลของผู้ใช้จะถูกเชื่อมข้อมูลจาก iCloud

ขณะที่เซสชั่นของผู้ใช้ยังทำงานอยู่และอุปกรณ์ยังออนไลน์ เอกสารและข้อมูลจะถูกจัดเก็บบน iCloud เมื่อสร้างหรือแก้ไข นอกจากนี้ กลไกเชื่อมข้อมูลเบื้องหลังจะช่วยให้มั่นใจได้ว่าการเปลี่ยนแปลงจะถูกผลักไปที่ iCloud หรือบริการเว็บอื่นๆ โดยใช้เซสชั่นพื้นหลัง NSURLSession หลังจากที่ผู้ใช้ลงชื่อออก หลังจากการเชื่อมข้อมูลเบื้องหลังสำหรับผู้ใช้รายนั้นเสร็จสมบูรณ์ ดิสก์โวลุ่ม APFS ของผู้ใช้จะเลิกการต่อเชื่อม และจะไม่สามารถต่อเชื่อมได้อีกครั้ง หากผู้ใช้ไม่ลงชื่อเข้ากลับมาใหม่

เซสชั่นชั่วคราวจะไม่เชื่อมข้อมูลกับ iCloud และแม้ว่าเซสชั่นชั่วคราวจะสามารถลงชื่อเข้าบริการเชื่อมข้อมูลของบริษัทอื่นได้ เช่น Box หรือ Google Drive ไม่มีคุณสมบัติที่จะเชื่อมข้อมูลต่อไปเมื่อเซสชั่นชั่วคราวสิ้นสุดลง

การลงชื่อออกจาก iPad ที่แชร์

เมื่อผู้ใช้ลงชื่อออกจาก iPad ที่แชร์ กระเป๋ากุญแจ (Keybag) ของผู้ใช้คนนั้นจะถูกล็อคโดยทันทีและแอปทั้งหมดจะถูกปิดระบบ ในการเพิ่มความเร็วกรณีที่ผู้ใช้คนใหม่ลงชื่อเข้า iPadOS จะเลื่อนการทำงานลงชื่อออกตามปกติบางรายการออกไปชั่วคราว แล้วแสดงหน้าต่างเข้าสู่ระบบสำหรับผู้ใช้คนใหม่นั้น ถ้าผู้ใช้ลงชื่อเข้าในช่วงเวลานี้ (ประมาณ 30 วินาที) iPad ที่แชร์จะดำเนินการล้างข้อมูลที่เลื่อนออกไปซึ่งเป็นส่วนหนึ่งของการลงชื่อเข้าบัญชีผู้ใช้ใหม่ อย่างไรก็ตาม ถ้า iPad ที่แชร์ไม่ได้ใช้งาน ระบบจะสั่งทำงานการล้างข้อมูลที่เลื่อนออกไป ในระหว่างระยะการล้างข้อมูล ระบบจะเริ่มการทำงานหน้าต่างเข้าสู่ระบบใหม่คล้ายกับการลงชื่อออกอีกครั้ง

เมื่อเซสชั่นชั่วคราวสิ้นสุดลง iPad ที่แชร์จะดำเนินขั้นตอนการออกจากระบบตามลำดับอย่างสมบูรณ์และลบดิสก์โวลุ่ม APFS ของเซสชั่นชั่วคราวโดยทันที

ความปลอดภัยของ Apple Configurator

Apple Configurator สำหรับ Mac มีการออกแบบที่ยืดหยุ่น ปลอดภัย และเน้นการใช้งานของอุปกรณ์เป็นหลัก ซึ่งช่วยให้ผู้ดูแลระบบกำหนดค่าอุปกรณ์ iOS, iPadOS และ tvOS หนึ่งเครื่องหรือหลายสิบเครื่องที่เชื่อมต่อกับ Mac ผ่าน USB (หรืออุปกรณ์ tvOS ที่จับคู่ผ่าน Bonjour) ได้อย่างรวดเร็วและง่ายดาย ก่อนที่จะมอบอุปกรณ์ให้กับผู้ใช้ด้วย Apple Configurator สำหรับ Mac ผู้ดูแลระบบสามารถอัปเดตซอฟต์แวร์ ติดตั้งแอปและโปรไฟล์การกำหนดค่า เปลี่ยนชื่อและเปลี่ยนภาพพื้นหลังบนอุปกรณ์ ส่งออกข้อมูลอุปกรณ์และเอกสาร และอื่นๆ อีกมากมายได้

Apple Configurator สำหรับ Mac ยังสามารถฟื้นฟูหรือกู้คืนคอมพิวเตอร์ Mac ที่มี Apple Silicon และชิป Apple T2 Security ได้อีกด้วย เมื่อ Mac ได้รับการฟื้นฟูหรือกู้คืนในลักษณะนี้ ไฟล์ที่มีการอัปเดตเล็กน้อยล่าสุดของระบบปฏิบัติการ (macOS, recoveryOS สำหรับ Apple Silicon หรือ sepOS สำหรับ T2) จะถูกดาวน์โหลดอย่างปลอดภัยจากเซิร์ฟเวอร์ Apple และติดตั้งบน Mac โดยตรง หลังจากฟื้นฟูหรือกู้คืนสำเร็จ ไฟล์จะถูกลบออกจาก Mac ที่ใช้ Apple Configurator ผู้ใช้ไม่สามารถตรวจสอบหรือใช้ไฟล์นี้ภายนอก Apple Configurator ได้

ผู้ดูแลระบบยังสามารถเลือกที่จะเพิ่มอุปกรณ์ไปยัง Apple School Manager, Apple Business Manager หรือ Apple Business Essentials โดยใช้ Apple Configurator สำหรับ Mac หรือ Apple Configurator สำหรับ iPhone ได้ แม้ว่าอุปกรณ์จะไม่ได้ซื้อโดยตรงจาก Apple, ตัวแทนจำหน่ายที่ได้รับอนุญาตจาก Apple หรือ ผู้ให้บริการเครือข่ายเซลลูลาร์ที่ได้รับอนุญาต เมื่อผู้ดูแลระบบตั้งค่าอุปกรณ์ที่ลงทะเบียนด้วยตนเอง อุปกรณ์จะทำงานเหมือนกับอุปกรณ์อื่นๆ ในบริการเหล่านั้น โดยมีการควบคุมดูแลและการลงทะเบียนสำหรับการจัดการอุปกรณ์เคลื่อนที่ (MDM) สำหรับอุปกรณ์ที่ไม่ได้ซื้อโดยตรง ผู้ใช้จะมีช่วงเวลา 30 วันในการนำอุปกรณ์ออกจากบริการเหล่านั้น การกำกับดูแล และ MDM

องค์กรยังสามารถใช้ Apple Configurator สำหรับ Mac เพื่อเปิดใช้งานอุปกรณ์ iOS, iPadOS และ tvOS ที่ไม่มีการเชื่อมต่ออินเทอร์เน็ตใดๆ ได้โดยเชื่อมต่อกับ Mac ที่เป็นโฮสต์ที่มีการเชื่อมต่ออินเทอร์เน็ตในขณะที่อุปกรณ์กำลังถูกตั้งค่า ผู้ดูแลระบบสามารถกู้คืน เปิดใช้งาน และเตรียมอุปกรณ์ด้วยการกำหนดค่าที่จำเป็น เช่น แอป โปรไฟล์ และเอกสาร โดยไม่จำเป็นต้องเชื่อมต่อกับ Wi-Fi หรือเครือข่ายเซลลูลาร์ คุณสมบัตินี้ไม่อนุญาตให้ผู้ดูแลระบบบายพาสข้อกำหนดการล็อคการเข้าใช้งานเครื่องที่มีอยู่ ซึ่งตามปกติแล้วต้องใช้ในระหว่างการเปิดใช้งานแบบไม่แชร์อินเทอร์เน็ต

ความปลอดภัยของเวลาหน้าจอ

เวลาหน้าจอเป็นคุณสมบัติในตัวสำหรับการดูและจัดการเวลาที่ผู้ปกครองและบุตรหลานใช้ไปกับแอป เว็บไซต์ และอื่นๆ ผู้ใช้แบ่งเป็นสองประเภท: ผู้ปกครองและบุตรหลาน (ที่มีการจัดการ)

แม้ว่าเวลาหน้าจอจะไม่ใช่คุณสมบัติใหม่ด้านความปลอดภัยของระบบ แต่จำเป็นต้องเข้าใจว่าเวลาหน้าจอจะปกป้องความเป็นส่วนตัวและความปลอดภัยของข้อมูลที่รวบรวมและแชร์ระหว่างอุปกรณ์ได้อย่างไร เวลาหน้าจอสามารถใช้ได้ใน iOS 12 ขึ้นไป, iPadOS 13.1 ขึ้นไป, macOS 10.15 ขึ้นไป และคุณสมบัติบางอย่างของ watchOS 6 ขึ้นไป

ตารางด้านล่างจะอธิบายคุณสมบัติหลักๆ ของเวลาหน้าจอ

คุณสมบัติ	ระบบปฏิบัติการที่รองรับ
ดูข้อมูลการใช้งาน	iOS iPadOS macOS
บังคับใช้การจำกัดเพิ่มเติม	iOS iPadOS macOS watchOS
ตั้งค่าการจำกัดการใช้งานเว็บ	iOS iPadOS macOS
ตั้งค่าการจำกัดแอป	iOS iPadOS macOS watchOS
กำหนดค่าเวลาไม่ใช้งาน	iOS iPadOS macOS watchOS

สำหรับผู้ใช้ที่จัดการการใช้งานอุปกรณ์ของตัวเอง ตัวควบคุมและข้อมูลการใช้งานเวลาหน้าจอสามารถเชื่อมข้อมูลบนอุปกรณ์ทุกเครื่องที่ผูกกับบัญชี iCloud เดียวกันได้โดยใช้การเข้ารหัสแบบต้นทางถึงปลายทาง CloudKit ซึ่งบัญชีของผู้ใช้จะต้องมีการตรวจสอบสิทธิ์สองปัจจัยเปิดใช้งานอยู่ (การเชื่อมข้อมูลจะเปิดอยู่ตามค่าเริ่มต้น) เวลาหน้าจอจะแทนที่คุณสมบัติการจำกัดที่พบใน iOS และ iPadOS เวอร์ชั่นก่อนหน้านี้และคุณสมบัติการควบคุมโดยผู้ปกครองที่พบใน macOS เวอร์ชั่นก่อนหน้านี้

ใน iOS 13 ขึ้นไป, iPadOS 13.1 ขึ้นไป และ macOS 10.15 ขึ้นไป ผู้ใช้เวลาหน้าจอและบุตรหลานที่ได้รับการจัดการจะแชร์การใช้งานบนอุปกรณ์ทุกเครื่องหากบัญชี iCloud เปิดใช้งานการตรวจสอบสิทธิ์สองปัจจัยอยู่ เมื่อผู้ใช้ล้างประวัติ Safari หรือลบแอป ข้อมูลการใช้งานที่เกี่ยวข้องจะถูกเอาออกจากอุปกรณ์และอุปกรณ์ที่เชื่อมข้อมูลทุกเครื่อง

ผู้ปกครองและเวลาหน้าจอ

ผู้ปกครองยังสามารถใช้เวลาหน้าจอบนอุปกรณ์ iOS, iPadOS และ macOS เพื่อทำความเข้าใจและควบคุมการใช้งานของบุตรหลานได้อีกด้วย ถ้าผู้ปกครองเป็นผู้จัดการครอบครัว (ในการแชร์กันในครอบครัวสำหรับ iCloud) จะสามารถดูข้อมูลการใช้งานและจัดการการตั้งค่าเวลาหน้าจอสำหรับบุตรหลานได้ บุตรหลานจะได้รับการแจ้งเมื่อผู้ปกครองเปิดใช้เวลาหน้าจอ และบุตรหลานสามารถตรวจสอบการใช้งานของตัวเองได้เช่นกัน เมื่อผู้ปกครองเปิดใช้เวลาหน้าจอให้บุตรหลาน ผู้ปกครองจะตั้งรหัสเพื่อให้บุตรหลานไม่สามารถเปลี่ยนการตั้งค่าได้ เมื่อบุตรหลานมีอายุที่บรรลุนิติภาวะ (อายุจะแตกต่างกันโดยขึ้นอยู่กับประเทศหรือภูมิภาค) พวกเขาจะสามารถปิดใช้การตรวจสอบนี้ได้

การตั้งค่าข้อมูลการใช้งานและการกำหนดค่าถูกถ่ายโอนระหว่างอุปกรณ์ของผู้ปกครองและบุตรหลานโดยใช้โปรโตคอลบริการข้อมูลประจำตัว (IDS) ของ Apple ที่เข้ารหัสแบบต้นทางถึงปลายทาง ข้อมูลที่เข้ารหัสอาจจะจัดเก็บอยู่ในเซิร์ฟเวอร์ IDS เป็นระยะเวลาสั้นๆ จนกว่าอุปกรณ์ที่รับจะอ่านข้อมูล (ตัวอย่างเช่น ทันทีที่เปิด iPhone, iPad หรือ iPod touch หากปิดเครื่องอยู่) Apple จะไม่สามารถอ่านข้อมูลนี้ได้

การวิเคราะห์เวลาหน้าจอ

ถ้าผู้ใช้เปิดใช้ แชร์การวิเคราะห์ iPhone และ Watch ข้อมูลที่ไม่ระบุชื่อต่อไปนี้เท่านั้นที่จะถูกรวบรวมเพื่อให้ Apple สามารถทำความเข้าใจได้ดียิ่งขึ้นถึงวิธีที่เวลาหน้าจอถูกใช้งาน:

- เวลาหน้าจอเปิดใช้อยู่ในระหว่างผู้ช่วยตั้งค่าหรือในภายหลังในการตั้งค่า
- เปลี่ยนในการใช้งานหมวดหมู่หลังจากสร้างการจำกัดสำหรับการใช้งาน (ภายใน 90 วัน)
- เวลาหน้าจอเปิดใช้อยู่หรือไม่
- เวลาไม่ใช้งานเปิดใช้อยู่หรือไม่
- จำนวนครั้งที่ใช้คำถาม “ขอเวลาเพิ่ม”
- จำนวนแอปที่มีการจำกัด
- จำนวนครั้งที่ผู้ใช้ดูการใช้งานในการตั้งค่าเวลาหน้าจอ ประเภทรายผู้ใช้ และประเภทรายมุมมอง (ภายใน ระยะไกล วิดเจ็ต)
- จำนวนครั้งที่ผู้ใช้ไม่สนใจการจำกัดตามประเภทรายผู้ใช้
- จำนวนครั้งที่ผู้ใช้ลบการจำกัดตามประเภทรายผู้ใช้

ไม่มีข้อมูลการใช้งานแอปหรือเว็บเฉพาะที่รวบรวมโดย Apple เมื่อผู้ใช้เห็นรายการแอปในข้อมูลการใช้เวลาหน้าจอ ไอคอนแอปจะถูกดึงจาก App Store โดยตรง ซึ่งไม่ได้เก็บรักษาข้อมูลใดๆ จากคำขอเหล่านี้

อภิธานศัพท์

กระเป๋ากุญแจ (Keybag) โครงสร้างข้อมูลที่ใช้เพื่อจัดเก็บคอลเลกชั่นคลาสกุญแจ แต่ละประเภท (ผู้ใช้ อุปกรณ์ ระบบ ข้อมูลสำรอง ข้อมูลที่ฝาก หรือข้อมูลสำรอง iCloud) จะมีรูปแบบเดียวกัน

ส่วนหัวประกอบด้วย: เวอร์ชั่น (กำหนดให้มีสี่เวอร์ชั่นใน iOS 12 ขึ้นไป), ประเภท (ระบบ ข้อมูลสำรอง ข้อมูลที่ฝาก หรือข้อมูลสำรอง iCloud), ค่า UUID ของกระเป๋ากุญแจ (Keybag), HMAC หากกระเป๋ากุญแจ (Keybag) มีการลงชื่อ และวิธีการที่ใช้สำหรับห่อคลาสกุญแจ: พันด้วย UID หรือ PBKDF2 พร้อมกับจำนวน salt และ iteration

รายการคลาสกุญแจ: UUID ของกุญแจ, คลาส (คลาสการปกป้องข้อมูลของไฟล์หรือพวงกุญแจ), ประเภทการห่อ (กุญแจที่ได้จาก UID เท่านั้น คือกุญแจที่ได้จาก UID และกุญแจที่ได้จากรหัส), คลาสกุญแจที่ถูกห่อ และกุญแจสาธารณะสำหรับคลาสแบบไม่สมมาตร

กลไกการเข้ารหัส AES ส่วนประกอบฮาร์ดแวร์โดยเฉพาะที่ใช้งาน AES

การเข้าถึงหน่วยความจำโดยตรง (DMA) คุณสมบัติที่ช่วยให้ระบบย่อยของฮาร์ดแวร์เข้าถึงหน่วยความจำหลักได้โดยตรง โดยไม่ผ่าน CPU ได้

การเทียบผังมุมรอยเส้นใต้ผิวหนัง การแสดงเชิงคณิตศาสตร์ของทิศทางและความกว้างของรอยที่ได้มาจากส่วนหนึ่งของลายนิ้วมือ

การปกป้องข้อมูล กลไกป้องกันไฟล์และพวงกุญแจสำหรับอุปกรณ์ Apple ที่รองรับ และอาจหมายถึง API ที่แอปใช้เพื่อปกป้องไฟล์และรายการในพวงกุญแจได้เช่นกัน

การปกป้องความสมบูรณ์ของหน่วยประมวลผลร่วมของระบบ (SCIP) กลไกที่ Apple ใช้ซึ่งได้รับการออกแบบมาเพื่อป้องกันการแก้ไขเฟิร์มแวร์ของหน่วยประมวลผลร่วม

การพัน กระบวนการเปลี่ยนรหัสของผู้ใช้เป็นกุญแจเข้ารหัสและเสริมด้วย UID ของอุปกรณ์ กระบวนการนี้ช่วยทำให้แน่ใจได้ว่าจะต้องทำการโจมตีด้วย Brute-force ในตัวอุปกรณ์ที่ระบุ จึงมีอัตราจำกัดและไม่สามารถโจมตีแบบคู่ขนานได้ อัลกอริทึมการพันคือ PBKDF2 ซึ่งใช้ AES ที่ใส่กุญแจด้วย UID ของอุปกรณ์เป็นฟังก์ชั่นแบบกึ่งสุ่ม (PRF) สำหรับการทำซ้ำแต่ละครั้ง

การสุ่มเค้าโครงพื้นที่ที่อยู่ (ASLR) เทคนิคที่ระบบปฏิบัติการใช้เพื่อทำให้การใช้ประโยชน์จากช่องโหว่ของข้อผิดพลาดของซอฟต์แวร์ยากขึ้นมาก โดยการทำให้แน่ใจว่าไม่สามารถคาดเดาที่อยู่หน่วยความจำและออฟเซ็ตได้ จึงทำให้ไม่สามารถเขียนโค้ดเพื่อเจาะช่องโหว่แบบตายตัว

การห่อกุญแจ การเข้ารหัสกุญแจหนึ่งด้วยอีกกุญแจหนึ่ง โดย iOS และ iPadOS ใช้การห่อกุญแจแบบ NIST AES ตาม RFC 3394

การอนุญาตซอฟต์แวร์ระบบ กระบวนการที่รวมกุญแจการเข้ารหัสที่สร้างอยู่ในฮาร์ดแวร์กับบริการออนไลน์เพื่อตรวจสอบให้แน่ใจว่ามีเพียงซอฟต์แวร์จริงจาก Apple ซึ่งเหมาะสมกับอุปกรณ์ที่รองรับเท่านั้นที่จะถูกส่งมอบและติดตั้งในช่วงเวลาที่อัปเกรด

กุญแจที่ได้จากรหัส (PDK) กุญแจการเข้ารหัสที่ได้จากการเชื่อมโยงรหัสผ่านของผู้ใช้เข้ากับกุญแจ SKP ระยะยาวและ UID ของ Secure Enclave

กุญแจระบบไฟล์ กุญแจที่เข้ารหัสเมตาดาต้าของแต่ละไฟล์ รวมถึงคลาสกุญแจ โดยจะเก็บอยู่ในพื้นที่จัดเก็บข้อมูลที่ลบได้เพื่อทำการลบข้อมูลอย่างรวดเร็ว แทนที่จะเก็บเป็นความลับ

กุญแจรายไฟล์ กุญแจที่ใช้โดยการปกป้องข้อมูลเพื่อเข้ารหัสไฟล์บนระบบไฟล์ กุญแจรายไฟล์จะถูกห่อด้วยคลาสกุญแจและจัดเก็บไว้ในเมตาดาต้าของไฟล์

กุญแจสื่อ ส่วนหนึ่งของลำดับชั้นกุญแจการเข้ารหัสที่ช่วยให้การลบข้อมูลปลอดภัยและทำได้โดยอัตโนมัติ ใน iOS, iPadOS, tvOS และ watchOS กุญแจสื่อจะห่อเมตาดาต้าบนดิสก์โวลุ่มข้อมูล (และถ้าไม่มี ก็จะไม่สามารถเข้าถึงกุญแจรายไฟล์ทั้งหมดได้ ทำให้ไฟล์ที่ปกป้องด้วยการปกป้องข้อมูลไม่สามารถเข้าถึงได้) ใน macOS กุญแจสื่อจะห่อข้อมูลการป้อน เมตาดาต้าทั้งหมด และข้อมูลบนดิสก์โวลุ่มที่ปกป้องด้วย FileVault ในกรณีใดกรณีหนึ่งนี้ การลบข้อมูลของกุญแจสื่อจะทำให้ข้อมูลที่เข้ารหัสไม่สามารถเข้าถึงได้

เงินอุดหนุนด้านความปลอดภัยของ Apple รางวัลที่ Apple มอบให้นักวิจัยที่แจ้งช่องโหว่ที่ส่งผลกระทบต่อระบบปฏิบัติการที่จัดส่งล่าสุดและเกี่ยวข้องกับฮาร์ดแวร์รุ่นล่าสุด

ตัวควบคุม SSD ระบบย่อยฮาร์ดแวร์ที่จัดการสื่อในพื้นที่จัดเก็บข้อมูล (ไดรฟ์โซลิดสเตท)

ตัวควบคุมหน่วยความจำ ระบบย่อยในระบบบนชิปที่ควบคุมอินเทอร์เฟซระหว่างระบบบนชิปและหน่วยความจำหลัก

ตัวระบุแหล่งทรัพยากรสากล (URI) สตริงอักขระที่ระบุแหล่งข้อมูลบนเว็บ

บริการการแจ้งผลักข้อมูลของ Apple (APNs) บริการของ Apple ที่ครอบคลุมทั่วโลก ซึ่งจะนำส่งการแจ้งเตือนแบบผลักข้อมูลไปที่อุปกรณ์ Apple

บริการข้อมูลประจำตัว (IDS) ของ Apple ไดเรกทอรีกุญแจสาธารณะ iMessage, ที่อยู่ APNs, และเบอร์โทรศัพท์และที่อยู่อีเมลของ Apple ใช้เพื่อค้นหากุญแจและที่อยู่อุปกรณ์

บิต Seed ซอฟต์แวร์ บิตสำหรับการใช้งานเฉพาะในกลไก AES ของ Secure Enclave ที่ผนวกกับ UID เมื่อสร้างกุญแจจาก UID บิต Seed ซอฟต์แวร์แต่ละรายการมีบิตล็อคที่สอดคล้องกัน Boot ROM และระบบปฏิบัติการใน Secure Enclave สามารถเปลี่ยนค่าของบิต Seed ซอฟต์แวร์ได้อย่างอิสระตราบเท่าที่บิตล็อคยังไม่ได้ตั้งค่า หลังจากตั้งค่าบิตล็อคแล้ว จะไม่สามารถแก้ไขทั้งบิต Seed ซอฟต์แวร์และบิตล็อคได้ บิต Seed ซอฟต์แวร์และล็อคของซอฟต์แวร์จะถูกรีเซ็ตเมื่อรีบูต Secure Enclave

โปรไฟล์การกำหนดสิทธิ์ ไฟล์รายการคุณสมบัติ (ไฟล์ .plist) ที่ลงชื่อโดย Apple ซึ่งมีชุดเอนทิตี้และสิทธิ์ที่ทำให้สามารถติดตั้งและทดสอบแอปต่างๆ บนอุปกรณ์ iOS หรือ iPadOS ได้ โปรไฟล์การกำหนดสิทธิ์การพัฒนาจะแสดงรายการอุปกรณ์ที่นักพัฒนาเลือกเพื่อแจกจ่ายเป็นการเฉพาะกิจ และโปรไฟล์การกำหนดสิทธิ์การแจกจ่ายจะมี ID แอปของแอปที่องค์กรพัฒนา

พวงกุญแจ โครงสร้างพื้นฐานและชุด API ที่ระบบปฏิบัติการของ Apple และแอปของบุคคลหรือบริษัทอื่นใช้เพื่อจัดเก็บและดึงข้อมูลรหัสผ่าน กุญแจ และข้อมูลยืนยันตัวตนที่เป็นความลับอื่นๆ

พื้นที่จัดเก็บข้อมูลที่ลบได้ พื้นที่หนึ่งในพื้นที่จัดเก็บข้อมูล NAND ที่ใช้จัดเก็บกุญแจเข้ารหัสโดยเฉพาะ ซึ่งสามารถจัดการได้โดยตรงและสามารถลบข้อมูลได้อย่างปลอดภัย ถึงแม้ว่าพื้นที่นี้จะไม่สามารถปกป้องข้อมูลหากอุปกรณ์อยู่ในครอบครองของผู้โจมตีแต่กุญแจที่เก็บอยู่ในพื้นที่จัดเก็บข้อมูลที่ลบได้จะสามารถใช้เป็นส่วนหนึ่งของลำดับชั้นกุญแจเพื่อทำการลบข้อมูลอย่างรวดเร็วและใช้ในการช่วยป้องกันภัยจากการโจมตีที่อาจเกิดขึ้นในอนาคต

เฟิร์มแวร์ Unified Extensible Firmware Interface (UEFi) เทคโนโลยีทดแทนสำหรับ BIOS เพื่อเชื่อมต่อเฟิร์มแวร์กับระบบปฏิบัติการของคอมพิวเตอร์

โมดูลรักษาความปลอดภัยฮาร์ดแวร์ (HSM) คอมพิวเตอร์ที่ทนต่อการแทรกแซงเป็นพิเศษซึ่งจะปกป้องและจัดการกุญแจดิจิตอล

ระบบบนชิป (SoC) วงจรรวม (IC) ที่รวมองค์ประกอบหลายส่วนไว้ในชิปชิ้นเดียว หน่วยประมวลผลแอปพลิเคชัน, Secure Enclave และหน่วยประมวลผลร่วมอื่นๆ เป็นส่วนประกอบของ SoC

วงจรรวม (IC) มีอีกชื่อหนึ่งว่า**ไมโครชิป**

ส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัย ชิปที่ออกแบบด้วยโค้ด RO ที่ไม่เปลี่ยนรูป ตัวสร้างหมายเลขแบบสุ่มในระดับฮาร์ดแวร์ กลไกการเข้ารหัส และการตรวจจับการดัดแปลงทางกายภาพ บนอุปกรณ์ที่รองรับ Secure Enclave จะจับคู่กับส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัยสำหรับพื้นที่จัดเก็บข้อมูลค่า Nonce ป้องกันการเล่นซ้ำ ในการอ่านและอัปเดตค่า Nonce นั้น Secure Enclave และชิปสำหรับจัดเก็บข้อมูลจะใช้โปรโตคอลความปลอดภัยที่ช่วยรับรองการเข้าถึงแบบพิเศษให้กับค่า Nonce เทคโนโลยีนี้มีหลากหลายรุ่น ซึ่งมีการรับประกันความปลอดภัยที่แตกต่างกันไป

หน่วยการจัดการหน่วยความจำข้อมูลเข้า/ข้อมูลออก (IOMMU) หน่วยการจัดการหน่วยความจำข้อมูลเข้า/ข้อมูลออก ระบบย่อยในชิปที่รวมเข้ามาซึ่งควบคุมการเข้าถึงพื้นที่ที่อยู่จากอุปกรณ์และอุปกรณ์ต่อพ่วงข้อมูลเข้า/ข้อมูลออกอื่นๆ

โหมดการกู้คืน โหมดที่ใช้กู้คืนอุปกรณ์ Apple หลายเครื่องหากไม่รู้จักอุปกรณ์ของผู้ใช้ ผู้ใช้จึงสามารถติดตั้งระบบปฏิบัติการอีกครั้งได้

โหมดอัปเกรดเฟิร์มแวร์อุปกรณ์ (DFU) โหมดที่โค้ด Boot ROM ของอุปกรณ์จะรอให้กู้คืนผ่าน USB หน้าจอจะเป็นสีดำเมื่ออยู่ในโหมด DFU แต่เมื่อเชื่อมต่อกับคอมพิวเตอร์ที่ใช้ iTunes หรือ Finder จะแจ้งข้อความต่อไปนี้: “iTunes (หรือ Finder) ตรวจพบ (iPad, iPhone หรือ iPod touch) ในโหมดการกู้คืน ผู้ใช้ต้องกู้คืน (iPad, iPhone หรือ iPod touch) เครื่องนี้ก่อนจึงจะสามารถใช้กับ iTunes (หรือ Finder) ได้”

อัลกอริทึมลายเซ็นดิจิตอลแบบเส้นโค้งรูปไข่ (ECDSA) อัลกอริทึมลายเซ็นดิจิตอลอิงตามการเข้ารหัสเส้นโค้งรูปไข่

AES (มาตรฐานการเข้ารหัสขั้นสูง) มาตรฐานการเข้ารหัสที่ได้รับความนิยมทั่วโลกสำหรับใช้เข้ารหัสข้อมูลเพื่อทำให้เป็นส่วนตัว

AES-XTS โหมดของ AES ที่ระบุอยู่ใน IEEE 1619-2007 ซึ่งทำหน้าที่เข้ารหัสสื่อในพื้นที่จัดเก็บข้อมูล

APFS (Apple File System) ระบบไฟล์เริ่มต้นสำหรับ iOS, iPadOS, tvOS, watchOS และคอมพิวเตอร์ Mac ที่ใช้ macOS 10.13 ขึ้นไป APFS มีคุณสมบัติที่โดดเด่นต่างๆ เช่น การเข้ารหัสที่ปลอดภัย การแชร์พื้นที่ สแนปช็อต การปรับขนาดไดเรกทอรีอย่างรวดเร็ว และพื้นฐานระบบไฟล์ที่ปรับปรุงแล้ว

Apple Business Manager พอร์ทัลบนเว็บที่เรียบง่ายสำหรับผู้ดูแลระบบ IT ซึ่งมอบวิธีที่รวดเร็วและมีประสิทธิภาพเพื่อให้องค์กรสามารถปรับใช้อุปกรณ์ของ Apple ที่ได้ซื้อจาก Apple โดยตรงหรือจากตัวแทนจำหน่ายที่ได้รับอนุญาตจาก Apple หรือผู้ให้บริการ องค์กรสามารถลงทะเบียนอุปกรณ์ในโซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) โดยอัตโนมัติได้โดยไม่ต้องแตะหรือเตรียมอุปกรณ์ก่อนที่ผู้ใช้จะได้รับ

Apple School Manager พอร์ทัลบนเว็บที่เรียบง่ายสำหรับผู้ดูแลระบบ IT ซึ่งมอบวิธีที่รวดเร็วและมีประสิทธิภาพเพื่อให้องค์กรสามารถปรับใช้อุปกรณ์ของ Apple ที่ได้ซื้อจาก Apple โดยตรงหรือจากตัวแทนจำหน่ายที่ได้รับอนุญาตจาก Apple หรือผู้ให้บริการ องค์กรสามารถลงทะเบียนอุปกรณ์ในโซลูชั่นการจัดการอุปกรณ์เคลื่อนที่ (MDM) โดยอัตโนมัติได้โดยไม่ต้องแตะหรือเตรียมอุปกรณ์ก่อนที่ผู้ใช้จะได้รับ

Boot Camp ยูทิลิตี้ Mac ที่รองรับการติดตั้ง Microsoft Windows บนคอมพิวเตอร์ Mac ที่รองรับ

Boot Progress Register (BPR) ชุดของธงฮาร์ดแวร์ระบบบนชิป (SoC) ที่ซอฟต์แวร์สามารถใช้ในการติดตามโหมดการบูตที่อุปกรณ์ใช้ได้ เช่น โหมดอัปเดตเฟิร์มแวร์อุปกรณ์ (DFU) และโหมดการกู้คืน หลังจากที่ตั้งค่าธง Boot Progress Register แล้ว ธงดังกล่าวจะไม่สามารถลบออกได้ วิธีการนี้จะอนุญาตให้ซอฟต์แวร์สามารถรับตัวบ่งชี้ที่เชื่อถือแล้วของสถานะของระบบได้

Boot ROM โค้ดแรกสุดที่หน่วยประมวลผลของอุปกรณ์จะดำเนินการเมื่อบูตเป็นครั้งแรก เนื่องจากเป็นส่วนสำคัญของหน่วยประมวลผล จึงไม่สามารถดัดแปลงได้ทั้งโดย Apple หรือผู้โจมตี

CKRecord พจนานุกรมของคู่ค่ากุญแจที่มีข้อมูลที่บันทึกไปยังหรือดึงข้อมูลจาก CloudKit

Data Vault กลไกที่บังคับใช้โดยเคอร์เนลเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตไม่ว่าแอปที่ร้องขอจะอยู่ใน Sandbox หรือไม่ก็ตาม

Elliptic Curve Diffie-Hellman Exchange Ephemeral (ECDHE) กลไกการแลกเปลี่ยนกุญแจตามเส้นโค้งรูปไข่ ECDHE จะอนุญาตให้ทั้งสองฝ่ายยินยอมที่จะใช้กุญแจลับที่สามารถป้องกันไม่ให้ผู้ที่แอบอ่านข้อความจากทั้งสองฝ่ายค้นพบกุญแจได้

Enhanced Serial Peripheral Interface (eSPI) บัสแบบออลอินวันที่ออกแบบมาสำหรับการสื่อสารที่เชื่อมข้อมูลแบบเป็นชุด

Exclusive Chip Identification (ECID) ตัวระบุแบบ 64 บิตที่เป็นเอกลักษณ์เฉพาะประจำหน่วยประมวลผลในอุปกรณ์ iOS และ iPadOS แต่ละเครื่อง เมื่อรับสายบนอุปกรณ์เครื่องหนึ่ง เสียงเรียกเข้าของอุปกรณ์ที่จับคู่ผ่าน iCloud ที่อยู่ใกล้เคียงจะหยุดลงโดยการโฆษณาผ่านบลูทูธพลังงานต่ำ (BLE) 4.0 เป็นเวลาสั้นๆ ไบต์ของการประกาศจะถูกเข้ารหัสโดยใช้วิธีการเดียวกับการแจ้งของ Handoff โดยจะใช้เป็นส่วนหนึ่งของกระบวนการปรับแต่งเป็นเฉพาะบุคคล และไม่ถือว่าเป็นความลับ

Gatekeeper ใน macOS มีเทคโนโลยีที่ออกแบบมาเพื่อช่วยให้มั่นใจว่าจะมีเพียงซอฟต์แวร์ที่เชื่อถือได้เท่านั้นที่ทำงานบน Mac ของผู้ใช้

HMAC รหัสการตรวจสอบสิทธิ์ข้อความแบบแฮชที่อิงจากฟังก์ชั่นแฮชการเข้ารหัส

iBoot Bootloader ขั้นที่ 2 สำหรับอุปกรณ์ Apple ทั้งหมด โค้ดที่โหลด XNU ซึ่งเป็นส่วนหนึ่งของลำดับการบูตอย่างปลอดภัย ขึ้นอยู่กับรุ่นของระบบบนชิป (SoC) iBoot อาจถูกโหลดโดย Low Level Bootloader หรือโหลดโดยตรงโดย Boot ROM

ID กลุ่ม (GID) เหมือน UID แต่จะเป็นข้อมูลทั่วไปของหน่วยประมวลผลทั้งหมดในคลาส

ID เฉพาะ (UID) กุญแจ AES แบบ 256 บิตที่ผู้ผลิตเขียนลงบนหน่วยประมวลผลแต่ละตัว ซึ่งเฟิร์มแวร์หรือซอฟต์แวร์จะอ่านไม่ได้ และจะใช้โดยกลไก AES ของฮาร์ดแวร์ของหน่วยประมวลผลเท่านั้น ในการรับกุญแจของจริง ผู้โจมตีจะต้องโจมตีซิลิคอนของหน่วยประมวลผลด้วยวิธีการทางกายภาพที่ซับซ้อนและมีราคาแพง UID ไม่เกี่ยวข้องกับข้อมูลจำเพาะอื่นใดบนอุปกรณ์ รวมถึงแต่ไม่จำกัดเพียง UDID

Joint Test Action Group (JTAG) เครื่องมือแก้ไขข้อผิดพลาดฮาร์ดแวร์มาตรฐานที่โปรแกรมเมอร์และนักพัฒนาวงจรใช้

Low Level Bootloader (LLB) บนคอมพิวเตอร์ Mac ที่มีสถาปัตยกรรมการบูตสองขั้นตอน LLB มีโค้ดที่ใช้งานโดย Boot ROM ดังนั้นจึงโหลด iBoot ด้วย เพื่อเป็นส่วนหนึ่งของลำดับการบูตอย่างปลอดภัย

Mobile Device Management (MDM) บริการที่ช่วยให้ผู้ดูแลระบบจัดการอุปกรณ์ที่ลงทะเบียนจากระยะไกล หลังจากลงทะเบียนอุปกรณ์แล้ว ผู้ดูแลระบบสามารถใช้บริการ MDM ผ่านเครือข่ายเพื่อกำหนดการตั้งค่าและทำงานอื่นๆ บนอุปกรณ์ได้โดยไม่ต้องโต้ตอบกับผู้ใช้

NAND หน่วยความจำแฟลชแบบถาวร

nonce หมายเลขครั้งเดียวที่ไม่ซ้ำกันที่ใช้ในโปรโตคอลความปลอดภัยต่างๆ

Sealed Key Protection (SKP) เทคโนโลยีการปกป้องข้อมูลที่จะปกป้องหรือ**ปิดผนึก**กุญแจการเข้ารหัสด้วยเคณฑ์ของซอฟต์แวร์และกุญแจของระบบที่มีเฉพาะในฮาร์ดแวร์ (เช่น UID ของ Secure Enclave)

sepOS เฟิร์มแวร์ Secure Enclave ซึ่งอิงจากไมโครเคอร์เนล L4 เวอร์ชั่นที่ Apple กำหนดเอง

xART ตัวย่อสำหรับเทคโนโลยีป้องกันการเล่นซ้ำแบบขยาย ชุดของบริการที่ให้บริการพื้นที่จัดเก็บข้อมูลถาวรที่เข้ารหัสและมีการตรวจสอบสิทธิ์สำหรับ Secure Enclave โดยมีความสามารถในการป้องกันการเล่นซ้ำตามสถาปัตยกรรมของที่จัดเก็บข้อมูล ดูส่วนประกอบพื้นที่จัดเก็บข้อมูลอย่างปลอดภัย

XNU เคอร์เนลที่เป็นหัวใจสำคัญของระบบปฏิบัติการของ Apple ซึ่งจะถูกอนุมานว่าเชื่อถือได้ และบังคับใช้มาตรการรักษาความปลอดภัยต่างๆ เช่น การลงชื่อโค้ด, Sandbox, การตรวจสอบสิทธิ์ และการสุ่มเค้าโครงพื้นที่ที่อยู่ (ASLR)

XProtect ใน macOS มีเทคโนโลยีป้องกันไวรัสสำหรับการตรวจจับและกำจัดมัลแวร์ด้วยลายเซ็น

ประวัติการแก้ไขเอกสาร

ประวัติการแก้ไขเอกสาร

วันที่	เนื้อหาสรุป
ธันวาคม 2022	หัวข้อที่เพิ่ม: • การปกป้องข้อมูลขั้นสูงสำหรับ iCloud หัวข้อที่อัปเดต: • ภาพรวมความปลอดภัยของ iCloud • การเข้ารหัส iCloud • ความปลอดภัยของข้อมูลสำรอง iCloud • ความปลอดภัยของผู้ติดต่อการกู้คืนบัญชี • ความปลอดภัยของผู้ติดต่อรับมรดก

วันที่	เนื้อหาสรุป
พฤษภาคม 2022	อัปเดตสำหรับ: • iOS 15.4 • iPadOS 15.4 • macOS 12.3 • tvOS 15.4 • watchOS 8.5 หัวข้อที่เพิ่ม: • ข้อจำกัดสำหรับ recoveryOS ที่จับคู่แล้ว • Local Operating System Version (love) • การแชร์ข้อมูลสุขภาพ • ความปลอดภัยของผู้ติดต่อการกู้คืนบัญชี • ความปลอดภัยของผู้ติดต่อรับมรดก • Tap to Pay on iPhone อย่างปลอดภัย • การเข้าถึงโดยใช้กระเป๋าสตางค์ • การเข้าถึงประเภทข้อมูลประจำตัว • บัตรประจำตัวในกระเป๋าสตางค์ • อุปกรณ์เสริม HomeKit ที่รองรับ Siri หัวข้อที่อัปเดต: • Magic Keyboard ที่มี Touch ID • Face ID, Touch ID, รหัส และรหัสผ่าน • ความปลอดภัยของการจับคู่ใบหน้า • บัตรโดยสารด่วนที่มีพลังงานสำรอง • โหมดการบูตสำหรับ Mac ที่ใช้ Apple Silicon • เนื้อหาของไฟล์ LocalPolicy สำหรับ Mac ที่ใช้ Apple Silicon • ความปลอดภัยของดิสก์โวลุ่มระบบที่ลงชื่อใน iOS, iPadOS และ macOS • ความปลอดภัยของระบบสำหรับ watchOS • อุปกรณ์การวิจัยด้านความปลอดภัยของ Apple • บทบาทของ Apple File System • การปกป้องการเข้าถึงข้อมูลผู้ใช้ของแอป • ข้อมูลเบื้องต้นเกี่ยวกับความปลอดภัยของแอปสำหรับ macOS • การป้องกันมัลแวร์ใน macOS • ภาพรวมความปลอดภัยของ iCloud • การเชื่อมข้อมูลพวงกุญแจที่ปลอดภัย • การกู้คืนพวงกุญแจ iCloud ที่ปลอดภัย • การชำระเงินด้วยบัตรโดยใช้ Apple Pay • บัตรผ่านแบบไร้การสัมผัสใน Apple Pay • การทำให้บัตรใช้งานไม่ได้ด้วย Apple Pay • การสมัคร Apple Card • ความปลอดภัยของ Apple Cash • การเพิ่มบัตรโดยสารและบัตร eMoney ไปยังกระเป๋าสตางค์ • Apple Messages for Business ที่ปลอดภัย • ความปลอดภัยของ FaceTime • ความปลอดภัยของกุญแจรถใน iOS • ความปลอดภัยของ Apple Configurator หัวข้อที่ถูกเอาออก: • อุปกรณ์เสริม HomeKit และ iCloud

วันที่	เนื้อหาสรุป
พฤษภาคม 2021	อัปเดตสำหรับ: • iOS 14.5 • iPadOS 14.5 • macOS 11.3 • tvOS 14.5 • watchOS 7.4 หัวข้อที่เพิ่ม: • Magic Keyboard ที่มี Touch ID • ความตั้งใจที่ปลอดภัยและการเชื่อมต่อกับ Secure Enclave • ปลดล็อคอัตโนมัติ และ Apple Watch • แฮชรายการ Image4 CustomOS (coih) หัวข้อที่แก้ไข: • เพิ่มสองธุรกรรมโหมดเร่งด่วนใหม่ในบัตรเร่งด่วนที่มีพลังงานสำรอง • เนื้อหาสรุปของคุณสมบัติ Secure Enclave ที่ได้รับการแก้ไข • เนื้อหารายการอัปเดตซอฟต์แวร์ถูกเพิ่มไปยังการบูตหลายรายการอย่างปลอดภัย (smb3) • เนื้อหาเพิ่มเติมสำหรับ Sealed Key Protection (SKP)

วันที่	เนื้อหาสรุป
กุมภาพันธ์ 2021	อัปเดตสำหรับ: • iOS 14.3 • iPadOS 14.3 • macOS 11.1 • tvOS 14.3 • watchOS 7.2 หัวข้อที่เพิ่ม: • การใช้ iBoot ที่ปลอดภัยสำหรับหน่วยความจำ • กระบวนการบูตสำหรับ Mac ที่ใช้ Apple Silicon • โหมดการบูตสำหรับ Mac ที่ใช้ Apple Silicon • การควบคุมนโยบายความปลอดภัยดิสก์เริ่มต้นระบบสำหรับ Mac ที่ใช้ Apple Silicon • การสร้างและการจัดการกุญแจที่ลงชื่อ LocalPolicy • เนื้อหาของไฟล์ LocalPolicy สำหรับ Mac ที่ใช้ Apple Silicon • ความปลอดภัยของดิสก์โวลุ่มระบบที่ลงชื่อใน iOS, iPadOS และ macOS • อุปกรณ์การวิจัยด้านความปลอดภัยของ Apple • การตรวจสอบรหัสผ่าน • ความปลอดภัยของ IPv6 • ความปลอดภัยของกุญแจรถใน iOS หัวข้อที่อัปเดต: • Secure Enclave • การเลิกเชื่อมต่อไมโครโฟนฮาร์ดแวร์ • recoveryOS และสภาพแวดล้อมการวินิจฉัยสำหรับ Mac ที่ใช้ Intel • การปกป้องการเข้าถึงหน่วยความจำโดยตรงสำหรับคอมพิวเตอร์ Mac • ส่วนขยายเคอร์เนลใน macOS • การปกป้องความสมบูรณ์ของระบบ • ความปลอดภัยของระบบสำหรับ watchOS • การจัดการ FileVault ใน macOS • การเข้าถึงของแอปไปยังรหัสผ่านที่บันทึกไว้ • คำแนะนำสำหรับความปลอดภัยของรหัสผ่าน • ความปลอดภัยของ Apple Cash • Apple Messages for Business ที่ปลอดภัย • ความเป็นส่วนตัวของ Wi-Fi • ความปลอดภัยของการล็อคการเข้าใช้เครื่อง • ความปลอดภัยของ Apple Configurator

วันที่	เนื้อหาสรุป
เมษายน 2020	อัปเดตสำหรับ: • iOS 13.4 • iPadOS 13.4 • macOS 10.15.4 • tvOS 13.4 • watchOS 6.2 รายการอัปเดต: • การเลิกเชื่อมต่อไมโครโฟนของ iPad ถูกเพิ่มไปยัง การเลิกเชื่อมต่อไมโครโฟนฮาร์ดแวร์ • เพิ่ม Data Vault ไปที่ การปกป้องการเข้าถึงข้อมูลผู้ใช้ของแอป • รายการอัปเดตสำหรับการจัดการ FileVault ใน macOS และเครื่องมือบรรทัดคำสั่ง • การเพิ่มเครื่องมือสำหรับเอามัลแวร์ออกในการป้องกันจากมัลแวร์ใน macOS • รายการอัปเดตสำหรับความปลอดภัยของ iPad ที่แชร์ใน iPadOS
ธันวาคม 2019	ผสานคู่มือความปลอดภัยของ iOS ภาพรวมความปลอดภัยของ macOS และภาพรวมชิป Apple T2 Security อัปเดตสำหรับ: • iOS 13.3 • iPadOS 13.3 • macOS 10.15.2 • tvOS 13.3 • watchOS 6.1.1 การควบคุมความเป็นส่วนตัว, Siri และคำแนะนำโดย Siri และการป้องกันการติดตามอัจฉริยะบน Safari ได้ถูกเอาออกแล้ว ให้ดูที่ https://www.apple.com/th/privacy/ สำหรับข้อมูลล่าสุดเกี่ยวกับคุณสมบัติเหล่านั้น
พฤษภาคม 2019	อัปเดตสำหรับ iOS 12.3 • รองรับ TLS 1.3 • คำอธิบายฉบับแก้ไขของความปลอดภัยของ AirDrop • โหมด DFU และโหมดการกู้คืน • ข้อกำหนดการตั้งรหัสสำหรับการเชื่อมต่อกับอุปกรณ์เสริม
พฤศจิกายน 2018	อัปเดตสำหรับ iOS 12.1 • FaceTime แบบกลุ่ม
กันยายน 2018	อัปเดตสำหรับ iOS 12 Secure Enclave • การปกป้องความสมบูรณ์ของ OS • บัตรโดยสารด่วนที่มีพลังงานสำรอง • โหมด DFU และโหมดการกู้คืน • อุปกรณ์เสริม HomeKit TV Remote • บัตรผ่านแบบไร้การสัมผัส • บัตรนักเรียน • คำแนะนำโดย Siri • คำสั่งลัดใน Siri • แอปคำสั่งลัด • การจัดการรหัสผ่านของผู้ใช้ • เวลาหน้าจอ • การรับรองความปลอดภัยและโปรแกรม

วันที่	เนื้อหาสรุป
กรกฎาคม 2018	อัปเดตสำหรับ iOS 11.4 • นโยบายทางชีวมิติ • HomeKit • Apple Pay • การสนทนาทางธุรกิจ • แอปข้อความบน iCloud • Apple Business Manager
ธันวาคม 2017	อัปเดตสำหรับ iOS 11.2 • Apple Pay Cash
ตุลาคม 2017	อัปเดตสำหรับ iOS 11.1 • การรับรองความปลอดภัยและโปรแกรม • Touch ID/Face ID • โน้ตที่แชร์ • การเข้ารหัสแบบต้นทางถึงปลายทาง CloudKit • อัปเดต TLS • Apple Pay, การชำระเงินด้วย Apple Pay บนเว็บ • คำแนะนำโดย Siri • iPad ที่แชร์
กรกฎาคม 2017	อัปเดตสำหรับ iOS 10.3 • Secure Enclave • การปกป้องข้อมูลไฟล์ • กระเป๋ากุญแจ (Keybag) • การรับรองความปลอดภัยและโปรแกรม • SiriKit • HealthKit • ความปลอดภัยของเครือข่าย • บลูทูธ • iPad ที่แชร์ • โหมดสูญหาย • การล็อคการเข้าใช้งานเครื่อง • การควบคุมความเป็นส่วนตัว
มีนาคม 2017	อัปเดตสำหรับ iOS 10 ความปลอดภัยของระบบ • คลาสการปกป้องข้อมูล • การรับรองความปลอดภัยและโปรแกรม • HomeKit, ReplayKit, SiriKit • Apple Watch • Wi-Fi, VPN • การลงชื่อเข้าครั้งเดียว • Apple Pay, การชำระเงินด้วย Apple Pay บนเว็บ • การเตรียมใช้งานบัตรเครดิต บัตรเดบิต และบัตรเติมเงิน • คำแนะนำโดย Safari

วันที่	เนื้อหาสรุป
พฤษภาคม 2016	อัปเดตสำหรับ iOS 9.3 • Apple ID ที่มีการจัดการ • การตรวจสอบสิทธิ์สองปัจจัยสำหรับ Apple ID • กระเป๋ากุญแจ (Keybag) • การรับรองความปลอดภัย • โหมดสูญหาย และการล็อคการเข้าใช้งานเครื่อง • โน้ตที่ปลอดภัย • Apple School Manager • iPad ที่แชร์
กันยายน 2015	อัปเดตสำหรับ iOS 9 การล็อคการเข้าใช้เครื่อง Apple Watch • นโยบายเกี่ยวกับรหัส • การรองรับ API ของ Touch ID • การปกป้องข้อมูลบน A8 จะใช้ AES-XTS • กระเป๋ากุญแจ (Keybag) สำหรับการอัปเดตซอฟต์แวร์ที่ไม่ต้องจัดการ • รายการอัปเดตใบรับรอง • โมเดลการเชื่อถือแอปขององค์กร • การปกป้องข้อมูลสำหรับที่คั่นหน้า Safari • ความปลอดภัยของการส่งข้อมูลแอป • ข้อมูลจำเพาะของ VPN • การเข้าถึง iCloud ระยะไกลสำหรับ HomeKit • บัตรสะสมแต้ม Apple Pay และแอปของผู้ออกบัตร Apple Pay • การทำดัชนีบนอุปกรณ์ของ Spotlight • โมเดลการจับคู่ iOS • Apple Configurator 2 • การจำกัด

© 2022 Apple Inc. สงวนสิทธิ์ทุกประการ

การใช้โลโก้ Apple “แป้นพิมพ์” (Option-Shift-K) เพื่อวัตถุประสงค์ทางการค้าโดยปราศจากการยินยอมเป็นลายลักษณ์อักษรจาก Apple ล่วงหน้าถือว่าเป็นการละเมิดเครื่องหมายการค้าและการแข่งขันที่ไม่เป็นธรรมซึ่งเป็นการฝ่าฝืนกฎหมายสหพันธรัฐและมลรัฐ

Apple, โลโก้ Apple, AirDrop, AirPlay, Apple Books, Apple Card, Apple Music, Apple Pay, Apple TV, กระเป๋าสตางค์, 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 และ Xcode เป็นเครื่องหมายการค้าของ Apple Inc. ซึ่งจดทะเบียนในสหรัฐอเมริกาและในประเทศและภูมิภาคอื่นๆ

แอปคลิป ค้นหาของฉัน และ Touch Bar เป็นเครื่องหมายการค้าของ Apple Inc.

App Store, AppleCare, CloudKit, iCloud, iCloud Drive, พวงกุญแจ iCloud และ iTunes Store เป็นเครื่องหมายบริการของ Apple Inc. ซึ่งจดทะเบียนในสหรัฐอเมริกาและในประเทศและภูมิภาคอื่นๆ

Apple Messages for Business เป็นเครื่องหมายบริการของ Apple Inc.

Apple
One Apple Park Way
Cupertino, CA 95014
apple.com

IOS คือเครื่องหมายการค้าหรือเครื่องหมายการค้าจดทะเบียนของ Cisco ในสหรัฐอเมริกาและประเทศอื่นๆ และมีการใช้ภายใต้ใบอนุญาต

เครื่องหมายและโลโก้ Bluetooth® เป็นเครื่องหมายการค้าจดทะเบียนของ Bluetooth SIG, Inc. และการใช้เครื่องหมายใดๆ เหล่านี้โดย Apple Inc. อยู่ภายใต้ใบอนุญาตให้ใช้สิทธิ์

Java เป็นเครื่องหมายการค้าของ Oracle และ/หรือบริษัทในเครือ

UNIX® เป็นเครื่องหมายการค้าจดทะเบียนของ The Open Group

ชื่อผลิตภัณฑ์และชื่อบริษัทอื่นๆ ที่อ้างถึงในที่นี้อาจเป็นเครื่องหมายการค้าของบริษัทที่เป็นเจ้าของ

เราได้พยายามดำเนินการทุกวิธีเพื่อให้มั่นใจว่าข้อมูลในเอกสารนี้ถูกต้อง Apple ไม่รับผิดชอบต่อข้อผิดพลาดที่เกิดจากการพิมพ์หรือการจัดทำเอกสาร

บางแอปไม่ได้มีในทุกพื้นที่ ความพร้อมให้บริการของแอปอาจมีการเปลี่ยนแปลง

TH028-00625