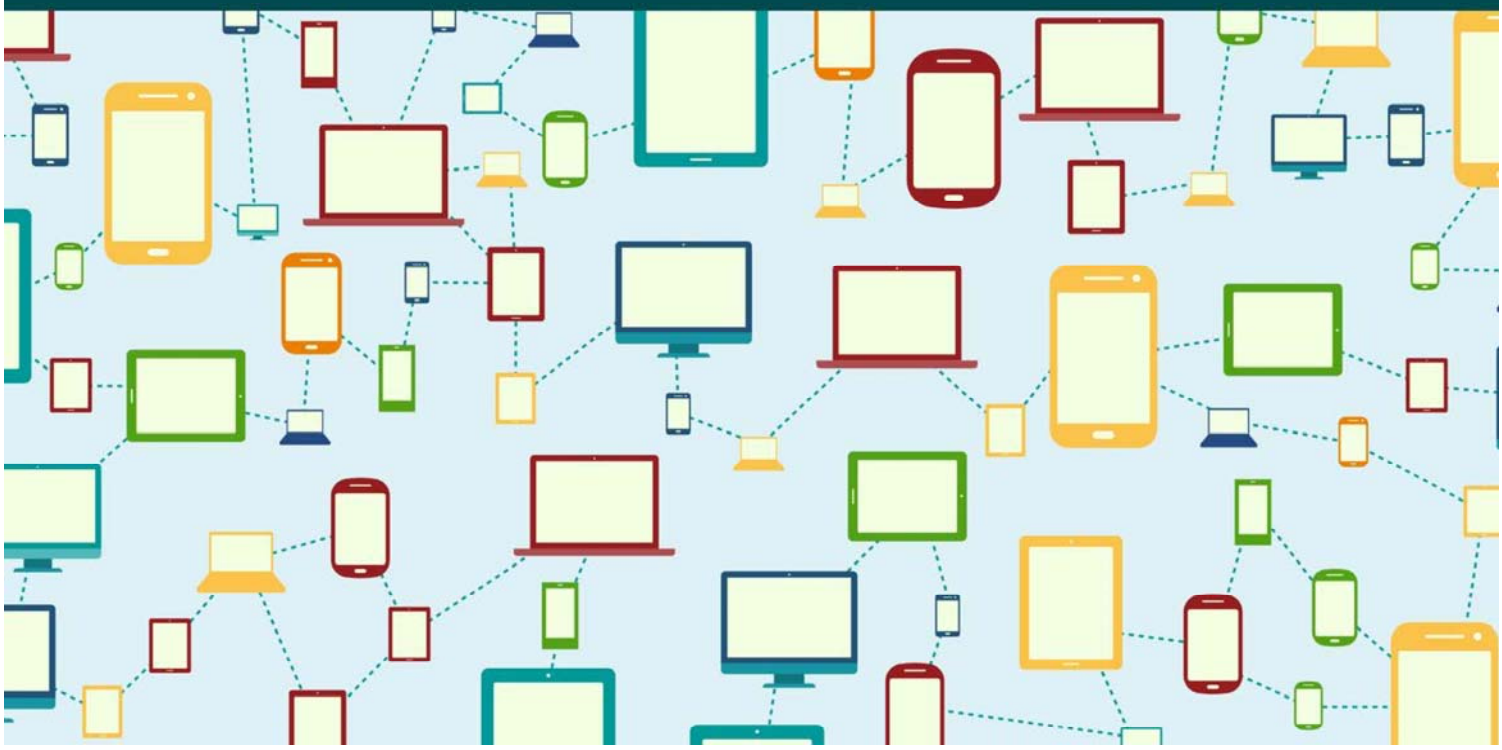
fido alliance | simpler stronger authentication



FIDO & PSD2

Meeting the needs for Strong Customer Authentication

Abstract

The revised Payment Services Directive (PSD2) is now into force in Europe, and Strong Customer Authentication (SCA) will soon become an obligation to secure access to bank accounts for the purpose of information aggregation or payment initiation.

The Regulatory Technical Standards (RTS), published by the European Banking Authority, and yet to be adopted by the European Commission, describe the principles of multi-factor authentication and authentication code generation. But they are not implementation specifications, and banks and service providers are left to decide how to authenticate customers, with a risk of fragmentation and higher costs.

The FIDO standards fill this gap by proposing fully defined specifications, compliant with the requirements of the RTS. The standardization work done by the FIDO Alliance, completed with a multi layered security certification program, guarantees to banks and service providers a choice of interoperable authenticators in multiple form factors and for multiple operating environments. Moreover, FIDO standards are designed to overcome the usability challenges of older, first-generation authentication solutions that degraded the customer experience. This white paper outlines how the FIDO standards can facilitate the implementation of this new disruptive regulation with user-friendly secure solutions.

A few words on the Regulatory Technical Standards

The European Banking Authority's document "Regulatory Technical Standards on strong customer authentication and common and secure communication" describes, in particular, the requirements to be met when implementing SCA.

The RTS also describe exemptions to SCA, but those are outside the scope of this white paper. As are the other aspects of the document on secure communication between the connecting parties.

At the core of the RTS are the following requirements:

- Users must be authenticated using a minimum of two-factor authentication: a mix of elements of possession, inherence and/or knowledge
- The authentication of a user should result in the generation of an authentication code, a cryptographic signature of the transaction. This authentication code must, in the case of remote payments, be linked to the amount and payee approved by the user
- The user's cryptographic material must be protected from unauthorized disclosure

What are the FIDO Alliance and the FIDO standards

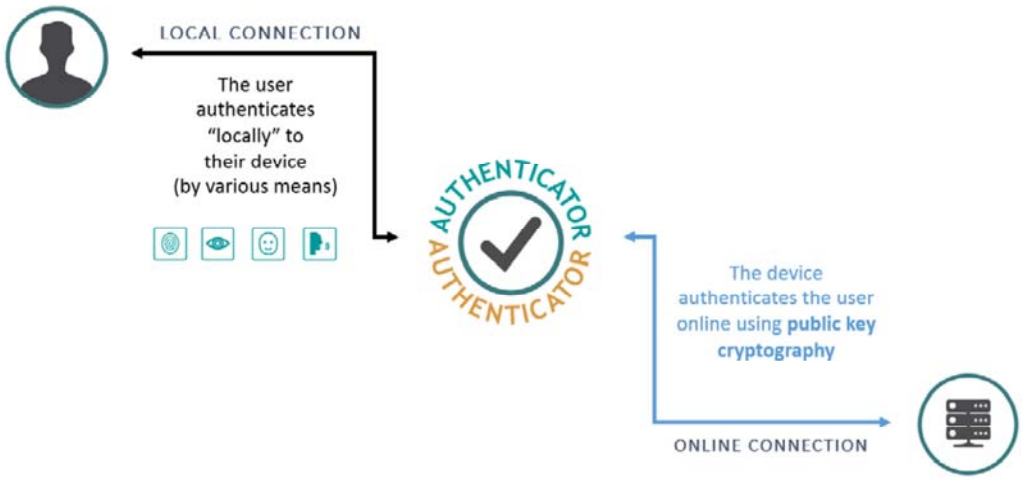
The Fast Identity Online (FIDO) Alliance was formed in 2013 to revolutionize online authentication by developing open, interoperable industry standards that leverage proven public key cryptography for stronger security and device-based user verification for better usability. Today, FIDO has more than 250 members representing a "who's who" in information technology, communications, hardware and software manufacturers, finance, health care, government and other sectors.

Through the collaborative efforts of FIDO, new standards and specifications have emerged that enable strong, easy-to-use authentication to be built into devices such as computers, tablets, smartphones, and dedicated authenticator hardware. Today, thanks to the FIDO specifications, many devices running major operating systems such as Windows, Android and iOS can support issuance of a strong, multi-factor credential - built around asymmetric, public key cryptography – as part of the device itself.

In a typical deployment of these standards, a user swipes a finger, speaks a phrase, looks at a camera on a device, or touches the button on a hardware authenticator to login, pay for an item, or use another service.

The biometric verification is used as an initial factor to then unlock a second, more secure factor: a private cryptographic key that works "behind the scenes" to authenticate a user to the service. Since biometrics and cryptographic keys are stored on local devices and never sent across the network - eliminating shared secrets - user credentials are secure even if service providers get hacked, thereby eliminating the possibility of scalable data breaches.

Figure 1: How FIDO Works



FIDO solutions can alternately be deployed via a standalone "security key" token that contains a chip similar to the secure hardware embedded in devices. With the security key architecture, a user can use a single token across several different devices, leveraging common interfaces such as USB, NFC and Bluetooth.

FIDO standards are currently being used to enable simpler, stronger authentication in offerings from Google, PayPal, Bank of America, NTT DOCOMO, BC Card (Korea), Microsoft, Dropbox, GitHub, AliPay, eBay, Samsung, Facebook, and other leading firms. In each of these deployments, end-users do not have to know how the authentication works or why it's more secure – they are getting login experiences that are easier to use, with great security baked in behind the scenes.

The FIDO approach has been embraced by the World Wide Web Consortium (W3C), which is expected to finalize a formal new "Web Authentication" standard built on FIDO specifications in 2017. The emergence of this new standard, combined with the wide industry and government support of the growing FIDO ecosystem, makes it an important tool in efforts to improve authentication.

User friendliness

The FIDO standards were built with user friendliness in mind - looking to overcome the shortcomings of many older, first-generation authentication technologies that offered enhanced security at the expense of the user experience.

The superior security, usability and privacy offered by FIDO specifications represents a fundamental paradigm shift in the world's approach to strong authentication; the rapid embrace of FIDO by so many of the world's leading firms and governments reinforces the credibility of the security behind the FIDO specifications and the

compelling value FIDO-compliant solutions offer when compared to alternative authentication approaches.

In a typical scenario where the user initiates a payment from a mobile app, he/she would press a button/icon and be switched to a payment screen of the bank or Payment Service Provider (PSP). The transaction details would be displayed on the screen and the user would approve payment by simply scanning a fingerprint, taking a selfie or touching a hardware device. The rest would be handled invisibly by the FIDO authenticator, communicating with the remote server to provide the required cryptograms.

In an out-of-band scenario, the user would initiate payment from a browser by clicking on a button which would cause their FIDO Authenticator to wake up, display the transaction details, and await confirmation of the user by identifying him/herself as just described.

The simplicity and self-evidence of these scenarios illustrate how the FIDO standards help banks and PSPs implement Strong Customer Authentication per the mandate of the regulation.

How FIDO standards help in implementing the RTS

Compliance to the RTS

The FIDO standards are defined on the principle of multi-factor authentication and are in line with the Strong Customer Authentication requirement of the RTS.

In particular, the FIDO U2F (Universal 2nd Factor) standard was created to reduce the reliance on passwords by adding a cryptographic second factor token. The FIDO UAF (Universal Authentication Framework) standard was created for password-less solutions relying on elements categorized as possession (the FIDO authenticator), knowledge (the authenticator PIN) and/or inherence (the biometric characteristic supported by the authenticator).

FIDO authenticators generate and securely hold the user's private key as one of the personalized security credentials described in the RTS. This private key is used to generate the authentication code, a cryptographic signature mandated in the standard. This authentication code is bound to server-provided data and is specific to each individual operation.

Moreover, FIDO standards support the Transaction Confirmation mechanism, which is particularly adapted to the RTS requirements. Through this mechanism, the server will send to the FIDO authenticator a challenge and the transaction details. The authenticator or client application will display the transaction details, and ask the user to confirm the transaction, for example by scanning a fingerprint or touching the authenticator. This will cause the authenticator to sign the challenge and transaction details with its private key and return the signature to the server.

This mechanism is compliant with the RTS requirement to generate an authentication code dynamically linked with the transaction amount and payee approved by the user.

Additionally, the RTS describe exemptions to Strong Customer Authentication (SCA) for which the user does not have to perform an action for authentication purposes. The FIDO standards can help improve security in some of these exemption situations, through extensions to the standards that allow for silent authenticators or user verification caching:

FIDO silent authenticators do not require user verification but nevertheless silently generate cryptographic signatures thus still proving possession of a valid authenticator. User verification caching is a feature that allows a bank or PSP to configure the FIDO authenticator to remember, for a period of time, that the user identified him/herself correctly to the device so that a new user verification is not necessary during that period. The user verification caching feature was developed together with the FIDO liaison partner EMVCo.

An implementation standard: reducing costs, simplifying deployment

The RTS edict principles but remain technology neutral and provide no implementation details.

This has the disadvantage that each vendor could propose proprietary authentication solutions, resulting in complexity for banks or PSPs that need to source multiple solutions in order to maximize reach.

For example, bank A decides to use a solution from a vendor based on a smartphone with a secure element and fingerprint scanner. However, all this bank's users may not have the proper model of phone and so bank A will also support a solution from another vendor based on a smartphone with PIN verification. And because all users may not have such a phone, in order to comply with the regulation, bank A will opt to source a hardware device from yet another vendor and distribute it to users without smartphones.

Without standardization, Bank A will see its PSD2 compliance costs increase.

On another note, a bank may find itself locked up in a vendor's solution due to the cost of implementing an alternative, to the detriment of PSD2's purpose of facilitating competition in the banking ecosystem.

The FIDO standards reduce these risks by proposing to banks and PSPs interoperable FIDO certified authenticators. A FIDO compliant server can access various types of FIDO authenticators whether based on a mobile phone, a PC-based browser or an external hardware device - regardless of operating system, and without additional development.

A certification program backed by hundreds of certified products

The RTS mandate that security measures be put in place, for example to ensure confidentiality and integrity of personalized security credentials and for the protection of cryptographic keys. They also mandate evaluating and auditing the implementation of the security measures, for the purpose of reporting on the compliance of the implementation to the regulation.

But the RTS do not specify the security measures nor the associated compliance testing. There is no description of an evaluation level or security target. National or regional bodies may decide to define this missing material but, at this stage, it is up to the bank or PSP to decide how to check on a particular vendor's compliance.

To help resolve this issue, the FIDO Alliance has developed a robust certification program. This program ensures that different FIDO implementations interoperate with each other on a technical level and comply with all technical specifications. Participation in these certification programs is voluntary but are a prerequisite for obtaining rights to use a FIDO Certified™ logo.

More than 350 products have been tested and certified under this program since it was launched in May 2015. More than 125 companies have certified their FIDO implementations through this program. A detailed list of these products can be found at https://fidoalliance.org/certification/fido-certified/.

In addition to this "functional testing," the FIDO Alliance has initiated a separate security certification program, focused on third-party security lab certification and security assurance verification. FIDO security certification focuses on five levels of security certifications corresponding to different implementations and security targets.

FIDO supports implementations using Secure Elements (SE), Trusted Execution Environments (TEE) or software only, with different levels of resistance to attacks up to Common Criteria EAL 5 security evaluation.

PISP and AISP authorization support

The PISP (Payment Initiation Service Provider) and AISP (Account Information Service Provider), defined by PSD2, need explicit consent from the user followed by authorization from the bank, to perform interactions with the user's bank account on its behalf.

FIDO solutions are frequently combined with authorization frameworks such as the Internet Engineering Task Force (IETF) standard OAuth 2.0. Both can be jointly used, in the scope of PSD2, to facilitate limited access to bank accounts for PISPs and AISPs, while ensuring strong customer authentication. As new OAuth 2.0-based APIs emerge to address PSD2 and other "open banking" efforts around the world, FIDO solutions provide the ideal way to address authentication requirements needed to enable these open APIs to deliver services in a way that is secure and easy to use.

Ease of deployment

In the FIDO standards, keys required by a bank or PSP to authenticate the user are generated within the FIDO authenticator at the time of user enrollment. The private key never leaves the authenticator while the public key (its certificate) is sent to the bank or PSP. Moreover, the authenticator may be used by the user to enroll at several banks or PSPs.

This method allows a bank or PSP to leverage FIDO authenticators already deployed. The characteristics of these authenticators are published (for example, on the FIDO MDS server) so that the bank or PSP may check at enrollment if they comply with its security policy.

Conclusion

The FIDO standards can facilitate compliance by banks and PSPs with the requirement of strong customer authentication mandated in the new PSD2 regulation.

The FIDO security certification program provides a means and framework to comply with the security evaluation and audit requirement of the RTS.

Thanks to the standardization of FIDO, banks and PSPs may accept a variety of interoperable FIDO compliant authenticators, thus providing choice to their users and increasing reach of their authentication solution.