FIDO Alliance White Paper:

FIDO for SCA Delegation to Merchants or Wallet Providers

Review Draft

March 2021

Editors:
Jonathan Grossar, Mastercard
Alain Martin, Thales
Melanie Maier, Entersekt
Bernard Joly, OneSpan
Felix Magedanz, Hanko
Arshad Noor, StrongKey

Abstract

The authentication of consumers during remote transactions has undeniable benefits in terms of security and approval rates but raises concerns of transactions being abandoned by consumers, as those consumers are not always able to authenticate properly to their banks.

Merchants and wallet providers have an existing relationship with consumers, and there is an opportunity to leverage authentication mechanisms established during that relationship to authenticate to remote transactions as a delegation of the bank's authentication.

This white paper reviews the different authentication mechanisms that can be used by merchants or wallet providers in the context of Strong Customer Authentication (SCA) Delegation and explains why FIDO is best positioned to meet the requirements from regulatory authorities, banks, merchants, or wallet providers.

FIDO is an industry standard designed to authenticate consumers with a high level of security and privacy but with minimal friction, and the implementation of FIDO standards is scalable across multiple consumer devices and platforms, making FIDO the recommended solution for SCA Delegation.

Audience

This paper is intended for:

- Merchants, Payment Service Providers, and wallet providers interested in implementing a FIDO solution to authenticate consumers as a delegation of a bank's authentication.
- Banks interested in understanding the benefits of FIDO in SCA Delegation, including how the implementation of FIDO meets their requirements.
- Authentication solution providers interested in providing FIDO solutions to merchants or wallet providers.

Contents

Tables

Figures

1. Introduction

1.1 Why SCA Delegation?

The Second Payment Services Directive (PSD2) and its associated Regulatory Technical Standards[1] (RTS) introduce a requirement for strong, multi-factor authentication for electronic commerce transactions.

While the regulation was introduced with an objective to increase the overall security of transactions, the need for SCA may result in transactions being abandoned as a result of added friction at checkout or difficulties for a consumer to authenticate adequately to their banks.

Banks are actively working on providing their consumers with authentication mechanisms that reduce friction during the authentication process. However, merchants or wallet providers may have established a prior relationship with consumers when they create an account and store a payment instrument on file. Consequently, merchants or wallet providers may already authenticate consumers when they access their accounts before, during or after the checkout process.

In such situations, there is an opportunity to leverage authentication mechanisms established by the merchant or wallet provider and authenticate the consumer with the merchant or wallet credentials in a consistent manner for access to their account as well as for transactions initiated with a payment instrument stored on file with that account.

The PSD2 regulation – and the Opinion of the European Banking Authority (EBA) on the implementation of the RTS on SCA and Common and Secure Communication (CSC)[2] –allows banks to delegate SCA to third-party providers such as merchants or wallet providers. Banks are likely to set conditions before they can accept the delegation of consumer authentication to third-party providers – including assurances on the security of such delegated authentications.

Delegated authentication is relevant in PSD2 markets to apply SCA with reduced friction but is also relevant in other markets where merchants or wallet providers can provide banks with assurances that the consumer has been authenticated to the transaction and therefore expects better approval rates.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.069.01.0023.01.ENG&toc=OJ:L:2018:069:TOC

[2] https://eba.europa.eu/sites/default/documents/files/documents/10180/2137845/0f525dc7-0f97-4be7-9ad7-800723365b8e/Opinion%20on%20the%20implementation%20of%20the%20RTS%20on%20SCA%20and%20CSC%20%28EBA-2018-Op-04%29.pdf?retry=1

1.2 Scope

The scope of this white paper is to:

- List prerequisites for SCA Delegation including regulatory requirements for using SCA Delegation in PSD2 markets, and the conditions for banks to agree on their participation in an SCA Delegation program.
- Review authentication mechanisms available to merchants or wallet providers in remote transactions, which can be used for SCA Delegation.
- Explain the value proposition for merchants or wallet providers to implement FIDO as a standardized and secure authentication solution for SCA Delegation, highlighting its compliance with PSD2 requirements and benefits to the payment ecosystem.
- Review steps for merchants or wallet providers to implement FIDO for SCA Delegation, and the consumer journey.
- Review how results of an authentication performed by a merchant or wallet provider with FIDO are shared with banks to approve the transaction in compliance with PSD2 – e.g. in an EMV®[3] 3D Secure message.

2. Assumptions

2.1 Types of Transactions Considered

The transactions in scope of this document are consumer-initiated remote transactions, during which SCA may be required by PSD2 regulation when both the merchant and the bank are in the European Economic Area (EEA).

This white paper covers the following remote transactions:

- Consumer-initiated with payment instruments, e.g. cards (domestic or international), stored on file with a merchant or a wallet
- Consumer-initiated as payment transfers from one bank account to another

2.2 Participants

The participants in remote transactions usually include:

- Consumer (or Customer or Account holder): a person or business that purchases goods or services, using a payment instrument issued by a bank.
- Bank: a financial institution that maintains accounts for their consumers and issues payment instruments for consumers to use in a remote transaction.
- Merchant: a person or company that sells goods or services. In a remote transaction, a merchant contracts with an Acquirer to accept payment instruments – e.g. payment cards.
- Acquirer: a financial institution that establishes a contractual service relationship with a merchant for the purpose of accepting payment instruments, and that processes payment transactions performed with a payment instrument on behalf of the merchant, which results in a transfer of funds to the merchant.
- Payment Service Provider: a service provider registered by an Acquirer to facilitate the acquiring of transactions by the Acquirer from multiple merchants.

[3] EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV® trademark is owned by EMVCo, LLC. See https://www.emvco.com/about/overview/ for more details.

- Wallet providers: a company operating a digital wallet which:
  - can be accepted as a payment method at one or multiple merchants,
  - stores payment instruments provided by the consumer for purposes of conducting remote transactions, and
  - shares payment instruments and data with the merchants (or Payment Service Providers) during a remote transaction.
- Payment system: an international or domestic payment scheme that defines the operating rules and conditions and requirements for the issuance of payment instruments and for merchant acceptance and allows the processing of remote transactions through a payment system network.

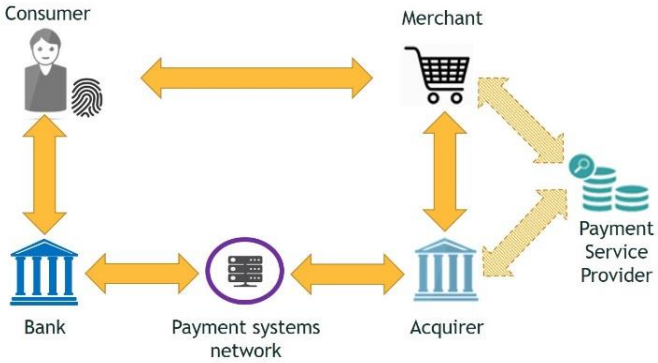

Figure 1 – Participants in remote transactions

3. Prerequisites for SCA Delegation

This section provides a description of the following:

- The regulatory requirements in PSD2 markets to allow SCA Delegation from banks to merchants or wallet providers.
- What is important for banks, i.e. what conditions need to be met for their participation in SCA Delegation.
- What is important for merchants and wallet providers, i.e. what are the needs that they want addressed.

3.1 Regulatory Requirements (PSD2 Markets)

The EBA has clarified in question 2018-4047[4] that banks may use third-party technology, such as a smartphone fingerprint reader, to support SCA and that they can delegate the execution of SCA to a third party with the conditions highlighted below.

The EBA has also provided more information on SCA Delegation in opinion EBA/OP/2020/10 published on June 4 2020[5].

[4] https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4047

[5] https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2020/884569/EBA%20Opinion%20on%20obstacles%20under%20Art.%2032(3)%20RTS%20on%20SCA%26CSC.pdf

3.1.1 Contractual Agreement

Banks are required to have a contractual agreement in place with the third parties (merchants or wallet providers) to which they agree to delegate their authentication. In order to get scale, it is expected that a multilateral contractual framework is provided by domestic or international payment schemes to avoid the need for bilateral agreements between all banks and merchants or wallet providers.

3.1.2 Security Level

To comply with provisions set in the RTS (Articles 4 and 9), banks should make sure that the third party has a satisfactory level of security and applies the following mitigating measures:

- separated secure execution environments
- mechanisms to ensure that the software or device has not been altered
- mechanisms to prevent an authentication code from being forged or generated based on the knowledge of any other previous authentication code
- mechanisms to block (temporarily or permanently) failed authentication attempts

3.1.3 Documentation and Testing

Banks should ensure that the implementation of the security measures is documented, periodically tested, evaluated, and audited (Article 3 of the RTS). This may include carrying out security evaluations of third-party devices or applications.

3.1.4 Dynamic Linking

The PSD2 regulation (Article 5 of the RTS) requires that the solution complies with the dynamic linking requirement, i.e. that:

- The consumer is made aware of the amount of the payment transaction and of the merchant.
- The authentication code generated is specific to the amount of the payment transaction and the merchant agreed to by the consumer when initiating the transaction.
- The authentication code accepted by the bank corresponds to the original specific amount of the payment transaction and to the identity of the merchant agreed to by the consumer.
- Any change to the amount or the merchant results in the invalidation of the authentication code generated.

3.2 What is important for banks

For banks to delegate their authentication to third parties such as merchants or wallet providers, it is important that:

- the authentication solution used by third parties meets the regulatory and the bank's security requirements.
- an initial registration process, which includes an identification and verification mechanism to ensure that the consumer is the legitimate cardholder or account holder, takes place before delegated authentication can be used.
- some evidence that SCA has taken place is provided to banks (or to an agent operating on their behalf) by the third party (merchant or wallet provider) during the transaction, allowing banks to have visibility on the authentication performed by the third party to which they delegate consumer authentication.

The remainder of this section describes options for providing this evidence as well as mechanisms for sharing the evidence with banks.

3.2.1 Trust Models

The amount of information provided as evidence that SCA has taken place varies based on the trust relationship between the merchant and the bank, and on the nature of the contractual agreement between them (e.g. in terms of liability in case of fraud) – as such, there are different levels of trust to consider.

The trust relationship could be impacted by several factors, including:

- The type of solution (and its security) used by the merchant or wallet provider.
- The level of fraud for remote transactions conducted at this merchant or wallet provider.
- The nature of the merchant business.
- The security of the environment in which the merchant or wallet provider operates – e.g. use of tokenization.

As a result, we have situations in which issuers have a high level of trust in the merchant or wallet provider, and others in which banks have a lower level of trust in the merchant or wallet provider but still agree to participate in an SCA Delegation program.

3.2.2 Evidence provided to banks

Since there are different trust models, banks may require different amounts of information to be shared with them or with an agent operating on their behalf. The following three options may be utilized to share information with banks:

- Minimal sharing, maximal trust: Merchant or wallet providers share a "success signal" to the bank. The bank does not validate the authentication results.
- Moderate sharing, moderate trust: Merchant or wallet providers share necessary data to the bank for risk assessment, which enables the bank, or an agent operating on its behalf, to:
  - perform a risk assessment of the transaction,
  - create a binding between the consumer's payment instruments and the SCA solution (which can be located on a personal device),
  - validate that the SCA solution meets their security policy, and/or
  - understand what authentication factors were used to authenticate the consumer.
- Maximal sharing, minimal trust: Merchant or wallet providers share adequate data to the bank – e.g. a cryptographic evidence of the authentication – to enable the bank, or an agent operating on their behalf, to perform full validation of the authentication performed by the merchant or wallet provider.

Delegated authentication frameworks may be provided by domestic or international payment schemes to determine the amount of data to share in each remote transaction use case. Banks are not expected to re-authenticate the consumer unless there is a high risk of fraud identified.

3.2.3 Protocols to share evidence

Section 7 describes the data which can be shared with banks when FIDO is used in combination with the EMV 3D Secure standard.

Other communication protocols may use the same level of data in their application programming interface (API) as the one standardized in EMV 3DS, for example EMV Secure Remote Commerce, Open Banking APIs, or other domestic or international standards.[6]

3.3 What is important for merchants or wallet providers

For merchants and wallet providers, SCA Delegation is expected to meet the following objectives:

- It simplifies checkout flows and makes them predictable so they can optimally guide consumers through the process.
- Consumer authentication is under their control, i.e. there is no redirection of the consumer to the bank for authentication.
- It avoids authenticating consumers twice – once for access to a merchant or wallet account, and once for the transaction, using different mechanisms (e.g. password for merchant account and bank authentication for transaction).

4. SCA Delegation Solutions

This section includes a description of the most popular authentication mechanisms which can be used by merchants or wallet providers to authenticate consumers with SCA as a delegation of a bank's authentication.

4.1 FIDO Solutions (two-factor)

FIDO solutions provide two-factor authentication of consumers: device possession (first factor) and knowledge or inherence (second factor) that authenticates the consumer to the device, thereby unlocking the FIDO private key to digitally sign the transaction.

[6] EMV 3D Secure: https://emvco.com/emv-technologies/3d-secure/
EMV Secure Remote Commerce: https://www.emvco.com/emv-technologies/src/
Open Banking: https://www.berlin-group.org/nextgenpsd2-downloads

Figure 2 below illustrates components provided by the FIDO standards to authenticate consumers:

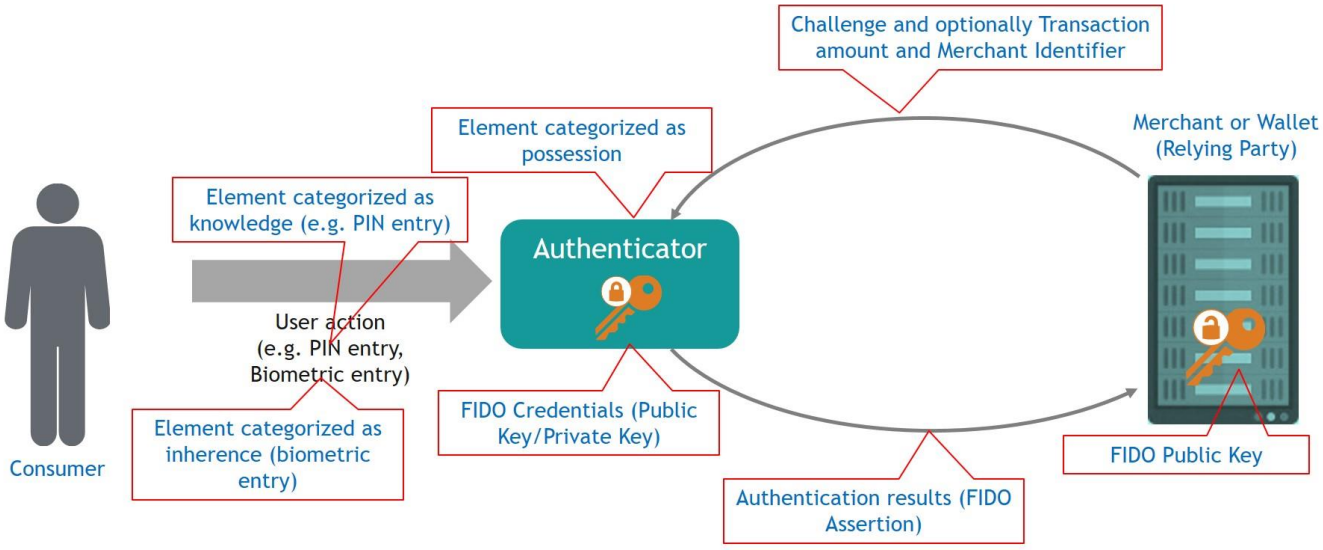

Figure 2 – FIDO components

To authenticate with FIDO, the consumer must possess a FIDO Authenticator that is either embedded in a general-purpose device (e.g. smartphone, laptop), or a separate device (e.g. security key, smart card). Examples of FIDO Authenticators are included in the table below.

	Platform authenticators		Roaming authenticators	
Multi Factor authentication (possession + knowledge/inherence)	PC with PIN or biometric capture	Smart phone with PIN or biometric capture	Smart card with PIN or fingerprint sensor	Security Key with PIN or fingerprint sensor

Table 1 – FIDO Authenticators

The first step of FIDO Authentication is the process of verifying that a consumer is the authorized owner of a FIDO Authenticator. This step is performed offline by the authenticator and is local to the authenticator; it can consist of the verification of a PIN code, a geometric pattern, or biometric data by the authenticator.

The fact that user verification data (PIN code, geometric pattern or biometric data) is stored and verified within the local device and is neither transmitted to nor shared with any server, is a strong security and privacy asset of the FIDO approach.

The second step of FIDO Authentication is an online authentication step to prove possession of the FIDO Authenticator. In this step, the merchant or wallet provider's server sends a challenge message to the authenticator (through the business application) which is cryptographically signed by a private key stored in the authenticator. The signed response is returned to the merchant or wallet provider and its positive verification serves as proof of possession of the private key that digitally signed the transaction.

FIDO standards are based on public key cryptography. The private key is part of a key pair randomly generated by the authenticator itself and is not known to any other party. At the time of generation, the public key of the key pair is sent to the Relying Party in a protected manner to ensure that it cannot be tampered with undetected.

The authenticator maintains unique private keys for each Relying Party. For example, if the consumer has accounts at Relying Party 1 (Merchant 1) and Relying Party 2 (Merchant 2), the authenticator generates and stores different private keys for Relying Party 1 (Merchant 1) and Relying Party 2 (Merchant 2), each restricted for use with its corresponding Relying Party.

FIDO Standards

FIDO UAF (Universal Authentication Framework) is a FIDO standard that completely replaces the use of passwords. FIDO UAF-compliant authenticators support the local verification of the user's PIN code or biometric data. Typical UAF implementations are found in smartphones.

FIDO2 is a FIDO standard that consists of WebAuthn (web authentication), a set of JavaScript APIs specified by the World Wide Web Consortium (W3C)[7] organization in collaboration with the FIDO Alliance, that are natively incorporated in recent browsers, and Client To Authenticator Protocol (CTAP), a communication protocol for applications such as browsers to connect to FIDO Authenticators. Like UAF, FIDO2 enables completely replacing passwords not only on mobile devices, but also on desktops and laptops when configured with appropriate security devices. Collectively, WebAuthn and CTAP standardize access from a browser on a platform (a personal computer or mobile device) to a FIDO Authenticator.

A high-level description of these standards as well as FIDO specifications can be found at https://fidoalliance.org/download/.

4.2 Non-FIDO Authentication Solutions

This section lists authentication solutions not based on FIDO, which merchants or wallet providers could use for SCA Delegation.

4.2.1 Non-FIDO Device Biometrics Solutions (one- or two-factor)

Non-FIDO biometrics solutions provide one- or two-factor authentication of consumers, e.g. possession of the biometric device (first factor) and knowledge or inherence to unlock the device for performing a sensitive operation (second factor).

These devices differ from FIDO solutions in that these solutions are proprietary, i.e. developed outside the bounds of an industry standard, and often leverage symmetric keys shared between the consumer device and the merchant or wallet provider's server (thereby creating the risk of a compromise of all devices with the compromise of a single device), rather than using public key cryptography (which localizes the risk of a compromised device to just that device).

4.2.2 SMS OTP (one-factor)

Short Message Service (SMS) One Time Password (OTP) provides single-factor authentication (possession factor) and can be used in combination with another factor, e.g. password (knowledge) or behavioral biometrics (inherence) to comply with SCA requirements.

[7] https://www.w3c.org

SMS OTP is a popular factor for a few reasons:

- It can be used on any device in possession of the user.
- It easily scales as it does not require any additional software or hardware.
- The requirements on Relying Parties' infrastructure are minimal, i.e. they can engage a partner for SMS delivery.

SMS OTP has however some drawbacks:

- It decreases user convenience to retrieve the OTP from the messaging application, take note of it, and type it in the merchant or wallet environment.
- It has security vulnerabilities (which are growing) – such vulnerabilities can be linked to the weakness of telecommunication systems, to the use of third-party service providers for SMS delivery with inadequate level of protection, phishing attacks, etc.

4.2.3 Passwords (one-factor)

Passwords provide single-factor authentication (knowledge) and can be used in combination with another factor – typically a possession factor – to comply with SCA requirements. Passwords are widely used as an authentication factor but have shortcomings in terms of usability (difficult to remember all passwords, different rules to set up passwords, etc.) and have security vulnerabilities (weak passwords, prone to phishing, database hacking, etc.).

4.2.4 Behavioral Biometrics (one-factor)

Behavioral biometrics provide single-factor authentication and can be used in combination with another factor – typically a device possession factor – to comply with SCA requirements.

Per the Opinion of the European Banking Authority on the elements of SCA under PSD2 (EBA-Op-2019-6[8]), behavioral biometrics is identified as an inherence factor as long as it "relates to physical properties of body parts, physiological characteristics and behavioral processes created by the body, and any combination of these. In addition, it is (the quality of) the implementation of any inherence-based approach that will determine whether or not it constitutes a compliant inherence element".

Behavioral biometrics are a way to passively authenticate the consumer without too much effort, based, for example, on the way that consumers type, swipe or hold the device, but may raise privacy concerns and may provide unreliable results if the number of measures is limited or performed at the wrong time (e.g. when the consumer is under stress).

[8] https://eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf

5. Why FIDO for SCA Delegation?

Consumers, merchants or wallet providers, and banks can all benefit of the use of FIDO for SCA Delegation. The primary benefits of FIDO solutions are that they:

- provide enhanced user experience,
- offer full compliance with PSD2,
- are standardized and therefore provide full interoperability and enhanced market acceptance,
- are highly secure, with resistance to phishing attacks,
- are designed with privacy in mind, and
- are scalable and easy to deploy.

5.1 Enhanced User Experience

Consumers prefer secure, low friction mechanisms to authenticate, with a consistent user experience across different payment methods. Unlike OTP/passcode solutions, FIDO requires no entry of authentication codes.

The user experience can be as simple as scanning a face or fingerprint (when biometrics are present) or entering a PIN or geometric pattern – consumers can use an authentication mechanism they use dozens of times daily to unlock computing devices, removing the need to remember different passcodes.

Behind the scenes, a full multi-factor authentication nevertheless takes place to the merchants or wallet providers.

5.2 Compliance with PSD2

Banks are responsible for the authentication of their consumers and are therefore looking for compliance with the PSD2 regulation.

The document "How FIDO standards meet PSD2's regulatory technical standard requirements on strong customer authentication"[9] explains how FIDO fully complies with PSD2 requirements, particularly the following:

- The authentication is based on two independent factors:
  - To authenticate with FIDO, the consumer must possess a FIDO Authenticator that is either integrated in a general-purpose device (e.g. smartphone, laptop, etc.) or in a separate device (e.g. security key, smart card, etc.). FIDO Authentication provides for a secure proof of possession thanks to the use of a private key securely held in the device that is used to generate nonreplicable assertions – possession of the FIDO Authenticator satisfies the first of two elements required to authenticate the consumer.
  - The second element consists of an inherence (biometric) factor or knowledge (e.g. PIN or geometric pattern) factor verified locally by the FIDO Authenticator (FIDO UAF and FIDO2). FIDO assertions are generated upon valid biometric verification and digitally sign the challenge, thus asserting the successful result of the verification.
- FIDO supports the dynamic linking requirement for remote payments, as the FIDO Authenticator can sign an incoming message that combines a challenge with transaction details.

5.3 Full Interoperability with a Standard-based Solution

Merchants and wallet providers seek mechanisms that are consistent across devices, platforms, and payment methods.

[9] https://fidoalliance.org/how_fido_meets_the_rts_requirements/

FIDO is a standard natively supported in platforms, therefore FIDO Authenticators can be implemented on most devices and accessed consistently from a merchant or wallet application on a device, or from web pages (using WebAuthn API[10]).

The FIDO certification program validates that FIDO products adhere to FIDO specifications and interoperate within the marketplace, e.g. a FIDO2 certified server can accept protocol messages from any FIDO2-certified authenticator, irrespective of its manufacturer. This enables merchants or wallet providers to use an authentication solution proven to be interoperable while adhering to FIDO specifications and allows consumers to leverage authenticators that work across devices and websites.

5.4 Security

FIDO can offer a similar level of security as in hardware OTP generators. Indeed, FIDO Authenticators can be found in Secure Element implementations as well as in Trusted Execution Environments.

The security level of a given FIDO Authenticator is attested by its FIDO certification. The FIDO Alliance indeed runs a stringent certification program that not only tests interoperability of solutions but also their level of security.

FIDO protocols have strong measures to prevent phishing attacks through:

- the verification of a web origin (the uniform resource locator or URL of the website) by the FIDO client, and
- a cryptographic assertion generated by the FIDO Authenticator that signs the web origin (among other data elements in the challenge message), which is verified by the Relying Party during the authentication step.

Collectively, these measures effectively prevent Man-In-The-Middle attacks and phishing attempts.

The FIDO security certification program[11] provides for an independent assessment of the security level achieved by a FIDO Authenticator implementation. The assessment is typically performed by a FIDO accredited laboratory and is completed by an evaluation of the FIDO technical staff, leading to an official FIDO certification.

5.5 Designed with Privacy in Mind

The FIDO approach uses public key cryptographic keys for authentication. It does *not* rely on sensitive biometric data to be shared with any Relying Party or stored on any Relying Party's internet facing systems. More details can be found in the FIDO Privacy Principles Whitepaper[12].

5.6 Deployment/scalability

Deployment and scalability are facilitated by the fact that FIDO is a standard natively supported in platforms and by the way registration is handled.

FIDO Authenticators do not need to be preconfigured to a specific merchant or wallet. The generation of cryptographic key pairs happens at the time the consumers register their FIDO device with the merchant or wallet provider. A FIDO Authenticator used with one merchant can be registered for use with another merchant; each time a new private/public key pair is generated specific to the merchant or wallet. As only the public key is transmitted to the merchant or wallet server (along with other data elements pertaining to the FIDO protocol), there is no need for secure provisioning servers as with other solutions.

[10] https://www.w3.org/TR/webauthn/

[11] https://fidoalliance.org/certification/authenticator-certification-levels/

[12] https://fidoalliance.org/fido-authentication/privacy-principles/

Native platform support: With the native support of FIDO Authentication in most recent Android and iOS versions, many smartphones come with FIDO Authenticators embedded in the device, which greatly simplifies deployment and scale. FIDO is also natively supported in Windows 10 so that external FIDO Authenticators, including smartphones, can connect to a Personal Computer through the embedded CTAP interface. No driver installation is required.

For devices, FIDO-enabled smartphones may be reached out of band for the purpose of user authentication.

Global reach: The fact that FIDO is an industry standard facilitates the deployment of authenticators to most consumers. The FIDO vendor community proposes a range of FIDO-certified devices that interoperate with FIDO-certified servers. The investment of merchants or wallet providers in a FIDO server will allow them to accept a variety of compatible FIDO devices.

Account recovery: As with other solutions relying on a device, the loss of a FIDO Authenticator may block the user from authenticating to a transaction. However, where other solutions require the shipment of a new device, FIDO Authenticators use any off-the-shelf FIDO-certified devices. For example, having lost their smartphone, the consumer could rapidly purchase another one and register with the merchant or wallet provider again to regain access.

Asymmetric cryptography: FIDO uses asymmetric cryptography, which makes it easy to share the public key with Relying Parties (merchants or wallet providers) and banks (or their agent) who would like to validate the FIDO assertion data. Solutions based on symmetric cryptography require the different parties to agree on a mechanism to securely share the symmetric keys.

6. How to Implement FIDO in a Compliant Way

This section describes the best practices for merchants or wallet providers to implement a FIDO solution to authenticate consumers from their applications or web pages, in compliance with PSD2, and reviews the steps of the consumer journey with an objective towards optimizing the user experience while complying with PSD2 requirements.

6.1 Integration of FIDO Components

The FIDO components include FIDO Authenticators and FIDO servers. These are used in conjunction with the application that leverages the FIDO protocol for SCA.

When implementing FIDO, merchants or wallet providers have the choice to develop the different FIDO components themselves or source those components from approved FIDO vendors. When it comes to FIDO Authenticators, they can use platform Authenticators natively embedded in the user device (APIs are readily available in Android or Windows 10 to integrate these platform authenticators in merchant or wallet solutions). The list of approved FIDO products is published on the FIDO website[13].

Merchants can choose to work with their Payment Service Provider, who either develops the FIDO components or sources them from approved vendors. The PSP could, for example, provide an SDK to the merchants, which the merchants integrate into their application. Merchants should check with their PSP if the solution can be used for consumer access to the merchant account (login) besides transaction authentication, thereby removing the need for separate authentication implementations.

6.2 Initial Registration Process

The initial registration process consists of three different steps, which need to be completed before a payment instrument can be used in a remote transaction with delegated authentication.

[13] https://fidoalliance.org/certification/fido-certified-products/

6.2.1 Identification and Verification (ID&V)

The bank must ensure that the consumer registering a payment instrument with a merchant or wallet is the legitimate owner of that payment instrument, before they can delegate their authentication for that payment instrument to that merchant or wallet.

Merchants or wallets may use different ID&V mechanisms to have the bank authenticate the consumer and confirm the consumer is the legitimate owner of the payment instrument. For card-based ID&V schemes, a standard approach is for the merchant or wallet provider to use the EMV 3DS protocol (payment or non-payment flow) with challenge flow.

Merchants or wallets may decide to perform the ID&V process during a transaction or outside of a transaction as long as the bank authenticates the consumer.

6.2.2 FIDO Authenticator Registration

Once the merchant or wallet has received confirmation from the bank that the consumer is the legitimate owner of the payment instrument, they ask the consumer to consent to registering their FIDO Authenticator for subsequent authentications.

If this is the first time a consumer uses a FIDO Authenticator on their device, they set up their user verification method (e.g. biometrics or PIN) in the FIDO Authenticator. Note that the set-up process may vary from one authenticator to another. This step can be skipped if the authenticator was previously set up with other Relying Parties or – in the case of a platform authenticator – was previously set up by the consumer when configuring their device.

Consumer consent involves a successful user verification, upon which a new FIDO key pair is generated for the consumer with the merchant or wallet.

6.2.3 FIDO Authenticator Binding

Once consent is provided, the merchant or wallet provider associates the FIDO Authenticator with the consumer profile and the payment instrument for which an ID&V was successfully performed. This step can be repeated when a new payment instrument is added (and a new ID&V is performed for that payment instrument).

Once the FIDO credentials have been created on the consumer's device, banks may expect that the merchant or wallet provider shares enrollment data with them or their agent – including information on the FIDO Authenticator being used. This can allow the bank (or their agent) to:

- verify that the FIDO Authenticator complies with the bank's policies,
- create a binding of the consumer's payment instrument to the merchant or wallet, and/or
- store necessary FIDO public-key data which will be used to verify subsequent authentications.

6.3 Checkout Process

6.3.1 FIDO Credential Identification

During the checkout, the consumer selects a payment instrument. The merchant or wallet provider recognizes that the payment instrument has been registered for delegated authentication, and that a FIDO credential was created for the consumer and associated with the payment instrument.

Before authenticating the consumer, the merchant or wallet provider needs to ensure that the FIDO credential can be accessed by the consumer, as it may have been deleted or created on a different device than the device on which the consumer initiates the checkout process. Where a browser is used, merchants or wallet providers may use cookies or local storage to identify that a FIDO credential is available on the consumer device.

6.3.2 Consumer Authentication

Once the merchant or wallet has identified that a FIDO credential is available for the consumer, they prompt for user verification in order to:

- enable access to the merchant (or wallet) account and stored payment instruments, and/or
- authenticate the transaction initiated with the stored payment instrument.

Upon successful user verification, a signed response (FIDO assertion) is generated and shared with the merchant or wallet's FIDO server for validation.

Consumer Journey

The consumer journey can be implemented in two different ways:

1. Consumer is not authenticated with FIDO to access their account with the merchant or wallet (login), but is authenticated with FIDO during the checkout, or
2. Consumer is authenticated with FIDO before the checkout to access their account with the merchant or wallet (login), in which case the merchant or wallet provider can either:
   a. Authenticate the consumer with FIDO a second time during the checkout, to comply with PSD2 dynamic linking and generate more confidence to the consumer that their purchase is secure, or
   b. If agreed in their contract with the bank, choose not to repeat FIDO Authentication if some conditions are met, which includes (but may not be limited to):
      i. The consumer finalizes the checkout within five minutes of the FIDO Authentication.
      ii. The consumer confirms the transaction amount and merchant identification.
      iii. Dynamic linking does not rely on the FIDO signed response, but on a different authentication code generated without the use of FIDO.

6.4 Use of Multiple FIDO Authenticators

Many consumers have multiple FIDO Authenticators, possibly located on multiple devices (phones, tablets, personal computers, etc.), and while it is possible to check out on one device and authenticate on another, there may be a desire from consumers to be able to authenticate on any of their devices, removing the need to be in possession of a specific device to authenticate.

One use case is a scenario in which consumers enroll multiple FIDO Authenticators for the same payment instrument during the initial registration phase (with ID&V performed). If this is agreed in the contractual agreement with the bank (or covered by the contractual framework provided by domestic and international schemes), merchants and wallet providers do not have to repeat ID&V process to register those FIDO Authenticators.

A second use case is a scenario in which consumers enroll multiple authenticators for the same payment instrument but at different times from the initial registration process. In this use case, consumers are normally expected to go through a new initial registration process each time they add a new FIDO Authenticator. If it is agreed in the contractual agreement with the bank (or covered by the contractual framework provided by domestic and international schemes), merchants and wallet providers may choose to authenticate the consumer without the need for the bank to be involved, e.g. by authenticating with the FIDO Authenticator that was initially registered for that payment instrument.

6.5 Use of FIDO Across Merchant Apps and Web Pages

The same FIDO Authenticator can be used across all merchant interfaces, without the need for the consumer to enroll a new FIDO credential for each interface. A signed FIDO response is consistently generated and shared with the merchant for validation.

The following use cases can apply:

1. A FIDO Authenticator is initially registered through the merchant app installed on the consumer device:
   a. The same FIDO Authenticator can be used from the merchant web page visited by the consumer on the same device.
   b. The same FIDO Authenticator can be used as a roaming authenticator i.e. to authenticate the consumer on a different device (out of band).
2. A FIDO Authenticator is initially registered through the merchant page visited by the consumer on their device; the same FIDO Authenticator can be used from the merchant app installed by the consumer on the same device.

6.6 Account Recovery

If the FIDO Authenticator or the consumer device on which the FIDO Authenticator is located is lost or stolen, consumers need to go through a new initial registration process to enroll a new FIDO Authenticator.

7. FIDO Data Shared with Banks

As indicated in section 3.2.1, banks have different levels of trust relationships with merchants or wallet providers and therefore require different amounts of information to be shared with them (or with their agent) at the time of transaction. This section provides details on the options described in section 3.2.2 for sharing evidence with the bank – protocols for sharing such evidence include EMV 3D-Secure and other communication protocols that may use similar levels of data sharing in their APIs, e.g. EMV Secure Remote Commerce, Open Banking APIs, and other domestic or international standards.

Delegated authentication frameworks may be provided by domestic or international payment schemes to determine which option is relevant for each remote use case, and the right amount of data to share with banks (or their agent).

7.1 Success Signal Only

In the "Minimal sharing, maximal trust" model, the merchant or wallet provider only indicates that authentication was performed with FIDO – but no FIDO data is shared with the bank.

For example, in EMV 3DS 2.2, the signal can be sent through the "3DS Requestor Challenge Indicator" field, as a value "07- No challenge requested, strong consumer authentication is already performed". The merchant or wallet provider can also indicate that FIDO was used in the "3DS Requestor Authentication Method" as a value "06- Login to the cardholder account at the 3DS Requestor system using FIDO Authenticator".

7.2 FIDO Authentication Data for Partial Validation

When sharing some amount of FIDO Authentication data, in addition to consumer, merchant and device data, banks (or their agent) have a better indication that the consumer has been authenticated to the transaction. As a result, the bank should rarely prompt the consumer for additional bank authentication.

In EMV 3DS, merchants and wallets can leverage the 3DS data element "3DS Requestor Authentication Information", and in particular the sub-field "3DS Requestor Authentication Data", to share FIDO Authentication Data.

The FIDO Authentication Data to share with banks for partial validation during initial registration and checkout processes include:

- Authentication time: time when FIDO Authentication was performed.
- Relying Party identifier: identifier of the Relying Party to which the FIDO Public Key was registered (FIDO2 or U2F).
- Public Key: generated on consumer device and registered with the Relying Party.
- Authenticator attestation identifier: identifier of the authenticator model.
- Confirmation that user gesture and/or user verification was performed.
- More information on how merchants or wallet providers can format the 3DS request with those fields is included in the FIDO whitepaper[14].

7.3 FIDO Authentication Data for Full Validation

When sharing the FIDO signed response (FIDO Assertion) as part of the FIDO Authentication data, banks (or their agent) can validate the FIDO Authentication performed by the merchant or the wallet provider. As a result, the bank should never prompt the consumer for additional bank authentication.

The FIDO Authentication Data to share with banks during the registration process includes the FIDO Registration Assertion, which itself includes the attestation statement and the FIDO Public Key.

The FIDO Authentication Data to share with banks during the checkout process includes the FIDO Authentication Assertion, which itself includes the FIDO signed response data.

Banks store the FIDO Public Key during the registration process and validate the FIDO Authentication Assertion using that FIDO Public Key during the checkout process.

[14] https://media.fidoalliance.org/wp-content/uploads/2020/09/FIDO-and-EMV-3DS-Technical-Note-2020-09-01.pdf

8. Conclusions

The use of SCA Delegation addresses the concerns of transactions being abandoned by consumers because of the added friction or difficulty for consumers to properly authenticate to their banks. Merchants and wallet providers have an opportunity to leverage authentication mechanisms that they have established during the course of their relationship with consumers, for access to their account or to authenticate to remote transactions, as a delegation of the bank's authentication.

FIDO is an industry standard that best fits the needs of banks for the implementation of SCA Delegation, as it is designed to authenticate consumers with a high level of security and privacy, and it provides full compliance with regulations like PSD2. Communication protocols like EMVCo 3D-Secure already allow banks to receive a confirmation that authentication has been performed with FIDO and to receive FIDO results from merchants or wallet providers, allowing them to partially or fully validate the authentication that was performed on their behalf.

FIDO is also the best fit for merchants and wallet providers as it delivers an intuitive and consistent user experience across different devices and platforms, making the solution fully interoperable and scalable, and it provides an easier way to authenticate without impacting the checkout process. Merchants and wallet providers can enroll consumers in just a few steps before they can authenticate consumers to access their accounts or authenticate to the transaction.

For more information, see:

- FIDO specifications, at https://fidoalliance.org/specifications/
- FIDO certification process, at https://fidoalliance.org/certification/
- FIDO certified products, at https://fidoalliance.org/certification/fido-certified-products/
- Implementation of SCA Delegation, by reaching out to domestic or international payment schemes, and to PSPs.