

HOW FIDO STANDARDS MEET PSD2's REGULATORY TECHNICAL STANDARDS REQUIREMENTS ON STRONG CUSTOMER AUTHENTICATION

December, 2018

1 Introduction

This document provides a detailed review of the security requirements listed in the Regulatory Technical Standards For Strong Customer Authentication and Common and Secure Open Standards Of Communication under PSD2 (the RTS) and describes how the FIDO standards meet such requirements.

The document analyses articles in the following relevant sections of the RTS:

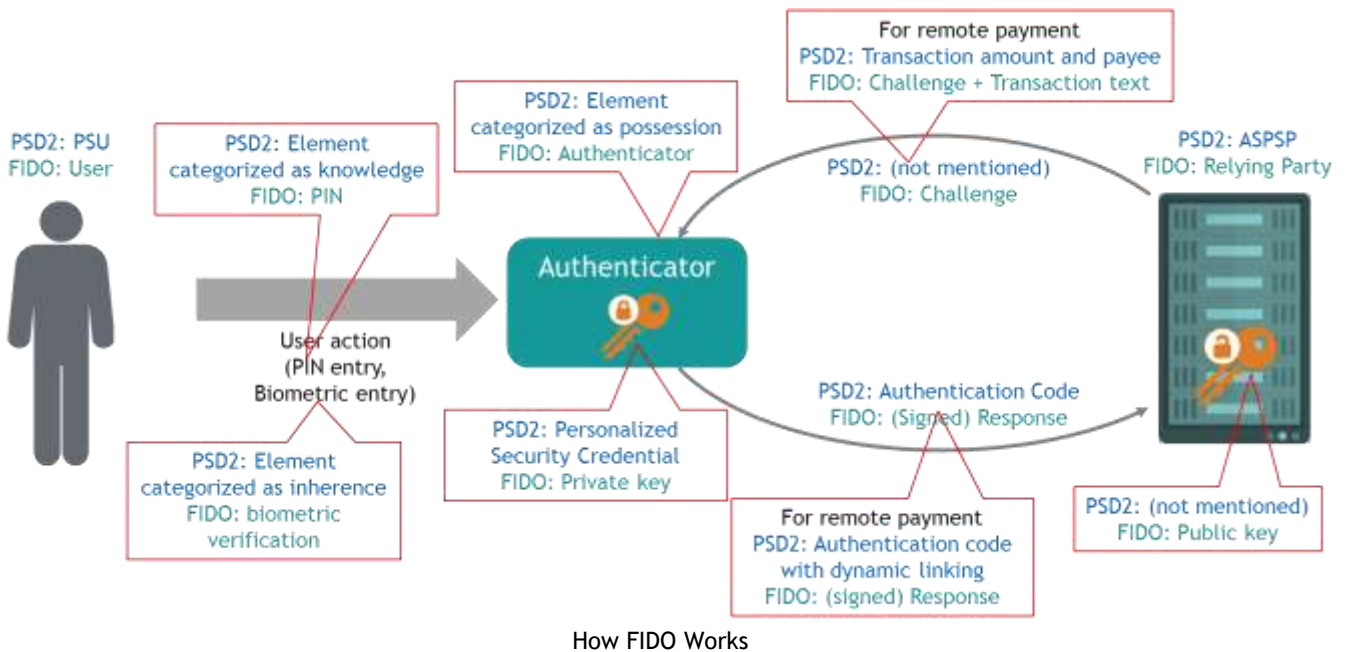
- [RTS Chapter I] General provisions
- [RTS Chapter II] Security measures for the application of Strong Customer Authentication
- [RTS Chapter IV] Confidentiality and integrity of the Payment Service User’s security credentials

When analyzing the requirements of the RTS, this document will from time to time refer to the different FIDO standards, UAF, U2F and FIDO2 to indicate specifically to which standard the description applies. Where not indicated, it is implied that the description applies to any of the FIDO standards.

2 FIDO essentials

2.1 FIDO authentication

The figure below illustrates the basic two step user authentication mechanism provided by the FIDO standards. The figure also maps PSD2 terminology with terminology used in the FIDO standards:



To authenticate with FIDO, the Payment Service User (PSU) must have a FIDO authenticator that can either be integrated in a general purpose device (e.g. Smartphone, Laptop) or be a separate device (e.g. Security Key, smart card).

User verification

The first step of FIDO authentication is the user verification step that is performed off-line, locally, by the authenticator. This user verification step can be:

- A verification of user presence whereby the user makes a gesture with the authenticator (for example, touches a security key or taps an NFC card on a reader).
- The verification of a PIN code or of biometric data by the authenticator. In this case, the local user verification constitutes one of the authentication factors mandated by the RTS.

The fact that the user verification data (PIN code or biometric data) is stored in the authenticator, verified locally and never transmitted to or shared with servers is a strong asset of the FIDO approach. As such, FIDO implements the privacy design requirement of the General Data Protection Regulation.

The local user verification step is a pre-requisite for the on-line authentication step.

On-line authentication








The on-line authentication step proves the possession of the FIDO authenticator and constitutes a second factor of authentication mandated by PSD2. In this step, the ASPSP server sends a challenge message to the authenticator which is then cryptographically signed by a private key stored in the authenticator. The signed response is returned to the ASPSP and its positive verification serves as proof of possession.

The FIDO standards are based on public key cryptography. The private key is the Personalized Security Credential described in the RTS. It is part of a key pair randomly generated by the Authenticator itself and is not known to any other party. At the generation time, the associated public key is sent in a protected way to the ASPSP.

The Authenticator maintains dedicated Personalized Security Credentials (private keys) for each ASPSP. For example, if the PSU has accounts at ASPSP1 and ASPSP2, the Authenticator would store different Personalized Security Credentials for ASPSP1 and ASPSP2, each being restricted for use with the respective ASPSP.

2.2 Authenticators

FIDO authenticators exist in several implementations and are classified as shown in the table below:

	Bound/Platform authenticators	Roaming authenticators
Multi Factor authentication (possession + knowledge/inherence)	 PC with TPM & PIN or biometric capture  Smart phone with TEE & PIN or biometric capture	 Smart card with PIN or fingerprint sensor  Security key with PIN or fingerprint sensor
2 nd factor (Login & Password + possession factor)	 PC with TPM only	 Smart card  Security key

Examples of FIDO authenticators

2.3 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 smart phones.

FIDO U2F (Universal 2nd Factor) is a FIDO standard that adds an authenticator, the possession factor, to an existing log-in + password authentication method. U2F devices are typically USB security keys.

FIDO2 is a FIDO standard that consists of **WebAuthn**, a set of web APIs, specified by the W3C organization in collaboration with the FIDO Alliance, that are natively incorporated in recent browsers; and **CTAP**, a communication protocol to connect to FIDO authenticators. Much like UAF, FIDO2 enables completely replacing passwords, not only on mobile devices, but also on desktops and laptops when configured with appropriate security devices. Additionally, U2F devices are compatible with CTAP. Collectively, WebAuthn and CTAP standardize access from a browser on a platform (a PC or mobile device) to a FIDO authenticator.

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

3 References

1. RTS: http://ec.europa.eu/finance/docs/level-2-measures/psd2-rts-2017-7782_en.pdf
2. FIDO Authenticator Certification Program: <https://fidoalliance.org/certification/authenticator-certification-levels/>
3. FIDO Security Requirements: <https://fidoalliance.org/specs/fido-security-requirements-v1.1-fd-20171108/fido-authenticator-security-requirements-v1.1-fd-20171108.html>
4. FIDO Specifications: <https://fidoalliance.org/download/>
5. FIDO Security Reference: <https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-security-ref-v1.2-rd-20171128.html>
6. FIDO Metadata Service: <https://fidoalliance.org/mds/>
7. FIDO Metadata Service Specification: <https://fidoalliance.org/specs/fido-uaf-v1.1-ps-20170202/fido-metadata-service-v1.1-ps-20170202.html>
8. FIDO Metadata Statement Specification: <https://fidoalliance.org/specs/fido-uaf-v1.1-ps-20170202/fido-metadata-statement-v1.1-ps-20170202.html> and <https://fidoalliance.org/specs/fido-v2.0-rd-20170927/fido-metadata-service-v2.0-rd-20170927.html>

4 [RTS Chapter I] General provisions

4.1 [RTS Article 3] - Review of the Security Requirements

Article	Requirement	How FIDO Meets It
Article 3.1	The implementation of the security measures referred to in Article 1 shall be documented, periodically tested, evaluated and audited in accordance with the applicable legal framework of the payment service provider by auditors with expertise in IT security and payments and operationally independent within or from the payment service provider	<p>The FIDO security certification program (see https://fidoalliance.org/certification/authenticator-certification-levels/) 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.</p> <p>Depending on the security level, the FIDO certification makes use of different partner programs, such as Common Criteria, Global Platform or FIPS, to simplify the work of the vendor in meeting FIDO evaluation goals.</p>

5 [RTS Chapter II] Security measures for the application of Strong Customer Authentication

5.1 [RTS Article 4] - Authentication code

Article	Requirement	How FIDO Meets It
Article 4.1	The authentication shall be based on two or more elements which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code	<p>To authenticate with FIDO, the Payment Service User (PSU) must possess a FIDO authenticator that is either integrated in a general purpose device (e.g. Smartphone, Laptop, ...) or in a separate device (e.g. Security Key, smart card...).</p> <p>As seen in chapter 2 of this document, possession of such a FIDO authenticator</p>

Article	Requirement	How FIDO Meets It
		<p>satisfies the first of the two elements required to authenticate the PSU.</p> <p>The second element required to authenticate the PSU consists in:</p> <ul style="list-style-type: none"> - For U2F, a password sent on-line and verified by the server - For UAF and FIDO2, an inherence (biometric) factor or knowledge (PIN) factor verified locally by the FIDO authenticator <p>The signed response, created by the authenticator and returned to the ASPSP, constitutes the authentication code mandated by the RTS.</p>
Article 4.2	<p>For the purpose of paragraph 1, payment service providers shall adopt security measures ensuring that each of the following requirements is met:</p> <ul style="list-style-type: none"> (a) no information on any of the elements referred to in paragraph 1 can be derived from the disclosure of the authentication code; (b) it is not possible to generate a new authentication code based on the knowledge of any other authentication code previously generated; (c) the authentication code cannot be forged. 	<p>With FIDO, the authentication code is generated with the private key stored in the authenticator, using public key cryptographic algorithms (RSA or Elliptic Curve).</p> <ul style="list-style-type: none"> (a) The elements of knowledge or of inherence are not typically used in the calculation of the authentication code and if they were, the cryptographic algorithms would make it extremely difficult to retrieve these elements from the knowledge of the authentication code (b) By design, the cryptographic algorithms make it extremely difficult to retrieve the private key necessary to generate a new authentication code based on the knowledge of previously generated authentication codes (c) Any change to the authentication code would be detected by the ASPSP as its verification, using the Public Key, would fail
Article 4.3	<p>Payment service providers shall ensure that the authentication by means of generating an authentication code includes each of the following measures:</p> <ul style="list-style-type: none"> (a) where the authentication for remote access, remote electronic payments and any other actions through a remote channel which may imply a risk of payment fraud or other abuses has failed to generate an authentication code for the purposes of paragraph 1, it shall not be possible to identify which of the elements referred to in that paragraph was incorrect; (b) the number of failed authentication attempts that can take place consecutively, after which the actions referred to in Article 97(1) of Directive (EU) 2015/2366 	<ul style="list-style-type: none"> (a) With FIDO U2F, a password is entered by the PSU and sent to the ASPSP. The U2F device will independently generate an authentication code that will be verified by the ASPSP. The authentication code carries proof of possession of the authenticator. The ASPSP may implement the authentication procedure so that no feedback is provided to the user (or an attacker) on which authentication element (password or authentication code) was incorrect. <p>With FIDO UAF and FIDO2, the correct submission of a PIN code (knowledge factor) or biometric data (inherence factor) is a pre-requisite to the generation by the authenticator of the authentication code (possession factor). An attacker can therefore not test the possession factor distinctly from the knowledge/inherence factor. Under normal circumstances, the attacker will not have possession of the authenticator and so will not be able to test the inherence or knowledge elements. If the attacker has succeeded to</p>

Article	Requirement	How FIDO Meets It
	<p>shall be temporarily or permanently blocked, shall not exceed five within a given period of time;</p> <p>(c) the communication sessions are protected against the capture of authentication data transmitted during the authentication and against manipulation by unauthorised parties in accordance with the requirements in Chapter V;</p> <p>(d) the maximum time without activity by the payer after being authenticated for accessing its payment account online shall not exceed 5 minutes.</p>	<p>get access to the authenticator, then although the attacker will be able to test the knowledge or inherence factor, the authenticator can implement a method to rapidly stop the attacker through a maximum number of attempts. The use of a Secure Execution Environment (see also RTS Article 9.2) helps enforcing this behavior. The use of a Secure Execution Environment, the method for managing local user verification and the maximum number of attempts can be published for an Authenticator through the FIDO Metadata Service.</p> <p>(b) The FIDO UAF or FIDO2 standards propose various ways of limiting the number of failed consecutive user verification (PIN or biometrics) attempts. In particular, authenticators that support local user verification can be designed to become blocked after 5 consecutive failed attempts, either temporarily, or permanently or until an alternative user verification method succeeds. For FIDO U2F, the ASPSP may implement the constraint within the application responsible for coordinating the FIDO authentication process between the FIDO U2F server and the FIDO U2F authenticator.</p> <p>(c) The FIDO standards require that the communication between the FIDO authenticator and the FIDO server must use a TLS protected channel</p> <p>(d) This requirement is not in the scope of FIDO: it is up to the ASPSP application to manage user inactivity after user was authenticated.</p>

5.2 [RTS Article 5] - Dynamic linking

Article	Requirement	How FIDO Meets It
Article 5.1	<p>Where payment service providers apply strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366, in addition to the requirements of Article 4 of this Regulation, they shall also adopt security measures that meet each of the following requirements:</p> <p>(a) the payer is made aware of the amount of the payment transaction and of the payee;</p>	<p>The FIDO standards support these requirements in two ways:</p> <ul style="list-style-type: none"> The message sent by the FIDO server to the authenticator can include the amount, payee ID and other data. The signed response will then cryptographically link this data to the authentication code. FIDO UAF's "Transaction Confirmation" mechanism or FIDO2's "Transaction Authorization" extensions can be used, when supported by the authenticator: Such authenticators will be able to display the transaction

Article	Requirement	How FIDO Meets It
	<ul style="list-style-type: none"> (b) the authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction; (c) the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer; (d) any change to the amount or the payee results in the invalidation of the authentication code generated. 	<p>text to the user and ask for user approval. Successful approval is securely indicated to the ASPSP. The ASPSP can cryptographically verify that the transaction text displayed to the user is identical to the original transaction text provided by the ASPSP. This concept implements the “What-you-see-is-what-you-sign” model.</p>
<p>Article 5.2</p>	<p>For the purpose of paragraph 1, payment service providers shall adopt security measures which ensure the confidentiality, authenticity and integrity of each of the following:</p> <ul style="list-style-type: none"> (a) the amount of the transaction and the payee throughout all of the phases of the authentication; (b) the information displayed to the payer throughout all of the phases of the authentication including the generation, transmission and use of the authentication code 	<p>(a) We distinguish 2 cases</p> <p>(a.1) use of FIDO Authentication (no transaction confirmation)</p> <p>The banking application may cryptographically bind the details (i.e. payee, amount,...) of the displayed transaction to the serverChallenge used in the FIDO protocol. As an example this could be done by computing the serverChallenge as a cryptographic hash computed over a random value generated on the server and transmitted to the App concatenated with the transaction details. The FIDO protocol will then cryptographically bind this serverChallenge to the authentication code computed using the personalized security credential. The FIDO Server will finally verify the integrity and authenticity by performing a cryptographic signature verification of the authentication code using the registered FIDO public key.</p> <p>It is the responsibility of the App to ensure correct display of the specific transaction details that is also used for this cryptographic binding. The FIDO protocol ensures that the authentication code is cryptographically bound to the serverChallenge.</p> <p>(a.2) use of FIDO UAF Transaction Confirmation or FIDO2 Transaction Authorization (if supported by the authenticator, the browser and the FIDO2 server)</p> <p>The banking application might generate the transactionText in the format supported by the Authenticator. The authenticator will then display the transactionText and cryptographically bind it to the authentication code.</p> <p>(b) With FIDO, the authentication code does not need to be displayed to the user. It is silently generated and securely transmitted by the authenticator to the FIDO server</p>

5.3 [RTS Articles 6/7/8/9] - Authentication Elements

Article	Requirement	How FIDO Meets It
Articles 6/7/8	<ol style="list-style-type: none"> 1. Payment service providers shall adopt measures to mitigate the risk that the elements of strong customer authentication categorised as knowledge/possession/inherence are uncovered by, or used by or disclosed to, unauthorised parties. 2. The use by the payer of those elements shall be subject to mitigation measures in order to prevent their disclosure to unauthorised parties or their replication or their unauthorised use. 3. Payment service providers shall ensure that access devices and software that read authentication elements categorised as inherence have a very low probability of an unauthorised party being authenticated as the payer. 	<p>The knowledge factor, such as a PIN code, and the inherence factor, typically biometric data, are stored in the FIDO (UAF or FIDO2) authenticator by the user at registration time. Once stored, they never leave the authenticator and cannot be read, copied or transferred. They can only be used, by the authenticator itself, to verify they match the knowledge factor and/or inherence factor presented by the user at authentication time.</p> <p>Moreover, because the authenticator itself performs the verification of the knowledge factor and/or inherence factor, this authenticator, which confirms the possession factor, cannot be used by an unauthorised party.</p> <p>FIDO authenticators that capture, store, read and compare biometric data are subject to a FIDO biometric certification that attests to the quality level of the biometric implementation. Criteria such as False Acceptance Rate, False Rejection Rate and Presentation Attack Detection are tested.</p>
Article 9 (1)	<p>Payment service providers shall ensure that the use of the elements of strong customer authentication referred to in Articles 6, 7 and 8 is subject to measures which ensure that, in terms of technology, algorithms and parameters, the breach of one of the elements does not compromise the reliability of the other elements.</p>	<p>The breach of the knowledge or inherence factor, i.e. the fraudster was able to obtain the user's PIN code or biometric data, does not compromise the possession factor: the fraudster cannot access the private key or duplicate it in another device.</p> <p>Conversely, the fraudster that steals a valid authenticator would face considerable difficulties trying to retrieve the PIN code or biometric data securely stored in this authenticator.</p>
Article 9.2 and 9.3	<p>Payment service providers shall adopt security measures, where any of the elements of strong customer authentication or the authentication code itself is used through a multi-purpose device, to mitigate the risk which would result from that multi-purpose device being compromised.</p>	<p>FIDO authenticators are commonly implemented in multi-purposes devices. The FIDO security standards call for a separation of the FIDO authenticator from other applications in the device. This is achieved by the use of a separated execution environment and protection of this environment from intrusion or alteration.</p> <p>FIDO authenticator implementations can be tested and certified both functionally and from a security perspective. The FIDO certification program defines 3 possible</p>

Article	Requirement	How FIDO Meets It
	<p>For the purposes of paragraph 2, the mitigating measures shall include each of the following:</p> <ul style="list-style-type: none"> (a) the use of separated secure execution environments through the software installed inside the multi-purpose device; (b) mechanisms to ensure that the software or device has not been altered by the payer or by a third party; (c) where alterations have taken place, mechanisms to mitigate the consequences thereof. 	<p>implementations of a FIDO authenticator in a multi-purpose device:</p> <p>One is using a pure software implementation hardened through security techniques such as white box cryptography and code obfuscation. Penetration tests performed by a FIDO accredited lab will measure the robustness of such implementations both in terms of protection of the security credentials or resistance to attacks and alterations of the code and of creating a firewall between the FIDO authenticator code and the rich OS environment of the multi-purpose device. This testing leads to a FIDO L1+ security certification.</p> <p>Another implementation uses a Restricted Operating Environment such as a Trusted Execution Environment (TEE) that are commonly found in smart phones and laptops. Completion of penetration testing that fails to compromise the device along with FIDO functional evaluation will lead to a FIDO L2+ security certification.</p> <p>A third type of implementation uses hardware components such as Secure Elements that are designed to resist probing and tampering and that incorporate firewalling features. Here again, completion of penetration testing that fails to compromise the Secure Element along with FIDO evaluation will lead to a FIDO L3 or L3+ security certification.</p> <p>During the registration of a PSU's FIDO credential with the ASPSP, the ASPSP can determine the type of implementation and security certification achieved by the authenticator based on an attestation provided by the device's manufacturer and judge if the device is suitable for its application.</p>

6 [RTS Chapter IV] Confidentiality and integrity of the Payment Service User’s security credentials

6.1 [RTS Article 22] - General Requirements

Article	Requirement	How FIDO Meets It
<p>Article 22.1 & 22.2</p>	<ol style="list-style-type: none"> 1. Payment service providers shall ensure the confidentiality and integrity of the personalised security credentials of the payment service user, including authentication codes, during all phases of the authentication. 2. For the purpose of paragraph 1, payment service providers shall ensure that each of the following requirements is met: <ol style="list-style-type: none"> (a) personalised security credentials are masked when displayed and are not readable in their full extent when input by the payment service user during the authentication; (b) personalised security credentials in data format, as well as cryptographic materials related to the encryption of the personalised security credentials are not stored in plain text; (c) secret cryptographic material is protected from unauthorised disclosure. 	<ol style="list-style-type: none"> 1. With FIDO, personalized security credentials (PSCs) are cryptographic key pairs created within the authenticator for each ASPSP account. The private key is held securely and never leaves the device (see requirement 2.1.2 and 2.1.6 https://fidoalliance.org/specs/fido-security-requirements-v1.1-fd-20171108/fido-authenticator-security-requirements-v1.1-fd-20171108.html#documentation). <p>The public key is securely transmitted to the ASPSP. The private key is used to create the authentication code by signing a message received from the ASPSP. This authentication code is not visible to the user and transmitted, using a secure channel (TLS), to the ASPSP for verification. Any tampering of the authentication code by the user or an attacker between the FIDO authenticator and the ASPSP application and/or the FIDO server, will be detected and rejected by the FIDO server.</p> <p>Furthermore, ASPSPs define a policy specifying acceptable authenticators. FIDO attestation securely conveys the authenticator model to the ASPSP which verifies whether the authenticator model is acceptable and will only allow use of acceptable ones. The FIDO Alliance runs an Authenticator certification program (see https://fidoalliance.org/certification/authenticator-certification-levels/). The program is based on third party testing of authenticators. The Certification Policy as well as the Security Requirements are publicly available.</p> <p>2(a). In the case of FIDO, the private key part of the PSC is not known by the user, is never displayed to the user and is not accessible.</p> <p>2(b), 2(c). The authenticator protects its private and secret key material. The protection level depends on the authenticator model (e.g. TEE, secure element). The authenticator model information is available through the attestation statement</p>

Article	Requirement	How FIDO Meets It
		<p>which can be published via the FIDO Metadata Service (see https://fidoalliance.org/mds/). The authenticator model specific Metadata Statements can be downloaded in a cryptographically secure way from https://mds.fidoalliance.org. The FIDO Server verifies the Metadata Statements and confirms that the authenticator is acceptable to the ASPSP based on information within the Metadata Statements.</p> <p>The FIDO Alliance’s authenticator certification program is designed to provide a third party verification of the authenticator’s protection level (see https://fidoalliance.org/certification/authenticator-certification-levels/).</p>
Article 22.3	Payment service providers shall fully document the process related to the management of cryptographic material used to encrypt or otherwise render unreadable the personalised security credentials.	<p>The authenticator related aspects are fully documented by</p> <ul style="list-style-type: none"> a) the FIDO Alliance specifications (see https://fidoalliance.org/download/) , b) the certification policy and security requirements see (https://fidoalliance.org/certification/authenticator-certification-levels/#Docs) and c) The Metadata Statements that include the authenticator security characteristics and certification status and that is downloadable from mds.fidoalliance.org (see https://fidoalliance.org/mds/, https://fidoalliance.org/specs/fido-uaf-v1.1-ps-20170202/fido-metadata-service-v1.1-ps-20170202.html and https://fidoalliance.org/specs/fido-uaf-v1.1-ps-20170202/fido-metadata-statement-v1.1-ps-20170202.html).
Article 22.4	Payment service providers shall ensure that the processing and routing of personalised security credentials and of the authentication codes generated in accordance with Chapter II take place in secure environments in accordance with strong and widely recognised industry standards.	<p>Personalized Security Credentials are cryptographic key pairs that are generated by the Authenticator and the related private keys are never disclosed by the Authenticator.</p> <p>Generation and protection of such keys is verified by the Authenticator certification (https://fidoalliance.org/certification/authenticator-certification-levels/) in accordance with the FIDO specifications, requirements that are based on recognised industry standards (such as ANSI X9.63-2011, FIPS 140-2, ISO15946-5, AIS 20/31 PTG.2 or PTG.3, NIST SP 800-90C and others).</p>

6.2 [RTS Article 23] - Creation and transmission of credentials

Article	Requirement	How FIDO Meets It
Article 23	<p>Payment service providers shall ensure that the creation of personalised security credentials is performed in a secure environment.</p> <p>They shall mitigate the risks of unauthorised use of the personalised security credentials and of the authentication devices and software following their loss, theft or copying before their delivery to the payer.</p>	<p>Personalized Security Credentials are cryptographic key pairs that are generated by the Authenticator and the related private keys are never disclosed by the Authenticator.</p> <p>Generation and protection of such keys is verified by the Authenticator certification (https://fidoalliance.org/certification/authenticator-certification-levels/) in accordance with the FIDO specifications, requirements that are based on recognised industry standards (such as ANSI X9.63-2011, FIPS 140-2, ISO15946-5, AIS 20/31 PTG.2 or PTG.3, NIST SP 800-90C and others).</p> <p>The use of the personalised security credential is subject to the correct presentation to the authenticator of a PIN code or of biometric information. An incorrect submission prevents the use of the personalised security credential and of the authenticator itself.</p>

6.3 [RTS Article 24] - Association with the payment service user

Article	Requirement	How FIDO Meets It
Article 24.1 & 24.2	<ol style="list-style-type: none"> 1. Payment service providers shall ensure that only the payment service user is associated, in a secure manner, with the personalised security credentials, the authentication devices and the software. 2. For the purpose of paragraph 1, payment service providers shall ensure that each of the following requirements is met: <ol style="list-style-type: none"> (a) the association of the payment service user's identity with personalised security credentials, authentication devices and software is carried out in secure environments under the payment service provider's responsibility comprising at least the payment service provider's premises, the internet environment provided by the payment service provider or 	<p>FIDO Authenticators support a registration step during which a random Personalized Security Credential (PSC) is securely generated and during which the user defines a PIN code or enrolls his/her biometric information.</p> <p>This subsequently ensures that the user is associated with the PSC as only a correct submission of the user verification data (PIN or biometric information) will unlock the PSC during user authentication.</p> <p>As part of the registration procedure, Payment Service Providers must ensure proper user identity proofing (Know-Your-Customer) in order to bind this identity with the personalised security credential. This step is outside of the scope of FIDO and is expected to be performed by the PSP's application(s).</p>

Article	Requirement	How FIDO Meets It
	<p>other similar secure websites used by the payment service provider and its automated teller machine services, and taking into account risks associated with devices and underlying components used during the association process that are not under the responsibility of the payment service provider;</p> <p>(b) the association by means of a remote channel of the payment service user's identity with the personalised security credentials and with authentication devices or software is performed using strong customer authentication.</p>	

6.4 [RTS Article 25] - Delivery of credentials, authentication devices and software

Article	Requirement	How FIDO Meets It
<p>Article 25.1 & 25.2</p>	<ol style="list-style-type: none"> 1. Payment service providers shall ensure that the delivery of personalised security credentials, authentication devices and software to the payment service user is carried out in a secure manner designed to address the risks related to their unauthorised use due to their loss, theft or copying. 2. For the purpose of paragraph 1, payment service providers shall at least apply each of the following measures: <ol style="list-style-type: none"> (a) effective and secure delivery mechanisms ensuring that the personalized security credentials, authentication devices and software are delivered to the legitimate payment service user; (b) mechanisms that allow the payment service provider to verify the authenticity of the authentication software delivered to the payment services user by means of the internet; (c) arrangements ensuring that, where the delivery of 	<p>1 & 2(a) With FIDO, Payment Service Providers (PSPs) can either deploy FIDO authenticators, such a security keys or smart cards, to PSUs or accept FIDO Authenticators already possessed by their customers, such as smart phones or PCs, provided they meet the PSP's security requirements.</p> <p>The deployment (delivery) of FIDO authenticators is not necessarily a sensitive operation as they do not contain secret keys or credentials belonging to the PSP at this stage.</p> <p>The PSC is generated as part of the FIDO registration step (see above).</p> <p>Assuming the PSP's application has verified the PSU's real-world identity (based on KYC processes), the FIDO registration step ensures that only the legitimate payment services user has access to the authenticator and can pass the user verification checks implemented by the authenticator.</p>

Article	Requirement	How FIDO Meets It
	<p>personalised security credentials is executed outside the premises of the payment service provider or through a remote channel:</p> <p>(i) no unauthorised party can obtain more than one feature of the personalised security credentials, the authentication devices or software when delivered through the same channel;</p> <p>(ii) the delivered personalised security credentials, authentication devices or software require activation before usage;</p> <p>(d) arrangements ensuring that, in cases where the personalised security credentials, the authentication devices or software have to be activated before their first use, the activation shall take place in a secure environment in accordance with the association procedures referred to in Article 24.</p>	<p>2(b) The authenticity of the authenticator is cryptographically verified by the ASPSP’s FIDO server as part of the FIDO Registration process (see above). This step is particularly supported by the Authenticator attestation.</p> <p>2(c) The PSC is generated only at a time when the PSU has physical access to the authenticator. The private key part of the PSC itself never leaves the authenticator - only the public key related to the PSC is sent with cryptographic integrity protection to the PSP. This ensures that only the legitimate PSU can create the PSC using his/her authenticator.</p> <p>2(d) With the FIDO registration process, no additional activation process is required.</p>

6.5 [RTS Article 26] - Renewal of personalized security credentials

Article	Requirement	How FIDO Meets It
Article 26	<p>Payment service providers shall ensure that the renewal or re-activation of personalized security credentials adhere to the procedures for the creation, association and delivery of the credentials and of the authentication devices in accordance with Articles 23, 24 and 25.</p>	<p>FIDO protocols do not require that the key pairs that constitute the PSCs expire - this is left to the Payment service providers as a policy decision for their applications. As such, should PSPs choose to expire a PSC for any reason, they can simply “re-activate” a PSC by marking the related public key as “valid” within their FIDO server.</p> <p>Each PSP may have distinct reactivation ceremonies that meet the needs of their users. Each PSP will document the organisational aspects of such re-activation process, i.e. describe how their process is triggered.</p>

6.6 [RTS Article 27] - Destruction, deactivation and revocation

Article	Requirement	How FIDO Meets It
Article 27	<p>Payment service providers shall ensure that they have effective processes in place to apply each of the following security measures:</p> <p>(a) the secure destruction, deactivation or revocation of the personalised security credentials, authentication devices and software;</p> <p>(b) where the payment service provider distributes reusable authentication devices and software, the secure re-use of a device or software is established, documented and implemented before making it available to another payment services user;</p> <p>(c) the deactivation or revocation of information related to personalised security credentials stored in the payment service provider’s systems and databases and, where relevant, in public repositories.</p>	<p>FIDO protocols do not require that the key pairs that constitute the PSCs expire. Payment service providers can simply “revoke” or “suspend” a PSC by marking the related public key as “revoked” or “suspended” within their FIDO server.</p> <p>The PSP will document the organisational aspects of such revocation / suspension process, i.e. describe how the process is triggered.</p> <p>Note: PSCs are always generated randomly when performing the initial “Registration” step. They are never re-used. Authenticators that are an integral part of a multi-functional device (such as a smartphone) may support a factory reset. This function will also erase all existing keys (see requirement 2.1.17 in https://fidoalliance.org/specs/fido-security-requirements-v1.1-fd-20171108/fido-authenticator-security-requirements-v1.1-fd-20171108.html).</p>