Information paper

Strong Customer Authentication under Payment Services Directive 2 (PSD2)

SWIFT launches advanced token technology to support banks and service providers in complying with new PSD2 regulatory security requirements on remote online banking channels, applicable as from 2018.

March 2017

Contents

Scope of Payment Services Directive 2 (PSD2)

On December 23, 2015, the second Payment Services Directive (PSD2) was published in the Official Journal of the European Union. By January 2018, PSD2 must be transposed into national legislation and become fully applicable, subject to some exceptions. PSD2 was put in place to boost transparency, innovation and security in the European payments market. It addresses new types of Payment Service Providers (PSPs), like Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs). While creating a playing level field for these new providers it simultaneously aims to bring these emerging types of payment services within regulatory scope.

In parallel, PSD2 establishes a stricter regime of payment service user authentication, with the aim of ensuring that PSPs can be confident in the authenticity of users. PSD2 requires PSPs to apply “Strong Customer Authentication” (SCA) in cases where an organisation or consumer tries to access their payment accounts online, initiates an electronic payment transaction or “carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.” It is clear that this requirement will impact a number of financial institutions by requiring them to revise the authentication mechanisms currently used in their online banking systems.

Strong Customer Authentication

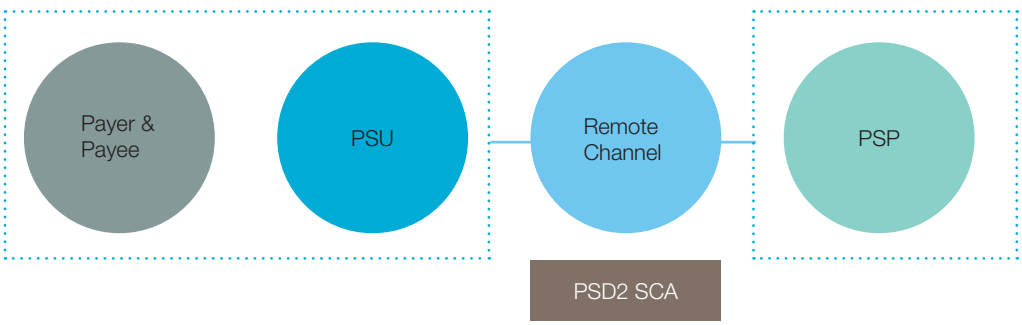
The European Banking Authority (EBA) developed the 'technical' requirements for SCA, in close cooperation with the European Central Bank (ECB).

The resulting Regulatory Technical Standards (RTS) also include:

- the requirements with which security measures have to comply in order to protect the confidentiality and integrity of the payment service users' personalised security credentials;
- the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification and information;
- and the requirements "for the implementation of security measures, between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers."

To prepare these RTS, EBA has made it clear that it is seeking to strike a balance between tough security standards and specific protocols, versus customer convenience and future innovative industry solutions. In PSD2, two-factor authentication is highlighted as a must for SCA. Therefore, authentication procedures must be based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence:

- something only the user knows; e.g., static password, code, personal identification number;
- something only the user possesses; e.g., token, smart card, mobile phone;
- something the user is; e.g., biometric characteristic, such as a fingerprint.



PSD2 = Payment Services Directive 2
SCA = Strong Customer Authentication

PSU = Payment Service User
PSP = Payment Service Provider

Regulatory Technical Standards

On February 23, 2017, the European Banking Authority released its final draft RTS on Strong Customer Authentication and common and secure communication.

This final draft provides the industry with the high-level specifications for strong customer authentication, the exemptions from the application of strong customer authentication, the requirements with which security measures have to comply in order to protect the confidentiality and the integrity of the Payment Service Users' (PSUs) personalised security credentials, and the requirements for common and secure open standards of communication between Account Servicing Payment Service Providers (ASPSPs), PISPs, AISPs, payers, payees and other payment service providers.

Strong Customer Authentication under PSD2

- Mandatory two-factor user authentication (knowledge, ownership, inherence)
- Authentication code must be linked to the AMOUNT and PAYEE of the transaction or batch; i.e., dynamic linking
- Adoption of security measures to ensure confidentiality, authenticity and integrity of the information displayed through all phases, including generation, transmission and use of the authentication code
- Applicable to payment services provided to natural and legal persons on remote channels in the European Union as from 2018

The RTS specifies that the authentication procedure shall result in the generation of an authentication code that is accepted only once by the payment service provider each time the payer, making use of the authentication code, accesses his or her payment account online, initiates an electronic transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses. The authentication procedure shall also provide that the payer is made aware at all times of the amount of the transaction and of the payee, and the authentication code shall be specific to the amount of the transaction and the payee agreed to by the payer when initiating the transaction.

Therefore, the authentication procedure shall have in place a technological solution ensuring the confidentiality, authenticity and integrity of the amount of the transaction and of the payee through all phases of the authentication procedure (any change to the amount or payee shall result in a change of the authentication code); and the confidentiality, authenticity and integrity of the information displayed to the payer through all phases of the authentication procedure – including generation, transmission and use of the authentication code.

It is also necessary to define requirements ensuring that the elements of strong customer authentication are independent, so that the breach of one does not compromise the reliability of the others. Security protections are required for the elements of strong customer authentication, in particular to mitigate the risk that those elements are uncovered, disclosed to and used by unauthorised parties.

The final draft RTS has now been submitted to the Commission for adoption, following which they will be subject to scrutiny by the European Parliament and the Council before being published in the Official Journal of the European Union. The RTS will become applicable 18 months after its entry into force, which would suggest an application date of the RTS in November 2018 at the earliest. The transitional period provides the industry with time to develop industry standards and/or technological solutions that are compliant with the EBA's RTS.

SWIFT's Digital Identity Solution

SWIFT, in partnership with the banking community developed 3SKey, a global multi-bank and multi-channel electronic identity and signature service. 3SKey was designed to respond to a growing demand from financial institutions and their corporate clients for an international and interoperable digital identity solution. It enables strong authentication and personal signatures using a secure, scalable and cost-effective shared infrastructure. 3SKey uses a trusted and reliable SWIFT Public Key Infrastructure (PKI) as well as FIPS 140-2 certified hardware security tokens, and is using common and widely used industry standards.

In the context of 3SKey, SWIFT is responsible for the centralised issuance and management of credentials, functioning as the Certification Authority. Individual banks register the association of their 3SKey users with a credential stored on a physical PKI token, independently of one another and applying their own registration and KYC procedures. As part of the registration process, the bank and its 3SKey users agree amongst themselves directly on the legal effect of the 3SKey signatures and other conditions governing their use of 3SKey. The model is distinguished from other security solutions, in which corporate customers typically require separate devices for each of their banks.

3SKey provides a common solution and technical infrastructure for strong authentication and digital identity, preventing the need to invest in proprietary security management. 3SKey significantly reduces the investments and running costs to manage in-house security infrastructures or contracting with a third-party provider. Additionally, 3SKey provides enhanced customer satisfaction by offering a single token which the user can use to execute transactions securely with multiple institutions in multiple countries and on any electronic banking channel.

3SKey

Advanced Reader Technology

In 2017, SWIFT will extend the 3SKey solution with the launch of an advanced reader technology to support banks and service providers looking to increase security in their online web channels and further mitigate the threat of growing and sophisticated web attacks. The new device will operate under the same multi-bank framework and complement the current 3SKey basic token. The advanced reader enables to comply with the new PSD2 security requirements. Banks and service providers can benefit from this advanced technology to upgrade current authentication mechanisms. The device offers two-factor authentication and enables dynamic linking of the user authentication to the amount and payee of any electronic remote payment transaction.

The new advanced 3SKey reader is targeted for use in online channels requiring secure strong user authentication whilst authorising critical transactions. The technology provides on-board mitigation against sophisticated web attacks, including when the user environment cannot be trusted, and it limits the risk for banks to rely on fraudulent transactions. A smart card holding the user's PKI certificate and protected with a personal password is used for digitally signing transactions and files, providing the highest levels of integrity, user authentication and non-repudiation. The reader has an integrated PIN pad for secure entry of the user PIN, mitigating the risk of keystroke logging attacks to which a standard keyboard on the user's workstation can be vulnerable.

The 3SKey reader additionally offers a secure display allowing banks to implement "See-What-You-Sign" (SWYS) user controls. SWYS mechanisms require the user to confirm critical transaction elements, such as the amount or payee(s) in a transaction or file, on the secure display of the trusted reader. Such security mechanisms mitigate the risk of Man-in-the-Browser (MitB) attacks. The request for a user confirmation is optional, triggered by the bank application and may be dependent on the institution's own risk policies. Banks and service providers will decide for which transaction scenarios such SWYS user confirmation is required, e.g., transactions above a certain threshold amount, and in which cases the transaction can be completed without additional verification by the user on the device; e.g., when the payee belongs already to a trusted list of beneficiaries.

The new 3SKey advanced reader offers a solution in the highest security spectrum to banks, service providers and their customers. The device addresses EBA's regulatory requirements for security protection. It ensures the confidentiality, authenticity and integrity of the information displayed to the payer through all phases of the authentication procedure. Moreover, the 3SKey advanced reader enables dynamic linking on an independent and segregated device from the channel used for initiating the electronic payment transaction. This provides for a strong implementation of EBA's requirements on 2-factor authentication and dynamic linking whilst enabling banks and service providers to strengthen the security for the use of their online web channels.

The impact on the user experience is minimal and limited to comparing key transactional elements with the original instruction without having to re-enter data on the reader or in the application. The bank application decides if and for which critical transaction sets or business users a SWYS confirmation is required. The new device can also operate without making use of its advanced security features such as for off-line transaction authentication, providing users full interoperability of a single device across their banking channels.

About SWIFT

SWIFT is a global member-owned cooperative and the world's leading provider of secure financial messaging services.

We provide our community with a platform for messaging, standards for communicating and we offer products and services to facilitate access and integration; identification, analysis and financial crime compliance.

Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories, enabling them to communicate securely and exchange standardised financial messages in a reliable way.

As their trusted provider, we facilitate global and local financial flows, support trade and commerce all around the world; we relentlessly pursue operational excellence and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies.

Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's global office network ensures an active presence in all the major financial centres.

About 3SKey and PSD2

If you are interested to learn more about the 3SKey solution and how this product can help you increase security in online banking channels, or you would like to receive further information on upcoming regulatory security standards under PSD2, please contact your SWIFT relationship manager or contact us via email at swiftforcorporates@swift.com.

57251 - March 2017