A Broadcom Company
technologies

Product Brief

CA Viewpoint

Interpreting the RTS on SCA and CSC for PSD2

Description

This document interprets the European Commission's Second Payment Services Directive (PSD2) for Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Secure Open Standards of Communication (CSC). This document also describes how CA Technologies can help financial institutions with compliance.

Features

- EMV 3DS
- PSD2 RTS SCA
- Risk-Based Authentication

Applications

- CA Payment Security Suite
- CA Risk Analytics Network
- CA Identity Risk Insight Suite

Interpreting the Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Open Standards of Communication for PSD2

The European Commission's Second Payment Services Directive (PSD2) updates and enhances the EU rules defined in the first PSD from 2007. The authors of PSD2 were focused on delivering a more tightly integrated European payments market, fostering innovation, and increasing customer protection with safer payments.

PSD2 introduces three key changes:

- **Strong authentication.** PSD2 requires "*that a payment service provider applies strong customer authentication where the payer: (a) accesses its payment account online; (b) initiates an electronic payment transaction; (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.*"[1]
- **Expanded coverage.** After the European Commission evaluated the first payment services directive, it found that it had "*given rise to significant challenges from a regulatory perspective. Significant areas of the payment market, in particular card, internet and mobile payments, remain fragmented along national borders. Many innovative payment products or services do not fall, entirely or in large part, within the scope*" of the previous directive. PSD2 aims to "*close the regulatory gaps while at the same time providing more legal clarity and ensuring consistent application of the legislative framework across the Union.*"[2]
- **Open secure communications.** PSD2 foresees that the European Banking Authority (EBA) will develop "*the requirements for common and secure open standards of communications for the purpose of identification, authentication, notification, and information, as well as 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.*"[3]

Key Areas of Focus

The key areas of focus for PSD2, regarding the Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Common and Secure Open Standards of Communication (CSC), are:

- **Strong authentication.** Introduce strong, two-factor authentication for e-commerce and online payments. The EU defines strong customer authentication as being formed of two factors, each from a different class of the following elements: possession, inherence, and knowledge.
- **Real-time risk assessment.** Deploy real-time risk assessments based on customer behavior to prevent transactions that might be fraudulent. Article 18 of the RTS on SCA and CSC specifically defines the measures that regulated bodies should be taking to comply, including detection of transactions coming from unusual or high-risk, locations as well as those transactions that are outside of the payer's normal behavior.
- **Level the playing field.** Leverage a holistic cross-channel view. A cross-channel view is the ideal solution for satisfying key areas of focus. This solution ensures that criminals who have stolen payment data or identity data are prohibited from achieving account takeovers, identity theft, personal data breaches, and so on.

[1] Directive (EU) 2015/2366 of the European Parliament and of the Council, 25 November 2015, Article 97
[2] Directive (EU) 2015/2366 of the European Parliament and of the Council, 25 November 2015, Recital 4 and Recital 6
[3] Directive (EU) 2015/2366 of the European Parliament and of the Council, 25 November 2015, Article 98

Implications for Card Issuers

Defining SCA - The EU defines SCA as a combination of two distinct elements where each element belongs to a different category from the following: inherence – something that you are, possession – something that (only) you have, and knowledge – something that (only) you know. As an SMS-based One-Time Password (OTP) is the most prevalent mode of dynamic authentication in Europe, much debate has taken place about whether it meets the EU criteria for SCA. Most arguments hinge on whether card data (such as PAN, expiry date, CVV2 / CVC2 and so on) can be used as the knowledge element to be combined with an SMS-based OTP to demonstrate possession. The EBA has not formally clarified their position, but there seems to be an even split between different National Competent Authorities (NCAs) about whether they consider an SMS-based OTP to conform with the SCA principles without being combined with a second factor.

Dynamic linking and 3-D Secure (3DS) - Articles 4 and 5 of the RTS on SCA and CSC state that the payer should be made aware of the payment amount, as well as the payee, during the authentication event. Also, the authentication should only be valid for the transaction initiated by the payee and for the same payment amount. Any 3DS protocol transaction will meet these requirements as each authentication request is indelibly linked with the authentication event and the authentication result. This linkage is a core part of both versions of the 3DS protocol (1.0.2 and 2.1+). This link is cryptographically signed to prevent bad-actors in the ecosystem from tampering with the authentication result before passing the result for authorization.

Allowable exemptions - Generally, the scope of transactions that fall under PSD2 are those where the issuer and acquirer are both located in the EU. Transactions where only a single party is in the EU should be handled on a best-effort basis.

The RTS on SCA and CSC allows for several circumstances where SCA does not have to be applied to each transaction. The following table shows the card-not-present (CNP) SCA exemptions:

<table>
<tr><th colspan="2"></th><th colspan="5">Transaction Value</th></tr>
<tr><th></th><th>Exemption Name</th><th>Up to € 30</th><th>€ 31 – 100</th><th>€ 101 – 250</th><th>€ 251 – 500</th><th>€ 500+</th></tr>
<tr><td>Article 13</td><td>Trusted beneficiaries</td><td colspan="5">Provided that the payee is present on a list of trusted beneficiaries previously created by the payer.</td></tr>
<tr><td>Article 14</td><td>Recurring transactions</td><td colspan="5">Provided that SCA was applied to the first transaction in the series, all subsequent transactions can be exempted from SCA.</td></tr>
<tr><td>Article 15</td><td>Credit transfers between accounts held by the same natural or legal person</td><td colspan="5">Credit transfers between the same person, at the same ASPSP, can be exempted from SCA.</td></tr>
<tr><td>Article 16</td><td>Low-value transactions</td><td>Provided that cumulative value of all subsequent transactions, since the application of SCA, does not exceed EUR 100 OR there have not been five consecutive transactions since application of SCA.</td><td colspan="4">—</td></tr>
</table>

		Transaction Value				
	Exemption Name	**Up to € 30**	**€ 31 – 100**	**€ 101 – 250**	**€ 251 – 500**	**€ 500+**
Article 17	Secure corporate payment processes and protocols	No amount threshold applies to Article 17, and while the EBA is still finalizing guidance for interpretation, it is likely that only a subset of corporate payment instruments will be eligible for this exemption; for example, virtual cards may be exempted whereas traditional T&E cards are unlikely to be eligible for this exemption.				
Article 18	Transaction risk analysis	Provided reference fraud rate doesn't exceed 13 basis points for remote card-based payments or 15 basis points for credit transfer.		Provided reference fraud rate doesn't exceed 6 basis points for remote card-based payments or 1 basis point for credit transfer	Provided reference fraud rate doesn't exceed 1 basis point for remote card-based payments or 1/2 a basis point for credit transfer.	—

NOTE There are two additional SCA exemptions from the card-present world for the use of contactless payments and unattended terminals. For example, parking machines and toll booths are exempt.

Payment instrument versus payment account – The RTS on SCA and CSC states that these exemptions should be tracked at the level of the payment instrument. For example, a debit card versus a fund transfer from a bank account would be two payment instruments; but when tracking usage of exemptions, both payment instruments must be combined into a single value for the payment account. Complicating the tracking of exemption use is that the EBA interpretation has yet to be finalized. NCAs are stating that, for example, the counters for the low-value exemption should only be incremented for those transactions that are exempted as opposed to all those that might have been exempted.

PSD2 RTS Timelines

Date	Event
November 2017	The final version of the RTS was adopted by the EU Commission
January 2018	PSD2 is live, excluding the security measures within the RTS
March 2018	EU Parliament approves EU-wide RTS on SCA and CSC, and 3rd-party account access is formally approved (taking effect September 2019)
September 2019	Most of the RTS on SCA and CSC provisions must be applied by firms from 14 September 2019. The RTS on SCA and CSC seeks to increase the security of customers' payments made by card and other means.

Because of the aggressive timelines, it would be wise to start raising PSD2 compliance projects immediately to eliminate the risk of missing crucial deadlines. CA Technologies has already been helping banks achieve their customer experience and fraud prevention goals while ensuring that their business is prepared to handle the regulations set forth in the PSD2 RTS on SCA and CSC. Please contact your CA representative as soon as possible to kick-off the simple, but imperative projects around the new regulations.

What this Means for Impacted Organizations and How CA can Help – Introducing EMV 3DS, Risk-Based Authentication, SCA, and More

Implementing EMV 3DS – It is currently being advised by some card schemes that their issuers should seriously consider the EMV 3DS protocol if they wish to make PSD2 compliance as simple as possible. The EMV 3DS protocol provides the ability to authenticate cardholders for online credit and debit card transactions seamlessly across web and mobile interfaces by providing access to data from the merchant and the card issuer, including in-app purchases. Although EMV 3DS is not required for PSD2 compliance, it is wise to contemplate both the EMV 3DS protocol and PSD2 together to make the entire transition a lot easier for banks, merchants, and customers. With the harmonization of both the EMV 3DS protocol and PSD2, banks can leverage the same ACS infrastructure to process SCA and e-commerce 3DS protocol transactions simultaneously.

Deploying risk-based authentication – As mentioned previously, one of the main objectives for PSD2 is to create a more competitive playing field that offers customers more choices for payments at lower costs, while also increasing security. PSD2 recognizes the need for a simple user experience and user-friendliness coupled with the flexibility to vary the authentication approach in different risk scenarios. In that sense, issuers have the freedom to use transaction risk analysis to assess each transaction on its own. This transaction analysis could be coupled with SCA for a best practices' strategy. Since SCA cannot be avoided regarding RTS on SCA and CSC, issuers must build their fraud detection and prevention strategy to achieve the goals of PSD2 while reducing the amount of friction caused. Even if fraud rates are too high to qualify for the transaction risk analysis exemptions, the RTS on SCA and CSC Article 2 (2) requires Payment Service Providers to deploy real-time transaction monitoring mechanisms.

Offering SCA capabilities – Under PSD2, SCA is the process for using multi-factor authentication during various online interactions such as account access and payment initiation. Traditional OTPs (such as OTP by way of SMS) do not comply with the current state of the RTS on SCA and CSC, as they do not support the dynamic linking necessity that the RTS on SCA and CSC calls for. Banks must be looking for a solution that can present customers with an out-of-band authentication method that combines with in-app dynamic linking capabilities; straight to the customer's mobile device.

Unified authentication experiences across digital channels – A cross-channel identity risk insight solution is a logical extension to an organization's existing authentication strategy due to its improvement in customer experience and fraud prevention. The EMV 3DS protocol, will prove to become even more valuable in this realm due to its improved data pool of more than 150 data elements. An ideal cross-channel identity risk insight solution combines multiple payment instruments into a single payment account (such as two cardholders on a single credit card, or fund transfers and debit card CNP transactions on a single account) for a holistic view of the business along with its active identities. The ability to share data across all of a business's digital channels provides a single view of an identity. This enables a real-time risk assessment to be made for digital activities in conjunction with other payment actions.

Cross-channel vulnerability is exacerbated with the number of accounts (credit and debit cards, online banking, mortgage, brokerage, and so on) that represent the way customers digitally interact with their financial institutions. If a fraudster is blocked from taking over a user's account, they just move on to the next user; either at the same bank or a different bank. A cross-channel identity risk insight solution is well equipped to handle this type of attack, tracking fraud across multiple financial entities.

How can CA help? – As the world's largest 3DS ACS provider, CA Technologies continues to lead the market in helping customers quickly turn PSD2 into a competitive advantage, leveraging the power behind 3DS 1.x and EMV 3DS. For nearly two decades, CA has made 3DS simple by facilitating a quick and secure implementation, improving customer experience, reducing fraud rates and much more for its customers. Partnering with CA allows customers to tap into the largest real-time consortium network that encompasses intelligent e-commerce authentication transaction data from around the world. It is a scheme-agnostic network that contains global fraud trends and a rich database of cards, devices, merchants, transaction values, and more.

With the products outlined in the following section, CA can help quickly optimize or create a fool proof authentication and fraud prevention strategy that focuses on either long-term strategic and shorter-term tactical requirements. These products provide keen insight into identity risk while securing and optimizing customer interactions across all digital financial services. With SaaS based real-time authentication and fraud prevention solutions, banks can provide a convenient and consistent online authentication experience for their cardholders; detecting and preventing fraudulent activity in an instant.

Even ignoring the regulatory landscape, risk scoring is needed for EMV 3DS, so all issuers should implement risk-based authentication to satisfy the behavioral profiling requirements. The RTS is very clear that risk evaluation techniques typical of a predictive model should be implemented to prevent fraud. In other words, the predictive model will still provide its core value of identifying suspicious transactions and the 3DS service provider still has the option to deny such suspicious transactions even if they have passed consumer authentication.

How can CA Technologies Help Financial Institutions Comply with RTS on SCA and CSC?

Issue to Address	Applicable CA Solution	Description	Response
Payment Security	CA Payment Security Suite; CA Risk Analytics Network	The PSD2 RTS on SCA and CSC requires an extra element for all remote transactions. A unique authentication code which dynamically links the transaction to a specific amount and a specific payee (for remote internet and mobile payments).	As a leader in in the payment industry for nearly two decades, CA Technologies developed CA Payment Security Suite. It combines flexible 3DS, advanced neural network models, and a dynamic rules engine to help our customers achieve their desired customer experience and fraud prevention goals. CA's global view of transaction risk and a customers' own policies help to keep customers in total control of their business. By adding CA Risk Analytics Network, which is driven by global transaction intelligence and data from CA 3DS clients, issuers can quickly assess the risk of a CNP transaction by analyzing data across multiple banks and regions. This data includes the type of device, location, behavior and historical trends in the context of both the card and device behavior. All of this happens in real time, under 5 ms, which minimizes the window of vulnerability for attackers, unlike like the competition that takes days (even weeks) to update. As part of the suite, customers can leverage CA Strong Authentication for Payments. When a transaction requires additional authentication or a challenge, a PSD2 compliant challenge will be sent to the customer. The strong authentication request is dynamically linked backed to the transaction with all required information as mandated in the RTS on SCA and CSC.
	CA Identity Risk Insight Suite	CA Identity Risk Insight Suite brings value to a customer through its sophisticated machine-fingerprinting technology, from the 3DS channel to online banking websites and mobile apps. By providing a consistent Device ID across all channels, CA correlates end-user behavior to provide a holistic view of activity, making it the perfect solution for PSD2 RTS on SCA and CSC compliance. In addition, this solution can then extend SCA to other digital channels and provide full cross-channel exemption management capabilities.	The CA payment security solutions tap into the largest network of global cardholder and financial transaction data. It's important to note that the real-time consortium model is truly scheme-agnostic, which allows any customer to benefit from global transaction data. This e-commerce payment risk and fraud data is uniquely valuable when it comes to managing fraud and risk across online channels (such as 3DS, Online Banking, and so on). The objective of a fraudster is to steal money or goods. Fraudsters who involve themselves in account takeovers, identity thefts, personal data breaches and so on are, in the end, going to attempt to forego fraudulent payments, usually with stolen payment or identity data. For this reason, specifically, it doesn't matter how many devices or data a competitor's network has; since on its own, this data doesn't give you full context. Global payment risk and fraud data across the largest consortium of worldwide e-commerce issuers provides uniquely powerful insights to mitigate online fraud and risk across all digital channels.

Copyright © 2019 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies, and the CA technologies logo are among the trademarks of Broadcom in the United States, the EU, and/or other countries. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.