EPSM

European Association
Of Payment Service Providers
For Merchants

Art. 97 PSD2 – SCA

'Strong Customer Authentication' for EU Payments

Current Overview and Considerations for further discussion

Please note:

- Any feedback, comments or corrections to this document are highly appreciated.
- Some aspects are discussed controversially presently. Certain markets (competent authorities or market participants) may have different views.
- This documentation shall not serve as a legal advice. Please note, that it only represents the view of the authors. Before making business decision, please consult with your specialists and lawyers.

10 July 2019
Version 1.0
Lars Tebrügge
on behalf of EPSM

Content

1. Background

- The European Banking Authority (EBA) was required by Art 98 (1) (a) PSD2 to develop a Regulatory Technical Standard (RTS) of Strong Customer Authentication (SCA) referred to in Art. 97 (1) and (2) PSD2.
- The market consultation by EBA in 2017 triggered a lot of feedback from the payments community and resulted in the Final RTS which were adopted in March 2018 by the European Parliament.
- The overall objective of the RTS on SCA is increasing the security for electronically initiated payments by introducing a two-factor authentication (2FA) – for all transactions that fall under the scope and which are not exempt.
- It is assumed that these RTS have significant impact in most of the European markets for the majority of payment- and online banking authentication processes.
- As so many processes need to be changed by 14 September 2019 there is still a lot of uncertainty for which transactions the new RTS apply, what needs to be done to become compliant and how.
- A lot of questions regarding the interpretation of the legal texts have been addressed to EBA. Unfortunately, only a small number has been answered and a high level of uncertainty remains.
- The RTS will be applicable in the Member States directly. But, it will be the national authorities to enforce them. Therefore, the interpretation of the RTS (as well as the level-one-text (PSD2)) might be different in the Member States.

1. Background

SCA needs to be applied 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.

When SCA needs to be applied, a two-factor-authentication (2FA) shall take place:

- **Possession:** Something only the user possesses (a card, a mobile phone, etc.).
- **Knowledge:** Something only the consumer knows.
- **Inherence:** Something the user is (biometric identification like fingerprint, iris or voice recognition, etc.).

Plus: Extra requirement for **remote payments** (internet and mobile):

For these transactions, the transaction amount and the name of payee to which the payer agreed to, need to be dynamically linked to the Authentication Code.

The 2FA shall result in the generation of an authentication code (AC).

The AC shall be only accepted once by the PSP when the payer uses the AC to access its payment account online, to initiate an electronic payment transaction or to carry out any action through a remote channel which may imply a risk of payment fraud...

2. Scope and Exemptions

The level-one-text (PSD2) got transposed by the national legislators. Consequently, all interpretations regarding this text reside with the national authorities, including the question of the scope.

Out of Scope (Examples, non exhaustive):

- Mail and telephone order,
- Anonymous prepaid cards,
- Cards at POS with imprinter,
- International, global transactions (only „one-leg“ in the EU-EEA).

According to several regulators:

- Card payments with signature (not verified electronically)
- Merchant initiated transactions (MIT)
- SDD mandates (not-verified by the payer‘s PSP)

The exemptions are defined in the RTS, developed by EBA. Consequently, EBA provides guidance on the interpretation of the exemptions.

In Scope (Examples, non exhaustive):

- Credit transfer via online banking,
- Standard ecommerce card payment,
- Card payment at POS (Chip and PIN),
- Card-on file (COF).

Exempt:

- **non-remote**: contactless (LVP), transport and parking
- **remote**: low value ecommerce, transaction risk analysis (TRA)
- **both**: corporate payments, whitelist (trusted beneficiaries)

3. Solutions

SCA will require a lot of changes in many aspects of payments.

Credit Transfer: The majority of the work for the respective adoption seems to be required by ASPSP (banks). Potentially, TPPs will offer services based on SEPA Credit Transfers or SCT Inst.

Direct Debit: In case of Rulebook compliant e-mandates, both PSPs and payees need to agree on processes. See slide 15.

Card Payment: Both PSPs need to agree on a number of issues for remote payments. Card schemes and EMVCo play an important role in coordinating the dialogue between acquirers and issuers.

In order to comply with the RTS on SCA, the schemes and EMVCo developed EMV 3DS 2.x. PSPs need to support it by September 2019 at the latest. Please, note that Version 2.0 is not compatible with Version 1.0.

Technical	• Work on technical solutions to comply with requirements and to ease payment methods in the future • Migration plan to EMV 3DS2
Legal	• Learn how exemptions from SCA can be applied • Illustrate impacts of SCA to Regulators / Authorities
Collaboration	• Help to find solutions to avoid disrupting effects • Build up cross-industry collaborations, e.g. on the mutual acceptance of authentication methods for biometrics
Communication	• Work on common understanding with all industry stakeholders • Educate customers, merchants

Source of helpful information

EMVCo (Core functions of 3DSec 2.0):

https://www.emvco.com/terms-of-use/?u=/wp-content/uploads/documents/EMVCo_3DS_Spec_v220_122018.pdf

3. Solutions

It is envisaged that Transaction Risk Analysis (TRA) can become a powerful exemption.

According to the TRA exemption, a transaction can be flagged as a low-risk-transaction in case the fraud rate of the respective PSP is below a certain threshold and a real time analysis has not revealed any risk (see Art 18 and 19 of RTS on SCA and the Annex for the reference fraud rate). In case the issuer agrees, this transaction can be exempt from SCA.

Considerations:

- As the issuers have the final say whether the exemption is granted, uncertainty remains on how extensively this exemption will be applied in the future. An interesting article can be found here.
- As the abstention from SCA means convenience for the consumers, competition on allowing exemptions could take place on the issuers' side.
- Acquiring PSPs may consider to establish a subsidiary PSP to bundle high risk merchants. As the fraud levels are calculated on legal entity level, they might then be able to meet the thresholds for the majority of their customers and apply the burdensome SCA process only for the high risk merchants.

3. Solutions

For further discussion:

White Listing (trusted beneficiaries):

- This could become a powerful exemption.
- Competition on 'Who will be whitelisted' is expected.

- Further developments should be observed.

Open to further discussion

3. Solutions

For further discussion:

Viewed as generally accepted SCA solutions:

a) POS (non-remote): - EMV Chip (DDA or CDA) and PIN (online-PIN and offline-PIN).

b) eCommerce (remote):
- EMV 3DS 2.1.0, and higher versions, including additional user-password plus mobile onetime-password (OTP), like an SMS-TAN
- EMV 3DS 2.1.0, and higher versions, including additional user-password plus hardware-based TAN generator

see constraints on slides 10 + 11

The following technical solutions (using “delegated authentication”) are likely to be accepted, but legal construction and technical requirements are not completely clear at present:

- PIN entry on a smartphone with additional user password or PIN
- Fingerprint sensor on a smartphone e.g. with Apple Pay and Google Pay, with additional user password or PIN

Remote Card Payment – Standard ecommerce Payment

According to a restrictive reading of the RTS by EBA, the online payment method 'Remote card payment using OTP, 3DS and card data' will not be allowed without e.g. an additional password or biometry, even if secured by EMV 3DS 2.x (the highest security level possible).

This would lead to significant market disruptions. Consumers would not be allowed to pay with this very secure payment method anymore. Therefore, a number of solutions are in discussion, to prevent a disaster for consumers and PSPs:

- Grant grace period for certain requirements – allow fall-back solutions
- Acknowledge that the combined use of the following elements is a valid SCA method:
  - Card data – knowledge (EBA opinion: not compliant)
  - OTP – ownership (EBA opinion: compliant)
  - EMV 3DS – inherence (EBA opinion: not compliant)

Dialogues with Authorities:

A number of dialogues with the respective authorities are taking place these days illustrating the importance and possible impact.

Unfortunately, there are no public statements available, but positive feedback (either by granting grace periods or by considering card data respectively EMV 3DS as 2nd factor) have been reported in the following markets: Belgium, Bulgaria, Denmark, Estonia, France, Hungary, Italy, Poland, Norway, Portugal, Slovakia, United Kingdom.

EU-wide certainty should be achieved!

POS: Card Payment With Signature

This topic has been discussed controversially.

Statements from **EBA**:

Regarding a card present transaction authorised with a signature, EBA argues that "A card transaction is electronic, as it is initiated in the terminal, as opposed to imprinter card transactions, which are paper-based and thus exempted from SCA under PSD2."

see EBA Analysis [272, 2] page 143

Statement from **BaFin** (German CA):

Regarding the initiation of electronic payments: One example of an electronically initiated transaction is the payment with card and PIN at the point of sale. No initiation of an electronic payment is the payment by card and signature, irrespectively if done by girocard or credit card.

Please click here to see the original German text.

The interpretation of the PSD2 text ("What is a an initiation of an electronic transaction?") should be subject to the analysis of the national legislators on the basis of Recital 95 of PSD2. EPSM supports in this regard the view of BaFin. Certainly, a common understanding within EU is needed.

POS: Card Payment

EPSM received the feedback, that the vast majority of the required adoptions to comply with the RTS on SCA have been adopted for POS transactions. Nevertheless, to resolve the remaining open issues, more time is needed.

Open issues are:

- How should the exemptions for contactless cards be implemented in detail. Are changes to the hardware of cards and terminals needed?
- How can the applicability of exemptions or Out-Of-Scope transactions be communicated?
- How can the RTS SCA requirements in special environments, e.g. in an offline environment, be resolved?

Mail and Telephone Order

This topic has been discussed controversially.

Statements from EBA:

- A number of respondents asked the EBA for clarification on the definition of electronic payment transaction and therefore the scope of the SCA. The respondents were unsure whether payments via email or telephone were considered within the scope.
- As mentioned in comment [46] the EBA is of the view that anything initiated via paper or telephone is out of the scope of SCA under PSD2 and therefore out of the scope of the RTS.

  See EBA Analysis [90] page 94

Considering the note of previous slide and the EBA Analysis to the left, MOTO transactions are out of scope. Nevertheless, please consider the following constraint:

Statement from EBA in Q&A 2018_4058

… Payment transactions initiated through a telephone order with the use of an automated solution such as Interactive Voice Response seem to be similar to a regular telephone order. However, where such technology is used to initiate an electronic payment transaction through internet or any other at-distance channels, the provisions on strong customer authentication apply.

Merchant Initiated Transactions (MITs) and Card-on-File (CoF)

According to the present understanding, MITs are out of scope (please refer to EBA Q&A 2018_4031 for details), while CoFs fall under the RTS and SCA will be required.

Challenges have been reported to mark MIT transactions accordingly.

	SDD	Card Payments	
		MIT	COF
Initiated by the payee only	***Yes***	**Yes**	No
Payee triggers each individual payment	***Yes***	**Yes**	No
Payer is off-session	***Yes***	**Yes**	No
Payer is not able to authenticate	***Yes***	**Yes**	No
Pre-existing agreement	***Yes***	**Yes**	No
Mandate provided with SCA to initiate subsequent payments	***Yes***	**Yes**	No

Examples:

MITs:

- Utility Bills
- Funding for e-wallets
- Mobile phone subscriptions

COFs:

- Card data stored at online merchant
- Payment initiated by payer in each case

SEPA Direct Debits in E-commerce Environments

Online Direct Debits - in General

- SEPA Direct Debits are initiated by the payee. As such, they are out of scope.
- Is SCA required for a valid mandate according to the SDD Rulebook?
- According to the Rulebook, a mandate can be given via paper (and signature) or by electronic mandate. For the latter, SCA is required.

EBA has confirmed that such a mandate given remotely requires SCA. Read the full text here.

Online Direct Debits – Common Practise in Germany:

As a valid mandate is difficult to achieve for remote payments (a paper based mandate is per se excluded and electronic signatures are not widely available) many merchants have accepted that they only have an invalid mandate for remote payment transactions.

For these (invalid) Direct Debits the payer has a chargeback right for 13 months, instead of 8 weeks in case of valid mandates.

BaFin (the German authority) has clarified that in the current practise of direct debits, SCA is not required. Read the full text (in German) here.

Remote Card Payments - Market Readiness and Specific Challenges

1. Applicability of exemptions and out-of-scope transactions can not be marked appropriately

- Due to a lack in the specifications presently rolled out, many merchants and acquirers can not appropriately flag transactions that are exempted or are out-of-scope of the RTS, e.g. Merchant Initiated Transactions, Key Entry Transactions, Mail and Telephone Order Transactions or Whitelisted Merchants appropriately.

→ This will lead to a situation where issuers will require SCA even if it would not be required for such an transaction. This will lead to significantly increased abandonment rates and unsatisfied customers.

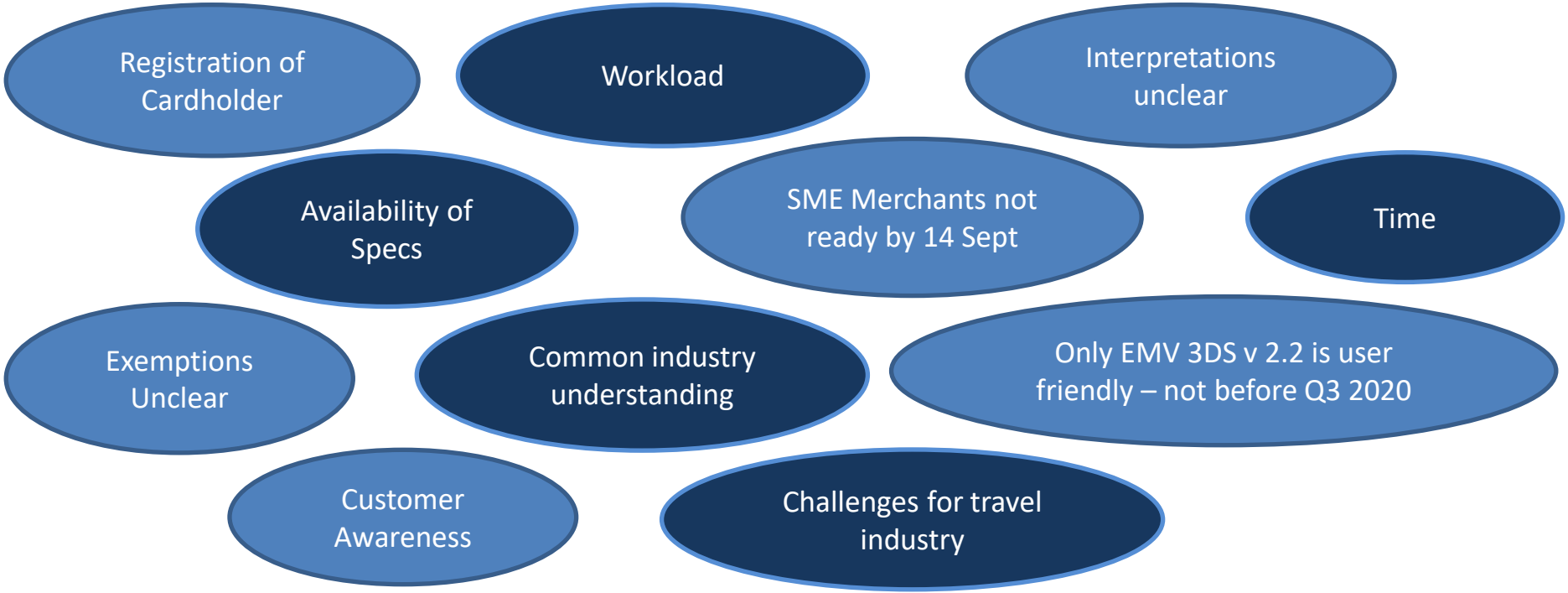
2. Unclear understanding lead to high abandonment rates

- As many issues are still seen differently in various European markets, uncertainty remains how certain transactions should be coded.

→ More time is needed to work on joint understandings on how different transaction types should be treated in order to allow the market to make use of the exemptions / out-of-scope transaction to prevent a scenario where SCA is required when the RTS are not applicable or the transactions are exempt.

Until these issues are resolved, issuers should not be required to decline transactions without SCA!

Remote Card Payments - Market Readiness and General Challenges



Remote Card Payments – EBA Opinion on SCA, dated 21 June 2019.

"The EBA … accepts that, on an exceptional basis and in order to avoid unintended negative consequences for some payment service users after 14 September 2019, CAs [national Competent Authorities] may decide to work with PSPs and relevant stakeholders, including consumers and merchants, to provide limited additional time to allow issuers to migrate to authentication approaches that are compliant with SCA, such as those described in this Opinion, and acquirers to migrate their merchants to solutions that support SCA. This supervisory flexibility is available under the condition that PSPs have set up a migration plan, have agreed the plan with their CA, and execute the plan in an expedited manner. CAs should monitor the execution of these plans to ensure swift compliance with the PSD2 and the EBA's technical standards and to achieve consistency of authentication approaches across the EU."

EPSM Assessment:

1. EBA has finally recognised that the SCA requirements mark a huge challenge for payments market and actions need to be taken to avoid major market disruptions for European online merchants.
2. EPSM fears that the uncoordinated delegation of the migration plan responsibilities to national CAs will lead to a very heterogeneous situation within the European Union.
3. Therefore, EPSM recommends that additional timeframes of 18 months for standard applications and up to 36 months for challenging applications, (e.g. in the travel and hospitality sector) across all regions should be agreed in a harmonised migration approach.

a) Appendix - EBA Q&A

Extract from EBA Answers (please refer to ESPM overview for more details, or click the links for full texts):	Links
PSPs should calculate their overall fraud level. No distinction on brand, scheme or product level.	2018_4090
The relevant fraud rate is not calculated per band, but per transaction type (card or credit transfer transaction)	2018_4033
Only issuers and acquirers are allowed to apply transaction risk exemption (not other PSPs involved).	2018_4035
White listing is also possible for face-to-face transactions.	2018_4056
A one-time-password sent via SMS is considered as a possession element (owner of the phone).	2018_4039
Transaction monitoring has to be performed before the transactions gets authorised.	2018_4090
Established list of trusted beneficiaries does not need to be re-created (using SCA) after RTS become applicable.	2018_4120
Series of recurring transactions does not need to be re-confirmed (using SCA) after RTS become applicable.	2018_4048
'Friendly fraud' shall not be included in the calculation of the fraud rate detailed in Article 19.	2018_4032
A payment initiation service provider cannot decide whether or not an exemption applies.	2018_4089
A signature on a screen of a digital device alone could be considered as behavioural biometrics.	2018_4238
Card payments transactions that are not initiated by the payer but by the payee only are not subject to SCA.	2018_4031
A SDD transaction is not subject to SCA as it is defined in PSD2 as a transaction that is initiated by the payee.	2018_4359

b) Appendix - Abbreviations

AC	Authentication Code
CA	national Competent Authority
CoF	Card on File
CT	Credit Transfer
EBA	European Banking Authority
ELV	Elektronisches Lastschriftverfahren (card-based direct debits at the POS in DE)
LVP	Low Value Payments
MIT	Merchant Initiated Transactions (card)
MOTO	Mail and Telephone Order
PSP	Payment Service Provider
RTS	Regulatory Technical Standards
SCA	Strong Customer Authentication
SCT	SEPA Credit Transfer
SDD	SEPA Direct Debit
TPP	Third Party Provider
TRA	Transaction Risk Analysis
2FA	Two-Factor-Authentication

c) Appendix - Links

Legal Documents	Links
Payment Service Directive 2	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=DE
Regulatory Technical Requirements on Strong Customer Authentication	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN
EBA website for Q&A	https://eba.europa.eu/single-rule-book-qa (please click on “Search for Q&As”)
EBA RTS adoption process documentation, including consultation and drafts	https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2
EBA Analysis of consultation replies with a lot of background information	https://eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+(EBA-RTS-2017-02).pdf
EBA Opinion on SCA	https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf

c) Appendix - Links

Market Information	Links
EMVCo documents	https://www.emvco.com/document-search/
Mastercard – Authentication Guideline	https://www.mastercard.de/content/dam/mccom/de-de/PDF/Authentication%20Guide%20Europe.pdf
Visa – Preparing for PSD2 SCA	https://www.visa.co.uk/dam/VCOM/regional/ve/unitedkingdom/PDF/visa-preparing-for-psd2-sca-publication-version-1-1-05-12-18-002-final.pdf
American Express – Towards SCA with 3DS 2.0	https://www.americanexpress.com/us/foreign-exchange/articles/payments-services-authentication/
Industry Letter – SCA Authentication Factors (by EPIF, Eurocommerce, EMOTA, MRC EU, DIGITALEUROPE, Ecommerce Europe)	https://www.digitaleurope.org/resources/joint-industry-letter-to-european-banking-authority-on-sca-and-cvv-authentication-factors/
3C Payment – SCA and Hotel Sector Adoption	https://www.3cpayment.com/business-insights/strong-customer-authentication-and-hotel-sector-adoption (registration required)
Finextra – Concerns of Payment Firms	https://www.finextra.com/newsarticle/33926/payment-firms-raise-fears-over-eu-security-rules