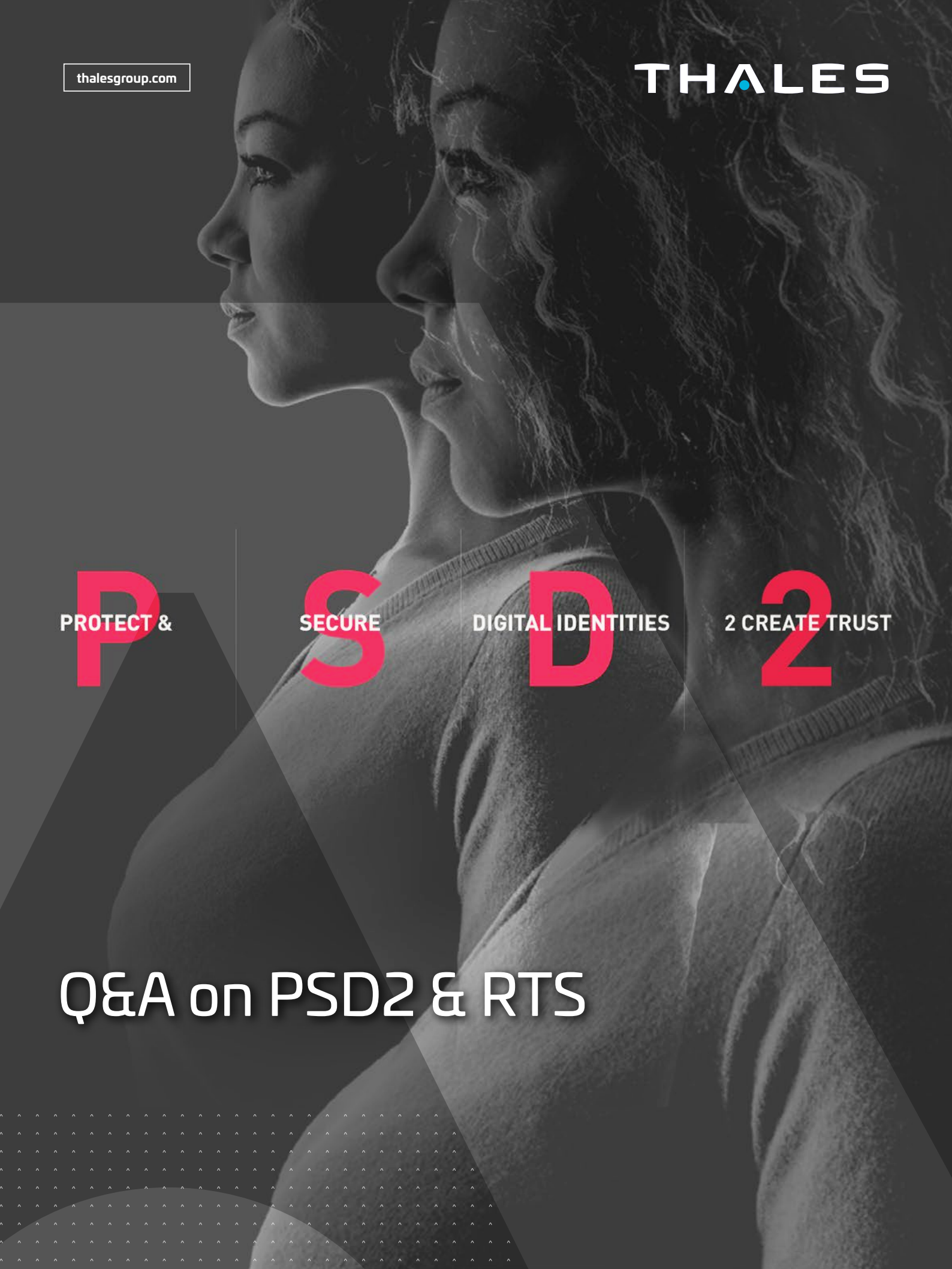
thalesgroup.com

THALES



Q&A on PSD2 & RTS

Contents

The scope of PSD2 and the Regulatory Technical Standards (RTS)

Which entities are affected by PSD2/RTS and must comply with their requirements?

PSD2/RTS target any Payment Service Provider (PSP) involved in payments, money transfer, or access to accounts.

- **Account Servicing Payment Service Providers (ASPSP):** entity that holds the consumer's account(s), mainly "banks".
- **Payment Initiation Service Provider (PISP):** provider that establishes a bridge between a merchant/payee and the online banking's platform of the payer to initiate the payment
- **Account Information Service Provider (AISP):** provider consolidating customer's financial information from different bank accounts.
- **Third-Party Provider (TPP):** term that covers AISP and PISP roles

What are the key points addressed by the RTS?

RTS covers:

- The mandate to implement Transaction Monitoring mechanisms to detect unauthorised or fraudulent payment transactions
- The implementation of Strong Customer Authentication (SCA), authentication codes and dynamic linking
- Exemptions to SCA
- Requirements on confidentiality and integrity of authentication data
- The implementation of secure and open communication between players including the obligation for ASPSPs to set up access to accounts interfaces for AISPs and PISPs

For which type of transactions does PSD2 apply?

PSD2 and RTS apply to any online access to a payment account, any electronic payment, or any action through a remote channel which may imply a risk.

So, proximity payments at cashier or at self-service machines and of course remote payments including card-not-present transactions in e-commerce are impacted.

Nevertheless, limited network / closed-loop payments are excluded of PSD2 and RTS scope.

Corporate banking is also covered by PSD2. RTS introduce a specific SCA exemption for corporate banking, if the system used for that purpose sticks to RTS other security requirements and is considered "satisfying" by the competent authorities.

Does PSD2 apply to banks and fintechs in the European Union only?

PSD2 and RTS requirements apply to all payment accounts (for access to accounts and payment initiation) hold by a PSP in the European Union (EU). These requirements don't apply in the case of:

- Access to account data when the account is hold by a PSP outside of the EU
- Transactions when the account is hold by a PSP outside of the EU

When will PSD2 and the RTS be enforced?

PSD2 came into force in January 2016. RTS have been released on November 27th, 2017 and formally approved by the European authorities on March 13th, 2018, opening to an 18 months delay for actual implementations. So, all European banking and payment players must be fully compliant on September 14th, 2019.

Six months before, on March 14th, 2019, banks shall have their Open APIs facilities ready to be tested by TPPs.

Finally, in October 2019, EBA has granted an additional delay of 15 months, until December 2020, for the implementation of RTS requirements on SCA for card remote payment.

In parallel, by January 13, 2018, all member states were expected to have transposed and implemented the PSD2 into national law

Does PSD2 define SEPA transfer flows?

No, the rules and technical standards for the execution of SEPA payment transactions are defined in the SEPA Credit Transfer (SCT) and SEPA Direct Debit (SDD) rulebooks and must be followed by adhering payment service providers. These schemes are developed

by the European Payments Council (EPC) based on technical standards defined by standard bodies such as ISO.

PSD2 and RTS only precise under which conditions, mainly from a security perspective, SEPA transfers and other electronic transactions should be operated.

Does PSD2 include the new interchange fee regulations?

The new interchange fee regulation is part of another European directive ((UE) 2015/751) released in April 2015. PSD2 does not replace this directive, and thus this new interchange regulation is still valid.

What is the registration process for TPPs? Are banks involved in this process?

The conditions and modalities according which TPPs will identify and be registered is described in the RTS (Art. 34 and ssq.). eIDAS certificates will be used for that purpose. Competent authorities (National or European) will register their respective TPPs.

Implementation of Strong Customer Authentication (SCA)

Does SCA require the use of a hardware token?

SCA requires the combination of (at least) 2 factors amongst 3 types: Possession (what I have) / Knowledge (what I know) / Inherence (what I am). A hardware token is a form of **possession** factor but it is not the only one, e.g. a payment card or a mobile phone leveraging devicebinding can also be used.

The use of a hardware token may not be sufficient to meet RTS requirements: a 2nd authentication factor (e.g. PIN code), dynamic linking and the generation of an authentication code are required.

Is the usage of a PIN or fingerprint sufficient for SCA?

SCA is the combination of (at least) 2 factors amongst 3 types: Possession (what I have) / Knowledge (what I know) / Inherence (What I am)

- A PIN alone is not sufficient (only "what I know")
- A fingerprint alone is not sufficient (only "what I am")
- A PIN + fingerprint combination is theoretically compliant but PIN or fingerprint are more commonly associated with a Possession factor (device)

SCA also requires dynamic linking and the generation of an authentication code.

Do the RTS specify the cryptographic technology to be used for SCA? (PKI, OATH, EMV...)

No, RTS never specify any explicit technology to be used for SCA.

Should SCA be systematically managed by the ASPSP?

RTS does not differentiate requirements for ASPSPs, PISPs or AISPs. All these PSPs are subject to RTS requirements. In practice:

- ASPSPs must manage SCA in the conditions described in RTS
- PISPs and AISP :
  - May rely on the sole ASPSPs' SCA process
  - May operate their own SCA processes
  - Must prove the consumer has given them a consent to operate on his behalf

Do TPPs have to use the same type of SCA method as the ASPSPs?

See previous answer. TPP may use the SCA method of the ASPSPs, or implement their own SCA method. Without specific agreement between TPP and ASPSPs, the ASPSPs will have the "final word" about SCA, as they are liable.

What is an authentication code?

An authentication code is the resulting certificate that reflects, at the end of a SCA process, that the customer has given his consent and has authenticated.

In case of remote payments or fund transfers, the authentication code must be "dynamically linked" to the transaction, meaning taking into account the transaction's amount and beneficiary. "Dynamic linking" is PSD2 / RTS wording for "Transaction signature".

Other requirements for authentication codes, such as unicity, are described in the RTS.

Does dynamic linking (transaction amount and payee) apply for proximity payments?

SCA applies to all kind of electronic payments. Dynamic linking only applies to remote transactions, due to their higher potential risk (RTS recital 3)

Does EMV standards meet the RTS requirements?

EMV standards do meet the RTS requirements for proximity payment transactions. EMV Chip-and-PIN transactions are fully compliant with SCA requirements from RTS. (As a reminder, dynamic linking requirements do not apply to proximity transactions.)

Are standard 3D Secure protocol (3DS) and SMS OTP compliant with RTS?

3D Secure is a protocol adopted by the main payment networks putting in relation a cardholder with his issuing bank ("ASPSP") as part of an e-commerce card-not-present transaction. It allows the issuer to trigger an out-of-band authentication.

The authentication methods the issuer uses within 3DS frame may be compliant or not with RTS actual security requirements.

SMS OTP is considered by EBA (June 2019's Opinion Paper) as a valid possession factor. It shall so be completed by a knowledge or an inherence factor. The creation and transmission of the OTP should also be managed in a secure way.

The new version of the 3DS protocol - 3D Secure 2.0 - will enforce a full compliance with RTS by mandating the use of Strong Customer Authentication methods.

Is 3D Secure mandatory?

Neither PSD2 nor RTS explicitly mandate an operational protocol or technology. So, formally, 3D Secure is not mandatory.

However, as 3DS actually allows to trigger SCA and is adopted by banks in Europe, merchants are likely to be de facto mandated to use 3DS by many acquirers and their PSPs.

What are the requirements for corporate banking?

RTS requirements apply to all electronic payment transactions and remote access to payment accounts. Corporate banking operations of this nature are thus also subject to PSD2 and RTS requirements. RTS introduce a specific SCA exemption for corporate banking, if the system used for that purpose sticks to RTS other security requirements and is considered "satisfying" by the competent authorities.

What are the audit processes and penalties planned for non-compliant PSP?

RTS state that all PSP's processes, security measures and tool, as well as risk management features, will have to be monitored, and audited by independent auditors, to be reported to competent authorities. These latter will clarify these processes and possible penalties.

What types of mobile security measures are necessary to protect the mobile device for SCA?

The RTS lists different security requirements applying to multi-purpose devices (as tablets and mobile phones).

These requirements cover:

- **Data protection:** ASPSP must ensure that confidential data are not stored on device, or are encrypted, and that access to such data requires SCA
- **Secured communication:** ASPS must ensure that all communication with/from the device are limited to needs, encrypted, and only between authenticated and legitimate sources
- **Separated environment:** Authentication data must be stored and processed in specific secure environments that cannot be accessed if the mobile is stolen or used by a non-legitimate user
- **Device and software integrity:** Strong obfuscation, anti-rooting, anti-debug (Runtime Application Self Protection technology)...

Risk management and exemptions to SCA

Is Risk Management mandatory?

Yes PSD2 / RTS mandate PSP to operate transaction and risk monitoring in order to:

- Assess, detect and prevent risks linked to payment and access to account operations
- Evaluate the level of risk in order to find a balance between security measures and user convenience

How do risk management systems interoperate with SCA?

Risk management systems allow to adapt SCA process according to transaction risk level:

- In a first step, a risk management engine allows to evaluate the risk of a given transaction and to check if this particular transaction is eligible to SCA exemption (no abnormal conditions or behavior, location, cumulative amounts, etc.)
- In a second step, the ASPSP will be able to decide to apply SCA exemption or to trigger a SCA process. Important point to notice here is that SCA exemptions aren't mandatory for ASPSPs. Exemptions are only a possibility given to ASPSPs.

Interfaces and data exchange

Are banks required to provide Open APIs? What types of accounts are concerned?

Yes, ASPSPs are required to provide dedicated interface (mainly Open APIs) allowing TPP to:

- Initiate Payments
- Access to Payment Accounts (XS2A)

These interfaces must allow TPP to rely on the authentication procedures provided by the ASPSP.

Only payment accounts are concerned by PSD2 and RTS (checking accounts etc...). Thus, savings accounts and other types of accounts don't have to be accessible via these Open APIs, it will be up to the banks to decide.

Who can access these Open APIs?

Any TPP will have the possibility to access these Open APIs, as long as:

- They have a clear consumer consent
- They are properly registered as TPP.

Do PSD2 or the RTS define a standard for Open Banking APIs?

No standard of Open Banking APIs is defined by PSD2 or the RTS. Each ASPSP is free to implement its own Open API layer, as long as they comply with RTS requirements in terms of SCA, risk monitoring, security and interface requirements.

Some banks have already launched API hubs like BBVA and Nordea.

In parallel, regional associations of banks or processors are working on a common standard of Open APIs (E.g. UK Open Banking Working Group, STET, Berlin Group...) and have recently published their first version of specifications. As an example, a first version of UK CMA Open Banking API specifications has been released public on the 5th of July, 2017.

Can banks monetize the access to APIs?

As banks are mandated to provide an access to TPPs without any existing contract between TPP and ASPSPs it will be difficult for banks to monetise the access to the required minimal APIs.

Banks can charge TPP and their end-users for the use of these Open APIs only if the bank charges its own customers for using the same service through the bank's online portal, app (or branch).

For example, if a bank decides to charge SEPA transfers done by its customers, it could monetise its future Payment Initiation API.

ASPSPs will have though the opportunity to offer premium Open API to TPPs allowing them to monetise supplementary data and services, provided on top of the minimal APIs mandated by PSD2:

- Access to other type of Accounts (savings, credit...)
- Enriched data (customer segmentation, extended transactions history...)
- New services (KYC, credit offer...)

Which Open API standards are banks most likely to follow?

It's hard to guess what will happen. It will depend on each bank's strategy, but also on the quality of the "standards" published by regional initiatives.

Are banks encouraged by EBA to share and exchange APIs?

The "spirit" of the PSD2 is to facilitate consumer access to their banking data and drive innovation by encouraging banks to securely exchange customer data with third parties. The best way to do so is to publish Open APIs.