secure chorus

WHITE PAPER

THE EU SECOND PAYMENT SERVICES DIRECTIVE (PSD2)

The EBA Regulatory Technical Standards on Payment Services Providers' interfaces & Secure Chorus' open cryptography and interoperability standards

February 2018

Contents

This document is provided for information purposes only and should not be relied upon as giving advice or as a basis for making any decisions. We do not warrant that this document is error free and shall not be liable for any use of, or reliance upon, this document. No contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

1 List of Acronyms

AISP	Account Information Service Provider
ASPSP	Account Servicing Payment Service Provider
HTTPS	Hyper Text Transfer Protocol Secure
EBA	European Banking Authority
ECB	European Central Bank
EU	European Union
ECDSA	Elliptic Curve Digital Signature Algorithm
GDPR	General Data Protection Regulation
3GPP	3rd Generation Partnership Project
IDPKC	Identity-Based Public Key Cryptography
IETF	Internet Engineering Task Force
PISP	Payment Initiation Service Provider
PSD1	EU First Payment Services Directive
PSD2	EU Second Payment Services Directive
PSP	Payment Service Provider
PSRs	Payment Services Regulations
PSU	Payment Service User
RTS	Regulatory Technical Standards (drafted by the EBA)
SCA	Strong Customer Authentication
TLS	Transport Layer Security
TPP	Third Party Payment Provider
TSP	Trust Service Provider

2 About Secure Chorus

Secure Chorus is a not-for-profit, membership organisation for the secure communication industry. Our vision is to promote the long-term security of digitally enabled economies by developing a global ecosystem of interoperable and secure data sharing technologies for enterprise users – based on open standards and private and public-sector collaboration – which democratises access to secure communications and data sharing.

Secure Chorus' work, based on its members' and observers' collaboration, has enabled the development of an ecosystem of Secure Chorus Compliant Products which offers specific features that are of great relevance for the secure processing of data in enterprise, in regulated industries.

All products provide for end-to-end encryption and can be used in a variety of environments, both at rest (e.g. storage) and in transit (e.g. network systems). However, users are not locked-in by a specific vendor. Users of different brands of products can communicate with one another securely.

The technology can be centrally managed, giving the enterprise full control of the security of the system and therefore the ability to comply with any auditing requirements through a managed and logged process.

Secure Chorus' Key Management Server (KMS) based approach allows domain managers to easily enable the processing of data between different user groups without bringing external user groups into the security perimeter of the organisation.

The standards use Identity-Based Public Key Cryptography (IDPKC), removing the need for an expensive and complex supporting infrastructure for distributing credentials, allowing for at-scale implementation.

Secure Chorus' standards support both real-time processing of data and deferred delivery of data. The standards are also agnostic to implementation and give organisations the complete freedom and flexibility to deploy platforms and infrastructure to meet their requirements

Since the specifications are known and open, it is possible to assess if the technology meets information assurance requirements.

We partner with governments, supranational organisations, telecommunication operators, system integrators, technology companies, academic institutions, regulators and industry bodies to rapidly scale our ecosystem of interoperable and secure information sharing technologies, achieving wide-spread access and adoption across private and public-sector enterprise.

3 Introduction

EU First Payment Services Directive (PSD1)

The EU First Payment Services Directive (PSD1) was published in 2007 and was implemented into national law in each EU Member State on 1 November 2009. It became UK law in 2009 through the Payment Services Regulations (PSRs).

The PSD1 created an EU single market for payments to make cross-border payments as efficient and secure as the 'national' payments within single EU Member States. Its objective was also to open up the market to innovative new firms.

EU Second Payment Services Directive (PSD2)

The EU Second Payment Services Directive (PSD2) updates the PSD1. EU Member States, including the UK, were required to implement it into national law by 13 January 2018.

Since the introduction of PSD1 the retail payment market experienced substantial disruptive innovation which was entirely or in large part not covered by PSD1. The rapid growth of fintech, the development of new business models for payment services providers, as well as the geographical expansion of digital payment services beyond the national markets into EU-wide markets led to legal uncertainty and new security risks.

PSD2 addresses these challenges and introduces several key improvements: it expands the directive's scope, it clarifies the exceptions from it and it strengthens security and customer authentication.

The directive introduces the notion of Third Party Providers (TPPs) namely Account Information Service Providers ('AISPs') and Payment Initiation Service Providers (PISPs)

AISPs allow payment service users to have an overview of their financial situation at any time, allowing users to better manage their personal finances.

PISPs allow consumers to pay via simple credit transfer for their online purchases, while providing merchants with the assurance that the payment has been initiated so that goods can be released, or services provided, without delay.

The directive responds to evolving customer demands for real-time, personalised and seamless payment experiences by opening the market to such TPPs and by defining common standards to drive technology interoperability amongst all the relevant parties.

As a result of the PSD2, banks are required to open their IT infrastructure to TPPs. At the same time, users of these services will have to provide their consent for the AISPs and PISPs to interact with their bank on their behalf.

This new digital environment, characterised by hyperconnectivity and interconnectedness of an increased number of parties and technologies, significantly increases attack vectors for cybercriminals. Therefore, the requirement to effectively protect data within the security perimeter of the banks, AISPs and PISPs, as well as the interactions between these participants, has become paramount.

The PSD2 reflects this, and places strong requirements for TPPs to protect the data they are entrusted with, as well as highlighting the importance of establishing safe and efficient communication channels between banks and TPPs.

In this paper, we will discuss and demonstrate how Secure Chorus' open standards can be leveraged to adhere to the requirements of the PSD2 by examining key parts of the directive, and of the Regulatory Technical Standard (RTS) adopted by the European Commission on 27 November 2017, as developed by the European Banking Authority (EBA), and later amended by the European Commission.

We will examine how identity-based public key encryption such as MIKEY-SAKKE – Secure Chorus' cryptography standard of choice – can be used to best address the requirements highlighted in the RTS.

In particular, we will highlight how MIKEY-SAKKE can be used to authenticate TPPs and banks with one another, while protecting the confidentiality and integrity of the data traveling between these parties.

We will also address how this standard is able to support the traceability and auditability requirements highlighted in the regulation.

Finally, we will examine how Secure Chorus' business model, based on private-public sector collaboration and open industry standards can best address the challenges banks and TPPs are facing with implementing the requirements of the aforementioned regulations.

4 EU Second Payment Services Directive (PSD2)

Full title of the EU PSD2 Directive:

Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [1].

The full text is available via this link:

http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32015L2366

Examining the Directive itself, PSD2 consists of six "Titles":

I. Subject Matter, Scope and Definitions

II. Payment Services Providers

III. Transparency of Conditions and Information Requirements

IV. Rights and Obligations in Relation to the Provision and Use of Payment Services

V. Delegated Act and Regulatory Technical Standards

VI. Final Provisions

In this section we provide an overview of several relevant Articles of the PSD2, which are related to Secure Chorus' discussion in this paper.

Technologies that allow for secure transmission of Payment Service User data between multiple parties

Title IV, Chapter 2, Article 66 of the PSD2 requires the Payment Initiation Service Provider (PISP), when accessing a Payment Service User (PSU) account, to ensure that the personalised security credentials of the PSU are not accessible by other parties (with the exception of the PSU and PISP) and that they are transmitted by the PISP through safe and efficient channels.

Every time a payment is initiated the PISP is also required to identify itself and communicate securely with the Account Servicing Payment Service Provider (ASPSP). Similarly, the ASPSP is required to communicate securely back to the PISP.

PSD2 - Title IV, Rights and Obligations in Relation to the Provision and Use of Payment Services, Chapter 2 Authorisation of Payment Transactions, Article 66 Rules on access to payment account in the case of payment initiation services

1. Member States shall ensure that a payer has the right to make use of a payment initiation service provider to obtain payment services as referred to in point (7) of Annex I. The right to make use of a payment initiation service provider shall not apply where the payment account is not accessible online.

2. When the payer gives its explicit consent for a payment to be executed in accordance with Article 64, the account servicing payment service provider shall perform the actions specified in paragraph 4 of this Article in order to ensure the payer's right to use the payment initiation service.

3. The payment initiation service provider shall:

(a) not hold at any time the payer's funds in connection with the provision of the payment initiation service;

(b) ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the payment initiation service provider through safe and efficient channels;

(c) ensure that any other information about the payment service user, obtained when providing payment initiation services, is only provided to the payee and only with the payment service user's explicit consent;

(d) every time a payment is initiated, identify itself towards the account servicing payment service provider of the payer and communicate with the account servicing payment service provider, the payer and the payee in a secure way, in accordance with point (d) of Article 98(1);

(e) not store sensitive payment data of the payment service user;

(f) not request from the payment service user any data other than those necessary to provide the payment initiation service;

(g) not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer;

(h) not modify the amount, the payee or any other feature of the transaction.

4. The account servicing payment service provider shall:

(a) communicate securely with payment initiation service providers in accordance with point (d) of Article 98(1);

(b) immediately after receipt of the payment order from a payment initiation service provider, provide or make available all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction to the payment initiation service provider;

(c) treat payment orders transmitted through the services of a payment initiation service provider without any discrimination other than for objective reasons, in particular in terms of timing, priority or charges vis-à-vis payment orders transmitted directly by the payer.

5. The provision of payment initiation services shall not be dependent on the existence of a contractual relationship between the payment initiation service providers and the account servicing payment service providers for that purpose.

Title IV, Chapter 2, Article 67 of PSD2 also requires the Account Information Service Provider (AISP), when accessing and using a PSU account, to ensure that the personalised security credentials of the PSU are not accessible to the other parties (with the exception of the PSU and AISP) and that they are transmitted by the AISP through safe and efficient channels.

Every time a payment is initiated, the AISP is also required to identify itself and communicate securely with the ASPSP. Similarly, the ASPSP is also required to communicate securely back to the AISP.

PSD2 - Title IV, Rights and Obligations in Relation to the Provision and Use of Payment Services, Chapter 2 Authorisation of Payment Transactions, Article 67, Rules on access to and use of payment account information in the case of account information services

> *1. Member States shall ensure that a payment service user has the right to make use of services enabling access to account information as referred to in point (8) of Annex I. That right shall not apply where the payment account is not accessible online.*
>
> *2. The account information service provider shall:*
>
> *(a) provide services only where based on the payment service user's explicit consent;*
>
> *(b) ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that when they are transmitted by the account information service provider, this is done through safe and efficient channels;*
>
> *(c) for each communication session, identify itself towards the account servicing payment service provider(s) of the payment service user and securely communicate with the account servicing payment service provider(s) and the payment service user, in accordance with point (d) of Article 98(1);*
>
> *(d) access only the information from designated payment accounts and associated payment transactions;*
>
> *(e) not request sensitive payment data linked to the payment accounts;*
>
> *(f) not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules.*
>
> *3. In relation to payment accounts, the account servicing payment service provider shall:*
>
> *(a) communicate securely with the account information service providers in accordance with point (d) of Article 98(1); and*
>
> *(b) treat data requests transmitted through the services of an account information service provider without any discrimination for other than objective reasons.*
>
> *4. The provision of account information services shall not be dependent on the existence of a contractual relationship between the account information service providers and the account servicing payment service providers for that purpose.*

Therefore Title IV, Chapter 2, Articles 66 and 67 of the PSD2 require that communication of a PSU's data between all the relevant parties, namely the PISP, AISP and ASPSP, be done securely.

This is an important point, articulating a clear requirement for technology solutions, based on common secure communication standards which will enable PISP, AISP and ASPSP to exchange a PSU's data securely and efficiently beyond the security perimeters of their own organisations.

Auditable technology solutions and the requirement for Payment Services Providers to provide evidence on authentication and execution of payment transactions

Title IV, Chapter 2, Article 72 of the PSD2, requires the Payment Service Provider (PSP), in the event of disputes, to be able to provide evidence on authentication and execution of payment transactions.

> *PSD2 - Title IV, Rights and Obligations in Relation to the Provision and Use of Payment Services, Chapter 2, Article 72, Evidence on authentication and execution of payment transactions*
>
> *1. Member States shall require that, where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider.*
>
> *If the payment transaction is initiated through a payment initiation service provider, the burden shall be on the payment initiation service provider to prove that within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.*
>
> *2. Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider, including the payment initiation service provider as appropriate, shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 69. The payment service provider, including, where appropriate, the payment initiation service provider, shall provide supporting evidence to prove fraud or gross negligence on part of the payment service user.*

Article 72 outlines a key requirement for adoption of technology solutions by the PSP which is designed to give the PSP the ability to comply with any auditing requirements, through a system that allows the retrieval of transaction data and security system logs.

This is relevant, as if we combine the requirements outlined in Articles 66, 67 and 72, the technology solutions should not only be based on common secure communication standards that provide for secure exchange of Payment Service Users' (PSUs) data, but also allow the PSP to audit its technology to be able to provide evidence regarding authentication and execution of payment transactions.

Data protection and risk management

According to Title IV, Chapter 4, Article 94 of the PSD2, a Payment Service Provider (PSP) is permitted to process personal data in specific circumstances, however any processing of personal data for the purposes of PSD2 shall be carried out in accordance with Directive 95/46/EC, the national rules which transpose Directive 95/46/EC, and with Regulation (EC) No 45/2001.

Please note that the EU 2016/679 General Data Protection Regulation (GDPR) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data will repeal Directive 95/46/EC (Data Protection Directive) as of 25 May 2018.

PSD2 - Title IV, Rights and Obligations in Relation to the Provision and Use of Payment Services, Chapter 4, Data Protection, Article 94, Data Protection

1. Member States shall permit processing of personal data by payment systems and payment service providers when necessary to safeguard the prevention, investigation and detection of payment fraud. The provision of information to individuals about the processing of personal data and the processing of such personal data and any other processing of personal data for the purposes of this Directive shall be carried out in accordance with Directive 95/46/EC, the national rules which transpose Directive 95/46/EC and with Regulation (EC) No 45/2001.

2. Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user.

Both the GDPR and the PSD2 share the aim of placing data subjects in control of their data and require organisations to put in place a number of technical and operational security measures relating to the “processing” of data.

In particular, the GDPR introduces the notion of “personal data”, ensuring that any and all information relating to an individual is adequately protected. The active data protection regulation in Article 94 of the PSD2 mandates that the “data subject” maintains the right granted to data subjects through GDPR to make a data access request regarding personal data relating to them, held by a PSP.

GDPR – Chapter 1, General Provision, Article 4 “Definitions”

For the purposes of this Regulation:

1. ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”

2. ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;”

Payment Service Providers are required to establish a framework to mitigate and control security risk

Title IV, Chapter 5, Article 95 of the PSD2 further requires the Payment Service Provider (PSP) to establish a framework to mitigate and control security risk, including the establishment and maintenance of effective incident management procedures.

The directive also requires the PSP to provide the competent authority on an annual basis an assessment of its operational and security risks relating to payment services. The assessment shall also include the adequacy of the management procedures implemented to mitigate such risk.

Please note that the PSD2 directive delegated to the European Banking Authority (EBA) to issue guidelines by 13 July 2017 in close cooperation with the European Central Bank (ECB) and after consulting all relevant stakeholders, with regard to the establishment, implementation and monitoring of the security measures, including certification processes where relevant. The EBA is further required to review these guidelines at least every two years.

PSD2 - Title IV, Rights and Obligations in Relation to the Provision and Use of Payment Services, Chapter 5, Operational and security risks and authentication Article 95, Management of operational and security risks

1. Member States shall ensure that payment service providers establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services they provide. As part of that framework, payment service providers shall establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.

2. Member States shall ensure that payment service providers provide to the competent authority on an annual basis, or at shorter intervals as determined by the competent authority, an updated and comprehensive assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

3. By 13 July 2017, EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, issue guidelines in accordance with Article 16 of Regulation (EU) No 1093/2010 with regard to the establishment, implementation and monitoring of the security measures, including certification processes where relevant.

EBA shall, in close cooperation with the ECB, review the guidelines referred to in the first subparagraph on a regular basis and in any event at least every 2 years.

4. Taking into account experience acquired in the application of the guidelines referred to in paragraph 3, EBA shall, where requested to do so by the Commission as appropriate, develop draft regulatory technical standards on the criteria and on the conditions for establishment, and monitoring, of security measures.

Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.

5. EBA shall promote cooperation, including the sharing of information, in the area of operational and security risks associated with payment services among the competent authorities, and between the competent authorities and the ECB and, where relevant, the European Union Agency for Network and Information Security.

This is relevant as it requires the EBA to consider auditable technology solutions to ensure the PSPs adopt technical solutions that allow them to establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.

EBA Regulatory Technical Standards on authentication and communication

Title IV, Chapter 5, Article 98 of the PSD2, requires European Banking Authority (EBA), in close cooperation with the European Central Bank (ECB), and after consulting all relevant stakeholders, to draft Regulatory Technical Standards (RTS) specifying:

a. the requirements of the Strong Customer Authentication (SCA),

b. the exemptions from the application of SCA,

c. the requirements with which security measures have to comply in order to protect the confidentiality and the integrity of the payment service users' personalised security credentials, and

d. the requirements for common and secure open standards of communication between Account Servicing Payment Service Providers (ASPSP), Payment Initiation Service Providers (PISPs), Account Information Service Providers (AISPs), payers, payees and other Payment Service Providers (PSPs).

PSD2 - Title IV, Rights and Obligations in Relation to the Provision and Use of Payment Services, Chapter 5, Operational and security risks and authentication, Article 98, Regulatory technical standards on authentication and communication

1. EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, develop draft regulatory technical standards addressed to payment service providers as set out in Article 1(1) of this Directive in accordance with Article 10 of Regulation (EU) No 1093/2010 specifying:

(a) the requirements of the strong customer authentication referred to in Article 97(1) and (2);

(b) the exemptions from the application of Article 97(1), (2) and (3), based on the criteria established in paragraph 3 of this Article;

(c) the requirements with which security measures have to comply, in accordance with Article 97(3) in order to protect the confidentiality and the integrity of the payment service users' personalised security credentials; and

(d) the requirements for common and secure open standards of communication 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.

2. The draft regulatory technical standards referred to in paragraph 1 shall be developed by EBA in order to:

(a) ensure an appropriate level of security for payment service users and payment service providers, through the adoption of effective and risk-based requirements;

(b) ensure the safety of payment service users' funds and personal data;

(c) secure and maintain fair competition among all payment service providers;

(d) ensure technology and business-model neutrality;

(e) allow for the development of user-friendly, accessible and innovative means of payment.

3. The exemptions referred to in point (b) of paragraph 1 shall be based on the following criteria:

(a) the level of risk involved in the service provided;

(b) the amount, the recurrence of the transaction, or both;

(c) the payment channel used for the execution of the transaction.

4. EBA shall submit the draft regulatory technical standards referred to in paragraph 1 to the Commission by 13 January 2017.

Power is delegated to the Commission to adopt those regulatory technical standards in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.

5. In accordance with Article 10 of Regulation (EU) No 1093/2010, EBA shall review and, if appropriate, update the regulatory technical standards on a regular basis in order, inter alia, to take account of innovation and technological developments.

Of specific interest to our discussion in this paper is Article 98 (1), (c) and (d) of the PSD2. These requirements have been developed in the EBA's RTS, Chapters IV and V.

5 The European Banking Authority's Draft Regulatory Technical Standards

Full title of the European Banking Authority (EBA) final draft Regulatory Technical Standards, as submitted in February 2017:

Final Report, Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2) [2].

The full text is available via this link:

https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf

Full title of the European Commission final text RTS, as adopted in November 2017:

COMMISSION DELEGATED REGULATION (EU) No …/… of XXX supplementing Directive 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication [3].

The full text is available via this link:

http://ec.europa.eu/finance/docs/level-2-measures/psd2-rts-2017-7782_en.pdf

As per Title IV, Chapter 5, Article 98 of the PSD2 quoted in the previous section of this paper, the European Banking Authority (EBA) in collaboration with European Central Bank (ECB) and after consulting all relevant stakeholders was mandated to produce a final draft of the Regulatory Technical Standards in February 2017.

Following this, the European Commission (EC) made some limited substantive amendments to the EBA's draft RTS and adopted a final text on 27 November 2017. The final text will then need to be approved by the European Parliament and the Council before publication in the Official Journal of the EU.

Thereafter the RTS will enter into force the following day, and an 18-month transition period will begin, at the end of which all Payment Services Providers will need to adhere to the RTS.

The EBA reached the conclusion that the RTS must not prescribe the use of any specific industry standard of internet communication; it instead proposes the requirements with which any communication solution must comply. As such, it is technology-neutral and business-model neutral.

As previously stated, this paper focuses on the EBA's draft RTS related to Title IV, Chapter 5, Article 98, (1), (c), (d) of the PSD2 and as amended and adopted by the EC.

Article 98, (1), (c) of the PSD2 requires the EBA to draft RTS to address the requirements with which security measures have to comply, in accordance with Article 97, (3) in order to protect the confidentiality and the integrity of Payment Service Users' (PSUs) personalised security credentials. This requirement is addressed in Chapter IV of the EBA's draft RTS.

Article 98, (1), (d) of the PSD2 requires the EBA to draft RTS to address requirements for common and secure open standards of communication between Account Servicing Payment Service Providers (ASPSPs), Payment Initiation Service Providers, (PISPs) Account Information Service Providers (AISPs), payers, payees and other Payment Service Providers (PSPs). This requirement is addressed in Chapter V of the EBA's draft RTS.

In this section we provide an overview of several Articles of the EC final text RTS that relate to the requirements identified in the PSD2 sections highlighted so far.

Confidentiality and integrity of users' personalised security credentials

Chapter IV of the EC final text RTS highlights that the confidentiality of personalised security credentials must be ensured, and that to do so, processing and routing of the data need to be done in secure environments. The security of these environments is ultimately the responsibility of the Payment Service Provider (PSP).

> *EC final text RTS - Chapter IV, Confidentiality and Integrity of the Payment Service Users' personalised security credentials, Article 22 General requirements*
>
> *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:*
>
> *(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 plaintext;*
>
> *(c) secret cryptographic material is protected from unauthorised disclosure.*
>
> *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.*
>
> *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.*

Crucially, the need for a secure environment doesn't limit itself to the boundaries and internet environment of the PSPs but includes the need for any credential material to be encrypted or otherwise made unreadable.

Common and secure open communication standards

Chapter V of the EC final text RTS addresses the requirements for secure open communication standards 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.

Chapter V is composed of two sections:

- Section 1 - which defines principle-based requirements in relation to standards of communication in general and
- Section 2 - which is dedicated to the requirements for common and secure open standards of communication, which focuses on the communication exchanges between AISPs, PISPs and ASPSPs, as well as for communication between PSPs in relation to confirmation regarding the availability of funds.

Examining Chapter V, Section 1 of the EC final text RTS, we see that there is a strong requirement for both identification between systems (Chapter V, Section 1, Article 28 of the EC final text RTS) and traceability of all interactions between systems (Chapter V, Section 1, Article 29 of the EC final text RTS).

This means that all Payment Service Providers (PSPs) must ensure not only that they adequately mitigate against risks of communication data falling into the hands of unauthorised parties, and that there is adequate detailed logging of the communication.

EC final text RTS - Chapter V Common and secure open standards of communication, Section 1 General requirements for communication, Article 28 Requirements for identification

1. Payment service providers shall ensure secure identification when communicating between the payer's device and the payee's acceptance devices for electronic payments, including but not limited to payment terminals.

2. Payment service providers shall ensure that the risks of misdirection of communication to unauthorised parties in mobile applications and other payment services users' interfaces offering electronic payment services are effectively mitigated.

EC final text RTS - Chapter V Common and secure open standards of communication, Section 1 General requirements for communication, Article 29 Traceability

1. Payment service providers shall have processes in place which ensure that all payment transactions and other interactions with the payment services user, with other payment service providers and with other entities, including merchants, in the context of the provision of the payment service are traceable, ensuring knowledge ex-post of all events relevant to the electronic transaction in all the various stages.

2. For the purpose of paragraph 1, payment service providers shall ensure that any communication session established with the payment services user, other payment service providers and other entities, including merchants, relies on each of the following:

(a) a unique identifier of the session;

(b) security mechanisms for the detailed logging of the transaction, including transaction number, timestamps and all relevant transaction data;

(c) timestamps which shall be based on a unified time-reference system and which shall be synchronised according to an official time signal.

Ultimately PSPs must ensure that full knowledge of all events relevant to any electronic transactions performed can be obtained by authorised parties, providing evidence of authentication and execution of payment transactions.

The requirement for banks to provide online access to Third Party Providers

Chapter V, Section 2, Article 30 of the EC final text RTS highlights the need for any Account Servicing Payment Service Providers (ASPSPs), such as banks, who provide online access to their customers, to also provide online access to Third Party Payment Providers (TPPs) via an interface – preferably one dedicated to this purpose – that supports standard financial messaging.

EC final text RTS - Chapter V Common and secure open standards of communication, Section 2 Specific requirements for the common and secure open standards of communication, Article 30, General obligations for access interfaces

1. Account servicing payment service providers that offer to a payer a payment account that is accessible online shall have in place at least one interface which meets each of the following requirements:

(a) account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments are able to identify themselves towards the account servicing payment service provider;

(b) account information service providers are able to communicate securely to request and receive information on one or more designated payment accounts and associated payment transactions;

(c) payment initiation service providers are able to communicate securely to initiate a payment order from the payer's payment account and receive all information on the initiation of the payment transaction and all information accessible to the account servicing payment service providers regarding the execution of the payment transaction.

2. For the purposes of authentication of the payment service user, the interface referred to in paragraph 1 shall allow account information service providers and payment initiation service providers to rely on all the authentication procedures provided by the account servicing payment service provider to the payment service user. The interface shall at least meet all of the following requirements:

(a) a payment initiation service provider or an account information service provider shall be able to instruct the account servicing payment service provider to start the authentication based on the consent of the payment service user;

(b) communication sessions between the account servicing payment service provider, the account information service provider, the payment initiation service provider and any payment service user concerned shall be established and maintained throughout the authentication;

(c) the integrity and confidentiality of the personalised security credentials and of authentication codes transmitted by or through the payment initiation service provider or the account information service provider shall be ensured.

3. Account servicing payment service providers shall ensure that their interfaces follow standards of communication which are issued by international or European standardisation organisations. Account servicing payment service providers shall also ensure that the technical specification of any of the interfaces is documented specifying a set of routines, protocols, and tools needed by payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments for allowing their software and applications to interoperate with the systems of the account servicing payment service providers. Account servicing payment service providers shall at a minimum, and no less than six months before the application date referred to in Article 38(2), or before the target date for the market launch of the access interface when the launch takes place after the date referred to in Article 38(2), make the documentation available, at no charge, upon request by authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments or payment service providers that have applied to their competent authorities for the relevant authorisation, and shall make a summary of the documentation publicly available on their website.

> *4. In addition to paragraph 3, account servicing payment service providers shall ensure that, except for emergency situations, any change to the technical specification of their interface is made available to authorised payment initiation service providers, account information service providers and payment service providers issuing card based payment instruments, or payment service providers that have applied to their competent authorities for the relevant authorisation, in advance as soon as possible and not less than 3 months before the change is implemented. Payment service providers shall document emergency situations where changes were implemented and make the documentation available to competent authorities on request.*
>
> *5. Account servicing payment service providers shall make available a testing facility, including support, for connection and functional testing to enable authorised payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers, or payment service providers that have applied for the relevant authorisation, to test their software and applications used for offering a payment service to users. This testing facility should be made available no later than six months before the application date referred to in Article 38(2) or before the target date for the market launch of the access interface when the launch takes place after the date referred to in Article 38(2). However, no sensitive information shall be shared through the testing facility.*
>
> *6. Competent authorities shall ensure that account servicing payment service providers comply at all times with the obligations included in these standards in relation to the interface(s) that they put in place. In the event that an account servicing payment services provider fails to comply with the requirements for interfaces laid down in these standards, competent authorities shall ensure that the provision of payment initiation services and account information services is not prevented or disrupted to the extent that the respective providers of such services comply with the conditions defined under Article 33(5).*

Beyond the need to standardise the format of messages themselves, the underlying secure communication channels between a TPP and the interface provided by a bank, should adhere to standards which are open and widely available.

Article 30 of the EC final text RTS further highlights that such standards must enable systems to identify and authenticate one another, as well as ensure that interfaces can communicate sensitive data securely. This article further states explicitly that the standards of communication used must be documented by international or European standardisation organisations.

Authentication of services

Chapter V, Section 2, Article 34 of the EC final text RTS highlights the requirement for banks and Third Party Payment Providers (TPPs) to identify and authenticate with one another prior to setting up an encrypted communication channel between the TPP and the bank's interface. The EC final text RTS highlights an approach where Payment Services Providers (PSPs) will rely on "qualified certificates" issued by a qualified Trust Service Provider (TSP).

These certificates can be certificates issued for electronic seals or those issued for website authentication. The certificates themselves must include such information as to whether the PSP is a bank, Payment Initiation Service Provider (PISP), Account Information Service Provider (AISP) or as an issuer of card-based payment instruments.

> *EC final text RTS - Chapter V, Common and secure open standards of communication, Section 2 Specific requirements for the common and secure open standards of communication, Article 34 Certificates*
>
> *1. For the purpose of identification, as referred to in Article 30(1)(a), payment service providers shall rely on qualified certificates for electronic seals as referred to in Article 3(30) of Regulation (EU) No 910/2014 of the European Parliament and of the Council or for website authentication as referred to in Article 3(39) of that Regulation.*
>
> *2. For the purpose of this Regulation, the registration number as referred to in the official records in accordance with Annex III (c) or Annex IV (c) to Regulation (EU) No 910/2014 shall be*

the authorisation number of the payment service provider issuing card-based payment instruments, the account information service providers and payment initiation service providers, including account servicing payment service providers providing such services, available in the public register of the home Member State pursuant to Article 14 of Directive (EU) 2015/2366 or resulting from the notifications of every authorisation granted under Article 8 of Directive 2013/36/EU of the European Parliament and of the Council4 in accordance with Article 20 of that Directive.

3. For the purposes of this Regulation, qualified certificates for electronic seals or for website authentication referred to in paragraph 1 shall include, in a language customary in the sphere of international finance, additional specific attributes in relation to each of the following:

(a) the role of the payment service provider, which maybe one or more of the following:

i. account servicing;
ii. payment initiation;
iii. account information;
iv. issuing of card-based payment instruments;

(b) the name of the competent authorities where the payment service provider is registered.

4. The attributes referred to in paragraph 3 shall not affect the interoperability and recognition of qualified certificates for electronic seals or website authentication.

Confidentiality and integrity of exchanged data

In addition to the authentication of the communicating parties, Chapter V, Section 2, Article 35 of the EC final text RTS highlights the requirements for strong and widely recognised encryption techniques to be applied between the communicating parties throughout the respective communication session, so as to safeguard the confidentiality and integrity of the data being exchanged.

EC final text RTS - Chapter V Common and secure open standards of communication, Section 2 Specific requirements for the common and secure open standards of communication, Article 35, Security of communication session

1. Account servicing payment service providers, payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers shall ensure that, when exchanging data by means of the internet, secure encryption is applied between the communicating parties throughout the respective communication session in order to safeguard the confidentiality and the integrity of the data, using strong and widely recognised encryption techniques.

2. Payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers shall keep the access sessions offered by account servicing payment service providers as short as possible and they shall actively terminate any such session as soon as the requested action has been completed.

3. When maintaining parallel network sessions with the account servicing payment service provider, account information service providers and payment initiation service providers shall ensure that those sessions are securely linked to relevant sessions established with the payment service user(s) in order to prevent the possibility that any message or information communicated between them could be misrouted.

4. Account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments with the account servicing payment service provider shall contain unambiguous references to each of the following items:

(a) the payment service user or users and the corresponding communication session in order to distinguish several requests from the same payment service user or users;

(b) for payment initiation services, the uniquely identified payment transaction initiated;

(c) for confirmation on the availability of funds, the uniquely identified request related to the amount necessary for the execution of the card-based payment transaction.

> *5. Account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing cardbased payment instruments shall ensure that where they communicate personalised security credentials and authentication codes, these are not readable, directly or indirectly, by any staff at any time. In case of loss of confidentiality of personalised security credentials under their sphere of competence, those providers shall inform without undue delay the payment services user associated with them and the issuer of the personalised security credentials.*

Taking Article 34 and 35 together, we can see that while the EC final text RTS states the requirements for certificates, it is not prescriptive about the encryption algorithm to be used nor what should be the relationship between the encryption keys used and the certificate provided by the Trust Service Provider (TSP).

This is especially relevant as there is an opportunity, through the use of identity-based public-key cryptography, to provide an effective method of meeting the requirements highlighted in the EC final text RTS.

Identity-based public key cryptography is a method of public-key cryptography that allows for data to be encrypted for a user, based upon the knowledge of the identity of a user in a system.

In the scenario of a Third Party Provider (TPP) communicating with a bank, an identity could be the credentials, or the account details, of a user. By encrypting payment data and payment instructions using identity-based public keys, the encryption applied to the data is directly linked to a consumer's account.

With such an approach, the data can thus remain encrypted across both organisations' boundaries throughout its lifecycle, stored and logged in its encrypted form by both parties, and decrypted as and when required, ensuring traceability and auditability, as mandated by Chapter V, Section 1, Article 29 of the EC final text RTS, while simultaneously authenticating the source PSP of this data.

In an identity-based public key approach, any given Payment Services Provider (PSP), whether bank or TPP, will need to run a Key Management Server (KMS) so as to generate keys for each user it manages. This PSP then need only share the public keys of its KMS to the third parties it wishes to receive data from.

By sharing its KMS' public keys, the PSP will allow third parties to encrypt data for any user it manages, and for those third parties to authenticate all data they receive.

These public keys can be mutually exchanged between PSPs or provided in the certificates issued by Trust Service Providers.

6 Secure Chorus: standards for securing data and assuring the identity of interfaces between Payment Service Providers

The PSD2 requires Account Servicing Payment Service Providers (ASPSPs) such as banks to open their IT infrastructure to third party providers. The EC final text RTS requires banks provide interfaces which enable the exchange of data between banks and Third Party Payment Providers (TPPs). The EC final text RTS further requires that these interfaces support secure data exchange and robust authentication.

In the consultations held by the European Bank Authority (EBA), some Account Information Service Providers (AISPs) and Payment Information Service Providers (PISPs) indicated that a solution to this requirement could consist of a combination of the use of Hyper Text Transfer Protocol Secure (HTTPS) over Transport Layer Security (TLS).

The EBA has however opted not to mandate a specific technology solution in order to ensure technology and business-model neutrality as well as allow for future innovations (see comment 6 on article 4(3)(c) of the EBA final draft RTF, found in "Summary of responses to the consultation and the EBA's analysis" [2]).

Beyond stating that strong and widely recognised encryption techniques should be used to safeguard the confidentiality and the integrity of the data, the EC final text RTS does therefore not provide guidance on the technology to be used to enable or protect this communication.

As presented in the previous section, an Identity-Based Public Key Cryptography (IDPKC) approach can provide an effective solution to addressing the requirements of the EC final text RTS. IDPKC can protect data by providing end-to-end encryption where encryption keys are directly associated with a consumer's identity, while also providing authentication of the Payment Service Provider from which the data has originated.

The interfaces of Payment Services Providers (PSPs) which adopt an IDPKC approach can enable secure and authenticated communication with each other by simply exchanging a single piece of data on a regular (typically monthly or yearly) basis: the public keys of their respective Key Management Servers (KMS).

The EC final text RTS mandates the use of qualified certificates to ensure a PSP can be appropriately identified. Certificates can be very effectively combined with an IDPKC approach. Instead of PSPs having to manually exchange public key material with one another, certificates provide a method for disseminating the public keys of the KMSs of each PSP. By issuing certificates, a Trust Service Provider (TSP) can provide assurance that these KMS keys are directly associated with the PSP.

MIKEY-SAKKE – Secure Chorus' cryptography standard of choice – is a cutting-edge open cryptography standard, which has been standardised in the Internet Engineering Task Force (IETF) and is based on contemporary IDPKC. MIKEY-SAKKE has been recently approved by 3rd Generation Partnership Project (3GPP) for use in mission-critical applications, such as emergency services communications.

MIKEY-SAKKE has been selected by Secure Chorus, as it ensures data is being communicated to the right person (authentication of identity) and makes certain that no unauthorised person can access the data (end-to-end encryption).

Secure Chorus is further producing, in collaboration with its vendor members, a full set of interoperability standards to ensure that any vendor member's Secure Chorus Compliant Product is able to share data with any other vendor member's Secure Chorus Compliant Product in the ecosystem.

The interoperability standards are underpinned by widely accepted communication standards, developed by international standards bodies including the IETF and 3GPP, as well as cryptographic standards written and approved by the National Cyber Security Centre (NCSC), the UK's authority on cyber security.

This marriage of cryptography and interoperability standards also meets a set of scale and usability requirements of PSPs, which, in our view, no other protocol is currently able to meet.

Origins of MIKEY-SAKKE

In 2012, the UK Government's National Technical Authority for Information and Assurance (CESG) - now the National Cyber Security Centre (NCSC) - defined MIKEY-SAKKE as an open cryptography standard, to answer to UK Government's secure communication requirements at OFFICIAL and have a cryptographic method for validating an identity for government communications.

This standard was based upon an existing standard for elliptic curve signatures, the Elliptic Curve Digital Signature Algorithm (ECDSA) and an identity-based cryptographic protocol developed by two Japanese researchers, SAKAI and KASAHARA. Combining these protocols for secure communications gave rise to MIKEY-SAKKE, defined by the IETF as RFC 6507 and RFC 6509.

Key Management Servers

The architecture of MIKEY-SAKKE defines that each system in a network exchanging data is attached to a Key Management Server (KMS). The server distributes key information to the systems it manages on a regular (monthly or yearly) basis.

Any participant in a communication session can validate the origin of the messages it receives by validating the signature against the public key material of the KMS controlling that system. In order to address the requirements outlined in the EC final text RTS, a KMS could be run by each Payment Service Provider (PSP) with unique key material for each user it manages. The KMS' public key material could then be disseminated via the certificates issued by a Trust Service Provider (TSP), or mutually exchanged between PSPs.

The existence of the KMS means that an organisation has access to its own encrypted data, without giving access to unauthorised third parties. With this access, data controllers can cost-effectively retrieve specific communication logs to comply with record-keeping requirements as defined in the PSD2 (Article 72) as well as those required by the General Data Protection Regulation (GDPR).

PSPs are free to decrypt specific data to ensure they can respond to regulatory requirements. Auditing of both the data communicated as well as the security mechanism is possible; for example, information regarding the encryption and signatures used for a particular communication interaction can be stored and audited.

7 Conclusion

In a closed environment such as the security perimeter of an organisation, securing sensitive data may be relatively straightforward. However, in the payment services market environment where Payment Services Providers (PSPs) share data through interfaces, namely outside the security perimeter of each PSP, there are issues of interoperability and the privacy of data, all of which are compounded by the need to ensure the PSPs sending or receiving the data via these interfaces are those who are authorised to do so.

The EC final text RTS requires PSPs to implement secure data exchange and robust authentication between one another through open standards of communication that are secure and auditable.

The EC final text RTS further requires PSPs to ensure they can appropriately monitor, assess and audit their cybersecurity capability. Finally, it sets out requirements regarding traceability, record-keeping and logging of transactions. At the same time, EU General Data Protection Regulation (GDPR) must be followed, bringing with it the obligation for PSPs to give data subjects access to their data.

Secure Chorus' open cryptography standard of choice addresses the requirement for secure data exchange and robust authentication between PSPs through open communication standards which are secure and auditable.

In terms of communication standards that provide for secure data exchange and robust authentication – Secure Chorus' open cryptography standard provides for end-to-end encryption and authentication between systems. This would enable all PSPs using Secure Chorus Compliant Products to securely process data in any environment, both at rest (e.g. record-keeping) and in transit (e.g. transmission of user credentials).

Secure Chorus' interoperability standards would also ensure secure data exchange within the security perimeter of a PSP and beyond. This would be achieved by ensuring that the technologies underpinning the PSPs' interfaces interoperate with one other.

Regarding communication standards that allow for auditability of the technology systems used by the PSPs, the Secure Chorus' cryptography standard of choice would allow a PSP to have full control of its security system, offering strong traceability and auditability capabilities.

The EC final text RTS wrestles to a certain extent with the issue of secure transmission of confidential data between PSPs and mandates the usage of open standards of communication documented by international or EU standardisation organisations to tackle this problem.

Secure Chorus' cryptography standard could be considered as the standard of choice for PSPs, given that it has been standardised in the Internet Engineering Task Force (IEFT) and has been recently been approved by 3rd Generation Partnership Project (3GPP) for use in mission-critical applications, such as emergency services communications. Emergency Services are complex multi-actor environment; hence it provides for a good comparative use case with PSPs.

Since the specifications of Secure Chorus' cryptography standards are known and open, it is possible for anyone to assess that the technology meets the desired security requirements. As such, vendors providing products compliant with the Secure Chorus' cryptography standard of choice can help PSPs overcome the challenge of meeting current compliance levels and as outlined in the EC final text RTS.

8 References

[1] European Parliament, Council of the European Union, “Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC,” 25 November 2015. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32015L2366.

[2] European Banking Authority, “Final Report, Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2),” 23 February 2017. [Online]. Available: https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf.

[3] European Commission, “COMMISSION DELEGATED REGULATION (EU) No …/.. of XXX supplementing Directive 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication,” 27 November 2017. [Online]. Available: http://ec.europa.eu/finance/docs/level-2-measures/psd2-rts-2017-7782_en.pdf.

secure chorus

CONTACT DETAILS:

One Canada Square,
Canary Wharf,
London E14 5AB

General Inquiries: **info@securechorus.org**
Membership Inquiries: **membership@securechorus.org**

www.securechorus.org

@SecureChorus

/company/secure-chorus-ltd/

Secure Chorus Ltd, a not-for-profit private company limited by guarantee, under The Companies Act 2006 and the situation of its registered office is in England and Wales.