Public Hearing on strong customer authentication & secure communication (SCA & CSC) under Aricle 97 PSD2

Dirk Haubrich, Geoffroy Goffinet
Consumer Protection, Financial Innovation and Payments

EBA offices, London, 23 September 2016

Agenda

1. Introduction
   - The purpose of public hearings
   - The creation of the EBA and its 'scope of action'
   - Legal instruments available to the EBA, and their meaning
   - Overview of EBA mandates under PSD2

2. The mandate on SCA & CSC under Article 98 PSD2
   - Wording of the mandate as provided in PSD2
   - EBA approach to deliver the mandate

3. Requirements of the draft RTS as proposed in the CP
   - Strong customer authentication (SCA) procedure;
   - Exemptions from the application of SCA;
   - Protection of the confidentiality and the integrity of the payment service users' personalised security credentials; and
   - Common and secure open standards of communication

4. Next steps

Introduction to the EBA

The purpose of EBA public hearings

For many of its technical standards and guidelines, the EBA organizes so called 'public hearings', which have a particular purpose.

- **An EBA hearing takes place during the consultation period, usually a month or so before the submission deadline of responses to the Consultation Paper (CP).**

- **The purpose of the hearing is not for attendees to convey their views about the provisions proposed in the CP. The EBA prefers to receive those views as written responses to the CP, in order to be able to assess them properly.**

- **Rather, in the hearing the EBA presents a summary of the CP, re-produces the questions of the CP, and asks attendees whether they require additional explanations or clarifications from the EBA so as to be be able to answer the questions in the CP.**

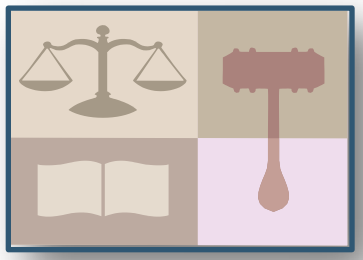
The creation of the EBA

- The EBA was established by Regulation (EC) No. 1093/2010 of the European Parliament and EU Council;
- came into being on 1 January 2011;
- took over all existing tasks and responsibilities from the Committee of European Banking Supervisors (CEBS);
- took on additional tasks, incl. consumer protection, the monitoring of financial innovation, and payments;
- is an independent authority;
- is accountable to the EU Parliament and Council;
- has as its highest governing body the EBA Board of Supervisors, comprising the Heads of the 28 national supervisory authorities.

Legal instruments available to the EBA

The EBA has different types of legal instruments at its disposal that differ in terms of purpose, legal status, and possible addressees.

- Technical standards
- Guidelines and recommendations
- Opinions / Technical Advice
- Warnings
- Temporary prohibitions
- Joint Positions
- Breach of Union law investigations
- Binding and non-binding mediation



The EBA's scope of action

The EBA's regulatory remit is defined by the EU Directives and Regulations that fall into its 'scope of action', either because they are listed in the EBA's founding regulation or because they confer tasks on the EBA. They include:

- Capital Requirements Directive (CRR/D IV)
- Deposit Guarantee Scheme Directive (DGSD)
- Mortgage Credit Directive (MCD)
- Payment Accounts Directive (PAD)
- Electronic Money Directive (EMD)
- Payment Services Directive (PSD1 + forthcoming PSD2)
- Anti–Money Laundering Directive (AMLD)
- Markets in Financial Instruments Directive (MiFID/R, for structured deposits)

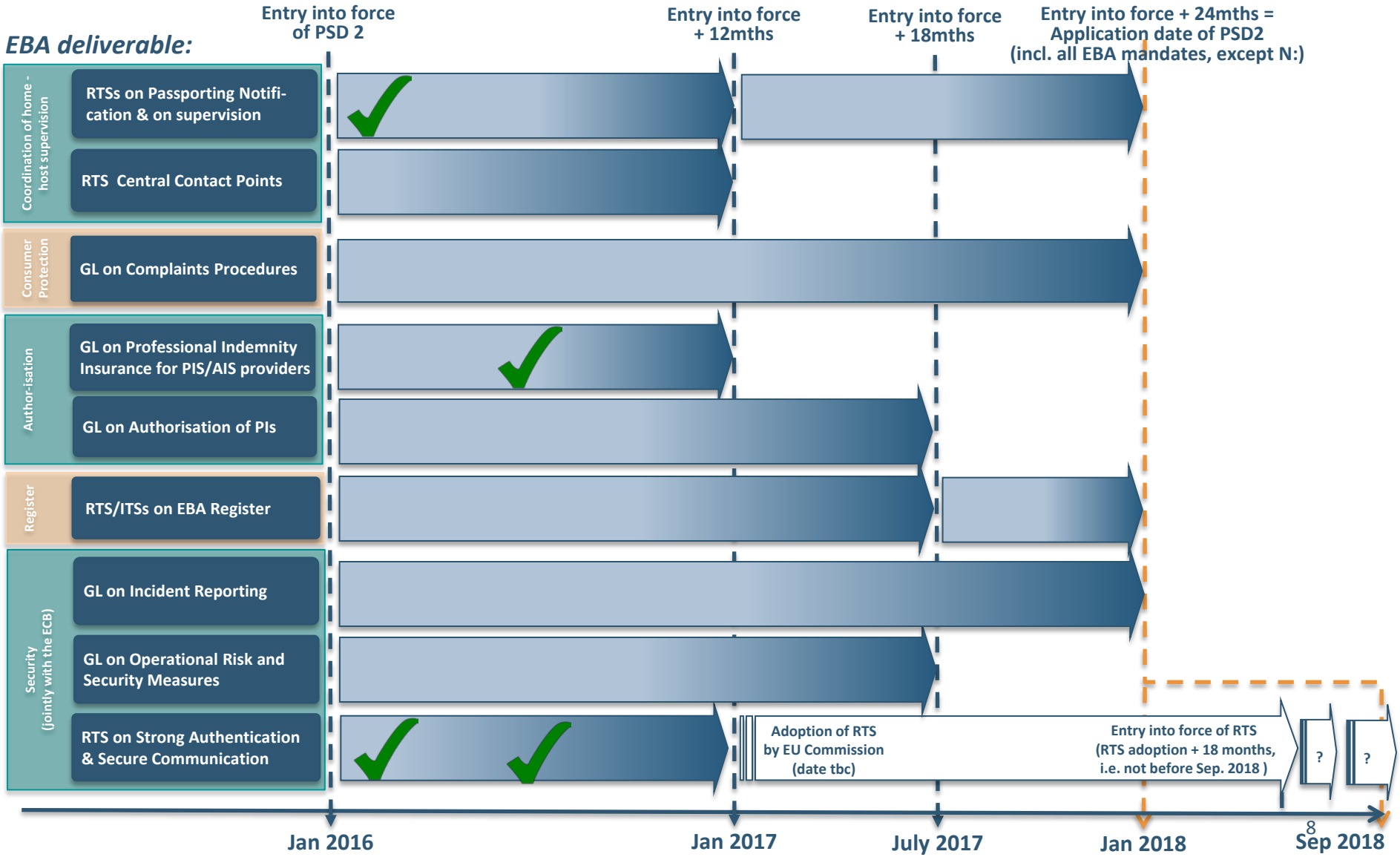
Output of the EBA to date

Since its creation in 2011, the EBA has issued more than 200 legal instruments, as well as more than 100 reports.

	2011	2012	2013	2014	2015	Total
Regulatory Technical Standards	0	1	39	22	15	77
Implementing Technical Standards	0	0	21	10	9	40
Guidelines	2	6	2	17	19	46
Opinions / Technical Advice	1	6	6	14	21	48
Published reports	6	12	26	23	34	111
Recommendations	2	0	4	1	2	9
Breach of Union Law investigations	0	0	0	1	0	1
Mediations	0	2	5	0	0	7
Peer reviews	0	0	1	1	1	3
Warnings	0	0	2	0	0	2
Stress tests	1	0	0	1	1	3

Overview of EBA mandates under PSD2

The PSD 2 has conferred on the EBA the development of 11 mandates.



The mandate on strong customer authentications and common & secure communication under Art 98 PSD2

Wording of the mandate under Art. 98 PSD2

- "EBA shall develop RTS establishing, in close cooperation with the ECB, draft Regulatory Technical Standards addressed to payment service providers (PSP) specifying:
  - a) the requirements of the strong customer authentication (SCA) when the payer accesses his payment account online; initiates an electronic payment transaction or carries out any action, through a remote channel, which may imply a risk of payment fraud or other abuses;
  - b) the exemptions from the application of Article 97 on strong customer authentication and adequate security measures to protect the confidentiality and integrity of PSCs, based on the level of risk involved in the service provided; the amount, the recurrence of the transaction, or both ; or the payment channel used for the execution of the transaction;
  - c) the requirements with which security measures have to comply in order to protect the confidentiality and the integrity of the payment service users' (PSU) 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 ASPSP, PIS providers, AIS providers, payers, payees and other payment service providers."

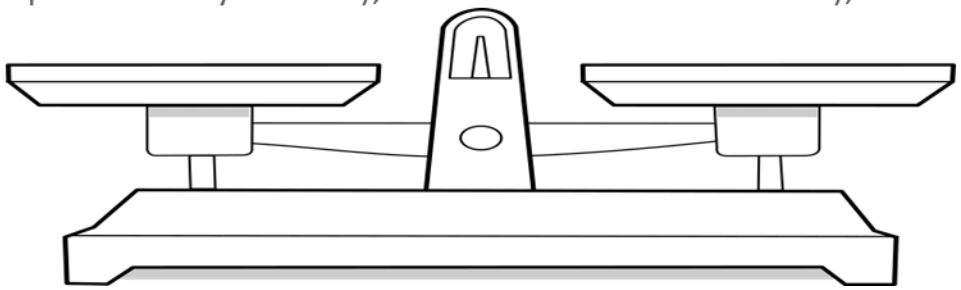
EBA's approach: trade offs to be made

When developing the RTS on strong customer authentication & secure communication, EBA and ECB will have to make difficult trade-offs between competing demands.

1) **Tough security standards** (which may suggest a high degree of prescription in the requirements to avoid circumvention of rules); **vs.** **Facilitation of innovative industry solutions in the future** (which may suggest the opposite, i.e. high level requirements that provide flexibility across space & time);

2) **Tough security standards** (which may suggest that payment user should be subject to several security and authentication steps); **vs.** **Customer convenience** (which may suggest the opposite, e.g. one-click payments);

3) **High degree of interoperability between all ASPSPs and all PISPs/AISPs** (which may suggest one single standard/ protocol to be prescribed by the EBA); **vs.** **Flexibility for market participants** (which may suggest the opposite, i.e. high level requirements that in turn allow for many different market-driven solutions);



EBA approach: publication of a Discussion Paper

- The Discussion Paper was published on 8 December 2015 and the consultation period closed on 8 February 2016.

- The EBA received 118 responses to the DP, among which 82 gave permission for the EBA to publish them on the EBA website. This represents the second highest number of responses ever received by the EBA to a discussion or consultation paper.

- Against this background, the CP

  - summarises the EBA's understanding of some of the PSD2 provisions where relevant for the development of the EBA mandates;
  - summarises the responses received to the Discussion Paper; and
  - elaborates on the options and policy choices that were made when developing the provisions proposed in the CP.

Content of the draft RTS, as proposed in the CP

Chapter 1: the SCA procedure (1)

- **Clarification of PSD2 provisions - EBA understands that :**
  - **a) SCA shall apply to :**
    - ✓ **electronic payments initiated by the payer, such as credit transfers or card payments, but does not apply to electronic payments initiated by the payee only, such as direct debits.**
    - ✓ **electronic mandate, under the category of "any action through a remote channel which may imply a risk of payment fraud or other abuses" as defined in Article 97(1)(c) of PSD2 ,wherever PSPs are involved in the signature of the e-mandate, either through direct communication with the payer or via the payee's PSP.**
  - **b) the SCA procedure will remain fully in the sphere of competence of the ASPSP (if a PISP issues its own personalised security credentials for the user, in place of the credentials issued by the ASPSP, this would however require a prior contractual agreement between the PIS and the ASPSP on the acceptance of such credentials by ASPSP. Such agreement would also be outside of the scope of PSD2.**
  - **c) Card acquiring PSPs should require payees to support strong customer authentication for all payment transactions, in order to allow the payer's PSP to perform SCA in compliance with PSD2. The EBA understands that Article 74(2) of PSD2, which allows the payee or the payee's PSP the option not to accept SCA, only applies during the short-time transitional period between the application date of PSD2 (13 January 2018) and the application date of the RTS under consultation (in October 2018 the earliest).**

Chapter 1: the SCA procedure (2)

- **Principles underlying the provisions for SCA in the draft RTS proposed by EBA:**
  - **a) Authentication elements include the Personalised Security Credentials (PSCs) as well as devices and software used to generate or receive authentication codes;**
  - **b) For SCA, PSPs have to ensure that a valid combination of authentication elements results in the generation of an authentication code to the payer's PSP that is only accepted once by the PSP for the same PSU;**
  - **c) For SCA with dynamic linking:**
    - ✓ **the authentication code to the payer's PSP shall be specific to the amount and payee agreed to by the payer when initiating the electronic remote payment transaction;**
    - ✓ **the one-time password (OTP) linked to the amount and payee may be alternatively generated by the payer's PSPs with or without any action required by the payer itself, according to the technological solution adopted;**
    - ✓ **the confidentiality, authenticity and integrity of the amount of the transaction and of the payee through all phases of the authentication procedure shall be ensured so that any change to the amount or payee results in a change of the authentication code;**
    - ✓ **When the SCA procedure relies on a mobile device, the channel, device or mobile application through which the information linking the transaction to a specific amount and a specific payee is displayed shall be independent or segregated from the channel, device or mobile application used for initiating the electronic payment transaction;**
    - ✓ **Special procedures foreseen for transactions where the amount might not be known or for bulk payments (articles 3(3) and 3(4) of the draft RTS).**

Chapter 1: the SCA procedure (3)

- **Principles underlying the provisions in the draft RTS proposed by EBA:**
  - **d) The SCA procedure shall include mechanisms to prevent, detect and block fraudulent payment transactions before the PSP's final authorisation;**
  - **e) PSPs periodically test, evaluate and audit the security of the overall strong customer authentication procedure to ensure resilience of SCA over time;**
  - **f) Synergies with e-idas: the draft RTS do not prevent the possibility to adopt SCA procedures based on the services of a public e-identity scheme under the e-IDAS regulation framework, as long as these public e-identity schemes comply with the draft RTS.**

Q1: Do you agree with the EBA's reasoning on the requirements of the strong customer authentication, and the resultant provisions proposed in Chapter 1 of the draft RTS?

Q2: In particular, in relation to the "dynamic linking" procedure, do you agree with the EBA's reasoning that the requirements should remain neutral as to when the "dynamic linking" should take place, under the conditions that the channel, mobile application, or device where the information about the amount and the payee of the transaction is displayed is independent or segregated from the channel, mobile application or device used for initiating the payment, as foreseen in Article 2.2 of the draft RTS.

Q3: In particular, in relation to the protection of authentication elements, are you aware of other threats than the ones identified in articles 3, 4 and 5 of the draft RTS against which authentication elements should be resistant?

Chapter 2: Exemptions to SCA (1)

- **Clarification of PSD2 provisions - EBA understands that :**

  a) **the draft RTS under consultation specifies the cases (the exemptions) in which payment services providers are not obliged to apply strong customer authentication;**

➔ **"Mandatory" nature of exemptions ? Outside the scope of EBA mandate. Pending further clarification, EBA is seeking views from respondents to the CP as to whether the proposed list of exemptions would also be compatible with a potential scenario whereby exemptions would be mandatory for the ASPSPs, meaning that ASPSPs would be prevented from implementing SCA on transactions that meet the criteria for exemption**

  b) **the exemptions to SCA as defined in the RTS under consultation constitute a part of the authentication procedures performed by the payer's PSP (also referred as ASPSP) and should therefore be applied by the ASPSP only**

➔ **Change compared to the exemptions to SCA specified in Guideline 7.5 of the EBA Guidelines on the security of internet payments (EBA GL/2014/12): PSPs offering acquiring services for card-based remote payment transactions can not decide to apply exemptions, only issuing card PSPs can.**

Chapter 2: Exemptions to SCA (2)

- **Principles underlying the provisions for exemptions in the draft RTS proposed :**

  a) **Distinction made between the exemptions to the application of SCA according to Article 97(1) and the exemptions to the application of SCA according to Article 97(2).**

  b) **No exemption to the application of security measures to protect the confidentiality and integrity of payment service users' personalised security credentials according to Article 97(3).**

  c) **List of exemptions to SCA (Article 97(1)) :**

  - ✓ **Exclusive access to information of payment account online (including AIS), without disclosure of sensitive payment data. However, SCA shall apply where the payer accesses the information for the first time and where the payer accesses the information later than one month after the last day in which strong customer authentication was applied.**
  - ✓ **Contactless electronic payment transaction at a point of sale where the individual amount of contactless electronic payment transaction does not exceed the maximum amount of 50 EUR and the cumulative amount of previous non-remote electronic payment transactions without application of strong customer authentication does not exceed 150 EUR.**

Chapter 2: Exemptions to SCA (3)

- **Principles underlying the provisions for exemptions in the draft RTS proposed by EBA:**

  d) List of exemptions to SCA with "dynamic linking" (Article 97(2)) :

  - ✓ **credit transfer where the payee is included in a list of trusted beneficiaries. However;, SCA shall apply where the payer creates for the first time or subsequently amends the list of trusted beneficiaries;**
  - ✓ **online a series of credit transfers with the same amount and the same payee. However, SCA shall apply where the payer initiates the series of credit transfers for the first time or amends the series of credit transfers;**
  - ✓ **online credit transfer where the payer and the payee are the same natural or legal person and the payee's payment account is held by the payer's account servicing payment services provider;**
  - ✓ **remote electronic payment transaction where the individual amount of the remote electronic payment transaction does not exceed the maximum amount of 10 EUR and the cumulative amount of previous remote electronic payment transactions without application of strong customer authentication does not exceed 100 EUR.**

Q4: Do you agree with the EBA's reasoning on the exemptions from the application of Article 97 on strong customer authentication and on security measures, and the resultant provisions proposed in Chapter 2 of the draft RTS?

Chapter 3: Protection of confidentiality & integrity of the payment service users' PSC credentials

- **Principles underlying the provisions for protection of payment security credentials (PSCs) in the draft RTS proposed by EBA:**

  a) **EBA proposes a principle-based approach that requires PSPs to implement measures to protect the creation, association with payment service users, delivery, renewal and destruction of the credentials;**

  b) **These requirements should guarantee (a) the confidentiality, and the integrity of the enrolled personalised security credentials and (b) their delivery to, or possession by, the intended PSU.**

  c) **PSU awareness programs related to the protection of PSCs, especially against social engineering attacks are considered to be more suitably included in the EBA mandate under Article 95 PSD2 in relation to Guidelines on Management of Operational and Security Risks, or as part of the user-friendly electronic leaflet to be developed by the EU Commission under Article 106 PSD2.**

Q6: Do you agree with the EBA's reasoning on the protection of the confidentiality and the integrity of the payment service users' personalised security credentials, and the resultant provisions proposed in Chapter 3 of the draft RTS?

Chapter 4: Common & secure open standards of communication for the purpose of identification, authentication, notification, and information (1)

- **Principles underlying the provisions for exemptions in the draft RTS proposed by EBA:**

  a) **Two sets of requirements:**

  - ✓ **A sub-section that defines principle-based requirements in relation to standards of communication in general. These requirements will be further complemented by the future Guidelines on Management of Operational and Security Risks that the EBA is mandated to issue under Article 95 PSD2.**
  - ✓ **A second subsection that is dedicated to the requirements for common and secure open standards of communication, which focuses on the communication exchanges between AIS/PIS providers and ASPSPs, as well as for communication between PSPs in relation the confirmation on the availability of funds (Article 65).**

  b) **Principle-based requirements in relation to standards of communication in general :**

  - ✓ **Secure bilateral identification when communicating between the payer's device and the payee's acceptance devices for electronic payments, including but not limited to payment terminals;**
  - ✓ **Mobile applications and other payment services users interfaces offering electronic payment services are protected against misdirection of communication to unauthorised third parties;**
  - ✓ **all payment transactions and other interactions with the payment services user, with other payment services providers and with merchants in the context of the provision of the payment service are traceable,**

Chapter 4: Common & secure open standards of communication for the purpose of identification, authentication, notification, and information (2)

- **Principles underlying the provisions for exemptions in the draft RTS proposed by EBA:**

  c) **Requirements for common and secure open standards of communication between AIS/PIS providers and ASPSPs, as well as for communication between PSPs in relation the confirmation on the availability of funds (Article 65):**

  - ✓ **Each ASPSP shall offer at least one communication interface (dedicated or not) enabling secure communication with AISPs, PISPs, and PSPs issuing card-based payment instruments which shall be documented and freely available on the ASPSP's website. AISPs, PISPs, and PSPs issuing card-based payment instruments shall use this communication interface for payment initiation or any exchange of information related to the access to payment accounts;**
  - ✓ **ASPSPs shall ensure that their communication interface allow PISP or AISP to rely on the authentication procedures provided by the ASPSP to the payment service user;**
  - ✓ **ASPSPs shall ensure that their communication interface uses common and open standards which are developed by international or European standardisation organisations and shall use ISO 20022 elements, components or approved message definitions, if available;**
  - ✓ **ASPSPs shall ensure that their communication interface is offering the same functionalities and the same level of availability, including support, as the online platform made available to the payment service user when directly initiating the payment transaction or directly accessing the information online.**

Chapter 4: Common & secure open standards of communication for the purpose of identification, authentication, notification, and information (3)

- **Principles underlying the provisions for exemptions in the draft RTS proposed by EBA:**

  c) **Requirements for common and secure open standards of communication (cted):**

  - ✓ **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;**
  - ✓ **The data elements made available by the ASPSP shall consist of the same information as the information made available to the payment service user when directly accessing the information of a designated payment account online or when directly initiating a payment transaction. For PSPs issuing card-based payment instruments, the data elements made available by the ASPSP shall consist of a simple 'yes' or 'no' answer in relation to the availability of funds, as foreseen by the PSD2;**
  - ✓ **AIS providers shall request information from designated payment accounts and associated payment transactions each time the payment service user is requesting such information or, where the payment service user is not actively requesting such information by connecting to the AIS, no more than two times a day;**
  - ✓ **For the purpose of identification, payment service providers shall rely on Qualified certificates for website authentication as per article 3(39) of Regulation (EU) No 910/2014. The certificate shall contain the authorisation number of the payment service provider, the role of the payment service provider and the name of the**

Chapter 4: Common & secure open standards of communication for the purpose of identification, authentication, notification, and information (4)

Q7: Do you agree with the EBA's reasoning on the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, and the resultant provisions proposed in Chapter 4 of the draft RTS?

Q8: In particular, do you agree that the use of ISO 20022 elements, components or approved message definitions, if available, should be required to ensure the interoperability of different technological communication solutions implemented between PSPs for the provision of AIS, PIS or for the confirmation on the availability of funds? Do you see any particular technical constraint that would prevent the use of such industry standards?

Q9: With regards to identification between PSPs, do you agree that website certificates issued by a qualified trust service provider under an e-IDAS policy would be suitable and allow for the use of all common types of devices (such as computers, tablets and mobile phones) for carrying out different payment services ?

Q10: With regards to the frequency with which AIS providers can request information from designated payment accounts when the payment service user is not actively requesting such information, do you agree that the proposed limit of no more than two times a day achieve an appropriate balance between allowing AISP to provide updated information to their users while not negatively impacting the availability of the ASPSP's communication interface? If not, please indicate what would be in your view the appropriate frequency and rationale for such frequency.

Next steps

Next steps

- End of Consultation Period: 12 October 2016;
- The EBA will assess the responses to the CP, will make changes where appropriate, and plans to publish the final draft RTS in 2017Q1. The publication will include a ‘feedback table’ that lists all the comments the EBA has received, and explains whether or not amendments have been made as a result, and why.
- The EU Commission will then carry out a legal review before adopting it, with the EU Council and EU Parliament having scrutiny rights in the process.
- As and when adopted by the Commission, the RTS will be published in the Official Journal of the EU, enters into force 20 days later. The PSD2 specifies that the RTS will apply 18 months after adoption by the Commission.
- Given these timelines, the application date of the RTS is October 2018 at the very earliest.