



Commission de Surveillance
du Secteur Financier

COMMUNIQUÉ

OBLIGATIONS REGARDING STRONG CUSTOMER AUTHENTICATION AND COMMON AND SECURE OPEN STANDARDS OF COMMUNICATION UNDER COMMISSION DELEGATED REGULATION (EU) 2018/389

The Commission de Surveillance du Secteur Financier (the “CSSF”) draws the attention of the payment service providers (**PSPs**¹) to a certain number of new obligations resulting from:

- The transposition of Directive (EU) 2015/2366 on payment services (“**PSD2**”) by the Luxembourg Law of 20 July 2018, amending the Law of 10 November 2009 on payment services (**the “Law”**); and
- The Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 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 (**the “RTS”, or the “RTS on SCA and CSC” or the “Regulation”**).

Section 1: Entities concerned by the new obligations

The payment service providers concerned by the new obligations are the ones defined in points (i), (ii), (iii) and (iv) of Article 1(37) of the Law and for which the CSSF is the designated competent authority for supervisory purposes under the Law:

- i) Credit institutions;
- ii) Electronic money institutions;
- iii) Post Luxembourg; and
- iv) Payment institutions.

The Regulation applies to the PSPs listed above who offer **payment accounts (including e-money accounts) that are accessible online**:

- regardless of whether this access allows consultative services only, transactional services only, or both; and
- irrespective of:
 - a presumed disinterest of the ASPSP's clients in using account information and/or payment initiation services offered by TPPs;
 - the size of the ASPSP and the number of its clients;
 - the fact that the ASPSP only has corporate clients;
 - the fact that the payment account only allows transactions to its owner's account held at another ASPSP.

¹ Refer to Annex 2 for a glossary of all acronyms used in this communiqué.

Section 2: Main new obligations resulting from the RTS

The CSSF urges the concerned PSPs (see section 1 above) to comply with the requirements of the RTS on SCA and CSC².

With regards to this Regulation, the CSSF would like to reiterate the following key points:

- A) The Regulation applies **from 14 September 2019**, with the exception of paragraphs 3 and 5 of article 30, which apply **from 14 March 2019**³. It underpins the new security requirements under PSD2 and regulates the access by AISPs, PISPs and CBPIIs to customer payment account data held in ASPSPs.
- B) **PSPs must apply Strong Customer Authentication (SCA)** in the use cases described under Article 105-3 of the Law, including for remote electronic payments with a “**dynamic linking**” feature (i.e. with elements which dynamically link the transaction to a specific amount and a specific payee). The Regulation defines the security measures for the application of SCA (i.e. the specifications a PSP must respect to define its SCA procedure) and the nine specific authorized exemptions from the application of SCA.
- C) **Each ASPSP who offers payment accounts that are accessible online has the obligation to offer at least one access interface** enabling secure communication with, and access, by the TPPs to the PSU payment account data. Each ASPSP is free to decide whether to offer as an access interface:
 - either a so-called “dedicated interface”, i.e. an interface that is dedicated to the communication with those TPPs and that shall offer at all times the same level of availability and performance, including support, as the interface(s) made available to the PSU for directly accessing its payment account online; or
 - an “adapted PSU interface”, i.e. to allow the TPPs to use the interface also used by the PSUs to access their payment accounts (e.g. an e-banking website), with an adaptation of this interface to allow the TPPs to identify themselves towards the ASPSP.

The CSSF would like to reiterate that **some obligations** resulting from the Regulation **are applicable to both types of interface, including the two below**:

- the ASPSP is required to make the interface technical specifications documentation available to the TPPs and to offer them a testing facility at least 6 months before the access interface is live;
 - the ASPSP is required to use a qualified eIDAS certificate⁴ for the purpose of TPP identification.
- D) In addition, the Regulation requires all ASPSPs that have opted to offer access via a dedicated interface **to also implement a contingency mechanism**⁵, **unless they receive an exemption from the CSSF** in accordance with the four conditions set out under Article 33(6) of the Regulation and further specified in the EBA Guidelines on exemption⁶.
- E) **All ASPSPs that would like to obtain such an exemption are required to fill in the form for exemption authorisation request** available on the CSSF website:
- for banks: www.cssf.lu/en/supervision/banks/forms/
 - for Post Luxembourg: www.cssf.lu/en/supervision/pfs/specialised-pfs/forms/

² Refer to Annex 3 for a link to the document.

³ Details are described under the last paragraph of point F.

⁴ As referred to in Article 34 of the RTS.

⁵ Also called « Fall back mechanism ».

⁶ EBA Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC). Refer to Annex 3 for a link to the document.

- for payment institutions/electronic money institutions: <http://www.cssf.lu/en/supervision/payment-institutionselectronic-money-institutions/forms/>

The PSPs should send their requests according to the instructions indicated in the form and should take into account the time required for the review of the file and the EBA consultation⁷.

- F) **The deadlines to respect vary** according to the ASPSP situation and to its willingness to apply for a contingency mechanism exemption or not. They are **indicated in Annex 1**. In particular, the CSSF draws the attention of the ASPSPs that would like **to obtain a contingency mechanism exemption as from 14 September 2019** to the fact that they should:
- make the interface technical specifications documentation available to the TPPs and to offer them a testing facility no later than 14 March 2019;
 - roll-out their dedicated interface in production no later than 14 June 2019 to ensure wide usage of the interface for at least 3 months before the RTS application date;
 - submit their exemption request no later than 01 May 2019, except for the information related to the three-month period of wide usage⁸, which has to be provided on 14 July 2019 and on 14 August 2019. **The CSSF cannot guarantee that files received after these deadlines will be processed for the date of application of the Regulation.**
- G) The CSSF also reiterates that an ASPSP may decide to have **only one dedicated interface for servicing all its customers or separate dedicated interfaces for different customer segments (e.g. retail vs corporate)**. In the latter case, ASPSPs would need to apply for a separate exemption for each dedicated interface, in order to be exempted from the obligation to implement a contingency mechanism. The exemption is specific to each dedicated interface.
- H) Finally, an ASPSP may decide to use the access interface solution developed and managed by its group or a third-party. The CSSF considers that **when an ASPSP has recourse to an outsourcing for a dedicated interface solution and asks for a contingency mechanism exemption, this outsourcing is material**. In that case the ASPSP has to ask for CSSF non-objection in line with the circulars CSSF 12/552 and 17/656.

Where the third-party is a **Support PFS⁹ offering PSD2 solutions, the ASPSP will not be automatically exempted** from the obligation to implement a contingency mechanism. The CSSF wants to underline that in the context of the approval process of Support PFS, its analysis is limited to the activity subject to authorisation (e.g. the operation of IT systems for financial entities) and does not prejudice any assessment of a PSD2 solution offered by the latter. **The compliance obligation** related to Article 33(6) of the RTS **is and will remain solely incumbent upon the ASPSP** and the latter will have to ensure that the services provided by its subcontractor(s), in combination with their own technical and organizational setup, services, processes and policies, meet all regulatory requirements. Therefore, the ASPSP implementing an access interface fully or partially relying on the solution offered by a Support PFS and who would like to benefit from the exemption to set up a contingency mechanism must submit the same exemption authorisation request to the CSSF.

Luxembourg, 28 February 2019

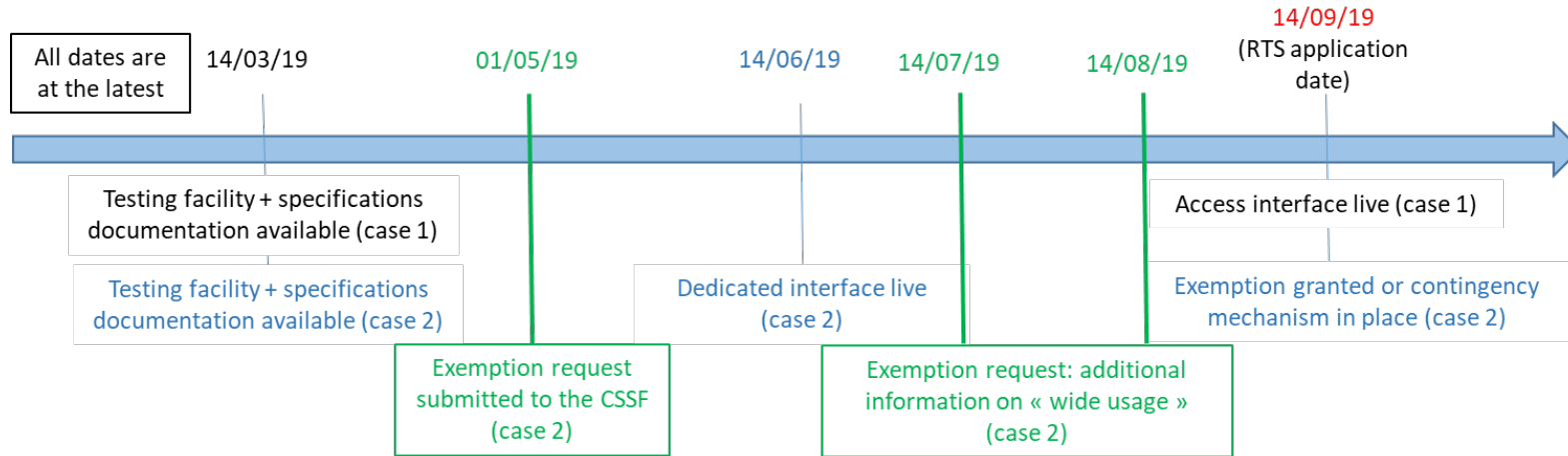
⁷ EBA consultation as referred to in Article 33(6) of the RTS and Guideline 9 of the EBA Guidelines on exemption.

⁸ The EBA has clarified in the Guidelines on exemption that the 6-month testing period may run concurrently with the 3-month "widely used" period.

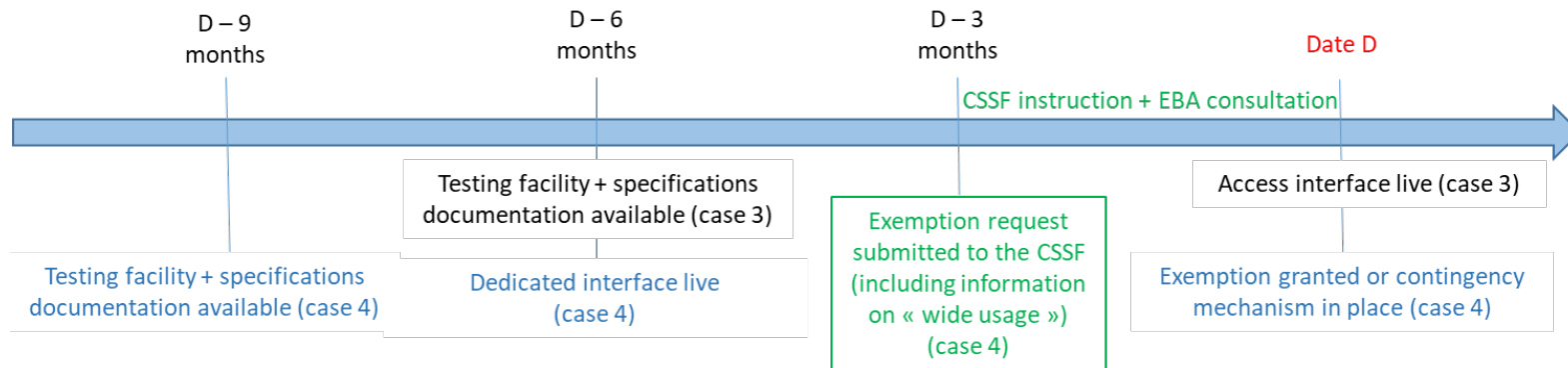
⁹ A professional of the financial sector authorised under Articles 29-3 or 29-4 of the Law of 5 April 1993 on the financial sector ("LFS").

Annex 1: Timelines and deadlines to respect with regards to access interface for TPPs and to contingency mechanism exemption

- 1. The ASPSP already offers or will offer as from 14 September 2019** (application date of the RTS) payment accounts that are accessible online and:
- either the ASPSP does not want to obtain an exemption from the obligation to set up a contingency mechanism (case 1- see RTS deadlines);
 - or the ASPSP wants to obtain an exemption from the obligation to set up a contingency mechanism (case 2 – see RTS deadlines and deadlines for authorisation request submission to CSSF).



- 2. The ASPSP plans to offer payment accounts that are accessible online after 14 September 2019 as from day D** and:
- either the ASPSP does not want to obtain an exemption from the obligation to set up a contingency mechanism (case 3 – see RTS deadlines);
 - or the ASPSP wants to obtain an exemption from the obligation to set up a contingency mechanism (case 4 – see deadlines considering RTS deadlines + time needed for CSSF instruction and EBA consultation).



Annex 2: Glossary of main terms used

- **PSP:** payment service provider as defined in Article 1(37) of the Law
- **ASPSP:** account servicing payment service provider as defined in Article 1(37b) of the Law
- **AISP:** account information service provider as defined in Article 1(37d) of the Law
- **PISP:** payment initiation service provider as defined in Article 1(37c) of the Law
- **CBPII:** payment service provider issuing card-based payment instruments
- **TPP:** term commonly used in PSD2-related communication to designate globally the account information service providers (AISPs), payment initiation service providers (PISPs) and payment service providers issuing card-based payment instruments (CBPIIs)
- **SCA:** strong customer authentication as defined in Article 1(2a) of the Law
- **PSU:** payment service user as defined in article 1(46) of the Law

Annex 3: Links to the main official texts related to the RTS on SCA and CSC

Regulatory technical standards for strong customer authentication and common and secure open standards of communication (Commission delegated regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council; the “Regulation”, “the RTS on SCA and CSC”).

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN>

EBA Opinion on the transition from PSD1 to PSD2 (EBA-Op-2017-16)

<https://eba.europa.eu/documents/10180/2067703/EBA+Opinion+on+the+transition+from+PSD1+to+PSD2+%28EBA-Op-2017-16%29.pdf>

Opinion on the implementation of the RTS on SCA and CSC (EBA-2018-Op-04)

<https://eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf>

Guidelines on the conditions to be met to benefit from an exemption from contingency measures under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)

<https://eba.europa.eu/documents/10180/2250578/Final+Report+on+Guidelines+on+the+exemption+to+the+fall+back.pdf/4e3b9449-ecf9-4756-8006-cbbe74db6d03>

Opinion on the use of eIDAS certificates under the RTS on SCA and CSC

<https://eba.europa.eu/documents/10180/2137845/EBA+Opinion+on+the+use+of+eIDAS+certificates+under+the+RTS+on+SCA+CSC.pdf>

EBA Single Rulebook Q&A on payment services

<https://eba.europa.eu/single-rule-book-qa/-/qna/search/legalAct/6>