

Luxembourg, 14 June 2019

To all payment services providers

## CIRCULAR CSSF 19/720

### **Re: Adoption of the Guidelines of the European Banking Authority 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) (EBA/GL/2018/07)**

Ladies and Gentlemen,

The purpose of this circular is to draw your attention to the Guidelines of the European Banking Authority (“**EBA**”) on the conditions to benefit from an exemption from the contingency mechanism<sup>1</sup> under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA and CSC<sup>2</sup>) (the “**RTS**”) - EBA/GL/2018/07 (the “**Guidelines**”) with which the CSSF commits to comply in its capacity as competent authority.

The circular further provides in a formal way the instructions to submit an exemption request to the CSSF in line with the Guidelines, which were already indicated in a *Communiqué*<sup>3</sup> published on our website on 28 February 2019. As a reminder, the RTS will enter into force on 14 September 2019<sup>4</sup> and the *Communiqué* was published to urge those account servicing payment service providers (“**ASPPs**”) which would like to obtain a contingency mechanism exemption as from that date, to submit their exemption request to the CSSF by no later than 01 May 2019.

### **1. The Guidelines**

As a reminder, the transposition of Directive (EU) 2015/2366<sup>5</sup> (“**PSD2**”) in Luxembourg through the Luxembourg law of 20 July 2018, amending the law of 10 November 2009 on payment services<sup>6</sup> (the “**Law**”), enshrined the right of account information service providers (“**AISPs**”), payment initiation service providers (“**PISPs**”) and card-based payment instrument

<sup>1</sup> Also called “fall back mechanism”

<sup>2</sup> 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

<sup>3</sup> <https://www.cssf.lu/en/2019/02/obligations-regarding-strong-customer-authentication-and-common-and-secure-open-standards-of-communication-under-commission-delegated-regulation-eu-2018-389/>

<sup>4</sup> With the exception of paragraphs 3 and 5 of article 30, which apply from 14 March 2019

<sup>5</sup> 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

<sup>6</sup> Law of 10 November 2009 on payment services, on the activity of electronic money institution and settlement finality in payment and securities settlement systems

issuers (“CBPIIs”<sup>7</sup>) (together also called “TPPs”<sup>8</sup>) to access payment service user (“PSU”) payment account data held with account servicing payment service providers (“ASPSPs”), based on the PSU’s explicit consent.

The RTS provide details on the new security requirements under PSD2 and regulate the access of TPPs to the PSU’s payment account data held with ASPSPs. These latter must offer at least one access interface to the former but are free to decide whether to establish such an interface by means of a so-called dedicated interface or by means of an adapted PSU interface.

In accordance with Article 33(4) of the RTS, all ASPSPs that have opted to offer access via a dedicated interface are also required to implement a contingency mechanism, unless they receive an exemption from the CSSF in accordance with the four conditions set out under Article 33(6) of the RTS. The Guidelines further specify these four conditions to exempt an ASPSP from the obligation to set up the contingency mechanism. They also provide guidance on how competent authorities should consult the EBA for the purposes of the exemption in accordance with Article 33(6) of the RTS.

## **2. Scope**

The present circular is addressed to the payment service providers as defined in Article 1(37) of the Law, for which the CSSF is the designated competent authority for supervisory purposes (“PSPs”).

More specifically, this circular is of particular interest to credit institutions, electronic money institutions, Post Luxembourg and payment institutions:

- which act as ASPSPs and offer payment accounts (including e-money accounts if they permit payment transactions in the sense of article 1(31) of the Law) that are accessible online to PSUs; and
- which would like to be exempted from the obligation to set up the contingency mechanism described in Article 33(4) of the RTS.

## **3. Application form to request an exemption**

All ASPSPs that would like to be exempted from the obligation to set up the contingency mechanism described in Article 33(4) of the RTS are required to fill in the application form to request an exemption which is available on the CSSF website:

- for banks: [https://www.cssf.lu/en/publication-data/?content\\_type=551&entity\\_type=480](https://www.cssf.lu/en/publication-data/?content_type=551&entity_type=480)
- for Post Luxembourg: [https://www.cssf.lu/en/publication-data/?content\\_type=551&entity\\_type=16](https://www.cssf.lu/en/publication-data/?content_type=551&entity_type=16)

---

<sup>7</sup> As referred to in article 81-1 of the Law

<sup>8</sup> TPPs or Third-party Payment Providers: 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)

- for payment institutions/electronic money institutions:  
[https://www.cssf.lu/en/publication-data/?content\\_type=551&entity\\_type=962,12,964,15](https://www.cssf.lu/en/publication-data/?content_type=551&entity_type=962,12,964,15)

The ASPSPs should send their requests according to the instructions indicated in the application form.

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, if the ASPSP wishes to be exempted from the obligation to implement a contingency mechanism for each of its dedicated interfaces, it will need to submit one application form per dedicated interface as an exemption is specific to one dedicated interface.

#### **4. Potential resort to outsourcing**

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 resorts to an outsourcing for a dedicated interface solution and applies for a contingency mechanism exemption, this outsourcing would be qualified as material. Consequently and in line with the circulars CSSF 12/552<sup>9</sup> and 17/656<sup>10</sup> as applicable, the ASPSP is required to address to the CSSF an outsourcing authorisation request, respectively an outsourcing notification when the service provider is a Support PFS<sup>11</sup>. Such request or notification must be submitted to the CSSF before, or at the latest together with, the exemption request.

Where the third-party is a Support PFS offering PSD2 solutions, the ASPSP will not be automatically exempted from the obligation to implement a contingency mechanism. 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 sub-contractor(s), in combination with its own technical and organizational setup, services, processes and policies, meet all regulatory requirements. Therefore, the ASPSP which implements an access interface fully or partially relying on the solution offered by a Support PFS and which would like to benefit from the exemption to set up a contingency mechanism must submit an exemption request to the CSSF as required in section 3 of the present circular.

#### **5. Deadlines to submit the exemption request**

##### **a. General deadlines**

The RTS require the ASPSPs which would like to obtain a contingency mechanism exemption:

---

<sup>9</sup> Circular CSSF 12/552 (as amended by Circulars CSSF 13/563, 14/597, 16/642, 16/647 and 17/655) on central administration, internal governance and risk management

<sup>10</sup> Circular CSSF 17/656 on administrative and accounting organisation; IT outsourcing

<sup>11</sup> A professional of the financial sector authorised as IT operator under Articles 29-3 or 29-4 of the Law of 5 April 1993 on the financial sector

- to make their interface technical specifications documentation available to PISPs, AISPs and CBPIIs that are authorised or in the process of authorisation with their competent authority and to offer them a testing facility at least 6 months before they can be exempted; and,
- to roll-out their dedicated interface in production at least 3 months before they can be exempted (as a necessary prerequisite for the condition of wide usage of the interface for at least 3 months before they can be exempted)<sup>12</sup>.

Considering the above requirements and the additional time required to allow the CSSF to instruct the file and consult the EBA in due time<sup>13</sup>, an ASPSP who would like to be exempted from the requirement to implement a contingency mechanism as from a target date D must submit its exemption request fully completed at least 3 months before the target date D.

b. Transitional period until the RTS application date (i.e. 14 September 2019)

To comply with the RTS, the ASPSPs that would like to obtain a contingency mechanism exemption immediately as from the RTS application date (i.e. 14 September 2019) should:

- make their interface technical specifications documentation available to PISPs, AISPs and CBPIIs that are authorised or in the process of authorization with their competent authority and offer them a testing facility no later than 6 months before the RTS application date (i.e. 14 March 2019); and,
- roll-out their dedicated interface in production no later than 3 months before the RTS application date (i.e. 14 June 2019) (as a necessary prerequisite for the condition of wide usage of the interface for at least 3 months before they can be exempted)<sup>14</sup>.

Considering the tight timeline, the ASPSPs that would like to obtain a contingency mechanism exemption as from 14 September 2019 have already been asked by way of a *communiqué* available on our website<sup>15</sup> to submit their exemption request no later than 01 May 2019, except for the information related to the three-month period of wide usage, which has to be provided on 14 July 2019 and on 14 August 2019<sup>16</sup>.

## 6. Date of application

The present circular shall apply with immediate effect.

<sup>12</sup> The EBA has clarified in the Guidelines that the 6-month testing period may run concurrently with the 3-month “widely used” period

<sup>13</sup> EBA consultation as referred to in Article 33(6) of the RTS and Guideline 9 of the Guidelines

<sup>14</sup> The EBA has clarified in the Guidelines that the 6-month testing period may run concurrently with the 3-month “widely used” period

<sup>15</sup> <https://www.cssf.lu/en/2019/02/obligations-regarding-strong-customer-authentication-and-common-and-secure-open-standards-of-communication-under-commission-delegated-regulation-eu-2018-389/>

<sup>16</sup> Refer to the application form for more details

The Guidelines are annexed to the present circular and available on the EBA website using the following link:

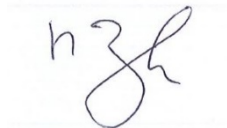
<https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-the-conditions-to-be-met-to-benefit-from-an-exemption-from-contingency-measures-under-article-33-6-of-regulation-eu-2018/389-rtS-on-sca-csc->

Yours faithfully,

COMMISSION de SURVEILLANCE du SECTEUR FINANCIER



Claude WAMPACH  
Director



Marco ZWICK  
Director



Jean-Pierre FABER  
Director



Françoise KAUTHEN  
Director



Claude MARX  
Director General

EBA/GL/2018/07

---

4 December 2018

---

# 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)

# 1. Compliance and reporting obligations

## Status of these guidelines

1. This document contains guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010<sup>1</sup>. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the guidelines.
2. Guidelines set out the EBA's view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom the guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where guidelines are directed primarily at institutions.

## Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA that they comply or intend to comply with these Guidelines, or give reasons for non-compliance, by ([dd.mm.yyyy]). In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website to [compliance@eba.europa.eu](mailto:compliance@eba.europa.eu) with the reference 'EBA/GL/2018/07'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to the EBA.
4. Notifications will be published on the EBA website, in line with Article 16(3) of Regulation No 1093/2010.

---

<sup>1</sup> Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, (OJ L 331, 15.12.2010, p.12).

## 2. Subject matter, scope and definitions

---

### Subject matter

These Guidelines specify the conditions, set out in Article 33(6) of Commission Delegated Regulation (EU) 2018/389<sup>2</sup> (the RTS), to exempt the account payment service providers that have opted for a dedicated interface from the obligation to set up the contingency mechanism described in Article 33(4) of the RTS.

These Guidelines further provide guidance on how competent authorities should consult the EBA for the purposes of the exemption in accordance with Article 33(6) of the RTS.

### Scope of application

These Guidelines apply in relation to the contingency **measures** for a dedicated interface set out in Article 33 of the RTS and, in particular, to the exemption from the obligation to set up a contingency mechanism in accordance with Article 33(4) of the RTS.

### Addressees

These Guidelines are addressed to competent authorities as defined in point (i) of Article 4(2) of Regulation (EU) 1093/2010 and to payment service providers as defined in Article 4(11) of Directive (EU) 2015/2366 (PSD2)<sup>3</sup>.

### Definitions

Unless otherwise specified, terms used and defined in PSD2 and the RTS have the same meaning in these Guidelines.

### Date of application

These Guidelines apply from 1 January 2019.

---

<sup>2</sup> 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, OJ L 69/23 (13.3.2018).

<sup>3</sup> 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 No 1093/2010, and repealing 2007/64/EC, OJ L 337/36 (23.12.2015).



### 3. Guidelines

---

## Guideline 1: Fulfilment of the conditions set out in Article 33(6) of Delegated Regulation (EU) 2018/389

- 1.1. Competent authorities should **assess** an account servicing payment service provider (ASPSP) as having fulfilled the four conditions set out in Article 33(6) of the RTS where the ASPSP is compliant with the requirements set out in Guidelines 2 to 8, subject to **compliance** with the requirements set out in PSD2 and the RTS.
- 1.2. ASPSPs should provide competent authorities with such information as is necessary to satisfy the competent authority that the requirements in Guidelines 2 to 8 are met.

## Guideline 2: Service level, availability and performance

- 2.1. The ASPSP should define key performance indicators (KPIs) and service level targets, including for problem resolution, out of hours support, monitoring, contingency plans and maintenance for its dedicated interface, that are at least as stringent as those for the interface(s) made available to its own payment service users (PSUs) for directly accessing their payment accounts online.
- 2.2. The ASPSP should define at a minimum, the following KPIs of the availability of the dedicated interface:
  - a. the uptime per day of all interfaces; and
  - b. the downtime per day of all interfaces.
- 2.3. In addition to the KPIs on availability in Guideline 2.2, the ASPSP should define, at a minimum, the following KPIs for the performance of the dedicated interface:
  - a. the daily average time (in milliseconds) taken, per request, for the ASPSP to provide the payment initiation service provider (PISP) with all the information requested in accordance with Article 66(4)(b) of PSD2 and Article 36(1)(b) of the RTS;
  - b. the daily average time (in milliseconds) taken, per request, for the ASPSP to provide the account information service provider (AISP) with all the information requested in accordance with Article 36(1)(a) of the RTS;
  - c. the daily average time (in milliseconds) taken, per request, for the ASPSP to provide the card-based payment instrument issuer (CBPII) or the PISP with a 'yes/no' confirmation in accordance with Article 65(3) of PSD2 and Article 36(1)(c) of the RTS;
  - d. the daily error response rate – calculated as the number of error messages concerning errors attributable to the ASPSP sent by the ASPSP to the PISPs, AISPs and CBPIIs in accordance with Article 36(2) of the RTS per day, divided by the number of requests received by the ASPSP from AISPs, PISPs and CBPIIs in the same day.
- 2.4. For the purpose of calculating the availability indicators set out in Guideline 2.2 for the dedicated interface, the ASPSP should:
  - a. calculate the percentage uptime as 100% minus the percentage downtime;

- b. calculate the percentage downtime using the total number of seconds the dedicated interface was down in a 24-hour period, starting and ending at midnight;
- c. count the interface as 'down' when five consecutive requests for access to information for the provision of payment initiation services, account information services or confirmation of availability of funds are not replied to within a total timeframe of 30 seconds, irrespective of whether these requests originate from one or multiple PISPs, AISPs or CBPIIs. In such a case, the ASPSP should calculate downtime from the moment it has received the first request in the series of five consecutive requests that were not replied to within 30 seconds, provided that there is no successful request in between those five requests to which a reply has been provided.

### Guideline 3: Publication of statistics

- 3.1 For the purpose of Article 32(4) of the RTS, the ASPSP should provide its competent authority with a plan for publication of daily statistics on a quarterly basis on the availability and performance of the dedicated interface as set out in Guidelines 2.2 and 2.3, and of each of the interfaces made available to its own PSUs for directly accessing their payment accounts online, together with information on where these statistics will be published and the date of first publication.
- 3.2 The publication referred to in Guideline 3.1 above should enable PISPs, AISPs, CBPIIs and PSUs to compare the availability and performance of the dedicated interface with the availability and performance of each of the interfaces made available by the ASPSP to its PSUs for directly accessing their payment accounts online on a daily basis.

### Guideline 4: Stress testing

- 4.1 For the purpose of the stress tests referred to in Article 32(2) of the RTS, the ASPSP should have in place processes to establish and assess how the dedicated interface performs when subjected to an extremely high number of requests from PISPs, AISPs and CBPIIs, in terms of the impact that such stresses have on the availability and performance of the dedicated interface and the defined service level targets.
- 4.2 The ASPSP should undertake adequate stress testing of the dedicated interface including but not limited to:
  - a. the capability to support access by multiple PISPs, AISPs and CBPIIs;
  - b. the capability to deal with an extremely high number of requests from PISPs, AISPs and CBPIIs, in a short period of time without failing;
  - c. the use of an extremely high number of concurrent sessions open at the same time for payment initiation, account information and confirmation on the availability of funds requests; and
  - d. requests for large volumes of data.

- 4.3 The ASPSP should provide the competent authority with a summary of the results of the stress tests, including the assumptions used as a basis for stress **testing** each of the elements in letters (a) to (d) of Guideline 4.2 above and how any issues identified have been addressed.

## Guideline 5: Obstacles

- 5.1 The ASPSP should provide the competent authority with:

- a. a summary of the method(s) of carrying out the authentication procedure(s) of the PSUs that are supported by the dedicated interface, i.e. redirection, decoupled, embedded or a combination thereof; and
- b. an explanation of the reasons why the method(s) of carrying out the authentication procedure(s) referred to in paragraph (a) is/are not an obstacle, as referred to in Article 32(3) of the RTS, and how such method(s) allow(s) PISPs and AISPs to **rely** on all the authentication **procedures** provided by the ASPSP to its PSUs, together with evidence that the dedicated interface does not give rise to unnecessary delay or friction in the experience available to the PSUs when accessing their account via a PISP, AISP or CBPII or to any other attributes, including unnecessary or superfluous steps or the use of unclear or discouraging language, that would directly or indirectly dissuade the PSUs from using the services of PISPs, AISPs and CBPIIs.

- 5.2 As part of the explanation referred to in letter (b) of Guideline 5.1, the ASPSP should provide the competent authority with a confirmation that:

- a. the dedicated interface does not prevent PISPs and AISPs from relying upon the authentication procedure(s) provided by the ASPSP to its PSUs;
- b. no additional authorisations or registrations are required from PISPs, AISPs or CBPIIs, other than those imposed in Articles 11, 14 and 15 of PSD2;
- c. there are no additional checks by the ASPSP on the consent, as referred to in Article 32(3) of the RTS, given by the PSU to the PISP or the AISP to access the information on the payment account(s) held with the ASPSP or to initiate payments; and
- d. no checks on the **consent** given by the PSU to the CBPII in accordance with letter (a) of Article 65(2) of PSD2 are performed.

## Guideline 6: Design and **testing** to the satisfaction of PSPs

- 6.1 For the purpose of evidencing **compliance** with the requirement in letter (b) of Article 33(6) of the RTS regarding the design of the dedicated interface, the ASPSP should provide the competent authority with:

- a. evidence that the dedicated interface meets the legal requirements for access and data in PSD2 and the RTS, including:
  - i. a description of the functional and technical specifications that the ASPSP has implemented; and

- ii. a summary of how the implementation of these specifications fulfils the requirements in PSD2 and the RTS; and
  - b. information on whether, and if so how, the ASPSP has engaged with PISPs, AISP and CBPIIs.
- 6.2 For the purpose of these Guidelines, a 'market initiative' means a group of stakeholders that have developed functional and technical specifications for dedicated interfaces and, in doing so, have obtained input from PISPs, AISP and CBPIIs.
- 6.3 Where the ASPSP is implementing a standard developed by a market initiative:
  - a. the information referred to in point (i) of letter (a) of Guideline 6.1 may consist of information regarding which market initiative standard the ASPSP is implementing, whether or not it has deviated in any specific aspect from such standard, and if so, how it has deviated and how it meets the requirements in PSD2 and the RTS;
  - b. the information referred to in point (ii) of letter (a) of Guideline 6.1 may include, where available, the results of the conformance testing developed by the market initiative, attesting compliance of the interface with the respective market initiative standard.
- 6.4 For the purpose of the requirement in letter (b) of Article 33(6) of the RTS regarding the testing of the dedicated interface, the ASPSP should make the technical specifications of the dedicated interface available to authorised PISPs, AISP and CBPIIs or payment service providers that have applied to their competent authorities for the relevant authorisation in accordance with Article 30(3) of the RTS including, at a minimum, publishing a summary of the specification of the dedicated interface on its website in accordance with the third sub-paragraph of Article 30(3) of the RTS.
- 6.5 The testing facility should allow ASPSPs, authorised PISPs, AISP and CBPIIs or payment service providers that have applied to their competent authorities for the relevant authorization to test the dedicated interface in a secure, dedicated testing environment with non-real PSU data, for the following:
  - a. a stable and secure connection;
  - b. the ability of ASPSPs and authorised PISPs, AISP and CBPIIs to exchange the relevant certificates in accordance with Article 34 of the RTS;
  - c. the ability to send and receive error messages in accordance with Article 36(2) of the RTS;
  - d. the ability of PISPs to send, and of ASPSPs to receive, payment initiation orders and the ability of ASPSPs to provide the information requested in accordance with letter (b) of Article 66(4) of PSD2 and letter (b) of Article 36(1) of the RTS;
  - e. the ability of AISP to send, and of ASPSPs to receive, requests for access to payment account data, and the ability of ASPSPs to provide the information requested in accordance with letter (a) of Article 36(1) of the RTS;

- f. the ability of CBPIIs and PISPs to send, and of ASPSPs to receive, requests from CBPIIs and PISPs and the ability of the ASPSP to send a 'yes/no' confirmation to CBPIIs and PISPs in accordance with letter (c) of Article 36(1) of the RTS; and
  - g. the ability of PISPs and AISPs to **rely** on all the authentication **procedures** provided by the ASPSP to its PSUs.
- 6.6 The ASPSP should provide the competent authority with a summary of the results of the **testing** referred to in Article 30(5) of the RTS for each of the elements to be tested in accordance with letters (a) to (g) of paragraph 6.5 above, including the number of PISPs, AISPs and CBPIIs that have used the **testing** facility, the feedback received by the ASPSP from these PISPs, AISPs and CBPIIs, the issues identified and a description of how these issues have been addressed.
- 6.7 For the purpose of assessing whether the ASPSP meets the requirements in letter (b) of Article 33(6) of the RTS, the competent authority may also take into account any problems reported to it by PISPs, AISPs and CBPIIs in relation to Guideline 6.5 above.

## Guideline 7: Wide usage of the interface

- 7.1 For the purposes of evidencing **compliance** with the requirement in letter (c) of Article 33(6) of the RTS, the ASPSP should provide the competent authority with:
  - a. a description of the usage of the dedicated interface for the period referred to in letter (c) of Article 33(6), including but not limited to:
    - 1. the number of PISPs, AISPs and CBPIIs that have used the interface to provide services to customers; and
    - 2. the number of requests sent by those PISPs, AISPs and CBPIIs to the ASPSP via the dedicated interface that have been replied to by the ASPSP.
  - b. evidence that the ASPSP has made all reasonable efforts to ensure wide usage of the dedicated interface, including by communicating its availability via appropriate channels, including, where relevant, the website of the ASPSP, social media, industry trade bodies, conferences and direct engagement with known market actors.
- 7.2 In addition to the evidence referred to in Guideline 7.1, the competent authority should take into account the information received in the context of Guidelines 6 and 8 when assessing whether or not the ASPSP meets the requirement in Article 33(6)(c) of the RTS.
- 7.3 The 3-month period referred to in letter (c) of Article 33(6) of the RTS may run concurrently with the **testing** referred to in Article 30(5) of the RTS.

## Guideline 8: Resolution of problems

- 8.1 For the purpose of Article 32(1) and letter (d) of Article 33(6) of the RTS, the ASPSP should provide the competent authority with:
  - a. information on the systems or **procedures** in place for tracking, resolving and closing problems, particularly those reported by PISPs, AISPs and CBPIIs; and

- b. an explanation of the problems, particularly those reported by PISPs, AISPs and CBPIIs, that have not been resolved in accordance with the service level targets set out in Guideline 2.1.

## Guideline 9: Consultation with the EBA

- 9.1 When consulting the EBA in accordance with Article 33(6) of the RTS, competent authorities should submit to the EBA the Assessment Form set out in Annex 1 in relation to each request for an exemption that they intend to grant. Competent authorities should not take any decision in relation to the exemption until the earlier of receiving the EBA's comments on the request or one month from the date that the competent authority consulted the EBA. Competent authorities should take due account of the EBA's comments when taking any decision on the request.
- 9.2 In derogation from Guideline 9.1, until 31 December 2019, competent authorities that have notified the EBA that they comply with these Guidelines can proceed to grant an exemption provided that they have consulted the EBA by informing it of their intention to grant the exemption using the Assessment Form set out in Annex 1. In such a case, the competent authorities may submit the Assessment Form covering one or more ASPSPs.
- 9.3 Competent authorities that have refused to exempt an ASPSP from the obligation to set up the contingency mechanism referred to in Article 33(4) of the RTS because its dedicated interface does not comply with the conditions set out in Article 33(6) of the RTS and with the requirements of Guidelines 2 to 8 should submit to the EBA the Assessment Form in Annex 1 without undue delay. The negative assessment should be provided for all denied requests to grant an exemption in accordance with Article 33(6) of the RTS.
- 9.4 Where an ASPSP is part of a group with subsidiaries in different Member States that will use the same dedicated interface, each of the competent authorities of those Member States should:
  - a. inform the other relevant competent authorities without undue delay if it intends to refuse to grant an exemption; and
  - b. on request from the other competent authorities and without prejudice to any confidentiality obligations, inform the other competent authorities of its reasoning why it intends to refuse to grant an exemption and, where relevant, of the issues reported by PISPs, AISPs and CBPIIs to the competent authority.

# Annex 1 - Assessment Form

---

## Assessment Submission

1)	Member State	
2)	Name of the competent authority in the Member State	
3)	Where the ASPSP is part of a group with subsidiaries in different Member States that will use the same dedicated interface	Confirmation that the competent authority has complied with Guideline 9.4 <input type="checkbox"/> Yes <input type="checkbox"/> No
4)	Contact person within the competent authority	
5)	Date of submission to the EBA	DD/MM/YY
6)	Name(s) of the ASPSP(s) and its/their unique identification number, as shown in the relevant national register for credit institutions, payment institutions and e-money institutions	
7)	Type(s) of ASPSP(s)	<input type="checkbox"/> Credit Institution <input type="checkbox"/> Payment Institution <input type="checkbox"/> E-Money Institution
8)	Decision of the competent authority	<input type="checkbox"/> Grant an exemption <input type="checkbox"/> Refuse to grant an exemption
9)	If applicable, rationale for the refusal to grant an exemption	