


POSITION PAPER



Draft EBA Guidelines on the conditions to be met to benefit from an exemption from contingency measures

ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

Transparency Register ID 8765978796-80

August 2018



ESBG Position Paper on Draft EBA 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)

Introduction

ESBG welcomes the opportunity to review and comment on these draft Guidelines, and moreover, ESBG welcomes the EBA's recent efforts, in the form of these draft Guidelines and their recent Opinion, with the aim to provide clarity on the implementation of certain aspects of the RTS on SCA and CSC. ESBG believes that a harmonised approach across National Competent Authorities is key when assessing banks whether conditions are met to be exempted from having to provide contingency measures.

ESBG generally agrees with the Guidelines as proposed and agrees with EBA's efforts to provide further guidance and clarity in respect of the service level, availability and performance of the interface that the ASPSP needs to have in place, the publication of the performance indicators, the stress testing to be carried out, obstacles to accessing payment accounts, the design and testing of the interfaces to the satisfaction of payment services providers, the wide usage of the interface, the resolution of problems, and the consultation by CAs with the EBA. Please find our input to the consultation herewith.

Q1: Do you agree with the EBA's assessments on KPIs and the calculation of uptime and downtime and the ASPSP submission of a plan to publishing statistics, the options that EBA considered and progressed or discarded, and the requirements proposed in Guideline 2 and 3? If not, please provide detail on other KPIs or calculation methods that you consider more suitable and your reasoning for doing so.

ESBG welcomes the opportunity to review and comment on these draft Guidelines, and welcomes EBA's efforts to provide clarity on the implementation of certain aspects of the RTS on SCA and CSC. ESBG believes that a harmonised approach across National Competent Authorities is key when assessing banks whether conditions are met to be exempted from having to provide contingency measures.

GL 2.1 states that among other requirements, ASPSPs should have in place the same "out of hours support" it has in place of the interface used by its own PSUs. However, ESBG would like to remind the EBA that articles 30(5) and 32(1) of the RTS only mention "support" as a general term. Therefore, extending support to out of hours support seems to be exceeding the content provided by the RTS. This does not mean that ASPSPs are not willing to provide out of hours support, but exemption should be based in conditions as set out in the RTS. Moreover, the out of hours support necessary for a payment initiation, AIS activity without a PSU present at the time or AIS activity with a PSU directly accessing its account information is not comparable. Therefore, we suggest sticking to the RTS and leaving the term in GL 2.1 as "support".

With respect to Guideline (GL) 2.3, as ASPSPs can only be held responsible for components within their control, ESBG prefers that it is explicitly stated that only the time spent in the ASPSP environment, so only after successful reception of a request, is taken into account for the performance indicators. Time spent at components that are outside the control of ASPSPs (for example, but not limited to, the transit level, the Internet Service Providers (ISPs) involved) cannot be measured by ASPSPs and hence should not be taken into account.



In relation to GL 2.4(b), EBA recalls the conditions required for considering the dedicated interface is “down”, say “when 5 consecutive requests for access to information for the provision of PIS or AIS are not replied to within 30 seconds”. However, ESGB would like to remind the EBA that article 33(1) of the RTS only relates these conditions to cases of “unplanned unavailability or a systems breakdown”. Therefore, the proposed EBA Guidelines would not be fully in line with the RTS, as the Guidelines relate the conditions to not only unplanned down-time, but also to planned down-time. In addition to that, it would be useful if the EBA specifies what it is to be understood by “planned down-time”, as currently the scope of the concept could seem to be too wide. Also, this KPI of the availability of the API would only be applicable for PIS and for AIS when the PSU is present. ESGB believes that circumstances that lead to the conclusion that there is a down-time should be further defined; taking only circumstances that are within the control of ASPSPs are taken into account. Moreover, planned down-times should not be considered in 2.4.b and c.

ESBG would also like to remind that the mere fact that, if in a specific case, the number of seconds exceeds the maximum level of seconds set, this does not have to imply at all that the API is down. Excessive numbers of data requests can for example cause longer response times. This might require monitoring external parties that, on purpose, submit an excessive number of API calls. If the latter is the case, this should be included in the unplanned downtime parameters in GLs 2.2.c and 2.4.b as these are beyond the control of ASPSPs.

ESBG would also like to remark that requests cannot be compared like-for-like as request can differ in terms of number of products, accounts consulted, number of transactions initiated, and moreover different channels can be used for such requests. As different channels may have different service levels, the API performance should only be compared to the PSU interface in the same channel. The Bank should monitor availability and performance of the API according to that interface that is most comparable in functionality to the API. It makes no sense to compare e.g. the API against a mobile banking application with reduced functionality (assuming that the performance will always be better than an API with much more features). For example, a single PSU request cannot easily be compared with a complex AIS request, and both requests are not necessarily supported (or comparable) via all channels. The only possible comparison would be between how much time a payment transfer takes on the ASPSP website versus how long it takes via the PISP, or between how long it takes to the PSU to obtain the account information through the ASPSP website versus via the AISP.

In terms of the comparability of the availability of different interfaces, as set in 3.1(b), ESGB considers that the KPIs measuring the availability should be different among channels, as each have different technical features that require different measurements. For example, AQMetrix¹ currently provides a comparison of the interfaces of diverse channels, and uses different metrics on each one. With respect to GL 3.1.a, publication of the daily indicators might serve the purpose of criminals that engage in Distributed Denial of Service (DDoS) attacks, or script kiddies, that want to measure their successes and who might even want to compete to hit ‘higher rankings’. ESGB believes that ASPSPs should have the possibility to protect themselves against such attacks properly and that these risks should be limited. A mitigating measure could be to limit these indicators to quarterly ones. This would also limit the reporting burden for ASPSPs and would be more proportional to the required goals. In addition, publishing the KPIs on the ASPSP website is questionable itself and should not happen. The reason for monitoring the KPIs is that the API should not discriminate TPPs. Hence, it would be sufficient to share the detailed information with the NCA. For competitive reasons these data should not be published.

¹ AQmetrix provides Performance and Functionality benchmarks for more than 200 companies; see <https://www.aqmetrix.com/> for more information.

On GL 3.1.b, ESBG is wondering how the “best-performing” interface is determined. One PSU interface may have a high throughput but a high latency, whilst another PSU interface may show the opposite. Which of the two is then considered “best-performing”?

Q2: Do you agree with the EBA’s assessments on stress testing and the options it considered and progressed or discarded, and the requirements proposed in Guideline 4? If not, please provide your reasoning.

ESBG’s reading of Article 32(2) of the RTS is that the dedicated interfaces should indeed be stress-tested, but that the article does not state that this include an assessment against an extremely high number of requests from PISPs and AISPs.

As ESBG believes that this stress-testing is part of the Competent Authority’s (CA) assessment on whether to grant an exemption to ASPSPs from having to provide a fall-back option, ESBG believes that it would assist both CAs and ASPSPs if specific requirements were provided for the execution of these stress-tests. In light of this, it is ESBG’s reading that stress testing is a one-off exercise in the exemption process, only to be repeated by the ASPSP when the exemption have been revoked and a new exemption is asked for.

Terms as “extremely high number of requests”, “unusually high number of requests”, “extremely high number of concurrent sessions” and “large volumes of data” are not defined at all and as such could give rise to subjective interpretations hence further guidance is expected. Also, a “extremely high number of requests” could, under normal circumstances, be an indicator for a DDoS attack, or an indicator to attempt fraud via a brute force attack, implying that catering for such “extremely high number of requests” might hamper ASPSP’s abilities to detect such anomalies. Therefore, ESBG suggests that either the EBA or the NCAs set the detailed scenarios under which stress tests need to be carried out and that will be part of the application for an exemption.

Q3: Do you agree with the EBA’s assessments on monitoring? If not, please provide your reasoning.

ESBG agrees with EBA’s assessment. ASPSPs are the only entities best positioned to monitor performance on their systems after a request has been successfully received and that monitoring should be limited to just that. Monitoring by external parties would only create unnecessary additional load on the ASPSP systems.

Q4: Do you agree with the EBA’s assessments on obstacles, the options it considered and progressed or discarded, and the requirements proposed in Guideline 5? If not, please provide your reasoning.

ESBG agrees with the EBA’s assessments, however, clarification is required with respect to “consent” as used in GL 5.2.c – is this the consent as mentioned in Article 67(2)(a) of PSD2? If not, ESBG believes that in the case of CBPPII, the consent is established between the PSU and his ASPSP and hence is managed within the environment of the ASPSP, whilst for the other use cases ASPSPs need to assess the validity of a consent established at another PSP.

ESBG also would like to stress out that actions taken by or on behalf of the PSU cannot be regarded as obstacles. For example, a PSU could desire set certain spending limits for payment transactions executed through specific payment instruments (as per requirement 9.4 of the Guidelines on security measures for operational and security risk under PSD2) or a PSU could desire to disable specific payment functionalities (as per requirement 9.3 of the Guidelines on security measures for operational



and security risk under PSD2). These examples contain actions by PSUs that are justified and as such cannot be considered as obstacles as meant in this legal framework (PSD2, RTS, GL).

Q5: Do you agree with the EBA's assessments for design and testing, the options it considered and progressed or discarded, and the requirements proposed Guideline 6? If not, please provide your reasoning.

ESBG agrees that only a summary of the specification should be published as per GL 6.1.a.

With respect to the certificates mentioned in GL 6.2.b, clarification on the ability to exchange certificates may be required; i.e. if these are test certificates the ability to verify the true identity behind the certificate may be complicated. Is the purpose of the exchange a technical testing requirement or connected to an onboarding process or both? Complicating matters is that Article 34 of the RTS mentions that “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 or for website authentication as referred to in Article 3(39) of that Regulation” whilst GL 6.2.b. speaks about “qualified certificates for electronic seals and qualified web authentication certificates”. If an ASPSP decides to support only one option in the production environment, ESBG believes it should not be a requirement to support both in the test environment. If the scope is limited to functional testing only, does EBA consider it a problem that potentially anyone could pose as a registered TPP if identity validation is not performed?

ESBG is of the opinion that the requirement to make changes available in the test environment before launching in production limits the ability for ASPSPs to innovate and to launch new competitive products and services if indeed EBA's intention is that such innovative launches should be shared with the TPP community first before these can be launched to the public. In the latter interpretation, innovations by ASPSPs are at risk because there are no agreements between ASPSPs and TPPs, and hence no Non-Disclosure Agreements (NDA) – it is understood that this interpretation severely disrupts the level playing field, limits the ability to innovate for ASPSPs and puts possible intellectual property at risk. Measures to avoid such are hence required.

In addition, ESBG believes that EBA should more clearly define that testing is performed on a dedicated test environment for which service levels differ from production. For testing, the focus of the PSP satisfaction has to be on “functionality” and not on performance.

With respect to GL 6.3, ESBG observes that there is a requirement for ASPSPs to provide test results of tests by third parties to the CA, whilst there is no similar obligation for AISP, PISP and CBPIIs to disclose such data. ESBG therefore cannot see how this can be input in the exemption granting process, as parts are not under the control of the ASPSP. For example, how can a claim that the “interface is not working” be assessed as being an ASPSP failure and not a TPP failure?

With respect to GL 6.4, it is recommended to include a definition of “market initiative standard”.

Q6: Do you agree with the EBA's assessment for 'widely used', the options it considered and discarded, and the requirements proposed Guideline 7? If not, please provide your reasoning.

It is not clear at what point in time the information as required in GL 7.1 has to be provided to the CA, nor whether this is a one-off or repetitive requirement. By default, at launch the numbers will start at zero and will ramp up over time, and whilst reporting on PISPs, AISPs and CBPIIs is required markets across the EU can differ significantly in terms of appetite for these TPPs. For example, it could very well be that in Member States where consumers tend to have only single bank relationships,

there is no viable business case for AISPs to enter that market. Alternatively, there may evolve less CBPIIs than PISPs. How will CAs ensure harmonisation and a level playing field across Member States with such possible differences, what levels of TPPs will be deemed acceptable?

GL 7.2 implies that there are conditions of “widely used” in GL 7.1, however the term “widely used” is not defined in GL 7.1. It merely states that the ASPSP should provide a summary of the availability of the technical specifications and testing facility to the market, including some statistics on the usage of the testing facility and the interface. Interpretations of the term can become subjective, leading to fragmentation across the EU, and actors may be able to interpret the term to their benefit. In summary, it is unclear what the definition of “widely used” is and what is needed in order to fulfil GL 7 as a whole.

Also, ESBG shares the EBA’s view on Recital 57 of the Guidelines, that states that credit institutions that are also undertaking payment initiation, account information and card based payment instrument issuing should be included in the assessment of ‘widely used’. However, ESBG considers that this issue has not been properly adopted by Guidelines 7.1, and ESBG therefore suggests including those credit institutions that EBA mentions on Recital 57, on Guideline 7.1.

“Guideline 7: Wide usage of the interface

7.1 The ASPSP should provide to the competent authority a summary as to the availability of the technical specification and testing facility to the market and should have taken all necessary steps for the interface to be operationally used. The information should include, but is not limited to

a. the total number of PISPs, CBPIIs, AISPs that have or have applied for the relevant authorisation, including credit institutions that are also undertaking payment initiation, account information and card based payment instrument issuing, that have made use of the testing facility; and

b. the number of AISPs, PISPs and CBPIIs using the interface.”

With respect to GL 7.2, ESBG would also like to limit the publication of the actual summaries of the specifications on the website only, whilst the other channels mentioned are examples for possible pointers to these summaries on the ASPSP website.

On GL 7.3, it is ESBG’s reading of the RTS that the three-month period is actually part of the six-month period which implies that ASPSPs should already engage with a large number of TPPs (to prove “widely used”) three months before market launch, which is challenging.

Q7: Do you agree with the EBAs assessment to use the service level targets and statistical data for the assessment of resolving problems without undue delay, the options it discarded, and the requirements proposed Guideline 8? If not, please provide your reasoning.

ESBG reads GL 8 in such a way that documentation required under GL 8.1.a are related to service level agreements related to the production environment, and that should be part of an ASPSP application for an exemption, whilst document requests under GL 8.1.b are related to issues that arise from testing, and that are only required by the CA under specific circumstances. To that end, a clarification of the meaning of “without undue delay” is required.

Q8: Do you agree with the proposed Guideline 9 and the information submitted to the EBA in the Assessment Form in the Annex? If not, please provide your reasoning.



ESBG believes that the one month waiting period as mentioned in GL 9.1 should only apply to the initial assessment of a request from an ASPSP for a specific API – subsequent fixes or resubmissions by the same ASPSP for the same interface should be handled expedient with priority over new submission, in order not to jeopardise timelines for that ASPSP. For the sake of speed and efficiency, ESBG also believes that ASPSPs with centralised operations but servicing multiple jurisdictions should only apply for an exemption once at the CA in the ASPSP Home Member State instead of having to apply at the CAs in all ASPSP Host Member States as well. Further, ESBG is of the opinion that it should be clarified that exemption process can be invoked separately for different interfaces serving different clients, such as retail versus corporate customers, as these may reside in different system and have different timelines as well as complexity on availability.

Q9: Do you have any particular concerns regarding the envisaged timelines for ASPSPs to meet the requirements set out in these Guidelines prior to the September 2019 deadline, including providing the technical specifications and testing facilities in advance of the March 2019 deadline?

The ESBG Membership is eager to apply for exemptions as soon as possible so wishes to start testing the sooner rather the later. To that end, ESBG acknowledges the timelines as envisioned by the EBA. However, ESBG also observes that the timelines are very challenging – with a planned publication date of January 2019 whilst ASPSPs need to publish specifications at around the same time, and whilst testing needs to start in March 2019 is pulling it short. Besides, a significant number of requests for exemptions can be expected which may put pressure on the CAs and the EBA. If response times take too long, in case of a rejection of the application, ASPSPs may be forced to develop fallback interfaces in an unrealistic short timeframe.

Q10: Do you agree with the level of detail set out in the draft Guidelines as proposed in this Consultation Paper or would you have expected either more or less detailed requirements on a particular aspect? Please provide your reasoning.

As per the input provided to the previous questions, ESBG believes that at some points further clarity is required, and that there is still some risk for subjective interpretations, which can lead to fragmentation across Member States.



About ESBG (European Savings and Retail Banking Group)

ESBG represents the locally focused European banking sector, helping savings and retail banks in 20 European countries strengthen their unique approach that focuses on providing service to local communities and boosting SMEs. An advocate for a proportionate approach to banking rules, ESBG unites at EU level some 1,000 banks, which together employ 780,000 people driven to innovate at 56,000 outlets. ESBG members have total assets of €6.2 trillion, provide €500 billion in SME loans, and serve 150 million Europeans seeking retail banking services. ESBG members are committed to further unleash the promise of sustainable, responsible 21st century banking.



European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ■ B-1000 Brussels ■ Tel: +32 2 211 11 11 ■ Fax : +32 2 211 11 99
info@wsbi-esbg.org ■ www.wsbi-esbg.org

Published by ESBG, August 2018