Single Rulebook Q&A

Question ID	2019_5054
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	97
Paragraph	-
Subparagraph	-
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication
Article/Paragraph	33
Date of submission	19/12/2019
Published as Final Q&A	23/04/2021
Disclose name of institution / entity	No
Type of submitter	Other
Subject matter	Contingency Measures under Article 33
Question	Does fallback access to a secondary instance of the dedicated interface in a different data center with dedicated resources, provide an acceptable strategy and plan for the contingency mechanism?
Background on the question	The RTS on strong customer authentication and secure communication under PSD2 requires Account Servicing Payment Service Providers (ASPSPs) to include, in the design of the dedicated interface a strategy and plans for

	contingency measures for the event the interface does not perform in compliance with Article 32, that there is unplanned unavailability of the interface and that there is a systems breakdown.
EBA answer	Article 31 of the Commission Delegated Regulation (EU) 2018/389, states that account servicing payment service providers (ASPSPs) shall 'establish the interface(s) referred to in Article 30 by means of a dedicated interface or by allowing the use by the payment service providers referred to in Article 30(1) of the interfaces used for authentication and communication with the account servicing payment service provider's payment services users.' Article 33(4) of the Delegated Regulation requires ASPSPs to set up a contingency mechanism and specifies that "as part of a contingency mechanism, payment service providers referred to in Article 30(1) shall be allowed to make use of the interfaces made available to the payment service users for the authentication and communication with their account servicing payment service provider, until the dedicated interface is restored to the level of availability and performance provided for in Article 32." Article 33(6) of the Delegated Regulation allows for ASPSPs to be exempted from the obligation to set-up the contingency mechanism if certain conditions are met. Provided that an ASPSP has not received such an exemption, they are required to set-up a contingency mechanism. As detailed in Article 33(4) of the Delegated Regulation, as part of the contingency mechanism third party providers shall be allowed to make use of the interface(s) made available to the payment service users for the authentication and communication with their ASPSPs. A secondary dedicated interface, available only to payment service providers, would not fulfill that requirement. Further, it should be noted that, in accordance with Article 33(5) of the Delegated Regulation, access to the interface made available to the payment service users for the authentication and communication with their ASPSPs, as part of the contingency mechanism, requires ASPSPs to ensure the payment service providers can be identified, avoiding the risk of unidentified access through the customer interface.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2019_5054