Single Rulebook Q&A

Question ID	2018_4375
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	98
Paragraph	4
Subparagraph	-
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication
Article/Paragraph	Article 34 / Paragraphs 1-4
Date of submission	19/11/2018
Published as Final Q&A	24/05/2019
Disclose name of institution / entity	Yes
Name of institution / submitter	MASTERCARD
Country of incorporation / residence	Belgium
Type of submitter	Credit institution
Subject matter	Certfication in relation to a Technical Service Provider (TSP)
Question	When performing the role of a Technical Service Provider (TSP) is the TSP required to update the certificate received from the Third Party Payment Service Providers (TPP) (to demonstrate our involvement) to enable the Account Servicing Payment Service Provider (ASPSP) to authorise the certificate and provide the appropriate requested data back through to the TPP and establish the session? Is this same certificate required for every type of transaction request and must it be real time checked by the ASPSP and how does this impact our role as a TSP? Also, by introducing a TSP between a TPP and an ASPSP is the concept of private keys and the transport layer broken, due to the introduction of a TSP between the TPP and the ASPSP?

	Finally, are there limits to the number of roles involved in the chain in terms of the certification or do we just need to be able to demonstrate the link back to the point of origin for the certificate (the TPP)?
Background on the question	We are launching a connectivity hub product, and as part of this we will be acting as a TSP on behalf of the TPP. We will need to be able to identify ourselves to the ASPSP and be able to demonstrate that we have the appropriate credentials and consent from the TPP.As part of the product we will be working with connectivity partners, who will make contact with the ASPSP. Whilst it's a white labelled product there will be two extra parties involved in the chain. We as the overall TSP and its partners who will receive the API request from Company X, and route with the consent to the appropriate ASPSP. Data returned from the ASPSP will be returned to the partner, then through Company X, transformed and returned to the TPP.We seek clarification on how to manage certificates across the various legs, and what steps are needed regarding authentication and consent to engage with a TPP and act on their behalf with an ASPSP.
Final answer	Article 34 of the Commission Delegated Regulation (EU) 2018/389 specifies that for the purpose of identification, as referred to in Article 30(1)(a), payment service providers (PSPs) 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. Paragraph 20 of the EBA Opinion on the use of eIDAS certificates (EBA-Op-2018-7) specifies that in the specific cases where PSPs have outsourced to technical service providers (TSPs) some of the activities related to access to the online accounts held within an account servicing payment service provider (ASPSP), competent authorities should encourage these PSPs to consider using multiple certificates simultaneously: one per TSP. This means that TSPs may present the eIDAS certificate on behalf of the PSP for the purpose of identification as required in Article 34 of the Delegated Regulation. A TSP may operate for more than one third party provider (TPP) and a TPP may use more than one TSP, including in the outsourcing chain, as long as the requirements for identification and secure communication under Articles 34-36 of the Delegated Regulation are met. In the case where a TSP is communicating with the ASPSP on behalf of the TPP, said TSP shall present the eIDAS certificate of the TPP. In addition, and as stated in paragraph 21 of the EBA Opinion, ASPSPs should be in a position to unequivocally identify the principal PSP in the presented certificate. In relation to the above, Q&A 2019_4507 further clarifies that eIDAS

	certificates should be issued to authorised/registered PSPs, that the name of the TSP may be included in the certificate if technically feasible, but that this is not legally mandatory, and that ASPSPs are required to identify the principle PSP only. With regard to the question whether the same certificate is required for every type of transaction request, Article 34(3)(a) of the Delegated Regulation specifies the roles of the PSPs that should be included in the eIDAS certificate for PSD2 purposes. Paragraph 19 of the EBA Opinion clarifies that Article 34(3) of the Delegated Regulation does not specify whether PSPs should hold single or multiple eIDAS certificates for the same role that they want to accommodate and that it is for the respective PSP to decide whether to use single or multiple certificates for each role. However, it should be noted that the Delegated Regulation does not specify the types of transaction requests. The use of a TSP is intended to facilitate the identification between the TPP and the ASPSP and does not affect the process of secure communication between the latter two parties. In that regard, it is the TPP (rather than the TSP(s)) who remains responsible for complying with the requirement on secure communication under Article 35 of the Delegated Regulation.
Link	https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4375

European Banking Authority, 25/03/2023
www.eba.europa.eu