EBA-Op-2018-7

10 December 2018

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

Introduction and legal basis

1. The competence of the European Banking Authority (EBA) to deliver this opinion is based on Article 29(1)(a) of Regulation (EU) No 1093/2010[1] as part of the objective of the EBA 'to play an active role in building a common Union supervisory culture and consistent supervisory practices, as well as in ensuring uniform procedures and consistent approaches throughout the Union".

2. In order to support the objectives of Directive (EU) 2015/2366[2] (the revised Payment Services Directive, or PSD2) of enhancing competition, facilitating innovation, protecting consumers, increasing security and contributing to a single EU market in retail payments, the Directive conferred on the EBA the development of 12 technical standards and guidelines.

3. The regulatory technical standards (RTS) on strong customer authentication and common and secure communication underpin the new security requirements under PSD2 and regulate the access by account information service providers (AISPs), payment initiation service providers (PISPs) and card-based payment instrument issuers (CBPIIs) to payment service user (PSU) payment account data held with their account servicing payment service providers (ASPSPs). The RTS were published in the Official Journal on 13 March 2018 as a Commission Delegated Regulation (EU) 2018/389[3] and will apply from 14 September 2019.

4. Article 34(1) of the RTS, specifies 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

[1] 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] 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, OJ L 337/35, 23.12.2015.

[3] 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.

referred to in Article 3(30) of Regulation (EU) No 910/2014[4] (eIDAS Regulation) or for website authentication as referred to in Article 3(39) of that Regulation'.

5. In order to fulfil its statutory objective of contributing to supervisory convergence in the EU/EEA, and to do so in the specific context of these RTS, the EBA has decided to issue an opinion to clarify specific aspects of the use of qualified certificates for electronic seals (QSealCs) and qualified certificates for website authentication (QWACs) under the RTS.

6. The opinion is addressed to competent authorities (CAs) but, given the supervisory expectations it conveys, should also prove useful for payment service providers (PSPs), technical service providers, and industry initiatives, such as the API (application programming interface) initiatives, to allow the identification of AISPs, PISPs and CBPIIs towards the ASPSPs, as well as the establishment of a secure communication between PSPs.

7. In accordance with Article 14(5) of the Rules of Procedure of the Board of Supervisors[5], the Board of Supervisors has adopted this opinion.

Use of eIDAS certificates for PSD2 purposes

8. Based on feedback from the industry, the EBA has identified the following specific areas that require clarification: (i) the use of QSealCs or QWACs, including which PSPs should choose the type of certificate to be used, and (ii) the use of single and multiple eIDAS certificates.

Use of QSealCs or QWACs

9. Article 34(1) of the RTS specifies 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'. This means that the RTS permits the use of either a QSealC or a QWAC.

10. In addition, Article 35(1) of the RTS prescribes that 'account servicing payment service providers, payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers shall ensure that, when exchanging data by means of the internet, secure encryption is applied between the communicating parties throughout the respective communication session in order to safeguard the confidentiality and the integrity of the data, using strong and widely recognised encryption techniques'.

11. QSealCs make it possible for the owner of the certificate to create electronic seals on any data that ensure the integrity and correctness of the origin (i.e. authenticity) of the signed/sealed data. This means that the persons receiving digitally signed data can be sure who signed the data, that the data have not been changed since being signed, and that they can also present

[4] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 28.8.2014, OJ L 257/73.

[5] Decision adopting the Rules of Procedure of the European Banking Authority Board of Supervisors of 27 November 2014 (EBA/DC/2011/01 Rev4).

these signed data to third parties as evidence of who signed the data and that they were not changed after being signed. This is in line with the provisions of Article 35(2) of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). Therefore, the electronic seal provides strong evidence that the data submitted are originated by the PSP identified in the certificate.

12. QSealCs are used to protect the data or messages in the application layer during or after the communication, but they do not provide confidentiality of the data (i.e. there is no encryption of application data).

13. QWACs make it possible to establish a channel for communication with the subject of the certificate using the Transport Layer Security (TLS) protocol, which guarantees confidentiality, integrity and authenticity of all data transferred through the channel (in the transport layer). This means that the person or system connecting to the website presenting the certificate can be sure who "owns" the end point of the communication channel (the owner of the certificate), that the data was not changed between the end points, and that nobody else could have read the data along the way. However, the data communicated by the QWAC are only protected only while they are travelling through a channel that uses TLS protocol. Therefore, the person or system connecting to the website can be sure who they are communicating with, but cannot prove this to third parties, which means that QWACs do not give legally assumed evidence of a transaction.

14. Taking into account the legal requirements of Article 34(1) and Article 35(1) of the RTS and the specificities of QSealCs and QWACs, the EBA has identified three possible alternatives for the use of QWACs and QSealCs by AISPs, PISPs and CBPIIs.

    a) *Parallel use of QWACs and QSealCs* – this will allow AISPs, PISPs and CBPIIs to identify themselves towards the ASPSPs and, at the same time, ensure that the communication is secure and that the data submitted originates from the PSP identified in the certificate.

    b) *Use of QWACs only* – this will allow AISPs, PISPs and CBPIIs to communicate securely with and identify themselves towards the ASPSP, but cannot provide evidence that the data submitted originates from the PSP identified in the certificate.

    c) *Use of QSealCs with an additional element that ensures secure communication* – QSealCs will allow AISPs, PISPs and CBPIIs to identify themselves towards the ASPSPs, but cannot ensure confidentiality during the communication session. Therefore, an additional element that ensures secure communication should be used in order to comply with the requirements of Article 35(1) of the RTS.

15. Although ASPSPs can choose any of the above three options, to ensure that (i) AISPs, PISPs and CBPIIs are able to identify themselves towards ASPSPs, (ii) AISPs, PISPs, CBPIIs and ASPSPs apply secure encryption throughout each communication session in order to safeguard the confidentiality and the integrity of the data and (iii) data provided are originated by the PSP identified in the certificate, the EBA recommends CAs to encourage ASPSPs to use both QWACs and QSealCs in parallel. However, the EBA reiterates that for establishing a secure

communication session under Article 35 of the RTS, the use of eIDAS certificates is not mandatory.

16. With regard to the question of which PSP should decide what type of eIDAS certificate to be used, Article 34(1) of the RTS does not explicitly specify which PSP should make the decision. Nevertheless, taking into account the provisions of the RTS, the EBA hereby clarifies that, since the ASPSP is the party that should provide the interface and ensure the security of the communication session, it should be the party that chooses the type of certificate to use under Article 34(1) of the RTS.

17. In addition, Article 30(1)(a) of the RTS provides that ASPSPs have an obligation to have in place at least one interface which meets the requirement that 'AISPs, PISPs and CBPIIs are able to identify themselves towards the ASPSP'. The EBA hereby clarifies that this identification should be ensured by the use of either of the two types of eIDAS certificates or preferably both, as mentioned in paragraph 15 above.

18. Furthermore, CAs should ensure that ASPSPs allow AISPs, PISPs and CBPIIs to use eIDAS certificates for identification through whichever access interface the ASPSP has chosen to provide, in accordance with Article 31 of the RTS, whether this is a dedicated interface or an interface used for authentication and communication with the PSUs (an adapted PSU interface). However, the EBA hereby clarifies that, in the case of an adapted PSU interface, ASPSPs should request the use of eIDAS certificates only from AISPs, PISPs and CBPIIs. On a related point, the EBA would also like to clarify that there is no obligation in PSD2 or in the RTS to request eIDAS certificates from PSUs.

Use of single and multiple eIDAS certificates

19. Article 34(3) of the RTS does not specify whether PSPs should hold single or multiple eIDAS certificates for the same role that they want to accommodate. Nevertheless, the EBA hereby clarifies that it is for the respective PSP to decide whether to use single or multiple certificates for each role.

20. However, in the specific cases where PSPs provide services through agents or EEA branches, or where they have outsourced to technical service providers some of the activities related to access to the online accounts held within an ASPSP, the EBA hereby clarifies that CAs should encourage these PSPs to consider using multiple certificates simultaneously: one per agent, EEA branch or technical service provider. This should ensure business continuity and better risk management of these PSPs because the legitimacy of one certificate would not be affected by the revocation of any other. PSPs remain fully responsible and liable for the acts of their agents and outsource providers as well as for the revocation and updating of the eIDAS certificates used by them.

21. CAs should also ensure that ASPSPs accept eIDAS certificates presented by agents or outsource providers acting on behalf of AISPs, PISPs and CBPIIs, provided that the ASPSP is in a position to unequivocally identify the principal PSP in the presented certificate.

Roles of payment service providers in an eIDAS certificate for PSD2 purposes

22. Article 34(3) of the RTS prescribes the additional specific attributes that should be included in QWACs and QSealCs for the purposes of the RTS, which are the role of the PSP and the name of the CA by which the PSP is authorised or registered. Article 34(3)(a) of the RTS distinguishes four roles that can be assigned to a PSP, namely 'account servicing', 'payment initiation', 'account information' and 'issuing of card-based payment instruments'.

23. The EBA hereby clarifies that these four roles can be assigned to PSPs that have been authorised to provide the respective payment services as referred to in Annex I to PSD2. The payment services that correspond to each role are specified below.

    a) *Account servicing* – in accordance with Article 4(17) of PSD2, an 'ASPSP' means a payment service provider providing and maintaining a payment account for a payer. However, there is not a specific payment service corresponding to that role, but in almost all cases PSPs that should be able to provide and maintain payment accounts for PSUs are those that provide the payment services as referred to in points (1), (2) and/or (3) of Annex I to PSD2.

    b) *Payment initiation* – this corresponds to payment initiation service as referred to in point (7) of Annex I to PSD2.

    c) *Account information* – this corresponds to account information service as referred to in point (8) of Annex I to PSD2.

    d) *Issuing of card-based payment instruments* – this corresponds to the issuing of payment instruments and/or acquiring of payment transactions as referred to in point (5) of Annex I to PSD2.

24. In the scenario where the PSP acts in its capacity as a third party provider (as an AISP, a PISP or a CBPII), it should be assigned the roles 'account information', 'payment initiation' and/or 'issuing of card-based payment instruments' respectively.

25. Payment institutions need to be authorised under Article 11 of PSD2 for each of the payment services they intend to provide. This means that the roles that could be assigned to payment institutions that would like to obtain an eIDAS certificate should be limited to the payment services for which the respective payment institution has been authorised.

26. Following the requirement of Article 111(1)(a) of PSD2, Article 11 of PSD2 applies *mutatis mutandis* to electronic money institutions. Therefore, the roles that could be assigned to electronic money institutions that would like to obtain an eIDAS certificate should also be limited to the payment services for which the respective electronic money institution has been authorised.

27. While payment institutions and electronic money institutions need to be authorised for each payment service they intend to provide, authorised credit institutions can provide all the payment services referred to in Annex I to PSD2 as part of their authorisation under Directive

2013/36/EU [6] without being authorised for each of the payment services they provide. Therefore, credit institutions that act in their capacity as a third party provider (whether as an AISP, a PISP and/or a CBPII) should be assigned the three roles 'payment initiation', 'account information' and 'issuing of card-based payment instruments' at the same time.

28. In the scenario where the PSP acts in its capacity as an ASPSP and offers to PSUs accounts that are accessible online, said PSP should be assigned the role 'account servicing'. While the RTS and PSD2 do not require ASPSPs to identify themselves towards the AISPs, PISPs and CBPIIs in a specific way, CAs could encourage ASPSPs also to obtain an eIDAS certificate for the purpose of mutual identification.

CA involvement in the revocation of an eIDAS certificate for PSD2 purposes

29. While Article 34(1) of the RTS requires ASPSPs to rely on eIDAS certificates to identify AISPs, PISPs and CBPIIs, many market participants expressed concerns that eIDAS certificates may not present the authorisation status of each PSP accurately at all times.

30. In the view of those market participants, this would mean that ASPSPs may want to verify the authorisation status of the AISPs, PISPs and CBPIIs requesting access, which would be contrary to the intention of Article 34(1) of the RTS and result in an additional step in the execution of the respective payment service that could potentially lead to delays to the 'customer journey'.

31. Qualified trust service providers (QTSPs) are responsible for checking the validity of the information in the eIDAS certificates at the time of issuance, and both QTSPs and PSPs are responsible for ensuring the information is kept up to date and for revoking the certificates. However, the EBA is of the view that CAs should consider requesting, where necessary, the revocation of an eIDAS certificate issued to a PSP authorised by the respective CA, which has had its authorisation/registration withdrawn or authorisation for a specific payment service revoked.

32. To facilitate the above, the EBA hereby clarifies that CAs may establish a standardised process for the exchange of notifications regarding the revocation of eIDAS certificates for the purpose of PSD2 with the following steps.

    a) *Issuing of an eIDAS certificate* – CAs may inform the EBA of an email address that they have set up for the purpose of receiving notifications on eIDAS certificates from QTSPs that will be made publicly available by the EBA. CAs could expect QTSPs to inform them about any certificates they have issued to PSPs authorised/registered by that CA;

    b) *Revocation of an eIDAS certificate* – PSPs are responsible for initiating the revocation of the certificate with the QTSP that issued it. CAs could expect that the PSP will inform

[6] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, OJ L 176/338, 27.6.2013.

them about the revocation of the certificate or alternatively that the QTSP that has issued the certificate will do so using the email address specified in item 'a' above.

c) *Revocation of an eIDAS certificate requested by a CA* – if a CA has withdrawn an authorisation/registration of a PSP providing AIS, PIS or CBPII, but the CA has not been informed about the revocation of the respective eIDAS certificate either by the PSP or by the QTSP, the CA may request the revocation of the certificate from the QTSP that has issued it.

33. However, although the above process involves the exchange of notifications between QTSPs and CAs regarding the issuance and revocation of eIDAS certificates, CAs should not obtain information about the attributes of the actual certificates that have been issued to the authorised/registered PSPs.

34. In addition to the above process, CAs should encourage PSPs to proactively inform QTSPs whether their authorisation/registration was withdrawn or their authorisation for a specific payment service was revoked.

35. CAs should also update their national public registers, the EBA electronic central register under PSD2 and the EBA Credit Institutions Register without delay following any decisions that affect the authorisation/registration status of PSPs, to allow QTSPs to rely on them in the process of issuing or revoking an eIDAS certificate.

This opinion will be published on the EBA's website.

Done at London, DD Month YYYY

[signed]

Andrea Enria

Chairperson

For the Board of Supervisors