Quali-Sign Ltd

www.quali-sign.com

Questions to EBA on PSD2

Michael Adams

31st March 2016

Table of Contents

1 Response from EBA

Unfortunately, we are unable to respond to your query as much as you would like. This is because some of the EU law to which you are referring, such as the eIDAs Regulation, does not fall into the regulatory remit of the EBA, so the EBA is not in a position to interpret it. You may wish to approach the EU Commission and co-legislators (EU Council and EU Parliament) with any question you may have. Furthermore, with regard to the particular mobile phone app that we understand you are developing, the EBA does generally not comment on any particular technical solution that market actors may be developing to meet legislative and/or regulatory requirements. The EBA stays technology-neutral to ensure a level playing field for all firms, including market incumbents and challengers.

What we indeed could comment on are your questions related to the PSD2. However, your questions arrive too early, as the EBA is still in the process of developing the 11 Technical Standards and Guidelines that the PSD2 has conferred on the EBA. Some of these 11 mandates touch directly upon the questions you are asking. We therefore suggest you wait until we have published these legal instruments for consultation, and that you provide your input in writing at that point time. In order for you not to miss any of the consultations, you may wish to have a frequent look at the following section of our website, where we will publish all documents related to PSD2: http://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money.

Complimentarily, you may also wish to subscribe to EBA email alerts, which you can do on the right hand side here: http://www.eba.europa.eu/news-press.

2 Questions

QUESTION 1)

With reference to PSD2 Article 4.30, where a 'legal person' (company) applies an electronic seal to a payment transaction, for example, using a private key stored in a hardware security module (HSM) (i.e. possession), would a 'natural person' be required to provide e.g. a PIN (knowledge) or fingerprint (inheritance), in order for the seal to qualify as 'strong customer authentication'?

QUESTION 2)

With reference to PSD2 Article 74.2, in the case of a payment instruction initiated by a payer, is the strong customer authentication 'signature proof' required to be made available to the payee and their payment service provider?

3 Supplementary Analysis on PSD2

The following analysis was supplied along with the questions:

PSD2 Article 4 Definition

(29) 'authentication' means a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials;

(30) 'strong customer authentication' means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inheritance (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;

The discussion paper gives an example, in the case of a natural person, of a private key being locked into the trusted zone of a mobile phone (possession) and unlocked with a pin (knowledge) or fingerprint (inheritance).

It is not clear to me how two or more elements would be used in the case of a legal person (company) applying an electronic seal using a private key stored in a hardware security module (HSM). This would constitute possession. Would a natural person be required to also supply a PIN, for example?

PSD2 Article 97.2. With regard to the initiation of electronic payment transactions as referred to in point (b) of paragraph 1, Member States shall ensure that, for electronic remote payment transactions, payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.

E.g. a digital signature, where the data to sign includes amount and payee details.

PSD2 Article 72 Evidence on authentication and execution of payment transactions 1. Member States shall require that, where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider.

The burden of proof is on the payment services provider. Other articles stipulate that the payer's provider must immediately refund the payer if their provider cannot provide proof.

PSD2 Article 74.2. Where the payer's payment service provider does not require strong customer authentication, the payer shall not bear any financial losses unless the payer has acted fraudulently. Where the payee or the payment service provider of the payee fails to accept strong customer authentication, it shall refund the financial damage caused to the payer's payment service provider.

I am not sure how to read this. I assume that the references to the payee and payee payment service provider relate to scenarios where the payee has initiated the transaction, i.e. collection. Otherwise does it indicate that each party in the chain must itself validate the signature proof? This would suggest that in the case of a disbursement, the payee should really validate the payer's signature before releasing goods (for example), as if the signature is not valid, funds can be refunded to payer.

PSD2 Article 92 Right of recourse 1. Where the liability of a payment service provider under Articles 73 and 89 is attributable to another payment service provider or to an intermediary, that payment service provider or intermediary shall compensate the first payment service provider for any losses incurred or sums paid under Articles 73 and 89. That shall include compensation where any of the payment service providers fail to use strong customer authentication.

Note reference to 'any of the payment service providers fail to use strong customer authentication.'

PSD2 Article 49 Information for the payee after execution immediately after the execution of the payment transaction, the payee's payment service provider shall provide the payee with, or make available to, the payee, in the same way as provided for in Article 44(1), all of the following data with regard to its own services:

(a) a reference enabling the payee to identify the payment transaction and, where appropriate, the payer and any information transferred with the payment transaction;

(b) the amount of the payment transaction in the currency in which the funds are at the payee's disposal;

(c) the amount of any charges for the payment transaction payable by the payee and, where applicable, a breakdown of the amounts of such charges;

(d) where applicable, the exchange rate used in the payment transaction by the payee's payment service provider, and the amount of the payment transaction before that currency conversion;

(e) the credit value date.

I cannot find any reference in the directive to the detail of what is provided (in the case of a disbursement) to the payee or their payment service provider with respect to the strong customer authentication signature proof.

4 Supplementary Analysis on eIDAS

The following analysis was supplied along with the questions:

e-IDAS Page 80 point 56

This Regulation should lay down requirements for qualified electronic signature creation devices to ensure the functionality of advanced electronic signatures. This Regulation should not cover the entire system environment in which such devices operate. Therefore, the scope of the certification of qualified signature creation devices should be limited to the hardware and system software used to manage and protect the signature creation data created, stored or processed in the signature creation device. As detailed in relevant standards, the scope of the certification obligation should exclude signature creation applications.

I.e. an individual android or apple app would not need to be certified for signature creation. Instead the underlying hardware / software would be certified.

e-IDAS Article 3 Definitions

(9) 'signatory' means a natural person who creates an electronic signature; (10) 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
(11) 'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26;
(12) 'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;
(13) 'electronic signature creation data' means unique data which is used by the signatory to create an electronic signature;
(14) 'certificate for electronic signature' means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;
(15) 'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;
(22) 'electronic signature creation device' means configured software or hardware used to create an electronic signature;
(23) 'qualified electronic signature creation device' means an electronic signature creation device that meets the requirements laid down in Annex II;
(24) 'creator of a seal' means a legal person who creates an electronic seal;
(25) 'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;
(26) 'advanced electronic seal' means an electronic seal, which meets the requirements set out in Article 36;
(27) 'qualified electronic seal' means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;
(28) 'electronic seal creation data' means unique data, which is used by the creator of the electronic seal to create an electronic seal;
(29) 'certificate for electronic seal' means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;

(30) ‘qualified certificate for electronic seal’ means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III;

e-IDAS refers to a electronic signatures being applied by a natural person and a legal person (company) applying an electronic seal. PSD2 refers to electronic signatures covering both natural and legal persons.

e-IDAS Article 24 Requirements for qualified trust service providers
1. When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued. The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:
(a) by the physical presence of the natural person or of an authorised representative of the legal person; or
(b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels ‘substantial’ or ‘high’; or
(c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or
(d) by using other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.

This suggests that posting or faxing a signed 'Certificate Signing Request' (CSR) is not enough. The signature would need to be witnessed by bank (/ certificate authority) representative. However if the person already has a certificate (e.g. in the form of a national identity card), they should be able to automatically provision additional certificates for new/replacement (personal authorisation) signature keys, for example, held within the trusted hardware zone of a mobile phone.

I have implemented some additional bespoke orders on a test EBICS server. This allows the app to upload a CSR, download the corresponding CA certificate, suspend and revoke the certificate. I intend to post a suggested change request on the ebics.org site to allow a personal user to initialize with a CSR rather than a CA certificate. As a workaround, I initialize a (temporary) transport user for the purposes of provisioning the CA certificate. I have added a page to the (transport user's) initialization letters for the CSR details.

3. If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.

4. With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.

Note that a CA will no longer be able to charge to access their revocation list.

e-IDAS Article 25 A qualified electronic signature should have the equivalent legal effect of a handwritten signature.
e-IDAS Article 35 2. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

e-IDAS Article 26 Requirements for advanced electronic signatures
An advanced electronic signature shall meet the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

e-IDAS Article 36 Requirements for advanced electronic seals
An advanced electronic seal shall meet the following requirements:
(a) it is uniquely linked to the creator of the seal;
(b) it is capable of identifying the creator of the seal;
(c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and
(d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

EBICS specification includes within the OrderSignatureData structure the ability (currently a future requirement) for a copy of the user's signature certificate to be included, within the X509Data tag. This will meet the requirement for advanced electronic signatures/seals.

e-IDAS Article 28 Qualified certificates for electronic signatures.

4. If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature:
(a) if a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension;
(b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.

Note a certificate can be suspended as well as revoked.

e-IDAS Article 33 Qualified validation service for qualified electronic signatures
1. A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who:
(a) provides validation in compliance with Article 32(1); and
(b) allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.

In the case of a disbursement initiated by the payer, where the payee or payee's payment service provider needed confirmation of a valid signature. If a qualified validation service was to provide this, the payer would be able to include multiple transactions to different payees in the same file and would be able to continue to sign the whole file rather than the individual transactions. The whole file would not need to be shared with each payee. The qualified validation service would be responsible for ensuring the confidentiality of the contents. The concern that I have with this assumption is that the use of a qualified validation service would need to be mandatory in this case.