ESI(17)60_035r1

ETSI / ERPB PIS Experts PSD2 Workshop Discussion Document on PSD2 Requirements for Qualified Certificate Date: 10 Oct 2017

Introduction

The report submitted by the ERPB PIS working group at the 12th June to the ERPB has requested ESI to review the Use Cases, Data Profiles and Management of Qualified Certificates for standardisation across the EU for use within Payment Services Directive 2.
https://www.ecb.europa.eu/paym/retpaym/euro/html/index.en.html
Following this request ETSI Technical Committee of Electronic Signatures and Infrastructures formed an ad hoc workshop to develop certificate profiles and management requirements for qualified certificates for PSD2.

This discussion document reflects discussions, reflecting on ETSI expert and ERPS expert initial views, responding to questions raised on how Qualified Certificates may be used to meet the requirements of PSD2 based on the 17th May version of the regulatory technical standards as included in commission letter "Commission intention to amend the draft regulatory technical standards on strong customer authentication and common and secure open standards of communication submitted by the EBA in accordance with Article 98(4) PSD2".

The PSD2 Legislation, Articles 66,67,68 provide the mandate for Third Parties to be able to use Bank provided Interfaces in order to operate Payment Services on behalf of Bank Customers, over the Internet.

As there are known issues with Man-in-the-Middle and other security threats to allowing this new access, further requirements have been delegated and drafted by the EBA, to establish requirements for Strong Customer Authentication and Common Secure Communication.

Within the EBA RTS, use of Certificates as specified by eIDAS is mentioned, along with requirements for Regulatory information to be contained within Certificates used.

As there are predefined protocols, industry interoperability, and security issues that may arise from incorrect or fragmented use of Certificates, ETSI and ESI WG have been requested to review and recommend standards for the EU implementation of eIDAS Certificates for PSD2, initially for Common Secure Communication, but perhaps later for Strong Customer Authentication.

The main principles required are that the ASPSP and the TPP can be assured of the Identity of each Communicating party and Secure their communications against other parties interception, in order to protect payment services data and to ensure that only the correct PSD2 Entities may access PSU funds and data.

This discussion document, along with the RTS expected to be published soon, will be used as the basis of the ETSI work item on "Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive 2015/2366/EU" (https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=53961). The views expressed below may be revised having worked on the details of this technical specification.

Glossary of Terms

EC –	European Commission
EBA –	European Banking Authority
ECB –	European Central Bank
ETSI –	European Telecommunication Standards Institute
ERPB –	European Retail Payment Board
ESI –	Electronic Signatures & Infrastructure
IETF -	Internet Engineering Task Force

PSD2 – Payment Services Directive 2 (L)

RTS –	Regulatory Technical Standards
ITS –	Implementing Technical Standards
MSCA –	Member State Competent Authority (i.e. PSD2 Regulator, per Member State)
ASPSP –	Account Servicing Payment Service Provider (e.g. a Bank)
PISP -	Payment Initiation Service Provider
PIISP -	Payment Instrument Issuer Payment Service Provider
AISP -	Account Information Service Provider
TPP –	Third Party Provider (encompassing PISP and AISP)
PSU –	Payment Service User (e.g. a Bank Customer)
SCA –	Strong Customer Authentication
CSC –	Common Secure Communications
XS2A -	Access to Account (services for PISP & AISP)

eIDAS – Electronic Identity and Trust Services for Electronic Transactions (L)

MSSB –	Member State Supervisory Body (i.e. eIDAS Regulator, per Member State)
CA/B –	Certification Authorities / Browser Forum
ICANN –	Internet Corporation for Assigned Names and Numbers
QTSP/TSP –	Qualified/ Trust Service Provider
QSealC –	Qualified Electronic Seal Certificate
QWAC –	Qualified Website Authentication Certificate
PKI –	Public Key Infrastructure
OCSP -	Online Certificate Status Protocol
CRL -	Certificate Revocation List
TS -	Technical Standard
EN -	European Notice
TLS	Transport Layer Security (replaces SSL – secure socket layer)

KEY QUESTIONS for ESI Guidance & Standardisation:

CERTIFICATE USAGE FOR PSD2

1. Qualified Electronic Seal Certificates (QSealC) or Qualified Website Authentication Certificates (QWAC)?
   a. When should they be used and for what purpose?
   b. Can either be used interchangeably/in place of each other?
   c. Is only one needed, or are both needed?
   d. What Certificates Standards are to be followed and who manages these?
   e. Recommend Uses & Non-Uses for eIDAS Certificates under PSD2

Response:

The main purpose of a digital certificate is to identify the owner of a public key (and the corresponding private key). Using the certificate it is possible to communicate securely with its owner. What "securely" means exactly depends on the type of certificate.

A website authentication certificate makes it possible to establish a Transport Layer Security (TLS) channel with the owner of the certificate, which guarantees confidentiality, integrity and authenticity of all data transferred through the channel. This means that the person or system connecting to the website presenting the certificate can be sure who “owns” the end point of communications channel (which is 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 communicated data is only protected while it is travelling through the TLS channel. The data is produced in plain (unencrypted) form by the sender system, and the data will appear in plain (unencrypted) form in the receiver system. Therefore, once the TLS channel is closed, the data loses the protection of its authenticity, integrity and confidentiality, unless it is protected by other means.

An electronic seal is a digital signature of a legal person. A certificate for electronic seals makes it possible for the owner of the certificate to create electronic seals on any data. The digital signature technology guarantees the integrity, and authenticity of the signed/sealed data. This means that the person receiving digitally signed data can be sure who signed the data (the owner of the certificate), that the data was not changed since it was signed, and they can also present this signed data to third parties as an evidence of the same (who signed it, and that it was not changed since). Therefore, digitally signed data can keep its authenticity and integrity over time when appropriately maintained, regardless of how it is stored or transferred. (An electronic seal can be validated by anyone, at any time, to check whether the integrity and authenticity of the data still holds. The seal provides strong evidence that given data is originated by the legal entity identified in the certificate.

Certificates for both website authentication and electronic seals can be qualified or non-qualified. The requirements on the issuance of a qualified certificate are more stringent, so using a qualified certificate provides a stronger association of the protected data with the identity of the owner of the certificate. As an example, before issuing a qualified certificate the issuer CA will verify the identity of the owner in a face-to-face meeting and based on government-issued photo ID documents, or by equivalently secure procedures. Hence, qualified certificates can have a stronger legal assumption of the evidential value than non-qualified ones.

Both QWACs and QSealCs are based on widely implemented technology. QWACs are derived from web sites certificates supported by all the modern web browsers and commonly used to provide system to system secure channels. QSealCs are derived from certificates used with digital signature technology such as widely employed for document security, business to business and in modern banking networks.

In consequence:

- A qualified website authentication certificate (QWAC) should be used to establish a secure TLS channel to protect the communication (in the transport layer) from potential attackers on the network. The person or system connecting to the website can be sure who they are communicating with, but cannot prove this to third parties. Using QWAC does not give legally assumed evidence of a transaction.
- A qualified certificate for electronic seals (QSealC) should be used to protect the data or messages (in the application layer) from potential attackers during or after the communication. The electronic seal does not provide confidentiality (i.e. there is no encryption of application data). The person receiving the sealed data can be sure who sealed the data, and can also prove this to third parties even after the communication has ended. QSealC provides evidence of a transaction with legal assumption.
- A certificate can be either for website authentication or electronic seals, but not both. Therefore, these two types of certificates are not interchangeable.

Examples:

- To make sure the data is not damaged or altered maliciously by external actors: QWAC or QSealC can be used.
- To make sure the data is not read or stolen by external actors on the network: QWAC should be used.
- To make sure the originator of the data is known by the receiver of the data: QWAC or QSealC can be used.
- To make sure the originator of the data can be proven by evidence to any third party: QSealC should be used. (e.g. This can be extremely useful to retain a proof of authorization for a transaction.)

Response to specific points:

a. When should they be used and for what purpose?

See above

b. Can either be used interchangeably/in place of each other?

Each certificate has to be used for the particular purpose as described above. The certificate has different legal implications and needs to meet differing legal requirements. Thus they cannot be used interchangeably. The certificate path validation technology when using QWAC and QSeals would be expected to enforce this policy of separating usage.

c. Is only one needed, or are both needed?

They have differing purposes and whether one or other is needed depends on its use as described above. It is suggested that both are used to meet both security of communications (QWAC) and legal certainty (QSealC) requirements.

d. What Certificates Standards are to be followed and who manages these?

i) The basis of the requirement of qualified certificates is the eIDAS regulation Annex III (QSealC) and Annex IV (QWAC),

ii) General requirements for Qualified certificates are specified in EN 319 412-5
Requirements for certificates for web site authentication (both QWAC and non-qualified certificates for web site authentication) are specified in EN 319 412-4
Requirements for certificates for electronic seals (both QSealC and non-qualified certificates for electronic seals) are specified in EN 319 412-3
Requirements for registration and revocation of qualified certificates are specified in EN 319 411-2, which builds on EN 319 411-1 (general requirements for certificates.

iii) EN 319 412-4 and EN 319 411-1/2 build on requirements for certificate as defined by the CA/Browser forum documents. In the case of QWACs this is their document

titled:
"Guidelines For The Issuance and Management of Extended Validation Certificates"
(Referred to as [CA/B EV] below)

iv) The CAB Forum and ETSI documents build on a number of IETF documents including:

a) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

b) IETF RFC 6960: "X.509 Internet Public Key - Infrastructure Online Certificate Status Protocol - OCSP".

c) IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and CertificationPractices Framework".

v) All the above are based on
ISO/IEC 9594-8/Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

Aim to keep any changes in the domain of ETSI standards listed above.

e. Recommend Uses & Non-Uses for eIDAS Certificates under PSD2

See above

SOURCES OF DATA

2. Where must the mandatory information SOURCED for a QWAC (and for which type of QWAC)? (Standardisation)

Response:

The information is provided by the subject (i.e. the "owner" of the key being certified) and verified by the QTSP (see due diligence below).

3. Where must the mandatory information SOURCED for a QSealC (and for which type of QSealC)? (Standardisation)

Response:

The information is provided by the subject (i.e. the "owner" of the key being certified) and verified by the QTSP (see due diligence below).

DATA ELEMENTS AND CERTIFICATE PROFILES

4. What is the mandatory information and where must it GO in a QWAC (and for which type of QWAC)? (Standardisation)

Response:

The requirements for the certificate contents for QWACs are as specified in [CA/B EV] clause 9.2 (as referenced from EN 319 412-4), with additional attributes relating to the qualified status. This includes:

i. Subject Organization Name Field: the legal person identity

ii. Subject Alternative Name Extension: the (DNS) domain name (or set of domain names) of the web site.
The domain name may also be held in the Common Name field although this is "deprecated". Only a single domain name can be held in the Common Name.

iii. Subject Business Category: This must be one of "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity". (see [CA/B EV] 9.2.4).

iv. Subject Jurisdiction: country, state or other locality information.

v. Subject Registration Number: Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate.. This is held in the serialNumber field (note this is different from requirement for QSealC).

vi. Optional Subject Physical Address of Place of Business.

vii. Other attributes are allowed but must be checked by the CA. See CA/B EV clause 9.2.8.

The CA/B Baseline, 7.1.2.3 item f, specifies that the extended key usage (relating to TLS client or server authentication) is required:

> "Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. id-kp-emailProtection [RFC5280] MAY be present. Other values SHOULD NOT be present."

The attributes required are the same for either TLS client or server authentication

Specific requirements for PSD2 attributes are to be addressed separately based on input from PSD2 experts.

5. What is the mandatory information and where must it GO in a QSealC (and for which type of QSealC)? (Standardisation)

Response:

The requirements for the certificate contents for QSealCs are as specified in EN 319 412-3. The following attributes are required as part of the subject name. Additional attributes are required relating to the qualified status.

i. countryName: the country in which the subject (legal person) is established.

ii. organizationName: the full registered name of the subject (legal person)

iii. organizationIdentifier: an identification of the subject organization different from the organization name. Certificates may include one or more semantics identifiers as specified in clause 5 of ETSI EN 319 412-1.

iv. commonName: a name commonly used by the subject to represent itself. This name need not be an exact match of the fully registered organization name.

The DNS name could optionally be carried in the Subject Alternative Name Extension as for QWACs but generally this is not included.

Specific requirements for PSD2 attributes are to be addressed separately based on input from PSD2 experts.

DUE DILIGENCE BY QTSP BEFORE CERTIFICATE ISSUING

6. What is the KYC and Due Diligence procedure for the QTSP with the TPP/ASPSP, to check they are who they claim to be, related to the Sourced Data BEFORE a cert has been issued:
   a. For QWAC
   b. For QSealC

Response:

For existing identity & DNS attributes:

The requirements for verification of attributes in QWACs are mostly covered by CA/B EV section 11. EN 319 411 parts 1 and 2 clause 6.2.2 includes a few additional requirements.

For existing identity attributes:

The requirements for verification of attributes in QSealCs are covered by EN 319 411 parts 1 and 2 clause 6.2.2.

Other PSD2 attributes are also required to be verified but there are currently no specific procedures for how this is done. The TSP will probably need to check any claimed PSD2 attributes with the PSD2 member state competent authority. It is planned to include requirements on the TSP to carry out checks in the work item referred to in the introduction.

CERTIFICATE MANAGEMENT AND LIABLITY

7. Accuracy of information (and whose Liability) AFTER the cert has been issued:
   a. For QWAC
   b. For QSealC

8. How to manage revocation of Certificate AFTER cert has been Issued:
   a. For QWAC
   b. For QSealC

9. Responsibility for status/revocation (and whose liability) AFTER the cert has been issued:
   a. For QWAC
   b. For QSealC

Response:

The QTSP is required under eIDAS Article 24 & article 13 on liabilities to verify the content of the certificate on issuance and renewal. Under current practice QTSP is not responsible for collecting information on changes to the certificate content (except on registration). The subject is obliged to inform TSP of any changes. Other parties may inform QTSP of changes (e.g.PSD2 member state competent authority). QTSP once informed has to check the information is liable for revocation within 24 hours if appropriate. The QTSP practices defines what revocation requests are handled. If any part of the information changes the certificate is revoked by the QTSP. The PSP may request a new certificate but this will need to go through registration checks.
Some non-critical changes (e.g. email address) do not force a revocation.

Additional requirements may needed to be added to EN 319 411-1 / 2 to handle revocation requests for PSD2.

RECEIVING PARTIES USING CERTIFICATES

10. How does an ASPSP/TPP to check the validity/status of a Certificate AFTER cert has been Issued:
    a. For QWAC
    b. For QSealC

11. How does an ASPSP/TPP check the signature of a Certificate AFTER cert has been Issued:
    a. For QWAC
    b. For QSealC

Response

For end user certificate revocation information is distributed done using a Certificate Revocation List (CRL – see X.509) or Online Certificate Status Protocol (OCSP – RFC 6960)

QWAC: Recommend use RFC 5280 . This describes how to validate certificate when channel is established by underlying software. Not all web browsers use RFC 5280 (see below). Any web browser may apply additional rules. Browsers may not currently use trusted list of qualified TSPs. Examples of browser specific rules for handling certificates are:

- Mozilla
  https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/

- Google CP (requires a “Certificate Transparency”) http://dev.chromium.org/Home/chromium-security/root-ca-policy
- Microsoft requires OID and EKU
  http://aka.ms/RootCert
- Apple accepts and removes root certificates as it deems appropriate in its sole discretion: http://www.apple.com/certificateauthority/ca_program.html

QSeal: validation procedures for QSeals (including QSealCerts) are defined in ETSI EN 319 102-1 which builds on RFC 5280 which builds on X.509. This is carried out at application level by the receiving party.

Qualified TSPs issuing a QWAC or QSealsC are listed in a set of Trusted List issued by each nation. It is expected that this list be used when validating a QWAC or QSealC. The Trust list may be viewed at:

- https://webgate.ec.europa.eu/tl-browser/#/
- http://tlbrowser.tsl.website/tools/
- https://www.eid.as/tsp-map/#/

However relying parties should refer to the definite source https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers