[**X**] Public – [ ] Internal Use – [ ] Confidential – [ ] Strictest Confidence
Distribution: General Public

eIDAS and TPP Identification (PSD2)

1. Introduction

The API Evaluation Group (EG) was informed about a potential conflict with the use of certain types of eIDAS certificates by third-party providers (TPPs) in payment service user (PSU) channels, like online banking, as it might preclude the PSUs from accessing the bank through that channel. In particular, it was suggested that QWAC certificates might not be suitable for identifying TPPs through those channels. And for an account information service provider (AISP) / payment initiation service provider (PISP) to identify itself towards a direct interface, a QSEAL certificate might be required.

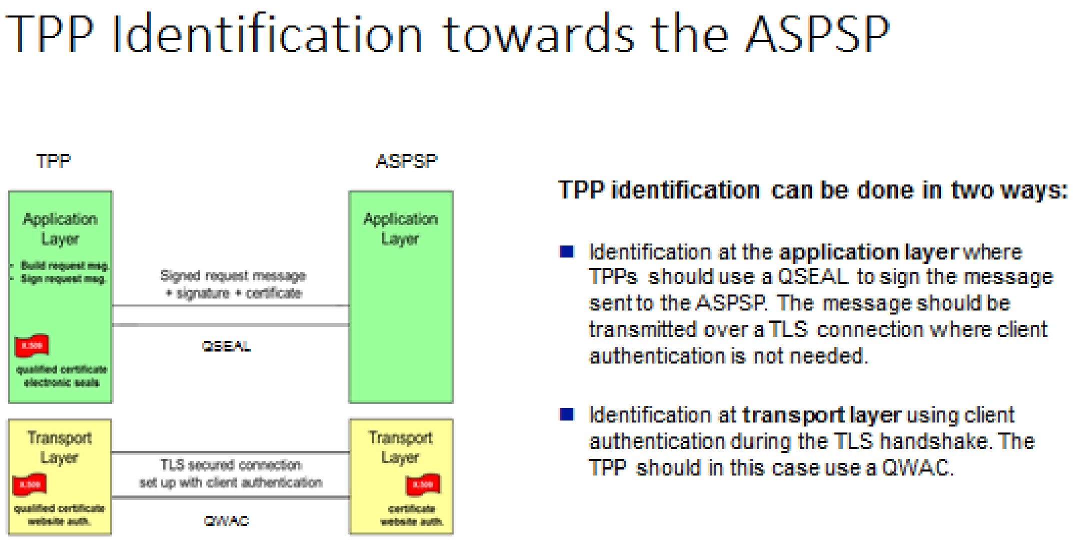
In order to respond to the question, and to further clarify the suitability of each type of certificates, for different scenarios, a working group (WG) was created consisting of technical experts both from the account servicing payment service provider (ASPSP) and TPP side, as well as participants from the API EG.

The ambition of the WG was to respond to the question from a technical perspective as neutrally as possibly without making any legal interpretation or recommendations. The WG also wanted to provide some in-depth background information and examples of possible application usage for QWAC and QSEAL certificates in order to put the outcome in the right context.

2. Outcome from the WG discussions

TPP identification can be done in two ways:

1. During the TLS handshake, as part of a mutual authentication TLS session, where TPPs should use a QWAC.
2. In the application layer (on top of a TLS session where mutual authentication is not needed), where the TPPs sign their requests with a QSEAL.



TPP Identification towards the ASPSP

TPP
ASPSP
Application Layer
- Build request msg.
- Sign request msg.
X.509
qualified certificate electronic seals
Signed request message + signature + certificate
QSEAL
Application Layer
Transport Layer
X.509
qualified certificate website auth.
TLS secured connection set up with client authentication
QWAC
Transport Layer
X.509
certificate website auth.

TPP identification can be done in two ways:

- Identification at the **application layer** where TPPs should use a QSEAL to sign the message sent to the ASPSP. The message should be transmitted over a TLS connection where client authentication is not needed.
- Identification at **transport layer** using client authentication during the TLS handshake. The TPP should in this case use a QWAC.

3. Background information:

The intended usage of a QWAC is to establish a TLS channel which guarantees confidentiality, integrity and authenticity of all data transferred through the channel between the TPP and the ASPSP. The most common usage is for identifying the server so that clients connecting to it know who controls it but a QWAC can also be used to identify the client so that the server knows who is connecting. (This is specified in CA/B Baseline, 7.1.2.3 item f: Either the value *id-kp-serverAuth* [RFC5280] or *id-kp-clientAuth* [RFC5280] or both values must be present.) 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.

The intended usage of a QSEAL is to sign any data, guaranteeing the integrity and authenticity of the signed data over time, but not confidentiality. The seal provides strong evidence that given data is originated by the legal entity identified in the certificate and the signed data can keep its authenticity and integrity over time when appropriately maintained, regardless of how it is stored or transferred.

For identifying a TPP in the context of PSD2, both kinds of certificates can be used and they both have their advantages and disadvantages.

There are multiple technical ways both kinds of certificates can be used, the following two ways are just one example for each kind of certificate:

- QWAC usage as part of a mutual authentication TLS session, "QWAC-TLS": One way of identifying TPPs by the use of a QWAC is that the ASPSP sends a *CertificateRequest* in the *ServerHello* message during the TLS handshake and the

TPP responds with its QWAC (with *id-kp-clientAuth*). The ASPSP can then verify the QWAC and know the identity of the TPP.

- QSEAL usage, "QSEAL-header": One way of identifying TPPs by the use of a QSEAL is that the TPP signs the data it intends to send to the ASPSP with its QSEAL and attaches the signature as a HTTP header. The ASPSP can then verify the QSEAL and know the identity of the TPP. In order to also guarantee confidentiality, the data could be sent over TLS but the TLS connection itself would not need to contain identification of the TPP (i.e. the ASPSP does not need to send a *CertificateRequest* in the *ServerHello* message).

One prerequisite with the QWAC-TLS is that the ASPSP must know that it's a TPP connecting and not a regular PSU since sending the *CertificateRequest* to a PSU would create a confusing popup if the PSU is using a web browser. There are multiple technical ways an ASPSP could solve that for non-dedicated interfaces and for dedicated interfaces the ASPSP can simply assume that it's only TPPs connecting.

If there needs to be an exchange of multiple HTTP requests between the TPP and ASPSP for performing PIS/AIS then for performance reasons, it's recommended that HTTP keep-alive is used in order to reduce the number of times the certificates have to be used. (If either the ASPSP or the TPP has internal security guidelines preferring to not use keep-alive then either party can close the TLS connection and open a new one for each request). For the QWAC-TLS example, the QWAC would only be needed when establishing the TLS connection and for the QSEAL-header, only the first HTTP request sent in a TLS session would need to contain the signature headers if the ASPSP supports keeping track of the TLS session otherwise all requests need to be signed. But since one of the advantages with a QSEAL is that the signature can be also be used as a proof that a TPP instructed the ASPSP to do something, requiring signing all important HTTP requests might be a good idea.

ASPSPs might also want to log which TPP it was that performed a specific action, such as initiating a credit transfer. With the QWAC-TLS example the ASPSP would need to propagate the certificate information from the TLS layer up to the application layer where the certificate information can be linked to the action performed. (One way of propagating such information is by the ASPSP itself adding the TLS certificate information as an X-header internally.) With the QSEAL-header example they will have the information in the header sent by the TPP.

Below are some examples, for illustrative purposes only, of how QWAC-TLS and QSEAL-header could be used in the context of PSD2:

- For dedicated interfaces:
  - QSEAL-header is used on those HTTP requests where the ASPSP wants to be able to prove that a specific TPP did something and QWAC-TLS is used as a general identification layer. HTTP-keepalive is used for reducing the number of times the certificates have to be used.
- For non-dedicated / PSU interfaces:
  - QSEAL-header is used on all HTTP requests. HTTP-keepalive is used to make it possible for the ASPSP to only verify the signature on those HTTP requests they deem important during a TLS session.

  - Or QWAC-TLS is used also on the non-dedicated interface by the ASPSP either detecting that it's a TPP connecting or they have a non-dedicated interface where all clients use mutual authentication TLS (such as the interface used by the ASPSPs mobile app).

4. Glossary

- eIDAS: a set of standards for electronic identification and trust services for electronic transactions in the European Single Market.

- QWAC: A qualified website authentication certificate (QWAC certificate) is a qualified digital certificate under the trust services defined in the eIDAS Regulation. 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.

- QSEAL: A qualified Electronic Seal Certificate is a qualified digital certificate under the trust services defined in the eIDAS Regulation. 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.

- TLS: Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. Several versions of the protocols find widespread use in applications such as web browsing, email, instant messaging, and voice over IP (VoIP). Websites can use TLS to secure all communications between their servers and web browsers.

- TLS Handshake: This protocol is used to exchange all the information required by both sides for the exchange of the actual application data by TLS. It defines the format of messages and the order of their exchange. These may vary according to the demands of the client and server – i.e., there are several possible procedures to set up the connection. This initial exchange results in a successful TLS connection (both parties ready to transfer application data with TLS) or an alert message.

- HTTP Header: HTTP header fields are components of the header section of request and response messages in the Hypertext Transfer Protocol (HTTP). They define the operating parameters of an HTTP transaction and can be used to transmit information such as a signed header for the purpose of identifying a TPP as indicated above.

- Mutual TLS authentication or certificate based mutual authentication refers to two parties authenticating each other through verifying the provided digital certificate so that both parties are assured of the others' identity. In technology terms, it refers to a client (web browser or client application) authenticating themselves to a server (website or server application) and that server also authenticating itself to the client through verifying the public key certificate/digital certificate issued by the trusted Certificate Authorities (CAs). Because authentication relies on digital certificates, trusted certification authorities provide an issuing service to create these certificates, in the context of PSD2 there are specific providers that needs to be used “QTSP” Qualified Trust Service Providers that can issue the PSD2 eIDAS QWAC certificate used to identify the client as part of the TLS mutual authentication process. From a high-level point of view, the process of authenticating and establishing an encrypted channel using TLS mutual authentication involves the following steps:
  - A client requests access to a protected resource.
  - The server presents its certificate to the client and asks the client to present its certificate.
  - The client verifies the server’s certificate.
  - If successful, the client sends its certificate to the server.
  - The server verifies the client’s credentials.

If successful, the server grants access to the protected resource requested by the client