OPEN BANKING EUROPE

Understanding Internet Security & eIDAS Certificates

Open Banking Europe - providing collaborative services to support PSD2 Access to Account (XS2A), in partnership with the financial industry

Version: 001-004
Date: 18 January 2021
Classification: Closed User Group

Contents

1. About Open Banking Europe

Purpose

The revised Payment Services Directive (PSD2) came into force in January 2018, with a requirement deadline of 14 September 2019 to implement Strong Customer Authentication (SCA). At this point, all regulated entities (Payment Service Providers) had to ensure that they individually complied with PSD2 and the Regulatory Technical Standards (RTS) set out by the European Banking Authority (EBA).

There is a clear regulatory expectation that the financial industry will organise itself to make sure that the implemented solutions for PSD2 are interoperable. However, at the time of writing, there remains a number of outstanding activities required to successfully achieve this expectation.

Open Banking Europe was created to support Payment Service Providers (PSPs) and Third Party Providers (TPPs) in meeting the Access to Account (XS2A) requirements of PSD2 and to facilitate the wider aims of Open Banking.

History

Following a series of stakeholder consultations that started in 2016 to determine industry requirements, PRETA S.A.S. launched Open Banking Europe to build a PSD2 Directory solution to support PSPs and TPPs in meeting the PSD2 XS2A requirements. The Open Banking Europe Directory Service was released in January 2019, providing a single, standardised reference point for banks to accurately identify which TPPs are authorised to access their interfaces and which roles and services they are authorised to perform on behalf of their customers. Additionally, a Transparency Directory has been developed to help TPPs understand developer portals, and to help Account Servicing Payment Services Providers (ASPSPs) understand TPP brands. Open Banking Europe continues to work with stakeholders on a range of initiatives to facilitate a greater understanding of Open Banking and enable collaboration between interested parties. Open Banking Europe is a subsidiary of Konsentus Ltd.

Audience

Open Banking Europe is aimed at the following audiences:

- Competent Authorities
- Payment Service Providers (PSPs), including:
  - Account Servicing Payment Services Providers (ASPSPs)
  - Third Party Providers (TPPs)
- Qualified Trust Service Providers (QTSPs)
- Service Providers, Solution Providers, and relevant consultancies

Disclaimer

Whilst care has been taken to ensure that the information contained in this document is true and correct at the time of publication, there are still clarifications needed around PSD2's scope and implementation and this may impact on the accuracy of the information contained within this document.

As such, Open Banking Europe cannot guarantee the accuracy or reliability of any information contained within this document at the time of reading, or that it is suitable for your intended use.

2. About This Guide

Scope

This guide summarises the existing technology framework that is already in place in order to use certificates for website authentication and identity verification and enable secure Access to Account (XS2A) services in Europe, as required under the revised Payment Services Directive (PSD2).

It focuses on the standardisation of Electronic Identification, Authentication & Trust Services Regulation (eIDAS) Qualified Certificates for PSD2.

The following subjects are covered:

- Technology Standards Bodies
- Regulations & Standards
- Internet Communications
- eIDAS Qualified Certificates

Audience

This guide is aimed at the following audiences:

- National Competent Authorities (NCAs)
- Supervisory Bodies
- Qualified Trust Service Providers (QTSPs)
- Account Servicing Payment Services Providers (ASPSPs)
- Third Party Providers (TPPs)

References

This guide cites the following sources:

- The EBA RTS on Strong Customer Authentication & Common Secure Communications Under Directive 2015/2366 (PSD2)
- The Electronic Identification, Authentication & Trust Services Regulation (eIDAS)
- The Revised Payment Services Directive (PSD2)

For links to the above sources, please see the Bibliography on page 19.

Terminology

Access to Account (XS2A)
The provision of secure access to accounts operated by ASPSPs using APIs, in order to enable TPPs to provide Payment Initiation Services (PIS), Account Information Services (AIS), and Card Based Payment Instruments Issuing (CBPII) to customers.

Account Servicing Payment Services Provider (ASPSP)
An entity authorised to operate customer accounts, with a line of credit and payment facilities online.

Application Programming Interface (API)
A set of definitions, protocols, and tools that can be used to create applications, interact with other applications, and exchange data.

Certificate
An electronic 'passport' used to certify the identity of a person, machine, or organisation over the Internet.

Electronic Seal
An electronic 'signature' used by a legal entity to certify electronic documents as genuine.

European Banking Authority (EBA)
The body responsible for publishing the Regulatory Technical Standards (RTS), Implementing Technical Standards (ITS), and a central register for PSD2.

Member State Supervisory Body (MSSB)
A Supervisory Body in an EU Member State with the designated authority to regulate QTSPs.

Payment Service Provider (PSP)
An entity authorised to provide payment services to customers. PSPs include ASPSPs and TPPs.

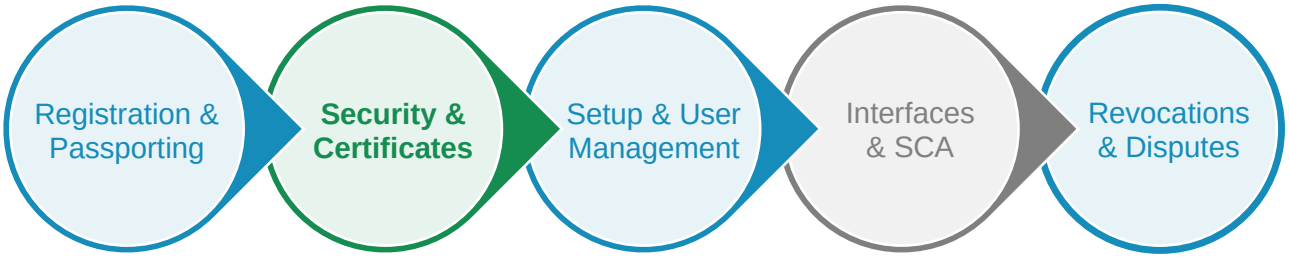
Payment Service User (PSU)
Either a payment account holder or payment payee.

Qualified Trust Service Provider (QTSP)
An entity permitted by MSSBs to issue Qualified Digital Certificates that are recognised across the EU.

Third Party Provider (TPP)
An entity authorised to access accounts on behalf of customers but that does not operate those accounts themselves. TPPs include PISPs, AISPs, and CBPIIPs.

Trust Service Provider (TSP)
An entity that provides digital services which enable the issuance and proving mechanisms to secure and protect information online. Examples include Certificates and Electronic Seals.

3. Overview



There is an existing technology framework in place to enable the use of certificates for website authentication & identity verification & enable secure XS2A services under PSD2 in Europe

Technology Standards Bodies

Both European and International organisations are contributing to the technology standards required to implement PSD2 and ensure a secure online payment services experience.

- The European Commission (DG CONNECT)
- The European Technology Standards Institute (ETSI)
- The International Organisation for Standardization (ISO)
- The National Certification Authority & Browser Forum (CA/Browser Forum)
- The Internet Engineering Task Force (IETF)
- The Institute of Standards & Technology (NIST)

➔ See **4. Technology Standards Bodies** on page 7

Regulations & Standards

Various regulations and standards are available that set out the Internet security and certificate requirements for implementing secure authentication and identification for Access to Account (XS2A):

- The Revised Payment Services Directive 2 (PSD2) sets out the general requirements for third party XS2A services on behalf of Account Servicing Payment Services Provider (ASPSP) customers.
- The EBA RTS for Strong Customer Authentication & Common Secure Communications Under PSD2 sets out the technical standards for identity and certificates to implement secure XS2A services.
- The Electronic Identification, Authentication & Trust Services Regulation (eIDAS) sets out the European Standards required for Trust Service Providers (TSPs) and the provision of trust services.

➔ See **5. Regulations & Standards** on page 9

Internet Communications

Two established sets of protocols can be employed in combination at various layers of the XS2A Communications Infrastructure in order to maximise security and maintain stability and interoperability:

- Transmission Control Protocols (TCP)
- Open Systems Interconnection (OSI) Protocols

➔ See **6. Internet Communications** on page 11

eIDAS Qualified Certificates

Qualified Certificates can be obtained from a Qualified Trusted Service Provider (QTSP) when setting up the XS2A services infrastructure, to maintain stability and interoperability and provide security:

- Qualified Website Certificates (QWACs) should be used for website authentication, so that ASPSPs and Third Party Providers (TPPs) can be certain of each other's identity.
- Qualified Electronic Seal (QSEAL) Certificates should be used for identity verification, so that transaction information is protected from potential attacks during or after a communication.

The use of Qualified Certificates must be standardised for PSD2, in line with the eIDAS regulation. By using eIDAS-conformant Trust Services and the appropriate technological protocols, all Payment Service Providers (PSPs) and Payment Service Users (PSUs) can be compliant and are provided with:

- Identification
- Confidentiality
- Authenticity/Integrity
- Non-Repudiation

➔ See **7. eIDAS Qualified Certificates** on page 13

4. Technology Standards Bodies

European Technology Standards Bodies

The European Commission (DG CONNECT)

DG CONNECT is the short term for the European Commission department for Communications Networks, Content & Technology.

The overall mission of DG CONNECT is to ensure that all European Union (EU) Member States provide and follow a baseline of Digital and Communications Technology standards within the EU. DG CONNECT creates legislation and regulations, which are adopted by the European Commission and passed to into law.

For the revised Payment Services Directive (PSD2), the area for certificates is under the remit of Directorate H: Digital Society, Trust & Cybersecurity.

Learn more about DG CONNECT's structure, governance, and remit on the DG CONNECT website[1].

The European Technology Standards Institute (ETSI)

ETSI is an independent industry body formed of technology providers within Europe.

ETSI is recognised by the European Commission as a market standardisation body that ensures that the regulations from the European Commission (DG CONNECT) are harmonised and operationally interoperable across the EU Member States.

ETSI also ensures that common security threats are collectively addressed, and that guidance or standards are officially published to prevent systemic issues in Europe.

ETSI provides an official community body for technology providers to assess and supply Europeans Standards (ENs), either in collaboration with the European Commission or with other technology standards bodies and International Organisation for Standardisation (ISO) Standards.

For PSD2, the area for certificates is under the remit of the Technical Committee for Electronic Signatures & Infrastructures (TC ESI).

TC ESI members are formed of Trust Service Providers (TSPs), Qualified Trust Service Providers (QTSPs), and government agencies from the EU Member States.

Learn more about ETSI's structure, governance, and remit on the ETSI website[2].

International Technology Standards Bodies

International Organisation for Standardization (ISO)

ISO is a global organisation that provides a baseline standard and harmonisation across the World and throughout many different industries.

New standards take a very long time to produce as ISO requires all countries (beyond the EU) to agree. In some cases, this can take years.

Some of the notable ISO Standards that are relevant to PSD2 include:

- ISO 3166-1: Country Codes
- ISO 4127: Currency Codes
- ISO 7498-1: Information Technology – OSI – Basic Reference Model
- ISO 7498: Information Processing – OSI – Basic Reference Model

Learn more about ISO's structure, governance, and remit on the ISO website[3].

Certification Authority & Browser Forum (CA/Browser Forum)

The CA/Browser Forum is a global standards body composed of Digital Certificate issuing and security companies, as well as the web browser companies that use certificates in their public applications.

Due to certificate use in relation to Internet security and secure data transmissions, these two groups

[1] See https://ec.europa.eu/info/departments/communications-networks-content-and-technology
[2] See http://www.etsi.org/
[3] See https://www.iso.org/

of companies regularly coordinate and sign up to a common code of conduct to operate effectively.

This partnership provides public Internet users with security, confidence, and ease of use when visiting websites and creating transactions such as payments, or providing personal data, (for example, by seeing the browser padlock symbol or getting warning messages about unsafe websites).

Additionally, the community formed within the CA/Browser Forum also allows for new threats and infrastructure issues to be identified quickly and addressed collectively.

The CA/Browser Forum is a global organisation and is fundamentally required to ensure that normal everyday users can access the Internet globally in the same way.

Both DG CONNECT and ETSI currently follow the guidelines from the CA/Browser Forum.

Learn more about the Forum's structure, governance, and remit on the CA/Browser Forum website[4].

Internet Engineering Task Force (IETF)

The IETF is an open public standards body that has developed heuristics and guides over many years, through Subject Matter Expert (SME) volunteer contributions, peer review, and market validation.

It is now trusted for providing the base principles for anyone trying to understand how Internet architecture or messaging schemes are applied.

The IETF publishes documents as 'Requests for Comment' (RFCs) which are peer reviewed and periodically updated. Because the Internet is reliant on core fundamentals, there are often some RFCs that have been in operation since the 1980s and are still in use today.

Some of the notable IETF RFCs that are relevant to PSD2 include:

- IETF 1180: A TCP/IP Tutorial
- IETF 3986: Uniform Resource Identifier (URI): Generic Syntax
- IETF 7231: Hyper Text Transfer Protocol (HTTP/1.1): Semantics and Content
- IETF 5246: The Transport Layer Security (TSL) Protocol
- IETF 2818: HTTP over TLS
- IETF 6749: The OAuth 2.0 Authorization Framework

Learn more about the IETF's structure, governance, and remit on the IETF website[5].

National Institute of Standards & Technology (NIST)

Although NIST is a United States Government body, many of the standards and documentation it publishes are accepted as being relevant to an international standard.

They are often quoted directly for the sake of efficiency (to not duplicate the writing efforts in the global technology standards communities), and to provide a level of interoperability between the United States and other territories.

NIST is used as a reference in the EU, but may be superseded by European Standards, such as those published by ETSI.

Some of the notable NIST standards that are relevant to PSD2 include:

- NIST Special Publication 800-52: Guidelines for the Selection, Configuration, and Use of TLS Implementations
- NIST Special Publication 800-63: Digital Identity Guidelines

Learn more about NIST's structure, governance, and remit on the NIST website[6].

[4] See https://cabforum.org/
[5] See https://www.ietf.org/
[6] See https://www.nist.gov/

5. Regulations & Standards

The Revised Payment Services Directive 2 (PSD2)

Reference: Directive (EU) 2015/2366

For the most part, PSD2 concerns the individual actions for Payment Service Providers (PSPs) in relation to their own regulations and operations.

However, Articles 65, 66, 67, 97, and 98 of PSD2 detail the general requirements for third party Access to Account (XS2A) services on behalf of Account Servicing Payment Services Provider (ASPSP) customers. These Articles point to the European Banking Authority (EBA)'s 'Regulatory Technical Standards (RTS) for Strong Customer Authentication and Common Secure Communications (SCA/SCS)' for further specific implementation requirements.

The EBA RTS for Strong Customer Authentication & Common Secure Communications Under PSD2

Reference: EBA RTS for SCA/CSC Under PSD2

The EBA RTS for SCA/CSC Under PSD2 is derived from PSD2 and sets out the conditions for:

- Customer Authentication
- Interfaces Requirements
- Data Exchanges
- Secure Identity & Communications

The key articles for identity and certificates are:

- Article 30.3: International or European Communication Standards
- Article 34: eIDAS Certificates for Identification
- Article 35: Security of the Communication Session
- Article 36: Data Exchanges

Within Article 34, the EBA points to eIDAS for standardisation, but introduces further data requirements above the existing international technology standards bodies.

The EBA has also published an Opinion of the European Banking Authority on the use of eIDAS certificates under the RTS on SCA and CSC.

The Electronic Identification, Authentication & Trust Services Regulation (eIDAS)

Reference: Regulation (EU) 910/2014

The eIDAS regulation sets the standards across the European Union (EU) required for Trust Service Providers (TSPs) and the provision of trust services through technical mechanisms, such as Digital Certificates and Cryptographic Signatures.

Trust Service Providers (TSPs)

TSPs are commercial organisations or government entities that provide digital services which enable the issuance and proving mechanisms to secure information from official sources and protect it against tampering in transit. This means users can 'trust' the information within these digital artefacts.

Qualified Status

A 'Qualified' status can be awarded to those TSPs that want to undergo national accreditation under eIDAS with their regulator through a written 'Conformity Assessment'.

This 'Qualified' status is intended to provide the European Market with a reliable standard that ensures a base level of confidence when choosing a trust service supplier, allows a Qualified Trust Service Provider (QTSP) to provide their services in other EU Member States, and guarantees a level of interoperability across the European trust infrastructure.

For certain services, such as Government Identity, a Member State may require that only a QTSP can provide that service, and in some cases the government itself may be the QTSP, meaning that no external parties are involved with the provision of that service (for example, passports).

To learn how to search for and display a list of QTSPs, please see the Appendix on page 21.

Member State Supervisory Bodies (MSSBs)

As set out in Article 17 of eIDAS, QTSPs are regulated by each EU Member State, under an appointed MSSB. These MSSBs are similar to the National Competent Authorities (NCAs) under PSD2 and cooperate cross-borders, as well as with other regulatory bodies in the case of incidents, for example, data breaches.

Non-QTSPs have 'light touch' regulation applied but come under the authority of an MSSB in the case of incidents involving trust services within that Member State.

Liability

All TSPs are bound by Article 13 of eIDAS to provide clear limitations for which their trust services may be used, and to assume a liability for any damage caused intentionally or negligently, or a failure to comply with eIDAS.

In the case of non-QTSPs, this liability will still apply in the case of the non-qualified services and the limitations they provided.

ETSI Technical Standard 119 495

Reference: Regulation (EU) 910/2014

The profiles and further requirements of both QWACs and QSEALCs are detailed within eIDAS[7].

ETSI is often tasked with technical (rather than legal) matters where strict technology standards are required and produce a European Standard (EN) document that becomes accepted as the European standard for that technology.

Given the new and industry-specific changes required in Article 34 of the EBA RTS for SCA/CSC Under PSD2 to support Financial Entity Identification (in relation to Articles 14 and 15 of PSD2), a new Digital Certificate profile work effort has been undertaken by ETSI, in order to align all EU/EEA countries.

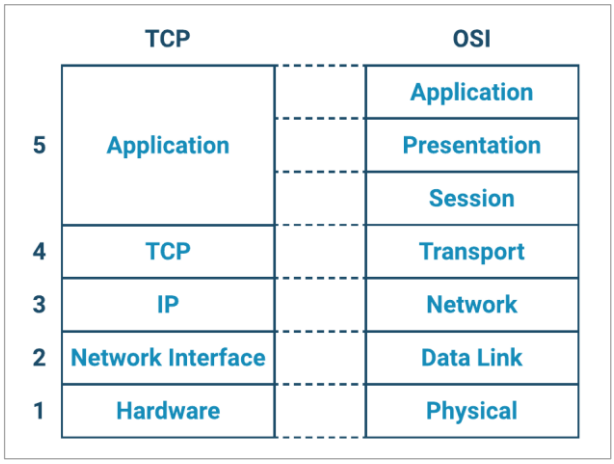
Following initial recommendations made by the financial industry through the Euro Retail Payments Board (ERPB), ETSI has created TS 119 495

In addition to the existing certificate standards for QWACs and QSEALCs, (which can be viewed on their website[8]), additional amendments for PSD2 have been created based on the requirements of PSD2 and the EBA RTS for SCA/CSC Under PSD2.

[7] See Annexes III & IV, Regulation (EU) 910/2014
[88] See https://portal.etsi.org/tbsitemap/esi/trustserviceproviders.aspx

6. Internet Communications

Transmission Control Protocol (TCP) & Open Systems Interconnection (OSI) Communications Layer Models



When two machines talk over the Internet, there is an established set of standard protocols that allow global common communications. These protocols provide a framework to discuss security and identity procedures at the relevant level:

- The Transmission Control Protocol (TCP) model was the first model defined of the two and is cited in the Internet Engineering Task Force (IETF) Requests for Comment (RFCs) (see IETF 1180: A TCP/IP Tutorial).
- The Open Systems Interconnection (OSI) model is a later, more defined model and is now detailed as an International Organisation for Standardisation (ISO) Standard (see ISO 7498-1: Information Technology - OSI - Basic Reference Model).

However, both models are abstractions and, for security reasons, the layers in both are used in combination and in sequenced protocols.

Communications Protocols & Identifiers

As OSI is more detailed, there are several protocols and identifiers that are used at various layers of Internet communications that should be explained in relation to Access to Account (XS2A) and Internet banking:

1. Data Link: The device or machine has a Media Access Control Address (MAC Address), which is unique to that machine.
2. Network Layer: An Internet Protocol Address (IP Address) is assigned by the network at this layer, which uniquely identifies that machine within that network for that connection.

   As the network is tied to a specific physical infrastructure and antennas (unless hidden by the user or network), the physical location of a machine can almost always be found by looking at the machine's IP Address and the physical provider's Network Address.

   You can see an example on findmyaddress.com.
3. Transport/Session Layer: The Transport Layer Security (TLS) Protocol can be used at this layer, as an update from the older Secure Sockets Layer (SSL) description, although both are still used interchangeably.

   SSL was originally developed by Netscape in 1994, to enable secure ecommerce transactions through its own browser. It has since been adopted by most major browser companies and standardised by the IETF many times.

   To learn more about the history of SSL/TLS (and why there are now Qualified and Non-Qualified Trusted Service Providers (TSPs) under eIDAS), see Feisty Duck's SSL/TLS and PKI History[9].

   The main benefits of SSL/TLS are:

   - Identification (Confidentiality)
   - Encryption

   When using the Internet there are two parties involved, where initially neither knows who the other really is - one entity could claim that they are someone, but how might the other trust this new and unknown Internet entity?

   - By using a Domain Name Registry and a Public Key Infrastructure (PKI) Signature, a Digital Certificate can be created using cryptography, and an Internet entity can be

[9] See https://www.feistyduck.com/ssl-tls-and-pki-history/

assigned a unique, human readable Identifier (a Domain Name) and prove that they are who they say they are by using a Digital Signature that only they know.

- These Digital Certificates are issued by TSPs, who have the tools necessary to handle cryptographic materials that are industry-recognised as secure.
- If both parties independently trust the TSP, and both obtain a Digital Certificate from the TSP, then each can check the other's certificate with the third party TSP and be sure of each other's identity.
- If both communication parties trust each other and use Digital Certificates (PKIs), they can talk to each other in confidence and exchange secure data in a secure session.
- As an additional benefit, now that the identity of the website can be validated, a human user will see a Trust Mark (browser padlock symbol) in the web browser, that shows to the user that the entity behind a web address is who they say they are.

4. Presentation Layer: Any encryption or decryption of a message usually takes place at this layer, provided that the SSL/TSL was completed successfully. Additionally, any message conversions or data translation can take place at this layer, allowing a message to be displayed for consumption or displayed in the application.
5. Application Layer: There are many protocols that can be used at this layer. Some of the key ones are:

- Domain Name Service (DNS): Instead of IP Addresses, an application can convert the IP Address to a Domain Name and a Domain Name to an IP Address. This allows a human user to find an Internet location by typing in an alphanumeric name, rather than a complicated numeric IP Address.

  For example, you can see the IP Addresses assigned to Google in Lifewire's The IP Addresses Used by Google[10].

- Security for Web Browsers: If the SSL/TLS Protocol has been used, a human user can use a web browser to see that the website is secure through its Trust Mark (browser padlock symbol) and be assured that they can provide sensitive information within the browser to that website.
- Security for APIs: Where there is no human user involved, two machines may be talking over the Internet through Application Programming Interfaces (APIs). Provided that the protocols described above have been used, the two machines can exchange messages securely. This may involve an additional exchange of security information and other access credentials to further ensure that an entity connecting to an API resource is known to the resource owner.
- Additional Security Measures: Further security for specific transactions or functions can be added at the Application level, for example, Strong Customer Authentication (SCA) or Third Party Identity Checking. These measures are independent from the communications protocols and layers discussed above and are specified by the application resource owner, specific to their service.

[10] See https://www.lifewire.com/what-is-the-ip-address-of-google-8181

7. eIDAS Qualified Certificates

eIDAS Qualified Certificates & Their Legal Effect on the Financial Services & PSD2

The Electronic Identification, Authentication & Trust Services Regulation (eIDAS) is legislation that provides a backbone of legal certainty and assurance through technical and operational requirements in the EU's Digital Trust Services Market. It gives all industries that conform to eIDAS (and industry security protocols) a definitive baseline, with legal responsibilities and clear definition of liabilities, boosting confidence and security for all actors within the EU Digital Trust Services Market.

Financial services are one of the most critical markets, with constant threats of fraud and security risk, and PSD2 is creating a new Digital Financial Services Market (along with new actors in the ecosystem). It is therefore important that the European Banking Authority's 'Regulatory Technical Standards for Strong Customer Authentication & Common Secure Communications Under PSD2' (EBA RTS for SCA/CSC Under PSD2) eIDAS requirements are adhered to, so that all Payment Service Providers (PSPs) and Payment Service Users (PSUs) are protected when conducting business online. For PSPs to be able to trust each other within the Access to Account (XS2A) transaction chain, all PSPs should implement and adhere to the same rules, to give the same legal confidence in any communication and transaction. eIDAS, as a common, legally applicable, EU-wide framework, also enables this to work in cross-border scenarios with non-standard certificates, instead of nationally deviated or proprietary identification and security models.

The 'Qualified' status of Trust Service Providers (TSPs) under eIDAS also gives legal confidence at a national level for a QTSP to have been assessed as legally and technically competent. These 'Qualified' TSPs can then be distinguished from other TSPs as being capable under EU law of providing a regulated service, whilst being able to address any issues in a legal manner with agreed liability. In some cases, this also requires the mandated gratis provision of certain services by the QTSPs, for which the PSP should not pay.

Whilst an Account Servicing Payment Services Provider (ASPSP) is free to accept any certificate as proof of a Regulated Entity's identity in order to give XS2A access, if the TSP and certificates used are not qualified under eIDAS:

- The PSP will be afforded no legal protection as it is actively choosing to step outside of eIDAS and would have to make additional legal arrangements for this.
- The PSP would not be compliant with the requirements to use Qualified Certificates, as set out in EBA RTS for SCA/CSC Under PSD2[11].
- An enforced use of a non-eIDAS certificate and protocols may be seen as non-conformant with EBA RTS for SCA/CSC Under PSD2[12], risking the loss of National Competent Authority (NCA) approval for interface exemptions.
- The PSP may not be technically or legally recognised by other PSPs or cross-borders, if using proprietary or non-eIDAS certificates, which may be sufficient grounds to deny access to PSD2 Interfaces.
- The format and structure of the Qualified Electronic Seal Certificates (QSEALCs) may be different than expected and require additional processing and routines to verify the certificate's contents. This will elicit increased costs and security risks/exposure for those PSPs using the certificates.

By using eIDAS-conformant trust services and the appropriate technological protocols, all PSPs and PSUs can be compliant and are provided with:

- Identification
- Confidentiality
- Authenticity/Integrity
- Non-Repudiation

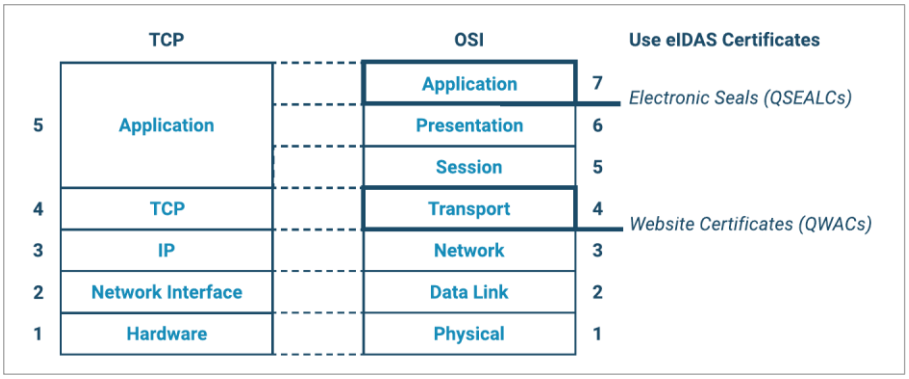
[11] See Article 34, EBA RTS FOR SCA/CSC Under PSD2
[12] See Article 32.3, EBA RTS FOR SCA/CSC Under PSD2

Qualified Certificates & Their Use at Each Communication Layer

Whilst it is possible to use any technology for new purposes, there are already existing precedents and TSPs that are in use today.

- Qualified Website Authentication Certificates (QWACs) provide a method to authenticate 'Internet Entity Identity' and encrypt communications in order to provide confidentiality. QWACs are used with specific protocols at the Transport Layer and are not designed to be used at the Application Layer.
- Qualified Electronic Seal Certificates (QSEALCs) are not designed to be used for 'Internet Entity Identity' or confidentiality at the Transport Layer for Transport Layer Security (TLS) or Mutual Authentication/ Transport Layer Security (MA/TLS). However, a QSEALC can be used at the Application Layer, with the messages being passed between communicating parties to prove origin, authenticity, and integrity that the data comes from the party that it is meant to. Additionally, due to the nature of QSEALC and EBA RTS for SCA/CSC Under PSD2 requirements needing information about the 'Legal Persons Owner' of that certificate, it can be used to establish the PSD2 'Financial Entity Identity' (as opposed to the 'Internet Entity Identity' in the QWAC).

Adhering to existing protocols and certificates enables the industry to maintain a level of stability and interoperability, when setting up the XS2A communications infrastructure. The two 'common' communications layers that are of interest for XS2A are the Transport Layer and Application Layer.



There are two different layers where two different certificates are used to check for different information and to use different protocols in combination.

Qualified Website Authentication Certificates (QWACs) at the Transport Layer

Under eIDAS, a QWAC is the legal term for the existing certificates that are issued under the Certification Authority & Browser Forum's standards for Extended Validation Secure Socket Layer (EV SSL) Certificates. The CA/Browser Forum website[13] states that EV SSL Certificates have primary and secondary objectives:

The primary objectives of an EV SSL Certificate are to:

1. *Identify the legal entity that controls a web site by providing reasonable assurance to the user of an Internet browser that the web site the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information; and*
2. *Enable encrypted communications with a web site by facilitating the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a web site.*

The secondary objectives (which are derived from the primary) are to help establish the legitimacy of an entity claiming to operate a Web site, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware, and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the entity, EV SSL Certificates may help to:

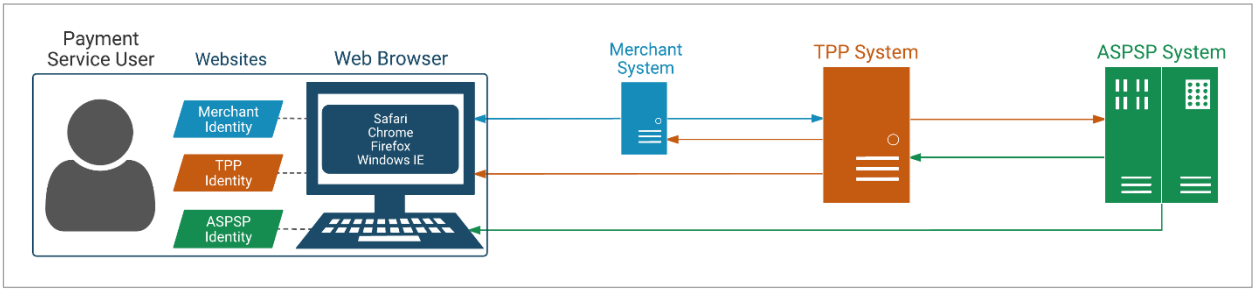
1. *Make it more difficult to mount phishing and other online identity fraud attacks using Certificates;*
2. *Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users; and*
3. *Assist law enforcement organizations in their investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the entity.*

[13] See https://cabforum.org/about-ev-ssl/

As set out in the EBA RTS for SCA/CSC Under PSD2[14], the use of QWACs will enable the following primary objectives:

1. Clear identification of all of the entities that are communicating with each other:

   a. To a PSU through a web or mobile browser,
   b. To a TPP from either a Merchant or the ASPSP,
   c. To an ASPSP through a connection over the Internet.



A Merchant website may also be the actual starting point for a transaction or data request from the PSU. Therefore, that Merchant Website is another entity in the communication chain. The Merchant (or fourth party) may also use a website authentication certificate with their legal entity recorded. However, this is not explicitly stated in the EBA RTS for SCA/CSC Under PSD2.

This authentication of identification, performed by all parties, such as between:

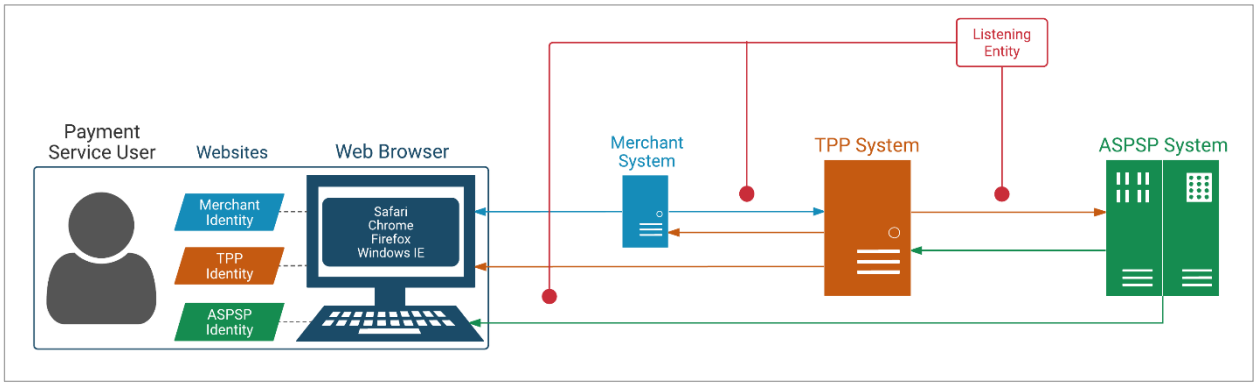
- the PSU to any party
- the Merchant to the TPP
- the TPP to the ASPSP
- the ASPSP to the PSU

ensures that everyone is communicating with the intended legal entity, and that there is no misdirection of communication, or disclosure of information, to any unintended party.

Active malicious entities trying to pretend or misrepresent themselves as another legal entity in order to gain information is commonly known as 'Phishing'. Phishing is mitigated by the use of QWACs, as the entity's identity can be authenticated and presented to PSUs with a browser padlock symbol, which provides high confidence. Web browser companies actively monitor for phishing attempts and will often advise PSUs of 'unsafe websites' by using in-built messages and/or alerts or preventing the PSUs or other entities from continuing a communication session.

2. Confidentiality of any messages passed between entities (including codes or the PSU's personalised security credentials)

   Many malicious actors who cannot 'phish' and pretend to be a legitimate legal entity to receive sensitive information, will instead try to 'listen' in as a passive entity during a communication session over the Internet. Imagine participating in a telephone conference call and speaking as if having called the attendees directly, but not knowing how many other listeners are also present on the line.



In order to protect against these 'listeners', encryption can be put in place by the two communicating

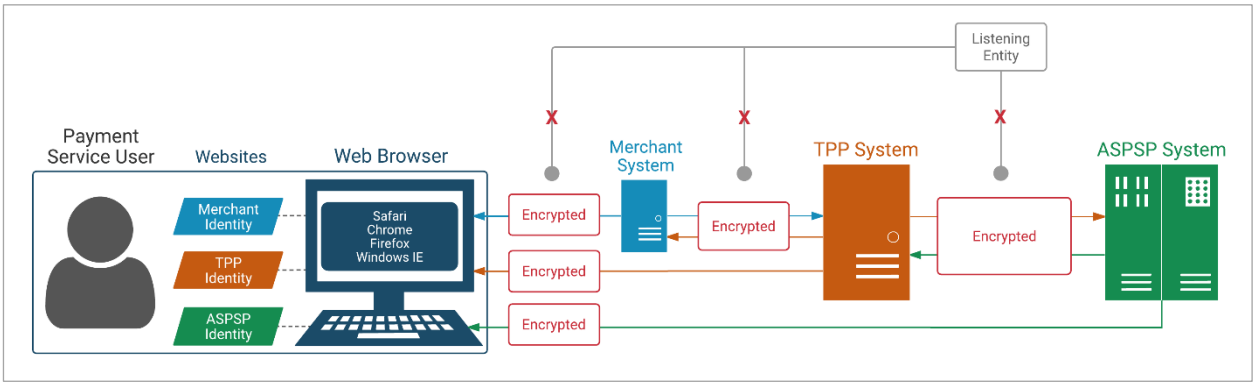
[14] See Articles 1, 22 & 34, EBA RTS for SCA/CSC Under PSD2

parties, so that only those two intended communicating parties can read what is being exchanged in that communication session.

The use of Transport Layer Security (TLS), or the more secure Mutual Authentication/Transport Layer Security (MA/TLS), ensures that a consistent and globally applicable security standard can be applied and is expected of both communicating parties.

More details about TLS can be found in IETF 5246: The Transport Layer Security (TSL) Protocol.

The correct use of TLS or MA/TLS effectively blocks any 'listeners' from being able to see the messages being exchanged between either of the two parties and ensures the confidentiality of the communication session between the two parties, in line with EBA RTS for SCA/CSC Under PSD2 requirements[15].



MA/TLS is the most recent protocol and provides a stronger encryption method than normal TLS, as it combines the secret keys of both parties to form a unique encryption specific to those two parties communicating. MA/TLS encryption requires both parties to have certificates (which can be QWACs) and to exchange associated secrets which are agreed to be used, before the actual communication session begins.

Previously for SSL and early TLS, an SSL Certificate required the Internet entity 'role' to be stated within the certificate as either a 'Client Certificate' or a 'Server Certificate'. However, the new CA/B Extended Validation (QWAC) Standard is now a dual-role certificate and can be used in either capacity by the communicating entity, with any SSL or TLS protocol.

As QWACs are required in the EBA RTS for SCA/CSC Under PSD2 by all PSPs for communicating, it is advisable to for them to obtain this new EV Certificate and also to implement the MA/TLS protocol in their systems.

PSD2-specific QWAC profile specifications, based on CA/B EV Certificates but conformant to eIDAS requirements in the EU, are being drafted by the European Technology Standards Institute (ETSI), to accommodate the EBA RTS for SCA/CSC Under PSD2 requirements for the new PSD2 regulatory data elements within the certificate itself, so these should be obtained once QTSPs have adopted the PSD2 Profile Specifications. The new PSD2-specific QWAC Profile Specifications are being drafted in such a way that they will operate as normal in any Internet communication session as a generic EV/QWAC would be expected to operate.

Qualified Electronic Seal Certificates (QSEALCs) at the Application Layer

A QSEALC is the eIDAS term for a Digital Certificate with associated Public Key Infrastructure (PKI) Signatures. A QSEALC's uses are varied and can be applied to a wide range of use cases. However, they are generally used to demonstrate the origin/author, authenticity, and integrity of any data being transmitted.

This data can be in many digital forms (for example, PDFs, JPEGs, or general form message text) but within the context of PSD2, the ability for all parties to be sure of the origin, authenticity, and integrity of data provides a legal basis (under eIDAS) to support non-repudiation in the cases of issues, suspected fraud, or other issues requiring investigation and resolution.

Without QSEALCs and PKI Signatures supported by the legal framework under eIDAS, PSUs, TPPs and ASPSPs would find it very difficult to establish proof and liability for any XS2A API transactions, should those transactions be later challenged.

Using QSEALCs to Prove a TPP's Identity for Access to APIs

Assuming that a TPP provides the ASPSP with a QSEALC, issued by a known QTSP under eIDAS, that

[15] See Articles 1(c), 5.2, 22.1, 30.2(c) & 35.1, EBA RTS for SCA/CSC Under PSD2

ASPSP can be sure of the Regulated Entity's identity as the owner of that QSEALC, and also save the Digital Signature associated with that certificate for any future transactions.

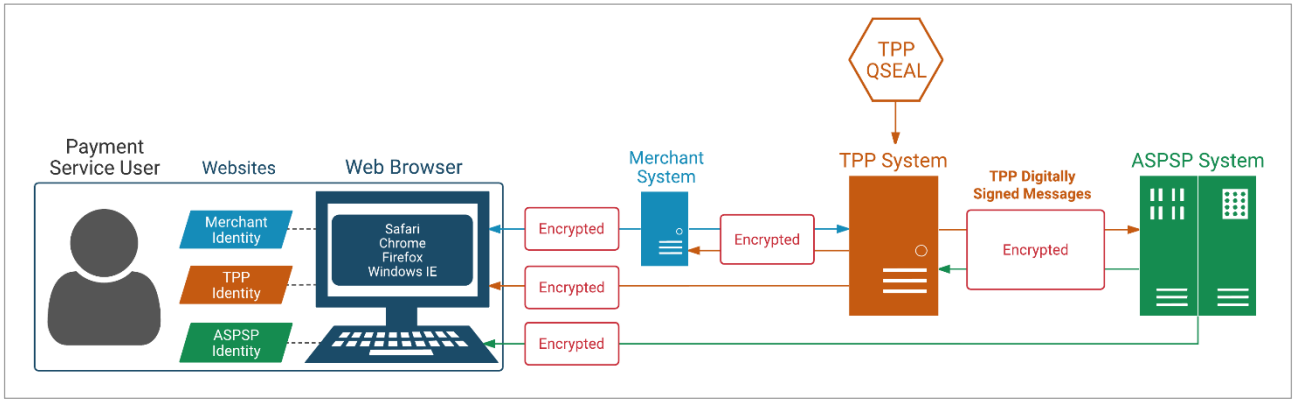
At this stage, it is advisable for the ASPSP to provide their own QSEALC to the TPP (which the TPP should also save), so that all messages from the ASPSP to the TPP (such as a payment instruction confirmation) can be signed by the ASPSP. This provides the TPP with the same non-repudiation legal effects under eIDAS.

The certificates can be passed each time they are requested by a relying party in an API. However, in modern computing, a Digital Certificate at the Application Layer can be stored by the relying party, then a verification of status and PKI signature can be used to check against it. This significantly reduces the size and complexity of API messages at the Application Layer and reduces the cost of calculating the cryptography involved, both of which save the PSP's overall IT costs.

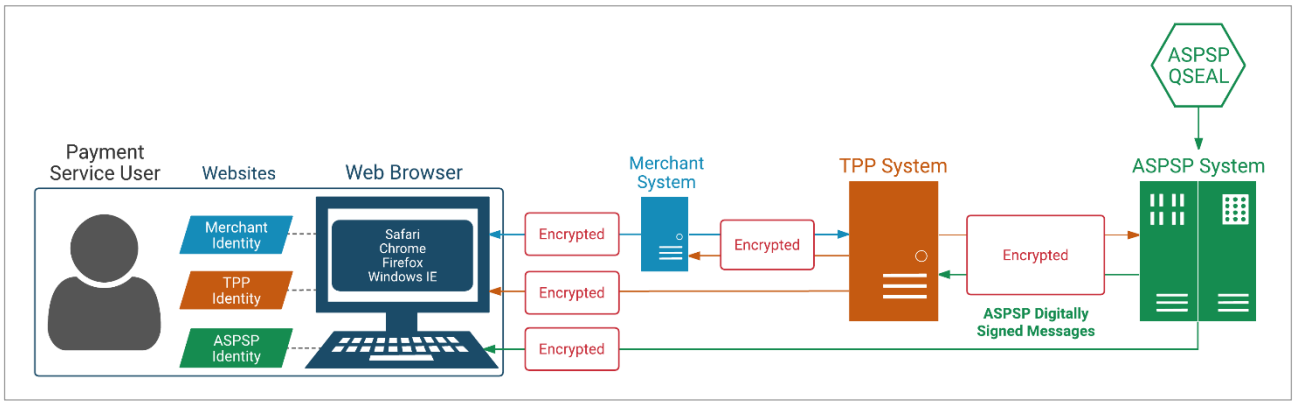
Using QSEALCs to Prove the Authenticity & Integrity of Transaction Messages

Once API access is given to a TPP, based on their authorised payment services and their passporting rights, the TPP can conduct Payment Initiation Services (PIS), Account Information Services (AIS), and Card Based Payment Instruments Issuing services (CBPII) and should sign each and every API message with the Digital Signature associated with the original TPP QSEALC that was provided, along with a timestamp for each API message as required in EBA RTS for SCA/CSC Under PSD2[16].

This ensures that the TPP is authenticating the integrity of the message it is passing to the ASPSP and can also be used as a legal proof record by the ASPSP later.



The ASPSP should also sign any API messages back to the TPP, using their QSEALC, so that the TPP is assured of the authenticity/integrity of the message, and can use it as a record of legal proof later.

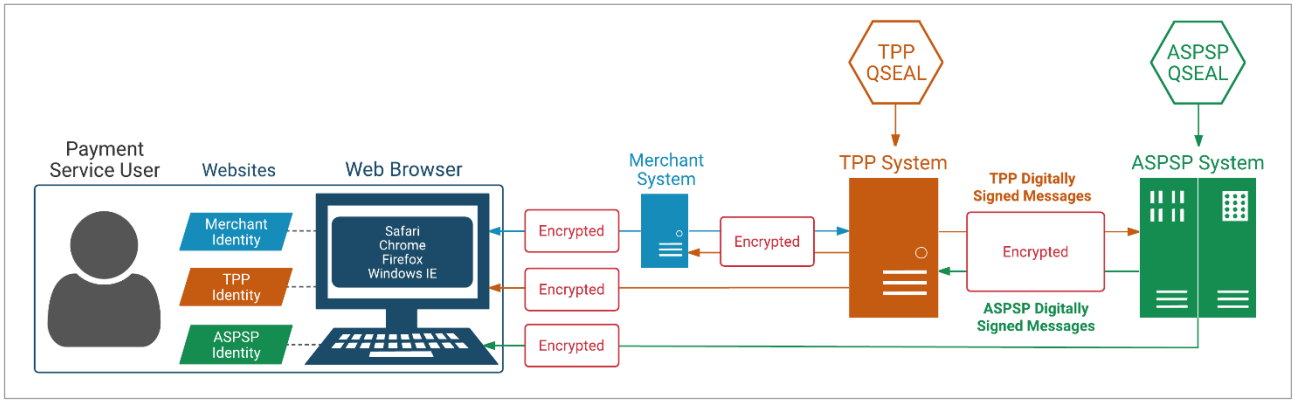


Combining QWAC & QSEALC Use for PSD2 XS2A Transactions

By providing both confidentiality by using QWACs and authenticity/integrity by using QSEALCs, all PSPs performing XS2A transactions can have confidence in both those transactions and any subsequent issues

[16] See Article 29.2, EBA RTS for SCA/CSC Under PSD2

that may occur, whilst also fulfilling EBA RTS for SCA/CSC Under PSD2 requirements[17].



PSUs & Digital Signatures

Digital Signing Device mechanisms that can be issued by ASPSPs to their PSUs for the purpose of SCA are not within the scope of PSD2 or Open Banking Europe's work.

[17] See Articles 1(c), 5.2,22.1, 30.2(c) & 35.1, EBA RTS for SCA/CSC Under PSD2

Bibliography

More information about Internet Security and eIDAS Certificates can be found at the following sources:

Technology Standards Bodies

- The European Commission (DG CONNECT)
  https://ec.europa.eu/info/departments/communications-networks-content-and-technology
- The European Technology Standards Institute (ETSI)
  http://www.etsi.org/
- International Organisation for Standardization (ISO)
  https://www.iso.org/
- Certification Authority & Browser Forum (CA/Browser Forum)
  https://cabforum.org/
- Internet Engineering Task Force (IETF)
  https://www.ietf.org/
- National Institute of Standards & Technology (NIST)
  https://www.nist.gov/

Regulations & Standards

- The Revised Payment Services Directive (PSD2 - Directive (EU) 2015/2366)
  http://eur-lex.europa.eu/eli/dir/2015/2366/oj
- The EBA RTS for Strong Customer Authentication & Common Secure Communications Under PSD2
  https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389
- Opinion of the European Banking Authority on the use
  of eIDAS certificates under the RTS on SCA and CSC
  https://eba.europa.eu/documents/10180/2137845/EBA+Opinion+on
  +the+use+of+eIDAS+certificates+under+the+RTS+on+SCACSC.pdf
- The Electronic Identification, Authentication & Trust Services Regulation (eIDAS)
  http://data.europa.eu/eli/reg/2014/910/oj
- European Technology Standards Institute (ETSI) Standards:
  - ETSI European Standards (EN)
    http://www.etsi.org/standards/different-types-of-etsi-standards
  - ETSI ENs on Certificates
    https://portal.etsi.org/tbsitemap/esi/trustserviceproviders.aspx
  - ETSI TS 119 495: Qualified Certificate Profiles and TSP Policy
    Requirements under the payment services Directive (EU) 2015/2366
    https://www.etsi.org/standards-search#page=1&search=TS119495
- International Organisation for Standardisation (ISO) Standards:
  - ISO 3166-1: Country Codes
    https://www.iso.org/iso-3166-country-codes.html
  - ISO 4127: Currency Codes
    https://www.iso.org/iso-4217-currency-codes.html
  - ISO 7498-1: Information Technology - OSI - Basic Reference Model
    https://www.ecma-international.org/activities/Communications/TG11/s020269e.pdf
  - ISO 7498-2: Information Processing - OSI - Basic Reference Model
    https://Webstore.iec.ch/preview/info_iso7498-2%7Bed1.0%7Den.pdf

- Internet Engineering Task Force (IETF) Requests for Comment (RFCs):
  - IETF 1180: A TCP/IP Tutorial
    https://tools.ietf.org/html/rfc1180
  - IETF 3986: Uniform Resource Identifier (URI): Generic Syntax
    https://tools.ietf.org/html/rfc3986
  - IETF 7231: Hyper Text Transfer Protocol (HTTP/1.1): Semantics and Content
    https://tools.ietf.org/html/rfc7231
  - IETF 5246: The Transport Layer Security (TSL) Protocol
    https://tools.ietf.org/html/rfc5246
  - IETF 2818: HTTP over TLS
    https://tools.ietf.org/html/rfc2818
  - IETF 6749: The OAuth 2.0 Authorization Framework
    https://tools.ietf.org/html/rfc6749
- National Institute of Standards & Technology (NIST) Special Publications:
  - NIST Special Publication 800-52: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
    https://csrc.nist.gov/publications/detail/sp/800-52/rev-1/final
  - NIST Special Publication 800-63: Digital Identity Guidelines
    https://pages.nist.gov/800-63-3/

Other Sources

- Feisty Duck's SSL/TLS and PKI History
  https://www.feistyduck.com/ssl-tls-and-pki-history/
- Lifewire's The IP Addresses Used by Google
  https://www.lifewire.com/what-is-the-ip-address-of-google-8181

Appendix

Qualified Trust Service Providers (QTSPs)

As set out in Article 4 of the eIDAS regulation, Trust Services Providers (TSPs) can freely passport their services within the European Union (EU), without the need for additional confirmation.

There is a website through which you can search for TSPs offering certain types of service, including issuers of Qualified Website Authentication Certificates (QWACs):

https://webgate.ec.europa.eu/tl-browser/#/

1. On the *Which type of service?* page, select **Search trust services**.
2. Check the **Qualified certificate for website authentication** box or the **Qualified certificate for electronic seal** box.
3. Select **Next step** near the bottom of the page.
4. On the *Which step?* page, check the **Check all** box (to select all countries).
5. Select **Search** near the bottom of the page to display the *Your trust service providers results* page, showing a list of all of the QTSPs issuing QWACs in the EU: