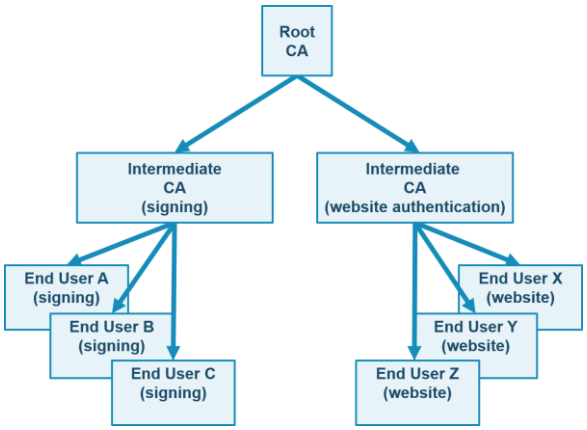
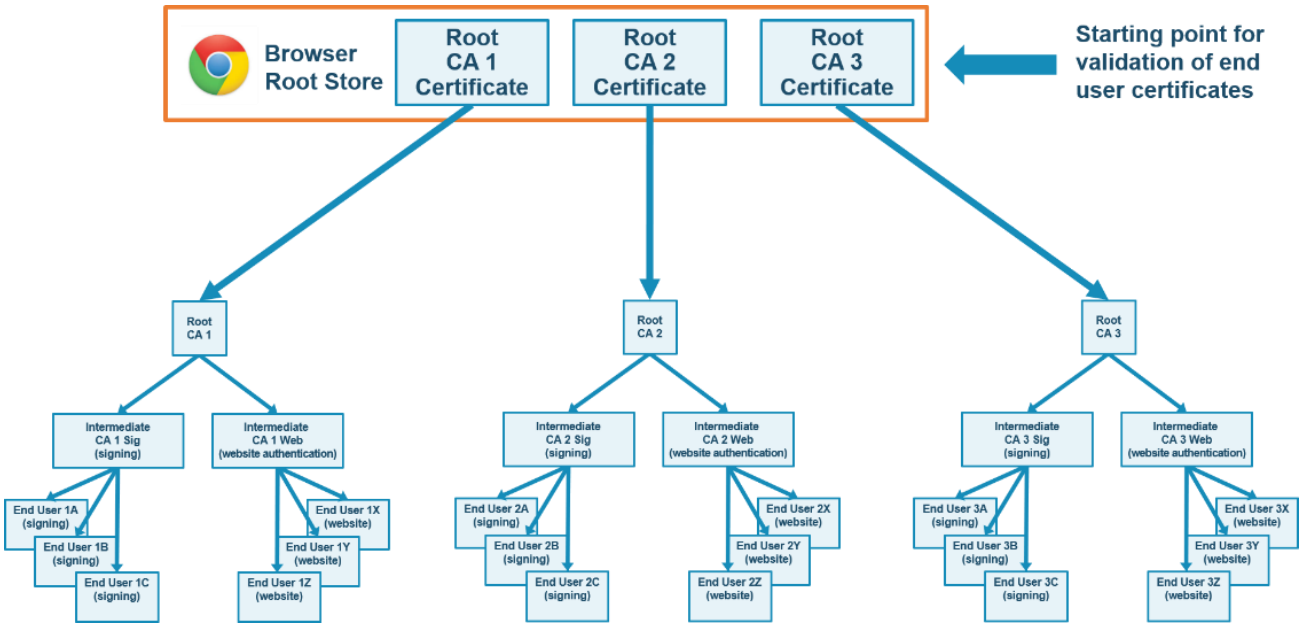
EU Trust Anchors vs Commercial Root Certificates: A Comparison in Approaches

Recently Open Banking Exchange Europe (OBE) has received several enquiries around how trust is managed in the EU for PSD2 security and how this differs from that conventionally used by commercial applications such as web browsers. The following description is aimed at illustrating the difference.

The trust in identities for PSD2 is based on well-established technology called public key certificates (or just certificates) that are used to prove the identity of PSD2 payment service providers. Certificates are issued by Certification Authorities (CA) which are commonly organised in a hierarchy with a 'root CA' certifying the 'intermediate CAs' that issue certificates for different purposes. This is illustrated in the example below with a Root CA certifying two Intermediate CAs: one intermediate CA issues certificates for identifying the creator of a digital signature, another issues qualified certificates for authenticating a website.



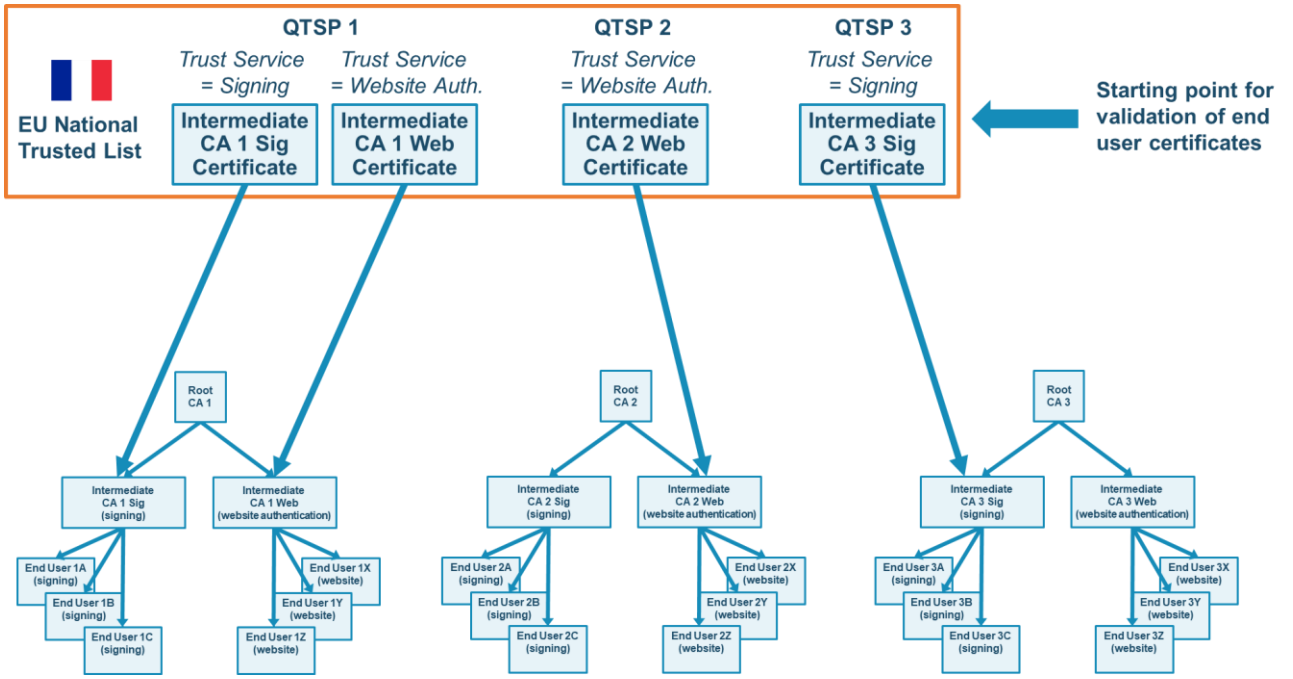
Application platforms, such as web browsers, accept certificates coming from different CA hierarchies managed by different trust service providers. The application platform maintains a 'Root Store' which holds lists of 'Root CA' certificates for trust service providers it trusts. In order to validate an identity certified by one of the trust service providers, the application finds the Root CA relating the end-user certificate provided and checks if it can be validated starting from the corresponding Root CA in its Root Store. This is illustrated in the following diagram:



OBE S.A.S, 40 Rue de Dunkerque, F-75010 Paris
E : membership@openbanking.exchange W: www.openbanking.exchange

V002-000 | 060622 | Classification: Member
Capital Autorisé: 1.605.000 € | RCS Paris 880 143 896 | No TVA: FR 35 880 143 896

The EU, under the eIDAS regulation ((EU) No 910/2014), has adopted a different approach which provides a greater degree of control of trust. This approach is based around 'Trusted Lists' issued by each EU nation with 'trust anchors' for each service supported. Certificates based on EU Trusted Lists are referred to as 'Qualified Certificates'. Whilst these trust anchors can be 'Root CA' certificates, commonly they hold intermediate CA certificates which enable finer control of which end-user certificates are to be trusted. This is illustrated in the following diagram:



In the above example, the French trusted list authorises TSP (Trust Service Provider) 1 for issuing Qualified Certificates for both signing and website authentication. Whilst TSP 2 is only authorised for issuing website authentication certificates and TSP 3 is only authorised for issuing Qualified Certificates for signing. By using trust anchors lower in the CA hierarchy, certificates aimed at signing from TSP 2 cannot be used, and similarly, certificates from TSP 3 aimed at website authentication cannot be used. Whereas with the conventional Root Store approach, the application cannot be stopped from using certificates for the purpose for which it has not been authorised.

The approach adopted in the EU trust framework is in line with the recognised standard for signature validation RFC 5280 which requires that validation starts at a trust anchor, not a root CA certificate, and eIDAS requires that validation starts at the trust anchor as in the EU trusted list not at any higher root CA certificate.

In the PSD2 world, the validation of certificates is often implemented in a PSD2 portal which validates all incoming messages. The confusion over the difference in the approach being applied in the EU is sometimes causing difficulties with the front end implementation looking for a root certificate as the basis for certificate validation rather than accepting a trust anchor from an intermediate CA as the starting point certificate validation. This potentially could cause messages to be unnecessarily rejected as invalid.

OBE S.A.S, 40 Rue de Dunkerque, F-75010 Paris
E : membership@openbanking.exchange W: www.openbanking.exchange

V002-000 | 060622 | Classification: Member

Annex: EU Requirements for Trust Anchors

The specific regulatory requirements for the use of Trust Anchors are given in commission implementing decision (EU) 2015/1505 on EU Trusted Lists following Regulation (EU) No 910/2014). This states:

> ***"Service digital identifiers" are to be used as Trust Anchors in the context of validating electronic signatures or seals*** *for which signer's or seal creator's certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.*

ETSI TS 119 612 v2.1.1, as referenced in the above implementing decision, defines "Service digital identifiers", in the case of PKI based trust services, as being a certificate identifying the QTSP.

The standard for validation of certificates adopted in ETSI standards under eIDAS is RFC 5280. This states:

> *In Section 6.1 [of RFC 5280], the text describes basic path validation. Valid paths begin with certificates issued by a trust anchor. The algorithm requires the public key of the CA, the CA's name, and any constraints upon the set of paths that may be validated using this key.* ***The selection of a trust anchor is a matter of policy: it could be the top CA in a hierarchical PKI, the CA that issued the verifier's own certificate(s), or any other CA in a network PKI.***

From the above highlighted text it is clear that:

1. The certificate held in the EU Trust List for a QTSP is to be used as the trust anchor for validation of certificates for electronic signatures and seals, and by extrapolation to other trust services, certificates for website authentication.
2. The certificate to be used as a trust anchor need not be the Root CA at the top of a PKI hierarchy.

About Open Banking Exchange

Open Banking Exchange (OBE) fosters innovation, competition, and efficiency to increase consumer choice and enhance security for online payments in the EU. We bring market players together to turn regulatory requirements into operational reality by supporting PSPs and TPPs in meeting the Access to Account (XS2A) requirements of PSD2 and facilitating the wider aims of Open Banking.

To learn more about OBE, email us today at ***europe@openbanking.exchange*** or visit our website:

https://www.openbanking.exchange/

OBE S.A.S, 40 Rue de Dunkerque, F-75010 Paris
E : membership@openbanking.exchange W: www.openbanking.exchange

V002-000 | 060622 | Classification: Member
Capital Autorisé: 1.605.000 € | RCS Paris 880 143 896 | No TVA: FR 35 880 143 896