ERPB Experts Contribution to ETS PSD2 Workshop  
Certificate Use Cases

Date: 7 Sept 2017

**General Note & Scope for ESI WG – PSD2**

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.

Specifically, from 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.

**NOTE:** we are referencing the latest EBA RTS for SCA/CSC, however this may be edited by EC, before final publication. We have raised an Issue with the ECB on the scope change across 3 versions, and have drafted our key questions and use cases to encompass all the situations that have been proposed by EBA so far.

**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

**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 (a Bank)

PISP - Payment Initiation Service Provider

AISP - Account Information Service Provider

TPP – Third Party Provider (encompassing PISP and AISP)

PSU – Payment Service User (a Bank Customer)

SCA – Strong Customer Authentication

CSC – Common Secure Communications

**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

QSEAL – 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

**KEY QUESTIONS for ESI Guidance & Standardisation:**

**CERTIFICATE USAGE FOR PSD2**

1. Qualified Electronic Seals “or” Qualified Website Authentication Certificates?
   1. When should they be used and for what purpose?
   2. Can either be used interchangeably/in place of each other?
   3. Is only one needed, or are both needed?
   4. What Certificates Standards are to be followed and who manages these?
   5. Recommend Uses & Non-Uses for eIDAS Certificates under PSD2

**SOURCES OF DATA**

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

**DATA ELEMENTS AND CERTIFICATE PROFILES**

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

**DUE DILLIGENCE BY QTSP BEFORE CERTIFICATE ISSUING**

1. 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:
   1. For QWAC
   2. For QSEAL

**CERTIFICATE MANAGEMENT AND LIABLITY**

1. Accuracy of information (and whose Liability) AFTER the cert has been issued:
   1. For QWAC
   2. For QSEAL
2. How to manage revocation of Certificate AFTER cert has been Issued:
   1. For QWAC
   2. For QSEAL
3. Responsibility for status/revocation (and whose liability) AFTER the cert has been issued:
   1. For QWAC
   2. For QSEAL

**RECEIVING PARTIES USING CERTIFICATES**

1. How does an ASPSP/TPP to check the validity/status of a Certificate AFTER cert has been Issued:
   1. For QWAC
   2. For QSEAL
2. How does an ASPSP/TPP check the signature of a Certificate AFTER cert has been Issued:
   1. For QWAC
   2. For QSEAL

**NOTE:** Previous Commentary and Queries for eIDAS Certificates are further noted below from various EU forums, with different ways of addressing, however these are supplementary background considerations to the Key Questions as above, which are the primary request.

**Use Cases for Common Secure Communications & Identity, under PSD2**



1. **PSU establishes secure communications with TPP:**
   * 1. Secure Communications via Internet Browser
        1. Certificate Used?
        2. Protocols Used?
        3. Certificate Data Used?
2. **PSU establishes secure communications with ASPSP:**
   * 1. Secure Communications for Internet Browser
        1. Certificate Used?
        2. Protocols Used?
        3. Certificate Data Used?
3. **TPP establishes secure communications with ASPSP:**
   * 1. Secure Communication via APIs
        1. Certificate Used?
        2. Protocols Used?
        3. Data Used?
        4. Use of PKI or other Security?
4. **ASPSP establishes secure communications with TPP:**
   * 1. Secure Communication via APIs
        1. Certificate Used?
        2. Protocols Used?
        3. Data Used?
        4. Use of PKI or other Security?



**[E] TPP provides PSD2 Identity to ASPSP:** Proof of Regulatory Identity under PSD2

- Certificate Used?

- Protocols Used?

- How to Proof Ownership/identity?

- Data Elements & Locations?

- Certificate Status Checking and Policies?

- Assurance and Liability?



**[F] ASPSP provides PSD2 Identity to TPP:** Proof of Regulatory Identity under PSD2

- Certificate Used?

- Protocols Used?

- How to Proof Ownership/identity?

- Data Elements & Locations?

- Certificate Status Checking and Policies?

- Assurance and Liability?

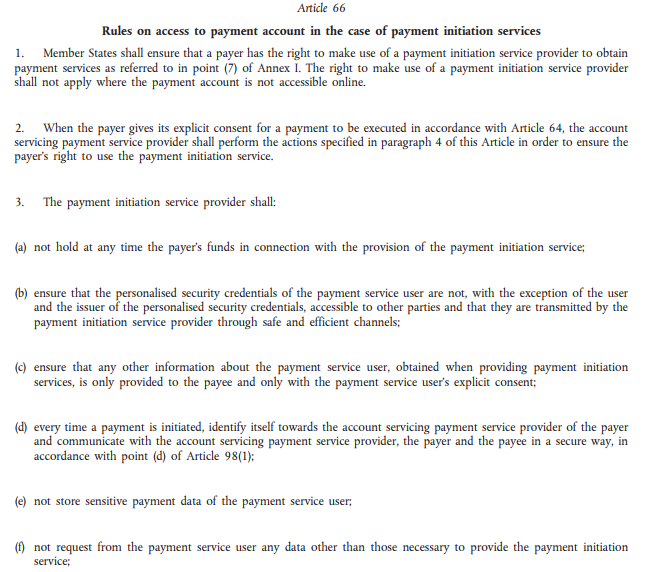
**Other Considerations:**

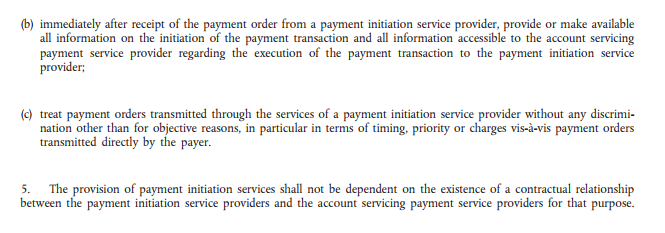
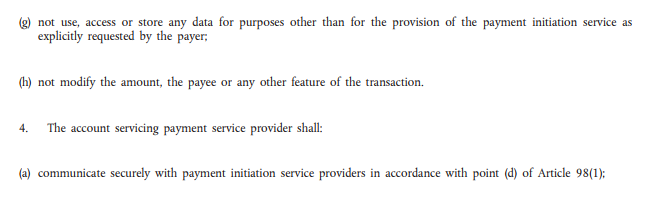
1. **CA/B Forum & QWACs**
   1. Differences between BV, OV and EV?
   2. Alignment to eIDAS Definition?
   3. Use of existing non-Qualified Website Certificates?
   4. Requirements for PSD2 QWACs for BV, OV and EV?
   5. Data Elements of PSD2 – differences with BV, OV and EV for Certificates profiles?
2. **ASPSP and TPP – SSL/TSL**
   1. Mutual Authentication Benefits/Downsides?
   2. Unidirectional Authentication Benefits/Downsides?
   3. Checking Storage of SSL/TLS Certificates?
3. **ASPSP and TPP – OAUTH2.0 & Certificates?**
   1. Certificates Required?
   2. Protocols Required?
4. **ASPSP and TPP – PKI**
   1. Methods of checking Signatures per Certificate?
   2. Further Security/Cryptography after PKI, per Protocols?

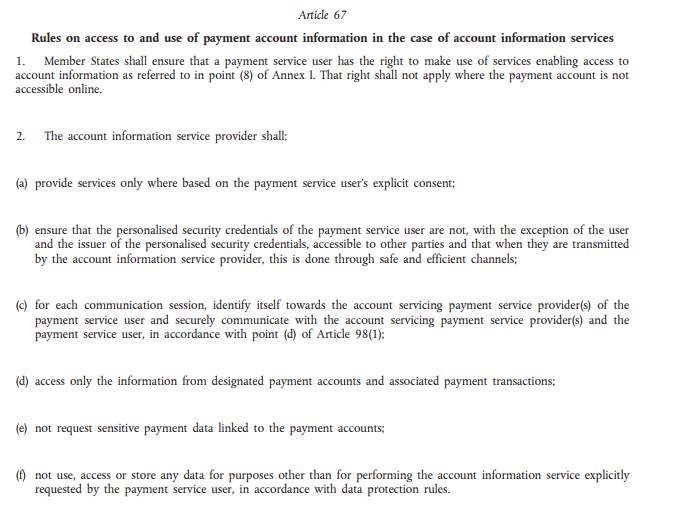
# **Background Information**

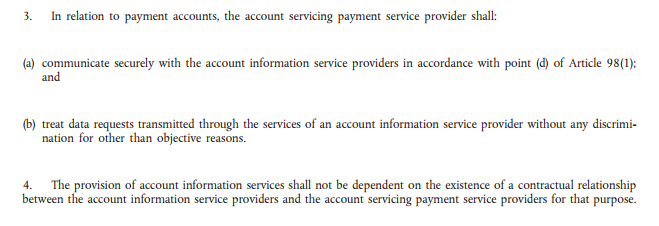
**References:**

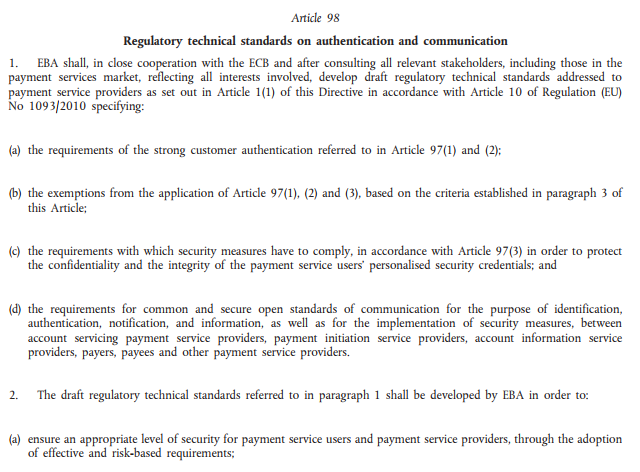
1. **Payment Services Directive 2:** [link](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN)

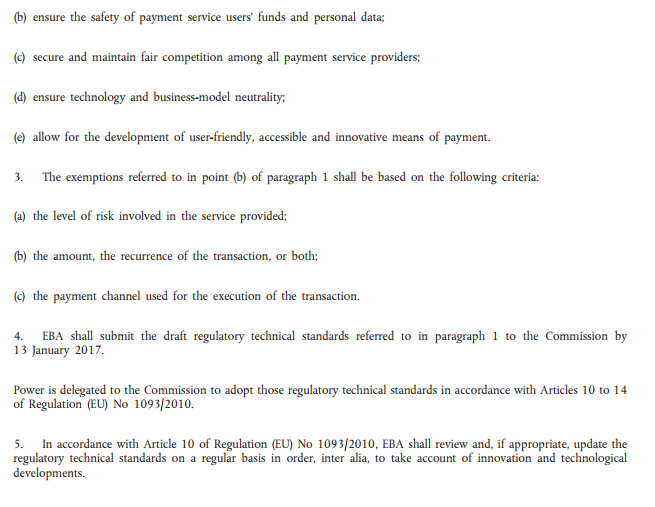










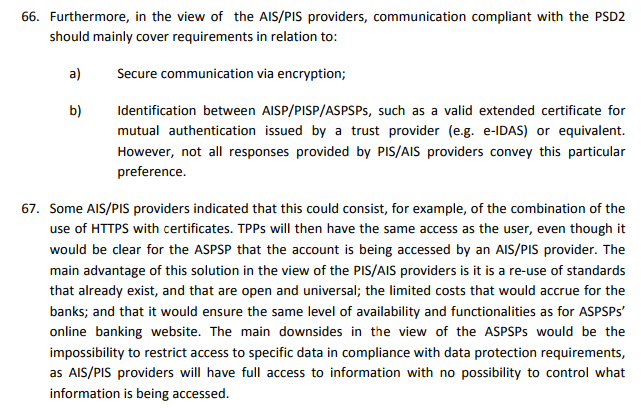


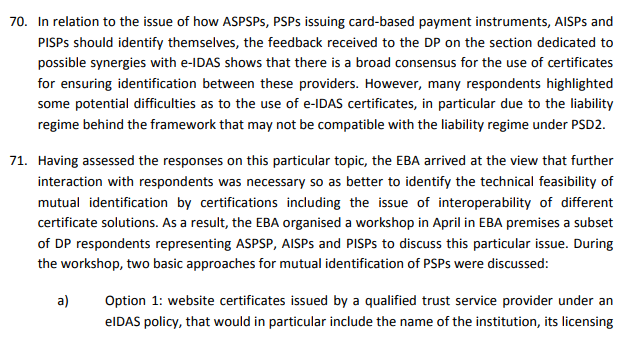
1. **EBA RTS for SCA/CSC:** [link](http://www.eba.europa.eu/documents/10180/1806975/%28EBA-2017-E-1315%29%20Letter+from+O+Guersent%2C%20FISMA+re+Commission+intention+to+amend+the+draft+RTS+on+SCA+and+CSC+-Ares%282017%292639906.pdf/efbf06e1-b0e9-4481-88e5-b70daa663cb9)

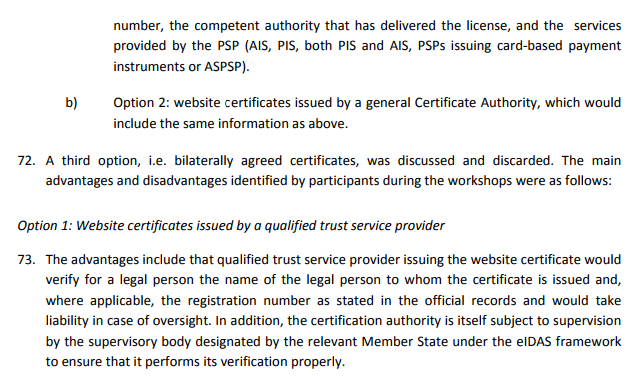
NOTE: Subject to final acceptance and publication by EC

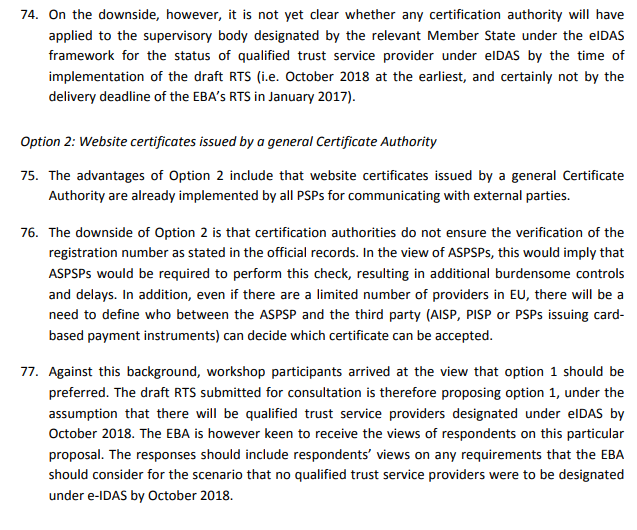
1. **Discrepancies on Scope:** Certificates for Mutual Identification for PSPs

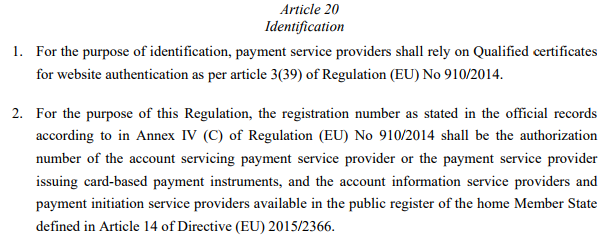
[EBA Consultation Paper](https://www.eba.europa.eu/documents/10180/1548183/Consultation+Paper+on+draft+RTS+on+SCA+and+CSC+%28EBA-CP-2016-11%29.pdf)version: August 2016

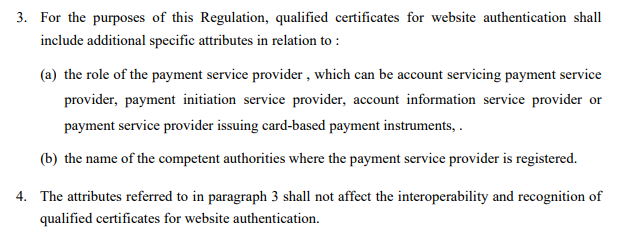






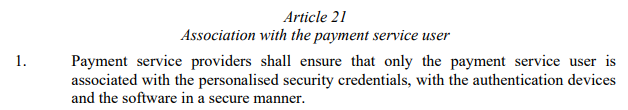


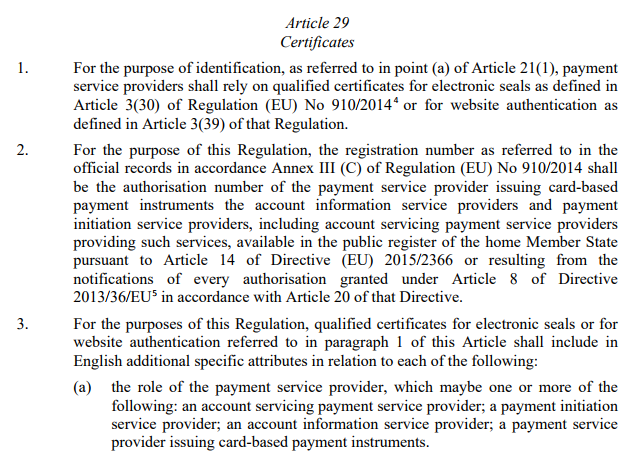


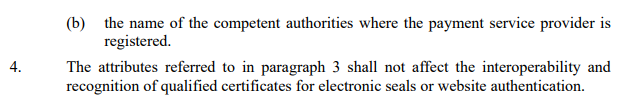


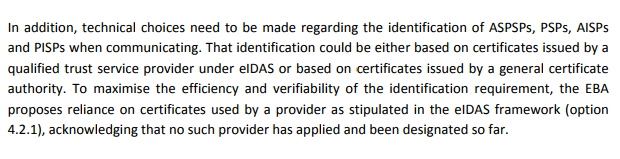
1. **Discrepancies on Scope:** Certificates in relation to the PSP and PSU Devices

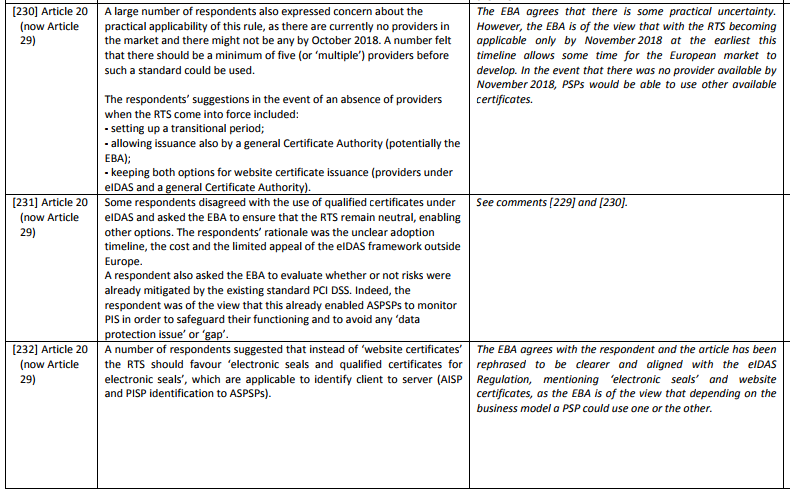
[EBA Final Draft](https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf) **version: 23 February 2017**

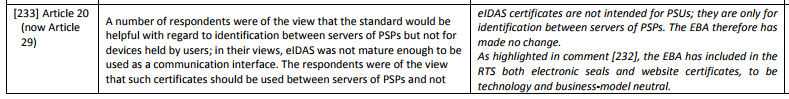


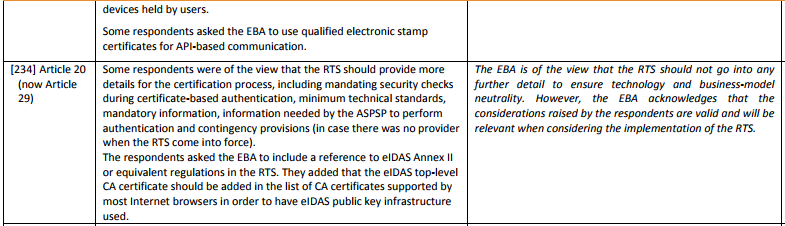






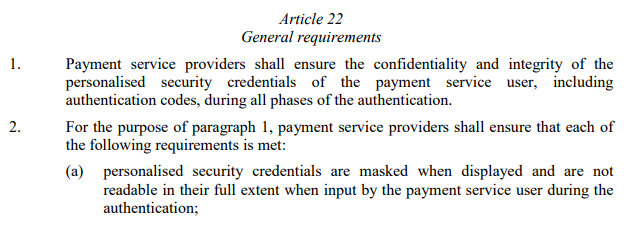


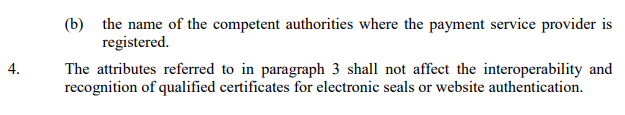
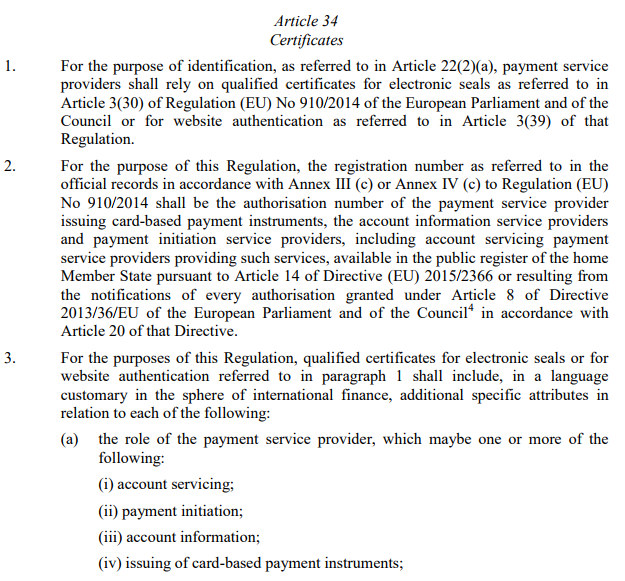




1. **Discrepancies on Scope:** Certificates in relation to PSPs and PSC of PSUs

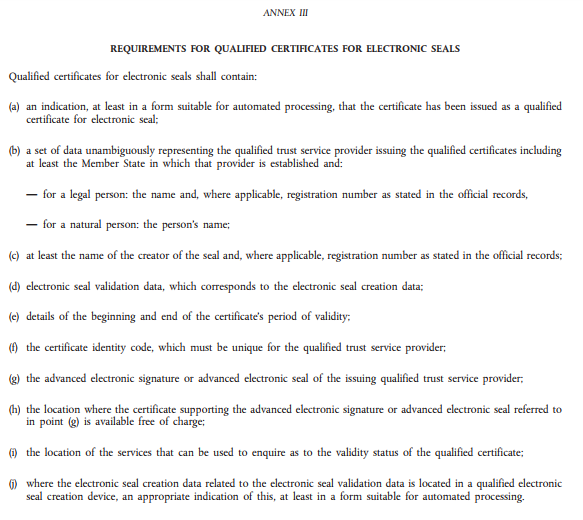
[European Commission Draft](http://www.eba.europa.eu/documents/10180/1806975/%28EBA-2017-E-1315%29%20Letter+from+O+Guersent%2C%20FISMA+re+Commission+intention+to+amend+the+draft+RTS+on+SCA+and+CSC+-Ares%282017%292639906.pdf/efbf06e1-b0e9-4481-88e5-b70daa663cb9) **version: 24 May 2017**



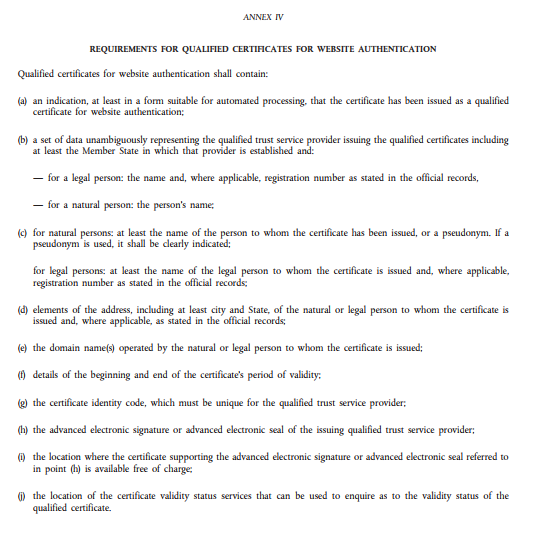


1. **Electronic Identity and Trust Services for Electronic Transactions:** [link](https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf)







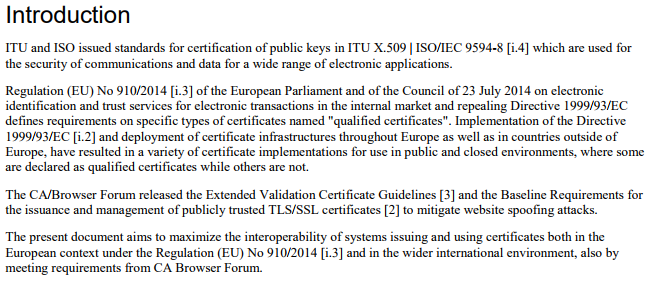


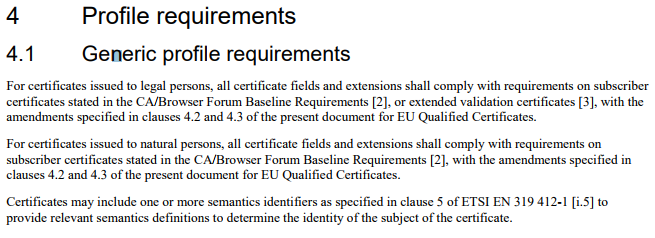
1. **ETSI – ESI Certificates Trust Service Providers and Profiles:**  [link](https://portal.etsi.org/tbsitemap/esi/trustserviceproviders.aspx)

**EN 319 412-2 Electronic Seals for Natural Persons:** [link](http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.01_60/en_31941201v010101p.pdf)

**EN 319 412-3 Electronic Seals for Legal Persons:** [link](http://www.etsi.org/deliver/etsi_en/319400_319499/31941203/01.01.01_60/en_31941203v010101p.pdf)(in addition to Natural Persons doc)

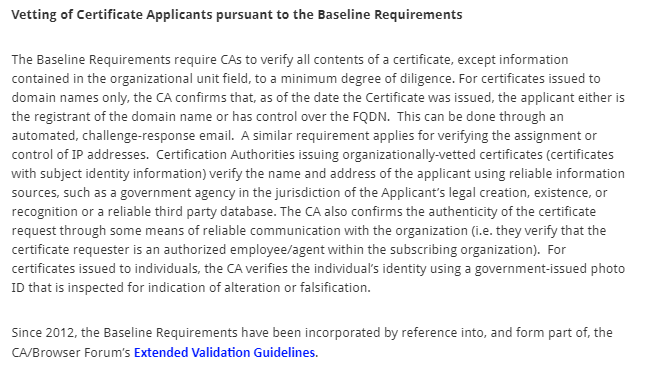
**EN 319 412-4 Website Certificates:** [link](http://www.etsi.org/deliver/etsi_en/319400_319499/31941204/01.01.01_60/en_31941204v010101p.pdf)





1. **Certification Authorities/Browser (CA/B) Forum:** [link](https://cabforum.org/)

**SSL: Baseline Validation Requirements (overview):** [link](https://cabforum.org/about-the-baseline-requirements/)



**SSL: Extended Validation Requirements (overview):** [link](https://cabforum.org/about-ev-ssl/)

