

Welcome to the World of Standards

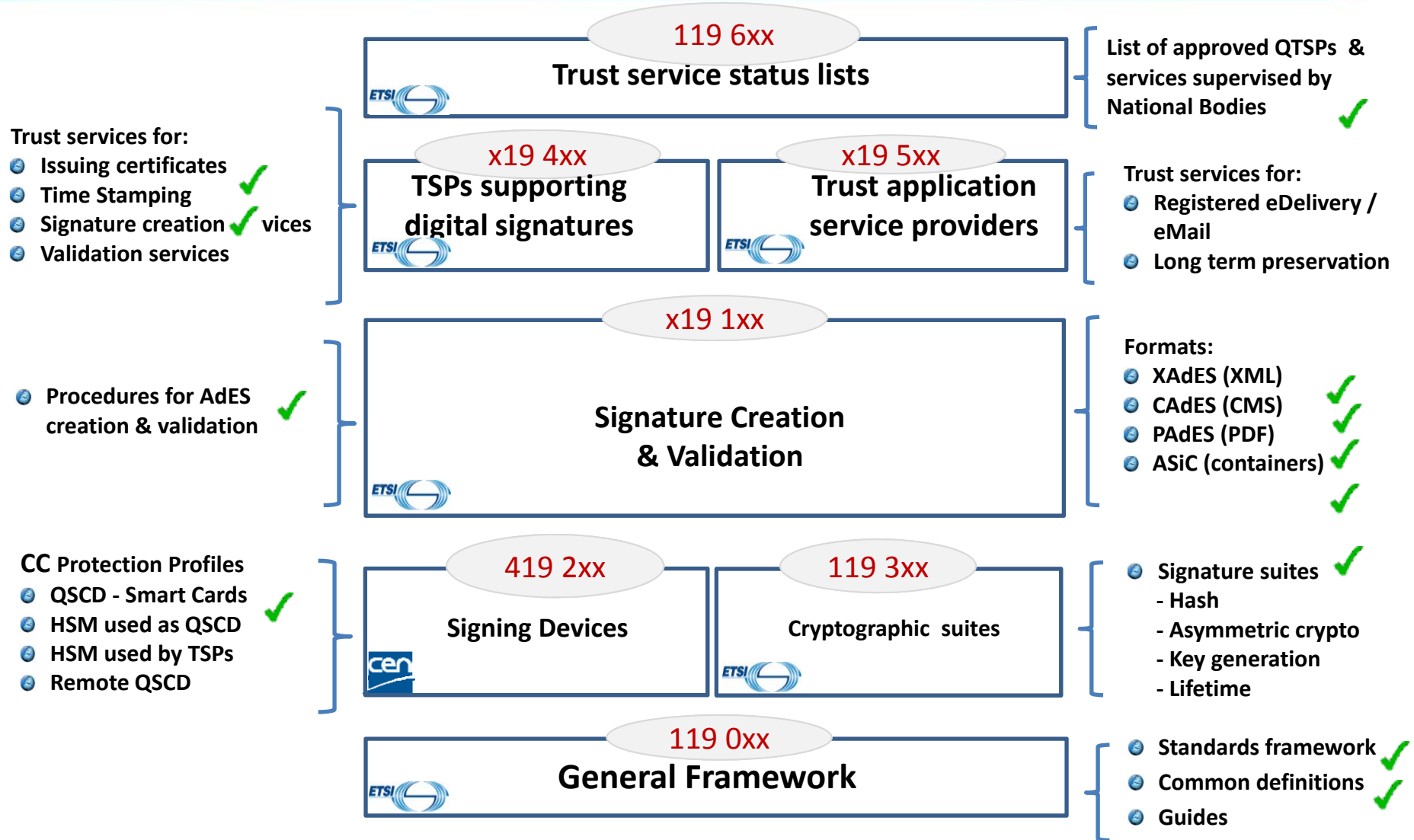


ETSI TC ESI WORK ON SECURITY AND POLICY REQUIREMENTS FOR ELECTRONIC REGISTERED DELIVERY SERVICES AND REGISTERED ELECTRONIC MAILS

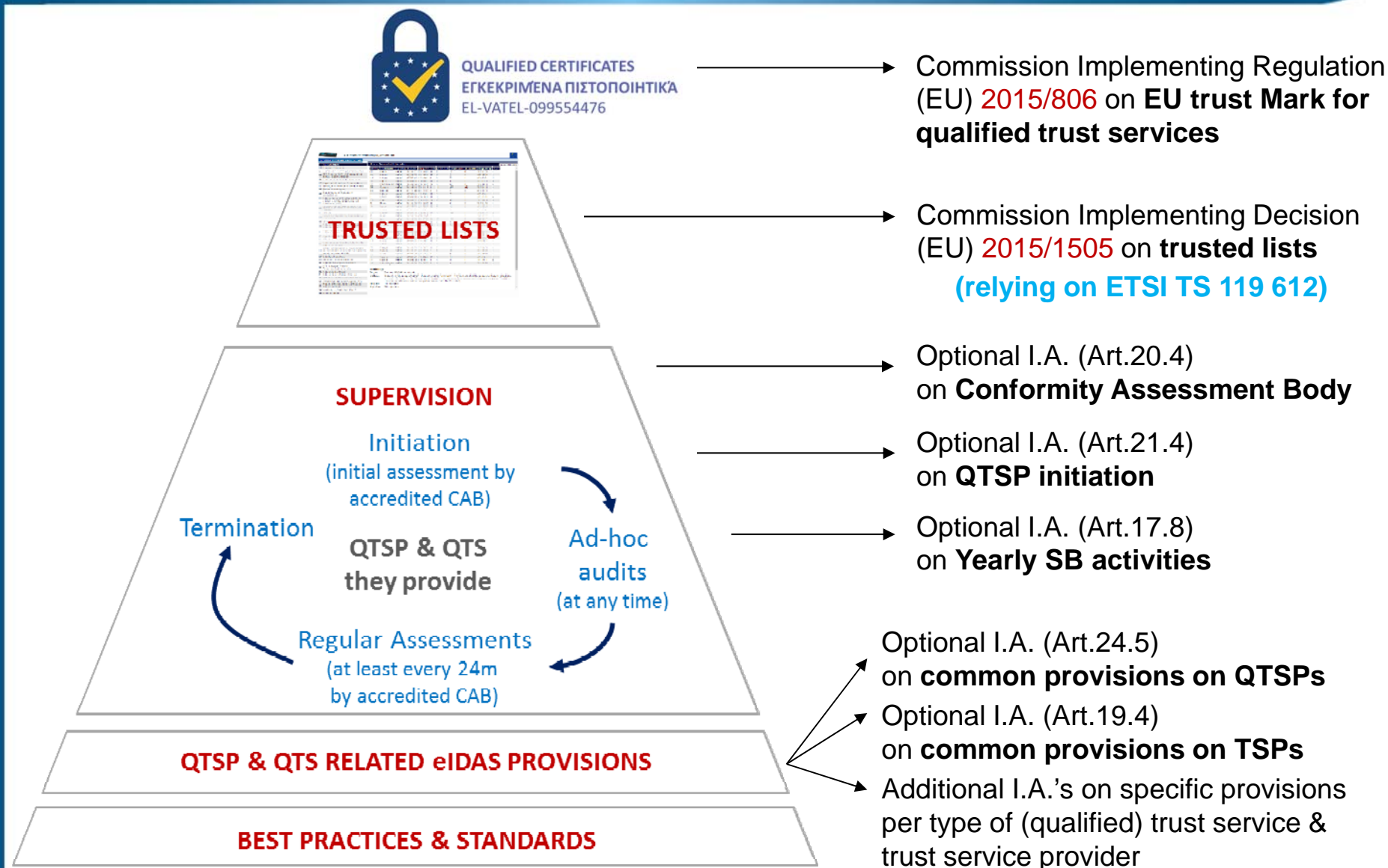
Presented by Paloma Llaneza – STF523

ETSI Security week – 14th June

Context (1) eIDAS Standards Framework: Published Standards



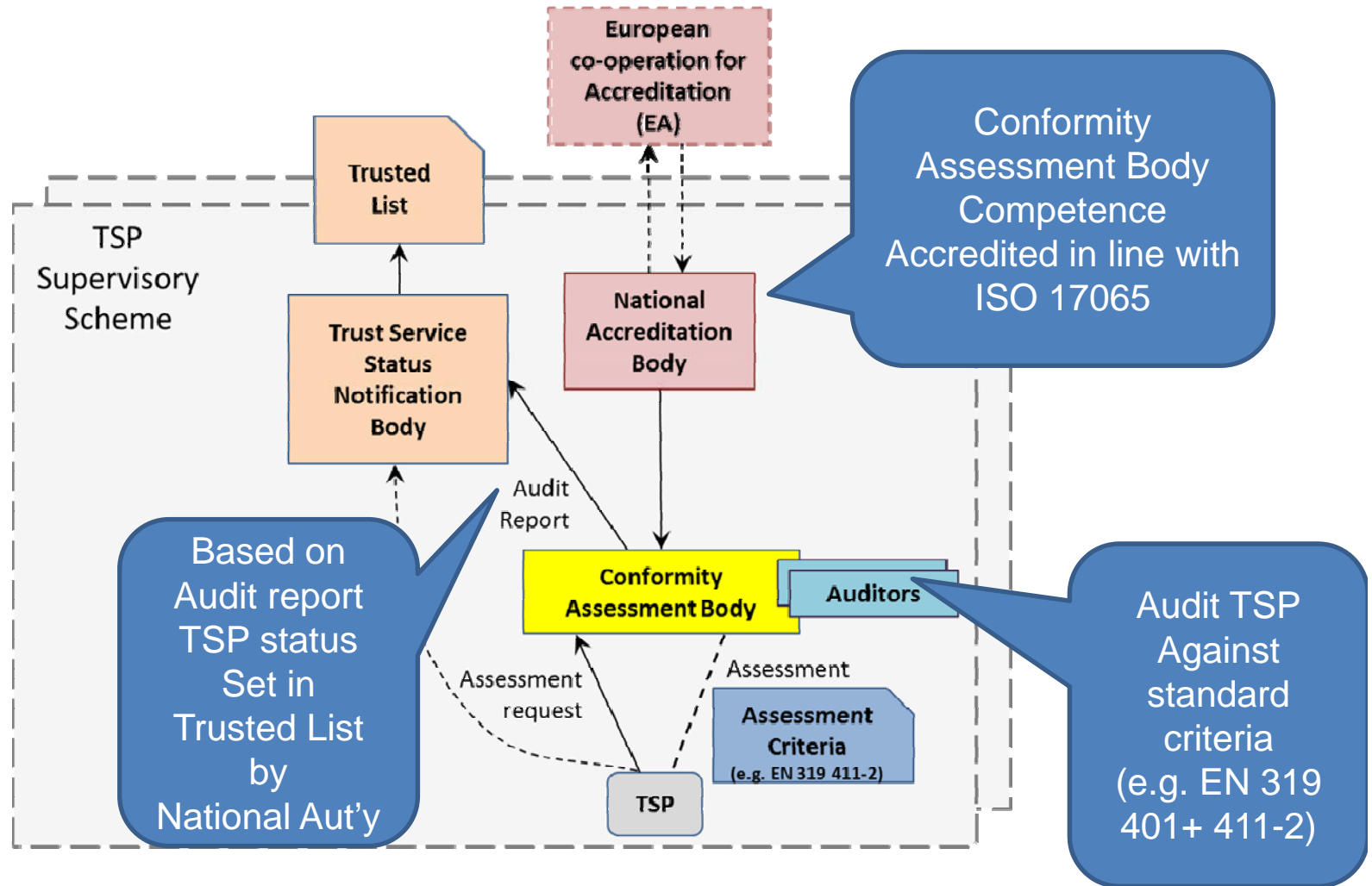
Enhanced trust model for QTSP's/QTS's



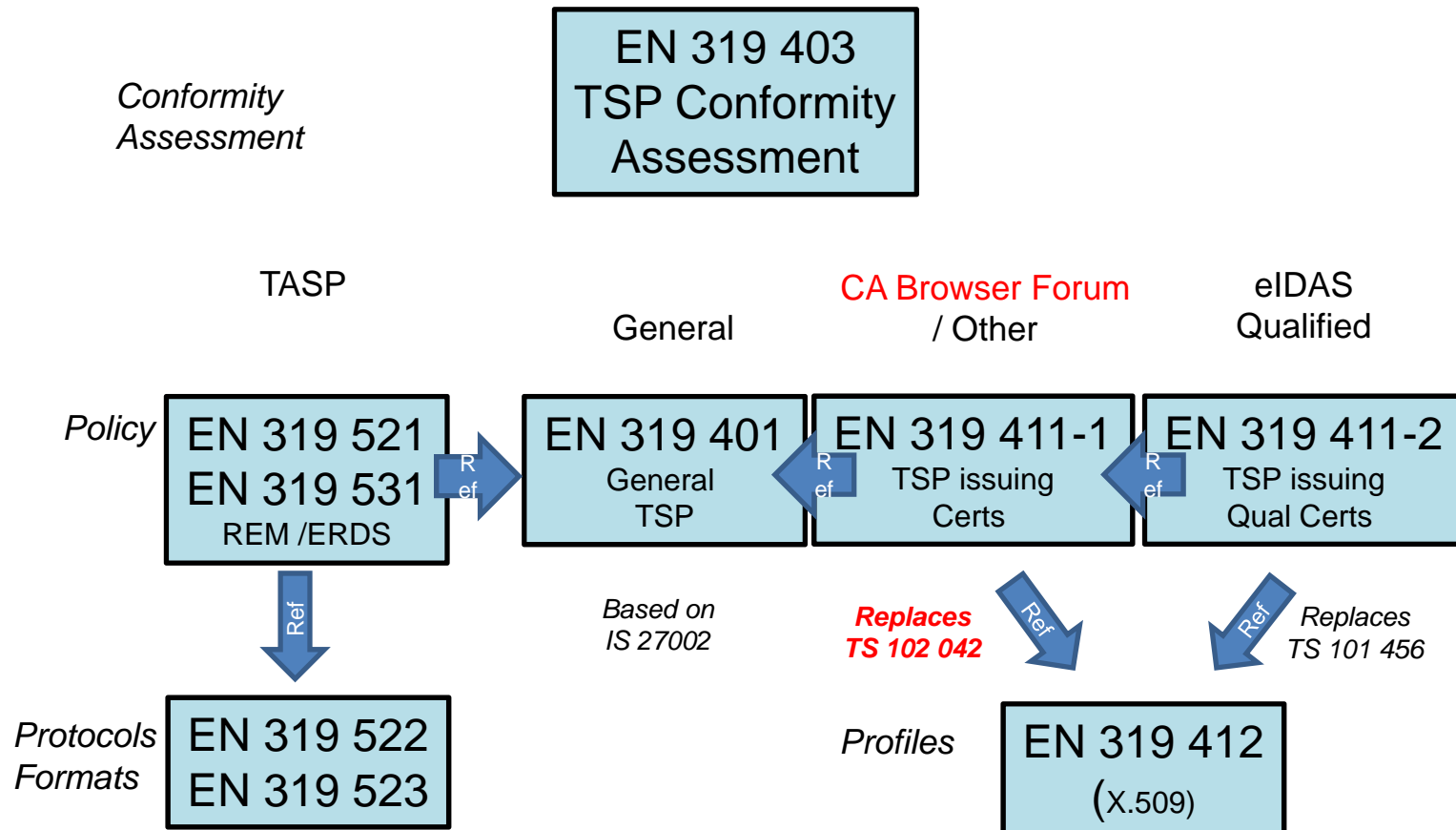
🌐 A layered model

- 🌐 Trusted list Art 22.5 IA: relies on TS 119 612 – v2.1.1 (end – point of the process)
- 🌐 Art.20.4 & CAB accreditation based on REG 765/2008:
 - 🌐 ISO 17065 + EN319 403 for accrediting CAB competencies (to assess products, services)
 - 🌐 ETSI EN 319 403 states the requirements CABs have to comply with in order to evaluate QTS(P)s
 - 🌐 TSP requirements: EN 319 401 (TSP requirements) + EN 319 4X1 OR EN 319 5X1 (Specific TSP requirements + service requirements)
 - 🌐 They are not mandatory in principle
 - eIDAS REG “eIDAS regulatory requirements on QTSP/QTS’s”
 - “missing (formal) link” between eIDAS “QTSP/QTS audit criteria” and standards → need for Art20.4 acts?

TSP Conformity Assessment Model



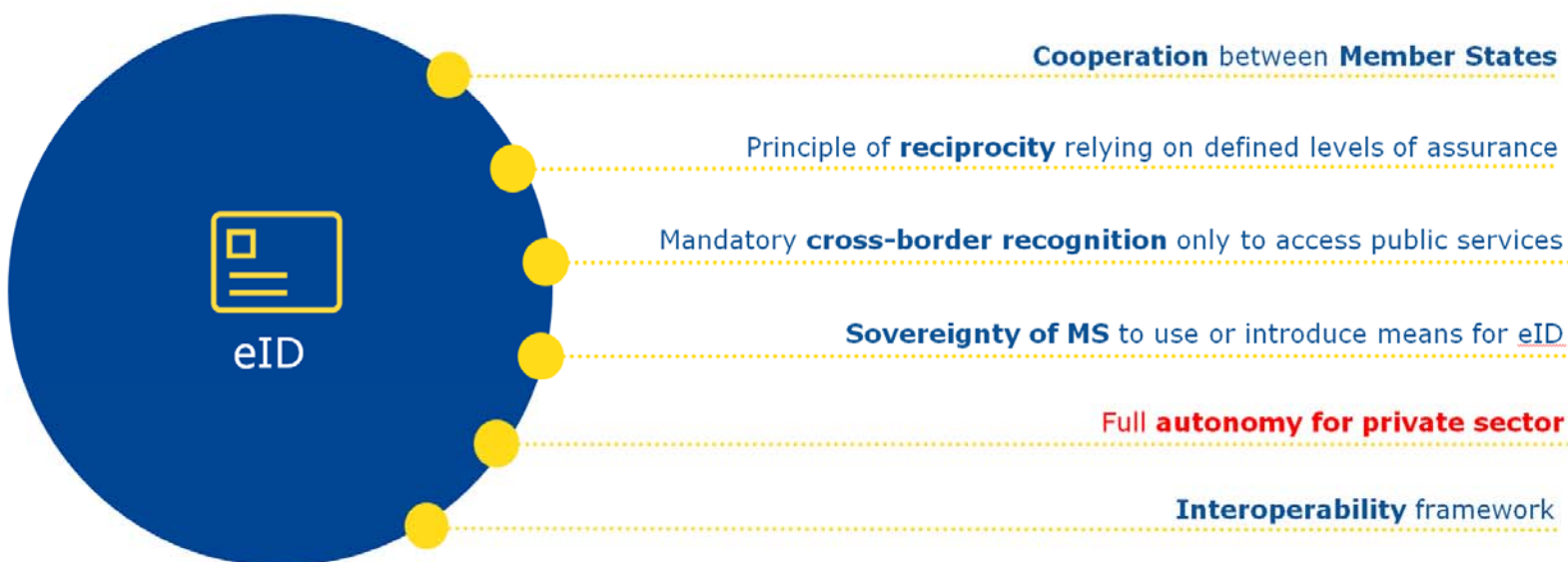
TSP Standards Overview (ETSI)



- **One standing-alone provider scheme**
- **Aligned with EN 319 401**
- **Conformity assessment requirements for QEDRSP and QEDRS.**
 - **Contains and EDRSP specifics requirements based on Section 7 of EN 319 401**
 - **Contains cumulative requirements for NonQEDRSP and QEDRSP**
 - **Addressed legal requirements from article 44 eIDAS Regulation: conformity assessment criteria**

eIDAS Requirement	eIDAS reference	Technical description	Requirements
Message Integrity	Article 3 (36) Article 19 Article 24 Article 44, (d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably; (e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;	Messages should be secured against any illegitimate manipulation during transmission. QERDSP - sending and receiving of user content is secured by an advanced electronic signature or an advanced electronic seal of a QTSP as to preclude the possibility of the data being changed undetectably - Notification of changes of user content to sender and recipient. - Evidence and logs	Draft 319521 EN 319 401 requirements and EDRS specifics 4 General provision on policies and practices 4.1 ERDS Practice statement 4.2 Terms and conditions 4.3 Information security policy 5 General provision on ERDS 5.1 User content/data integrity
Users Identity validation	Article 24 Article 44 (b) they ensure with a high level of confidence the identification of the sender; (c) they ensure the identification of the addressee before the delivery of the data;	QERDSP Sender's identity shall be validated with a high level of confidence. Recipient's identity shall be validated	Draft 319521 4 General provision on policies and practices 4.1 ERDS Practice statement 4.2 Terms and conditions 5 General provision on ERDS 5.2. Users Identification and Authentication 5.2.1. Initial identity validation 5.2.2 Identity verification renewal 5.2.3 Authentication

eIDAS: Key principles for eID



eIDAS Requirement	eIDAS reference	Technical description	Requirements
Recipient identity validation prior delivery of user content	Article 44 (c) they ensure the identification of the addressee before the delivery of the data;	QERDSP Recipient's identity shall be validated before the delivery of the user content.	Draft 319521 4 and practices 4.1 4.2 5 5.2. Authentication 5.2.1. 5.2.3 General provision on policies ERDS Practice statement Terms and conditions General provision on ERDS Users Identification and Initial identity validation Authentication
Time-Reference	Article 44 (f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.	QERDSP The date and time of sending and receiving a message shall be indicated via a QTS.	Draft 319521 4 and practices 4.1 4.2 4.3 5 5.3 General provision on policies ERDS Practice statement Terms and conditions Information security policy General provision on ERDS Time reference
Proof of Send/Receive	Article 3 (36) "... provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data..."	QERDSP Users shall be provided with evidence of user content's sending and receiving.	Draft 319521 4 and practices 4.1 4.2 4.3 5 5.4 5.4.1 General provision on policies ERDS Practice statement Terms and conditions Information security policy General provision on ERDS Evidence Retention period

Thanks!!!

