Updates to European signature standards

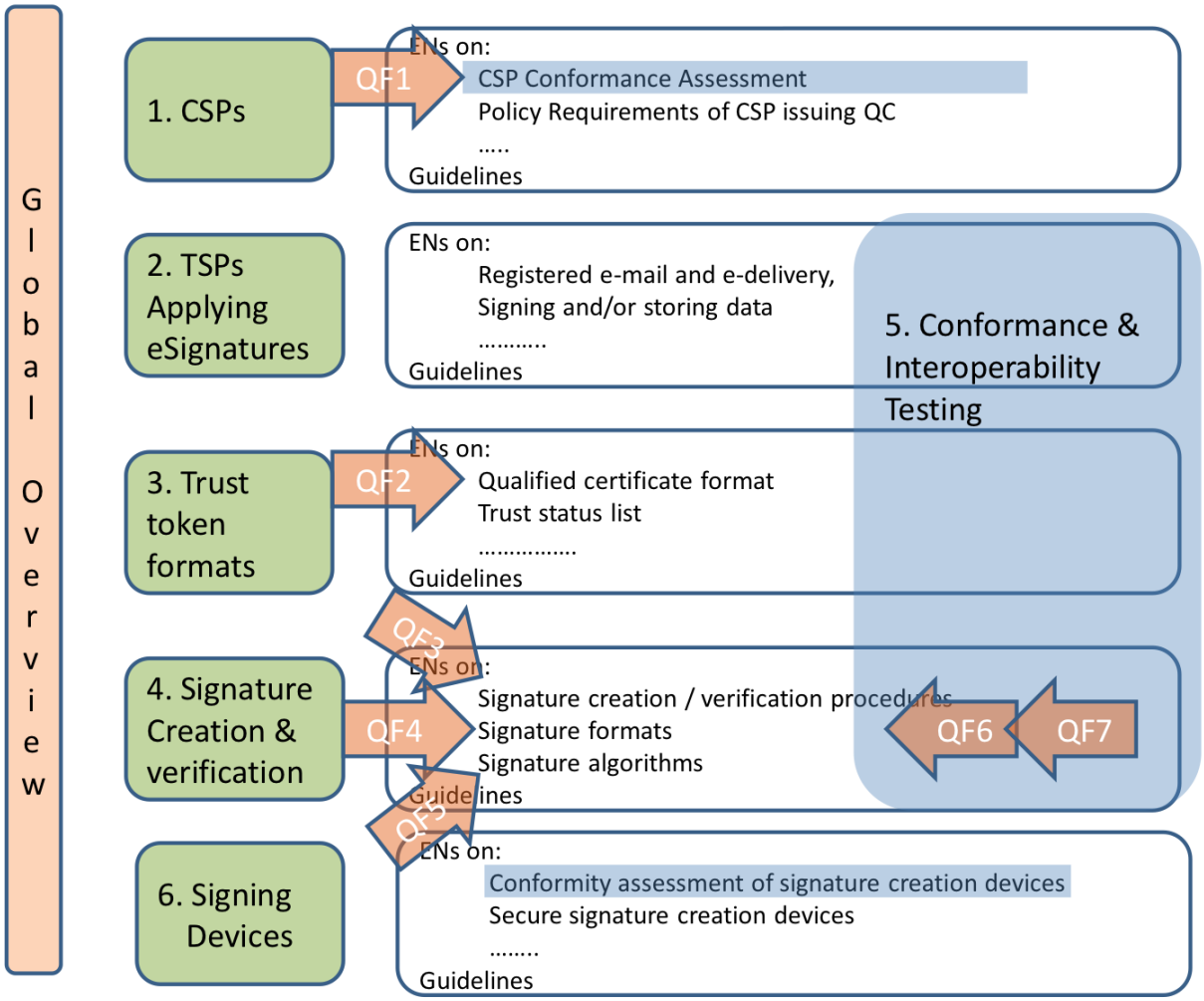
Stefan Santesson

3xA Security

General

- Updates mandated by the European Commission (M460)
- ETSI has launched 4 Specialist task forces (STF). 1 is of relevance to PKIX work
  - STF 427 – Quick fixes to electronic signature and related standards.
    - QF 2 – Quick fixes to Qualified Certificate profile and certificate profile for certificates issued to natural persons

The overall plan



Updates related to PKIX Work

- TS 101 862 – Qualified certificates profile (Profiling RFC 3739 and RFC 5280)
- TS 102 280 – Profile for certificates issued to natural persons (Profiling RFC 3739 and RFC 5280)

Nature of fixes

- Expression of names
  - Identification of data types (e.g. semantics of identifiers in serial number attributes)
  - Identification of organizational and personal data elements (e.g. company identifier and personal identifier in same certificate)
- Expression of quality of underlying private key protection
  - Key stored in a secure signature creation device according to EU directive.
- Expression of policy (This is a QC)
  - Implementation of certificate policy broken in about 50% of EU implementations,