ANNEX:

EU future electronic identification, authentication and signature (eIAS) policy

(Summary of a Workshop hosted by the European Commission, Sept 5th 2012, Brussels, based on the presentations used and topics covered)

Principles of the proposed Regulation

The EC Proposal for a "Regulation on Electronic identification and trust services for electronic transactions in the internal market" (COM (2012) 238, Jun 6th, 2012) has a clear aim. The ambition is to strengthen EU's Single Market by boosting TRUST and CONVENIENCE in secure and seamless cross-border electronic transactions.

The old framework – the e-Signature Directive of 1999 – was a big step. However, the European commission feels that a unique instrument across Europe is needed; therefore a REGULATION appears to be the appropriate tool.

The European Commission would like to achieve this by:

- Ensuring that people and businesses can use and leverage across borders their national eIDs to access at least public services in other EU countries
- Removing the barriers to the internal market for e-Signatures and related online trust services across borders (i.e. by ensuring that trust services have the same legal value as in traditional paper based processes.)

The scope of the proposed Regulation

1. Mutual recognition of electronic identification
2. Electronic trust services:
   - i. Electronic signatures interoperability and usability
   - ii. Electronic seals interoperability and usability
   - iii. Cross-border dimension of:
     - a. Time stamping
     - b. Electronic delivery service
     - c. Electronic documents admissibility
     - d. Website authentication

Mutual recognition and acceptance of eID

A EU Member State:

- May '**notify**' to European Commission the 'national' electronic identification scheme(s) used at home for access to public services;
- Must recognise and accept 'notified' eIDs of other Member States for cross-border access to its public services requiring e-identification;
- Must provide online free eID **authentication** facility;
- Is **liable** for unambiguous identification of persons and for authentication;
- May allow the private sector to use 'notified' eID

Electronic trust services

Common Principles:

- Mutual recognition of «qualified» electronic trust services
- Strengthens and harmonises national supervision of qualified trust service providers and trust services
- Reinforces data protection + obligation for data minimization
- Uses delegated and implementing acts as a mechanism to ensure flexibility vis-à-vis technological developments

eSignature:

- Clarifies the concepts related to eSignature (natural persons)
- Introduces eSeals (legal persons)
- Clarifies validation of qualified eSignatures
- Ensures long term preservation
- Allows for full reference to standards
- Allows «server / remote» and «mobile» signing

What is not covered?

eID:

- Member States are **not obliged to have** an e-identification scheme
- Member States are **not obliged to notify** their e-identification scheme(s)
- «Notified» eID are not necessarily ID cards
- **No "EU database"** of any kind
- **No "EU eID"**
- **No coverage «soft ID»** (ex. Facebook); only «official eID»

Trust services:

The draft does not address / require / contain:

- EU supervision (vs. national / regional level)
- Prior authorization to start qualified service or accreditation
- Details on trust services other than eSig / eSeals
- Persons' roles and/or attributes
- Certification of products other than eSig/eSeal creation devices
- Format of e-documents
- Establishment of proof
- Encryption

The European Commission believes the proposal for a Regulation will make a difference:

Creates confidence in electronic trust services:

- Effective state supervision (done on the membership level)
- Systematic usage of "trusted lists“

Easy eSignature:

- Harmonisation power of Regulation
- Enables full eSig specification via secondary legislation + standards

Related trust services:

- Address clear market needs: eSeals, eDelivery, eDocuments, …
- Harmonise national legislation: time stamping, eDelivery
- e-Document admissibility: « big bang » for de-materialisation
- Website authentication is an implicit expectation of the citizens

Comprehensive “toolbox” of trust building instruments

- One single legislation across EU

Foster eID usage (“world premiere”):

- Leverage eID cards and mobile ID infrastructure
- Reliable eID to allow cross border eBusiness and enable eGov services
- Private sector is invited to build on «notified» eID schemes
- Leverage Large Scale Pilot project STORK

To complete the necessary legal framework, the proposed regulation uses delegated and implementing acts.

The understanding is:

- The proposal contains all essential core rules
- Smaller details can be adopted later via delegated acts / implementing acts:
  - Delegated: acts of general application to supplement or amend certain non-essential elements of a legislative act, adopted by the Commission
  - Implementing: acts of general application to ensure uniform implementation, adopted by the Commission
- 16 references to delegated acts, 29 to implementing
- Not all of these options will actually be adopted, and they could be combined into single acts

Example: delegated / implementing acts for eID

Article 7 (4): Notification process (I)
Article 8 (2): eID cooperation mechanisms (I)
Article 8 (3): eID interoperability measures (D)

Possible next steps:

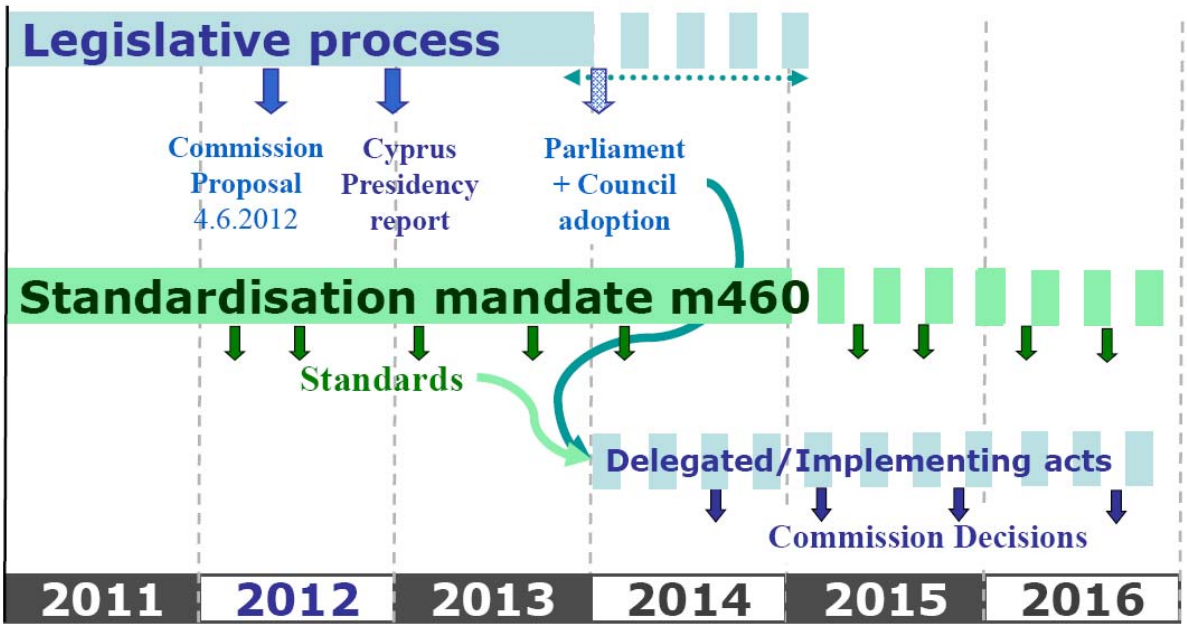
- Notification formats, procedures and templates to be determined. What information should MS provide, and how should it be processed?
- Cooperation for the exchange of best practices, experiences etc. Establishment of an expert group would be possible.
- eID cross border interoperability by setting minimum technical requirements. Could be used to formalize outputs from e.g. STORK (security requirements, quality assurance, standard references, etc). [Some say that STORK is only one possible way forward – so other means of cross border interoperability are possible]

Example: supervision

Article 13 (5): Supervision procedures (D)
Article 13 (6): Reporting requirements (I)
Article 16 (5): Requirements auditing bodies (D)
Article 16 (6): Supervision of QTSPs (I)

Possible next steps:

- Detailing steps for supervision: what to check, to what extent, how, etc. Ref. to e.g. EN 19 403 - General requirements and guidance for Conformity Assessment of TSPs Supporting Electronic Signatures)
- Supervisory bodies must report annually to the Commission. A template of the report can be established and/or a description of contents (e.g. market statistics, incidents, etc.)
- Definition of recognition requirements and procedures for recognized independent bodies conducting audits



Example: Effects / acceptance of eSignatures

Article 20 (6): Definition of security levels (D)
Article 20 (7): References to applicable standards (I)

Possible next steps:

- Defining multi-level security policies. Could be done to create a more refined EU level mechanism for defining security requirements, and be linked back to trusted lists.
- Linking to standards. Such policies would likely be formalised as standards, which would be referenced by an implementing act.

General observations

Many references to secondary acts, but unlikely that all will be implemented. Competences exist if needed.

Past decisions will need to be replaced by new acts:

- Commission Decision 2003/511/EC on reference numbers of generally recognised standards
- Commission Decision 2000/709/EC on minimum criteria for designating bodies
- Commission Decision 2009/767/EC on 'points of single contact' (Trusted Lists) (and Decision 2010/425/EU)
- Commission Decision 2011/130/EU on minimum requirements for e-documents

New decisions can be adopted to plug current holes:

- Common supervision requirements, improved coordination, eID interoperability norms, etc.

Aspects of Supervision of Qualified Trust Services (Providers)

Key principles

Trust services as key enablers in boosting use of online environment

- Qualified Trust Services (QTS) and their specific outputs being given a specific legal effect enhancing their legal certainty and admissibility over the EU

Regulation proposal supervision model:

Maintaining national supervisory bodies but with stronger and harmonised rules (process, mutual assistance, TSP security requirements, requirements for QTPs, trusted lists)

Monitoring of Trust Service Providers and their Trust Services to ensure information security risk management Supervision of QTS(P)s and Trusted Lists as essential building blocks for trust building (claim vs confirmation) **Monitoring of Trust Services (Providers)**

Supervisory Bodies to monitor TSPs for taking appropriate technical and operational risk management measures wrt. the security of their trust services

- TSPs may submit an audit security report carried out by an recognized independent body to confirm such measures

Possible next steps:

- Clarify who exactly is to be considered as a TSP providing TS and who is not (e.g. ISP's, free mailbox providers, etc.)
- Promote ISO/IEC 27001 certification to be carried out by an accredited certification body as EU wide common minimum requirement for "Art15.1 security audit reports"
- Trusted List of "monitored" compliant TSP's
- Evaluate impact on Supervisory Bodies, on TSP's, on effective security of monitored Trust Services

Supervision of QTS(P)s

Supervisory Bodies to supervise Qualified Trust Service Providers and their Qualified Trust Services

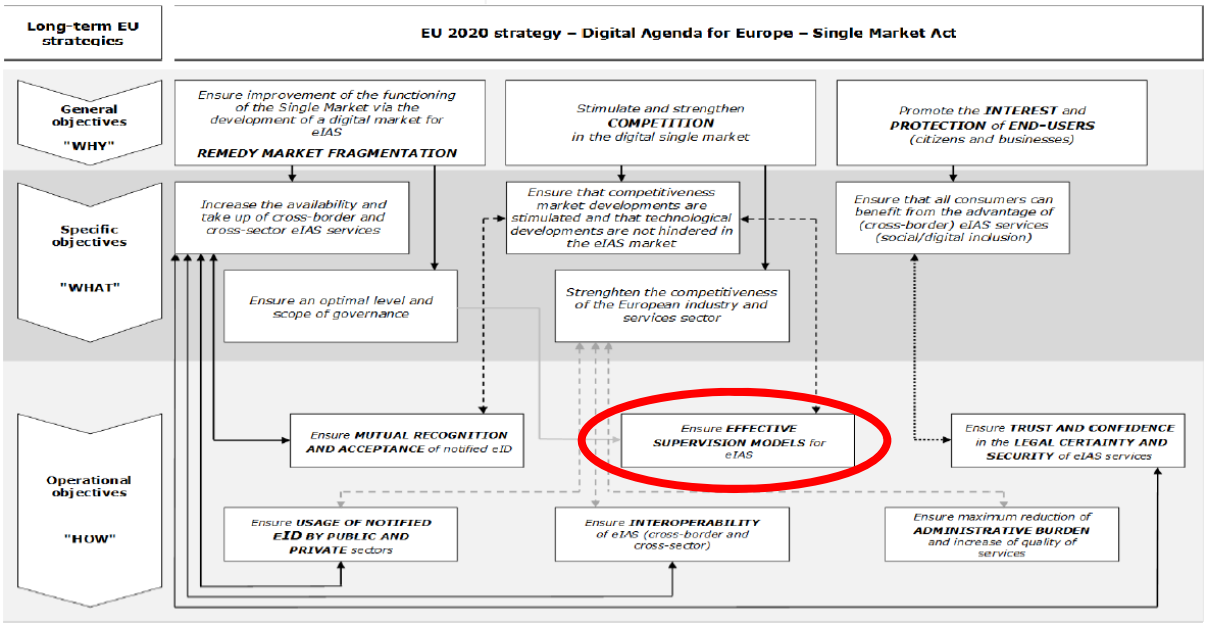
- Chapter 2 - Art.13 to 19.

Possible next steps:

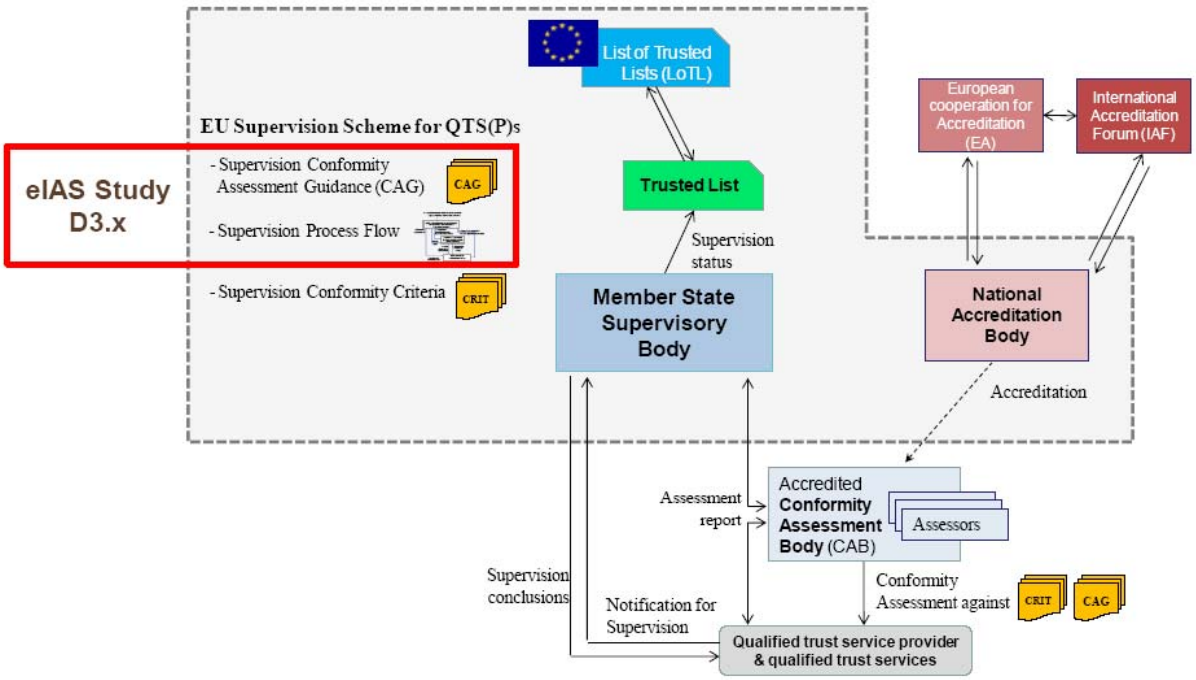
- **Consider a full prior authorization model** (versus the hybrid model proposed in the Regulation that may lead to practical implementation / discriminatory issues)
- **Establish a European Supervision Scheme for QTS(P)s based on**
  - **a Conformity Assessment Guidance – CAG** : including the description of the Supervision Process flow , taking into account the qualified status flow in Trusted Lists;
  - **Conformity Assessment Criteria – CRIT** : Mapping legal provisions to standards per type of qualified trust service
  - **Trusted List specifications updated** from CD 2009/767/EC as amended by CD 2010/425/EU.

eIAS proposed model for EU Supervision Scheme

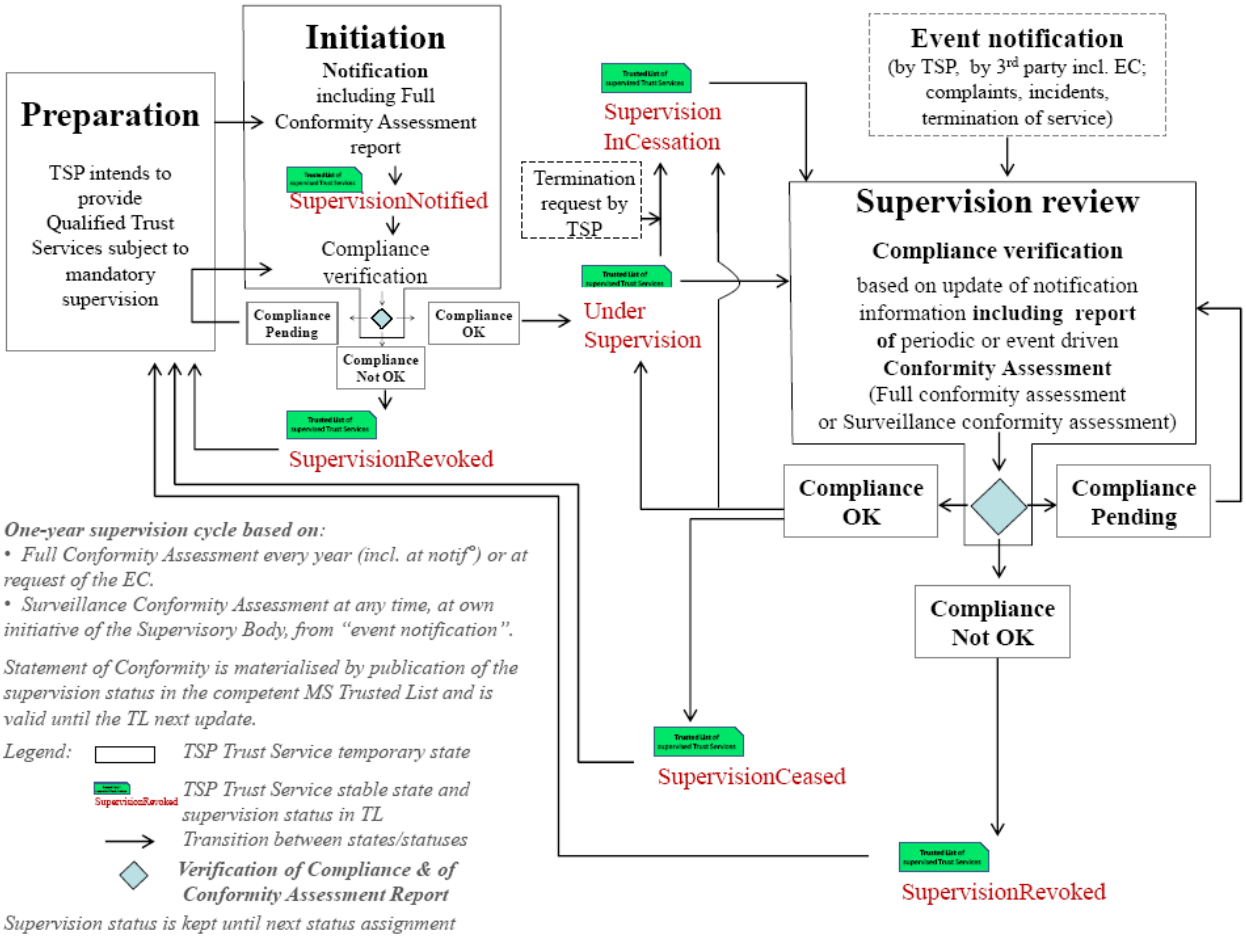
Following the EU strategy – Digital Agenda for Europe – Singe Market Act, an effective supervision model for eIAS has to be provided:



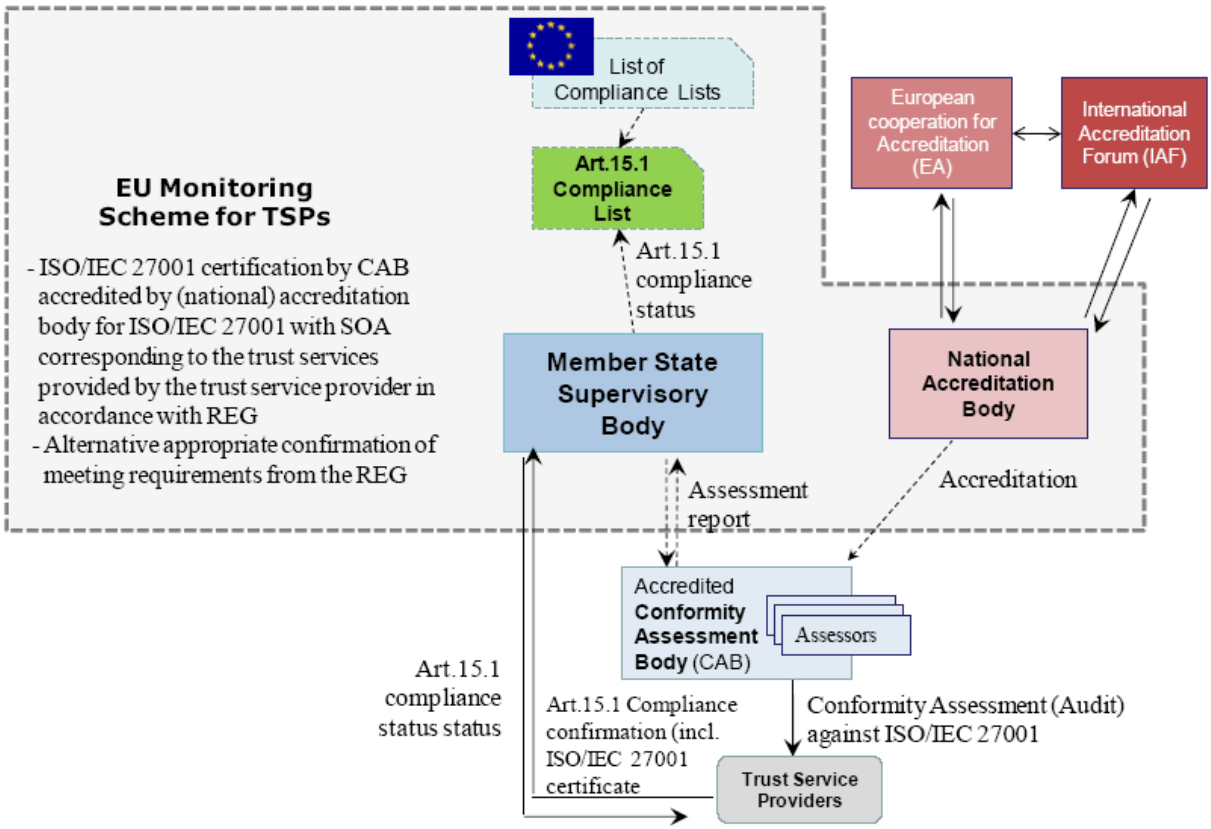
Following the overall eIAS strategy, the proposed European framework might look like this:



- ISO/CASCO based model (preferred to other models like ISAE 3000, AICPA, IFAC/IAASB/ISRS)
- Allow international recognition through EA and IAF
- Aligned with COM(2012) 238 proposal
- Conformity Assessment Guidance (CAG), Criteria (CRIT) and Trusted Lists specifications may be either part of such acts or standardized (e.g. ETSI EN 319403 drafted accordingly) & referenced in such acts.
- Backward compatible with Trusted Lists (CD 2009/767/EC amended by CD 2010/425/EU) – limited updates
- Allows monitoring of TSPs (based on ISO/IEC 27001 certification)
- EU Supervision Scheme common to all MS:
  - Increase trust & confidence level of QTS(P)s in EU, transparency, equality, better preparation of QTSPs, harmonised and stronger rules
  - Trust recognition in EU and **beyond** as benchmarking reference for mutual recognition with 3rd countries and international organizations
- Delegated and implementing acts mechanism allow implementation of such a common EU **Supervision Scheme**



Monitoring as part of the proposed scheme:



Conclusions

- EU Supervision Scheme common to all MS
  - Increase trust & confidence level of QTS(P)s in EU, transparency, equality, better preparation of QTSPs, harmonized and stronger rules
  - Trust recognition in EU and beyond as benchmarking reference for mutual recognition with 3rd countries and international organizations
- Delegated and implementing acts mechanism allow implementation of such a common EU Supervision Scheme

Walter Trezek, 07.09.2012