Welcome to the World of Standards

ETSI

World Class Standards

NIST-Workshop 10 & 11 April 2013

EUROPEAN APPROACH TO OVERSIGHT OF "TRUST SERVICE PROVIDERS"

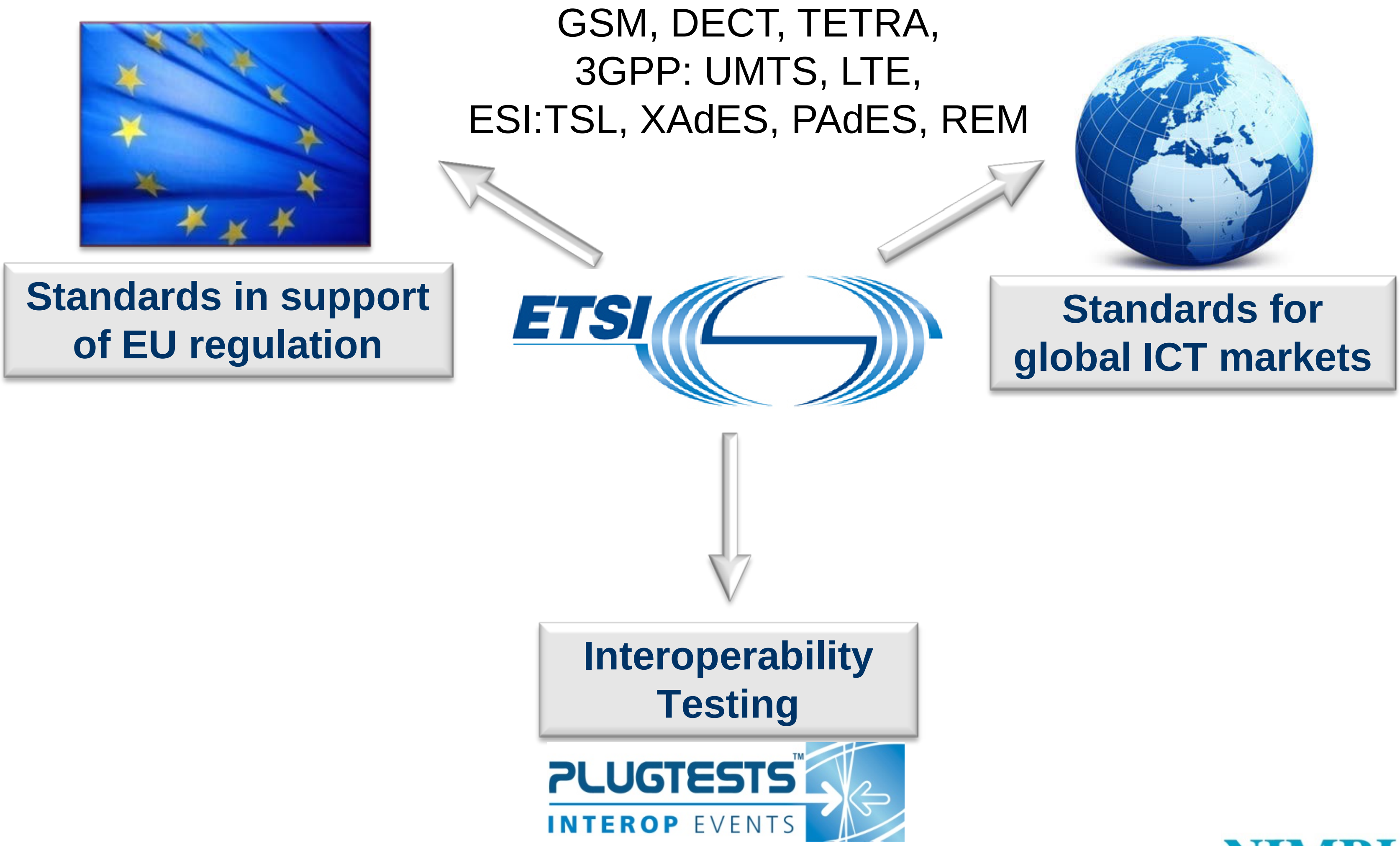
Presented by Arno Fiedler, Member of **E**uropean **T**elecommunications **S**tandards **I**nstitute
Electronic Signatures and Infrastructures, Specialist Task Force 458

NIMBUS
Technologieberatung GmbH

Topics

- 1. ETSI at a glance
- 2. Current voluntary Audit Scheme for TSP issuing SSL-Certificates based on ETSI Standards and Specs
- 3.1. **Legal** Framework: EU **Draft** regulation on EIDAS
- 3.2. Shaped **Standards** Framework: EU Mandate 460
- 3.3. Proactive **Trust** Framework
- 4. Next Steps
- 5. Summary

1. ETSI activities



GSM, DECT, TETRA,
3GPP: UMTS, LTE,
ESI:TSL, XAdES, PAdES, REM

Standards in support of EU regulation

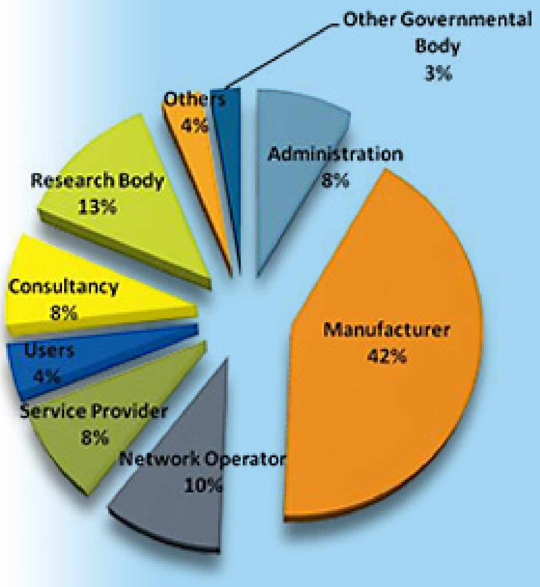
Standards for global ICT markets

Interoperability Testing

1. Membership

- Over **700 companies**, big and small, from **62 countries** on **5 continents**

- Manufacturers, network operators, service and content providers, national administrations, ministries, universities, research bodies, consultancies, user organizations



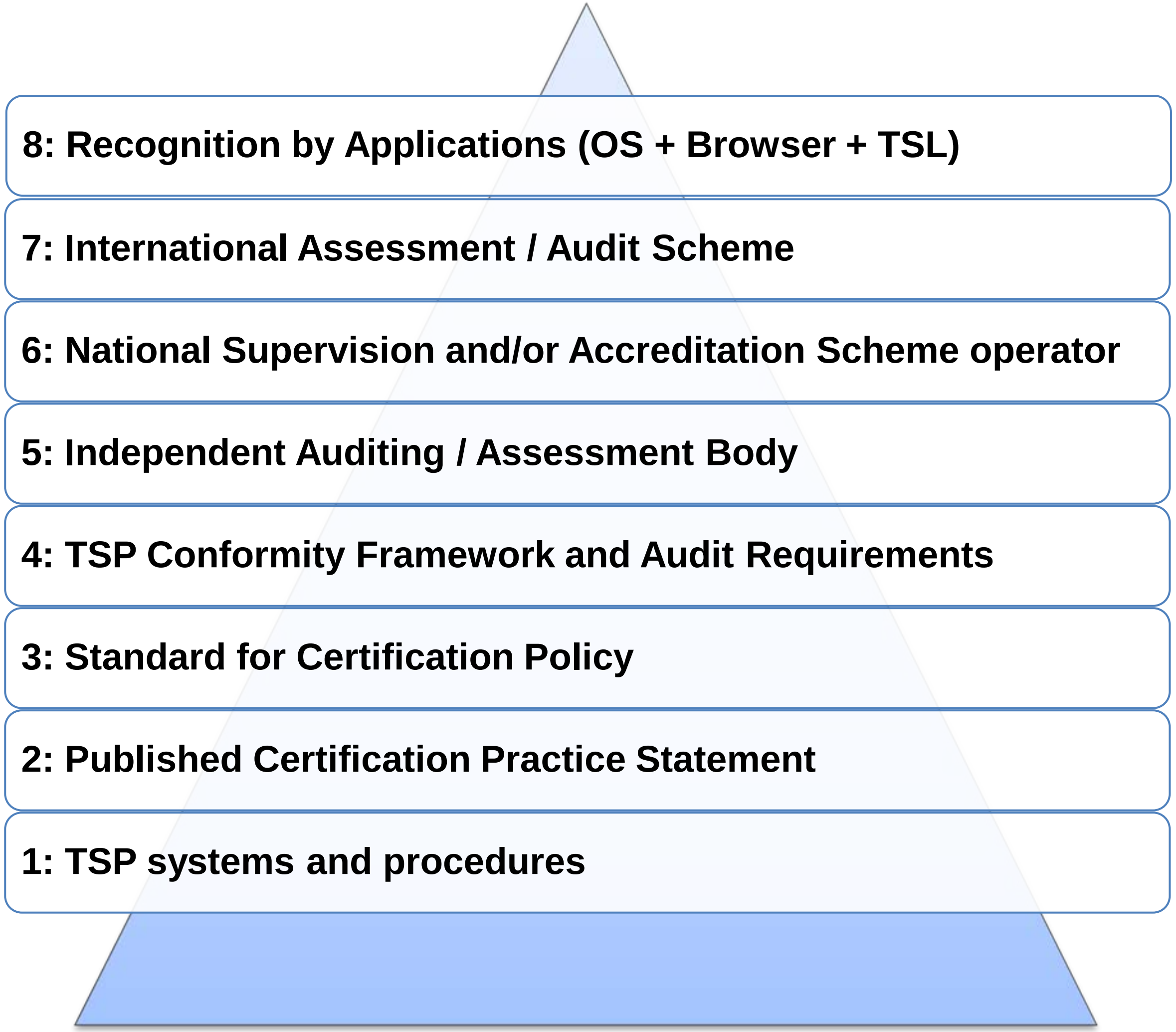
A powerful and dynamic mix of **skills, resources and ambitions**

2. ETSI Recommended Practices for CAs issuing Web Certificates

- Year 2008 ETSI Published TS 102 042 “Policy Requirements for Certification Authorities issuing Public Key Certificates” that Generalizes requirements specified in TS 101 456 for **Qualified Certificates.**
- Year 2010 Versions TS 102 042 references CAB guidelines for specific requirements for **Extended Validation** Web Certificates
- Year 2012 CAB Forum **“Baseline”** guidelines to be adopted by all Certification Authorities issuing web certificates - Only compliant CAs to be included in browsers
- End of Year 2012: ETSI issued actual policy and audit guides for **Baseline and Extended Validation**.

NIMBUS
Technologieberatung GmbH

2. Assessment & Certification – Actual (Best) Practise for SSL



8: Recognition by Applications (OS + Browser + TSL)

7: International Assessment / Audit Scheme

6: National Supervision and/or Accreditation Scheme operator

5: Independent Auditing / Assessment Body

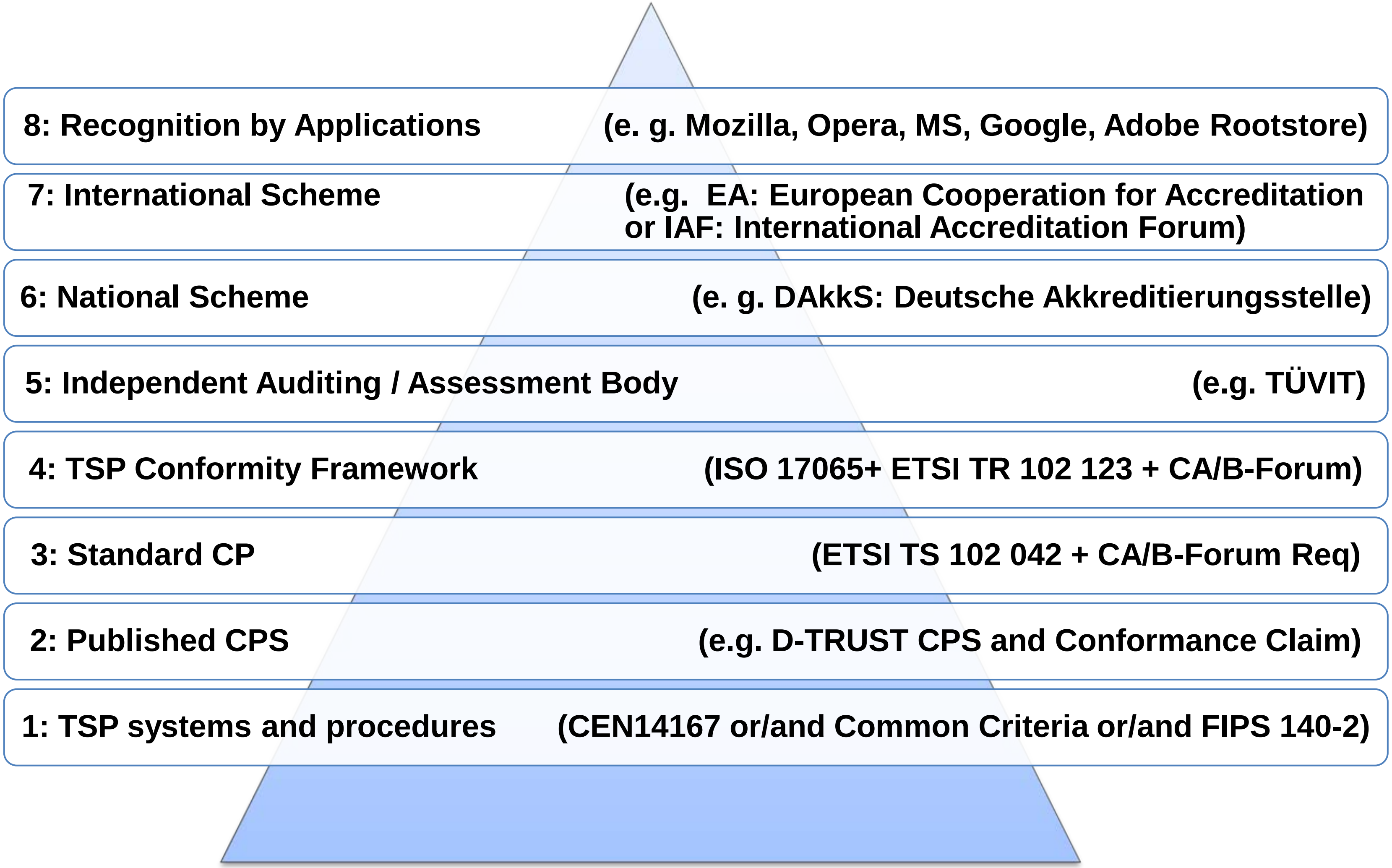
4: TSP Conformity Framework and Audit Requirements

3: Standard for Certification Policy

2: Published Certification Practice Statement

1: TSP systems and procedures

2. Assessment & Certification – actual TSP Perspective (german example)



8: Recognition by Applications (e. g. Mozilla, Opera, MS, Google, Adobe Rootstore)

7: International Scheme (e.g. EA: European Cooperation for Accreditation or IAF: International Accreditation Forum)

6: National Scheme (e. g. DAkkS: Deutsche Akkreditierungsstelle)

5: Independent Auditing / Assessment Body (e.g. TÜVIT)

4: TSP Conformity Framework (ISO 17065+ ETSI TR 102 123 + CA/B-Forum)

3: Standard CP (ETSI TS 102 042 + CA/B-Forum Req)

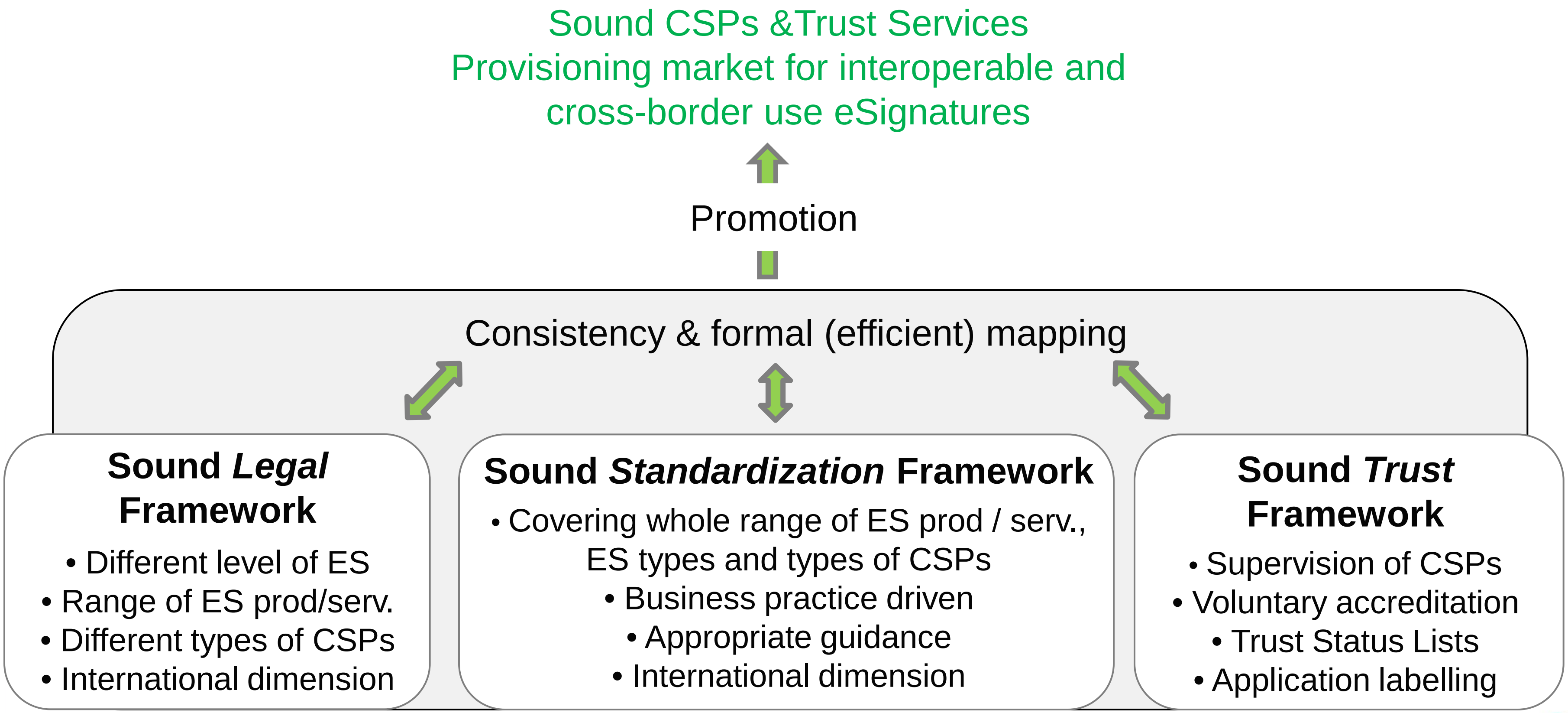
2: Published CPS (e.g. D-TRUST CPS and Conformance Claim)

1: TSP systems and procedures (CEN14167 or/and Common Criteria or/and FIPS 140-2)

New approach to I-A-S in Europe

3. Crobies Study in 2010:
Key success factors for eSignatures

Realizations, consistency and mapping of efficient Legal, Technical, Trust and Promotional frameworks are key success factors to convince market & business stakeholders of the possible ROI of eSignatures securing their eProcesses.



Sound CSPs &Trust Services
Provisioning market for interoperable and
cross-border use eSignatures

Promotion

Consistency & formal (efficient) mapping

Sound *Legal* Framework

- Different level of ES
- Range of ES prod/serv.
- Different types of CSPs
- International dimension

Sound *Standardization* Framework

- Covering whole range of ES prod / serv., ES types and types of CSPs
- Business practice driven
- Appropriate guidance
- International dimension

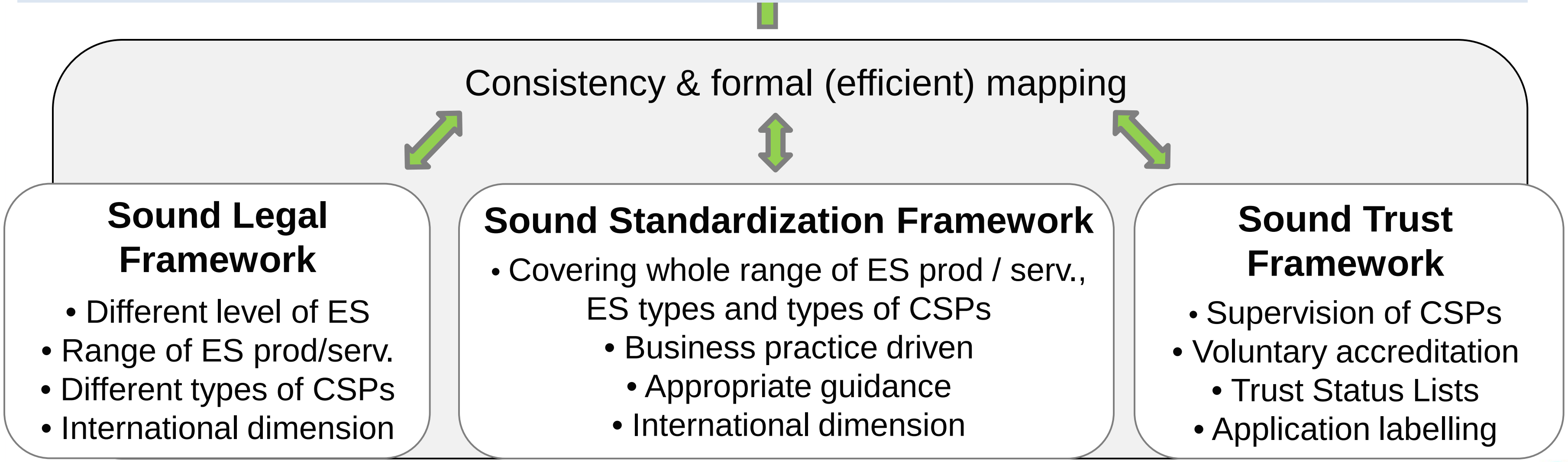
Sound *Trust* Framework

- Supervision of CSPs
- Voluntary accreditation
- Trust Status Lists
- Application labelling

3. Crobies Study in 2010:
Key success factors for eSignatures

Realizations, consistency and mapping of efficient Legal, Technical, Trust and Promotional frameworks are key success factors to convince market & business stakeholders of the possible ROI of eSignatures securing their eProcesses.

Also applicable for SSL-Certs!



Consistency & formal (efficient) mapping

Sound Legal Framework

- Different level of ES
- Range of ES prod/serv.
- Different types of CSPs
- International dimension

Sound Standardization Framework

- Covering whole range of ES prod / serv., ES types and types of CSPs
- Business practice driven
- Appropriate guidance
- International dimension

Sound Trust Framework

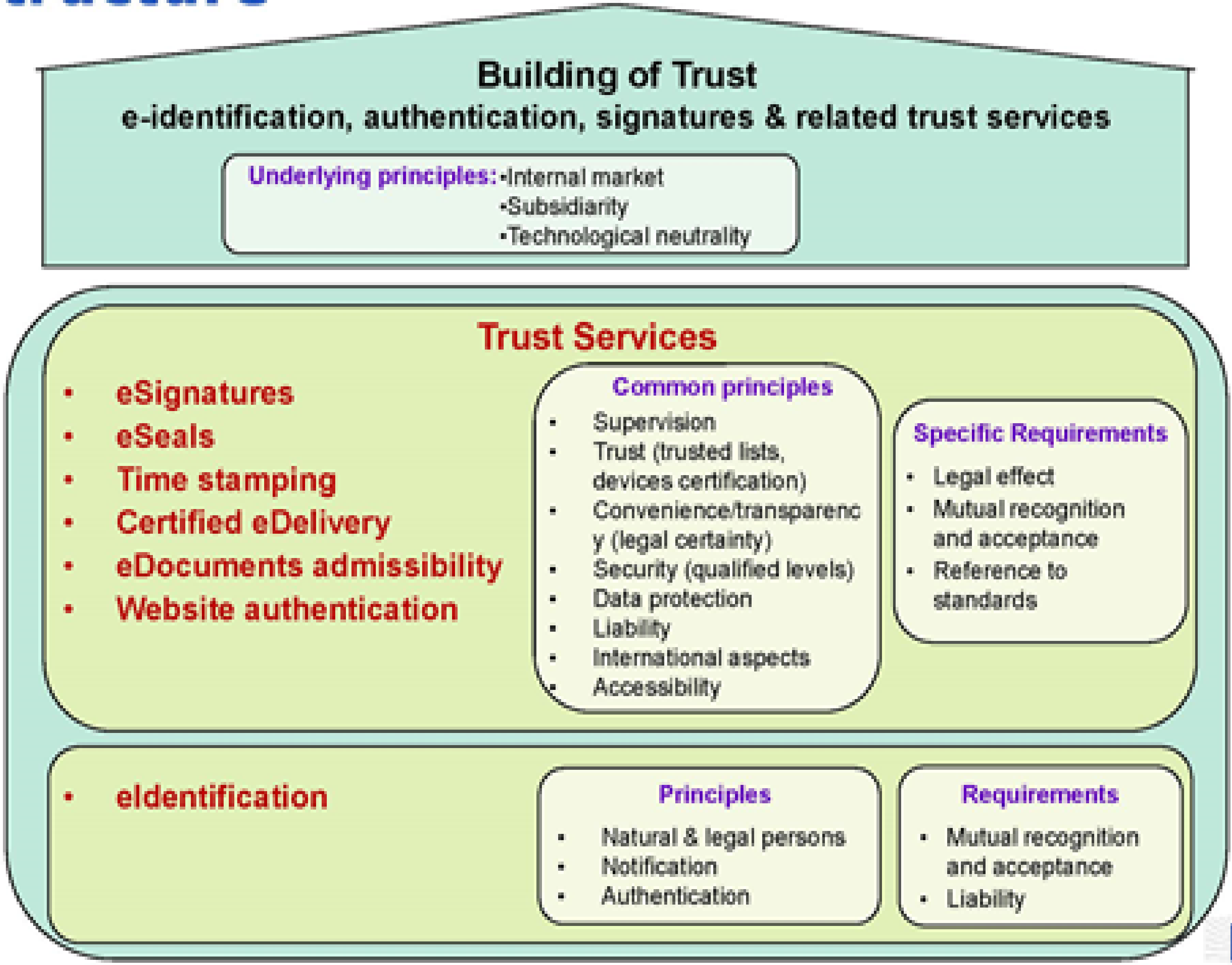
- Supervision of CSPs
- Voluntary accreditation
- Trust Status Lists
- Application labelling

3.1 New approach for legal framework: Draft EU EIDAS- Regulation

June 2012 – EU Commission publish first draft regulation **"on electronic identification and trust services for electronic transactions in the internal market".**

- Added Mutual recognition of electronic identification [E-ID]
- Extended Supervision of "Certification Service Providers" to "Trust Service Providers", includes "proactive supervision"
- Qualified Electronic trust services:
  - Electronic signatures interoperability and usability,
  - Electronic seals interoperability and usability,
  - Time stamping,
  - Electronic delivery service,
  - Electronic documents admissibility,
  - Website authentication.

Structure



Building of Trust

e-identification, authentication, signatures & related trust services

Underlying principles:
- Internal market
- Subsidiarity
- Technological neutrality

Trust Services

- **eSignatures**
- **eSeals**
- **Time stamping**
- **Certified eDelivery**
- **eDocuments admissibility**
- **Website authentication**

Common principles

- Supervision
- Trust (trusted lists, devices certification)
- Convenience/transparency (legal certainty)
- Security (qualified levels)
- Data protection
- Liability
- International aspects
- Accessibility

Specific Requirements

- Legal effect
- Mutual recognition and acceptance
- Reference to standards

- **eIdentification**

Principles

- Natural & legal persons
- Notification
- Authentication

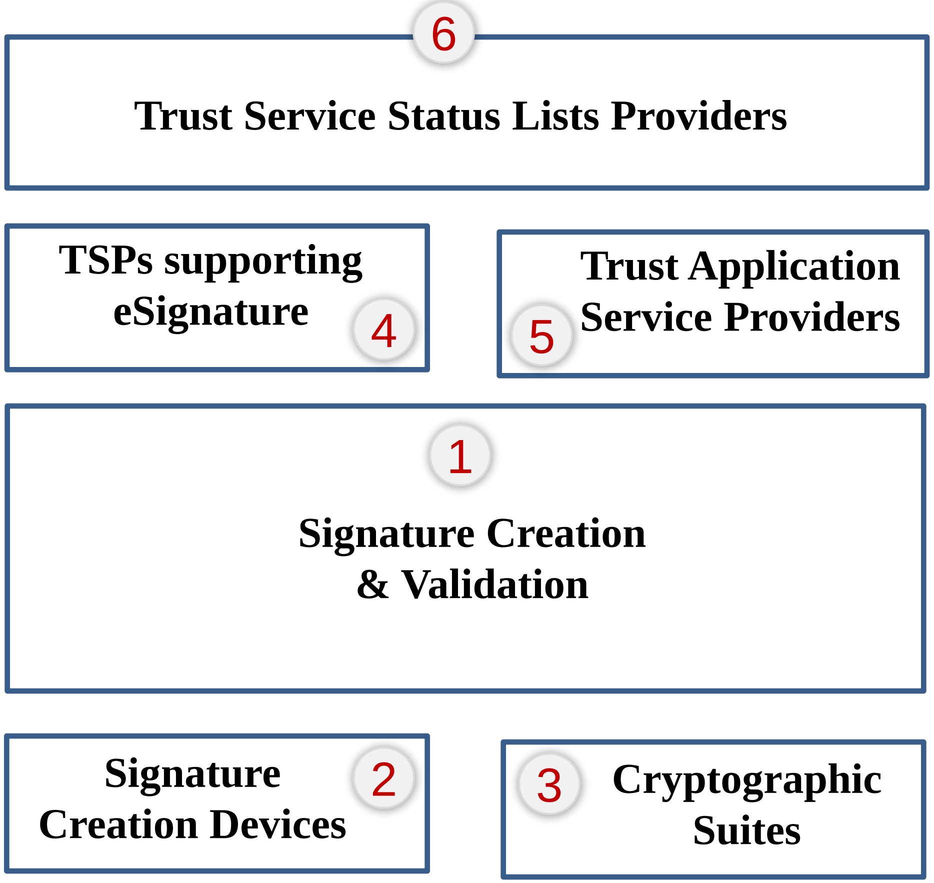
Requirements

- Mutual recognition and acceptance
- Liability

3.2 Standards Framework I:
M460 European Commission mandate

- EC founded eSignatures standardization activities
- 4 years: 2011-2015
- 1st phase (executed)
  - definition of a rationalized standardization framework, in collaboration with CEN
  - several specifications upgrades primarily aimed at providing quick technical fixes to existing electronic signatures standards, and definition of test specifications
- 2nd phase (starting now)
  - implement the rationalized standardization framework
  - support the new EU Regulation on electronic identification and trust services for electronic transactions in the internal market (exp. approval in 2014)

3.2 Standards Framework II Mandate/460



- List of TSP services approved (supervised) by National Bodies (e.g. Trusted Lists)

6 Trust Service Status Lists Providers

- Issuing certificates
- Time-stamping
- Signing Servers
- Validation Services

4 TSPs supporting eSignature

5 Trust Application Service Providers

- Registered eMail
- Long term preservation

- Rules & procedures
- Formats
- Signature Creation / Validation Protection Profiles

1 Signature Creation & Validation

- XAdES (XML)
- CAdES (CMS)
- PAdES (PDF)
- AdES in Mobile envmts
- ASiC (containers)

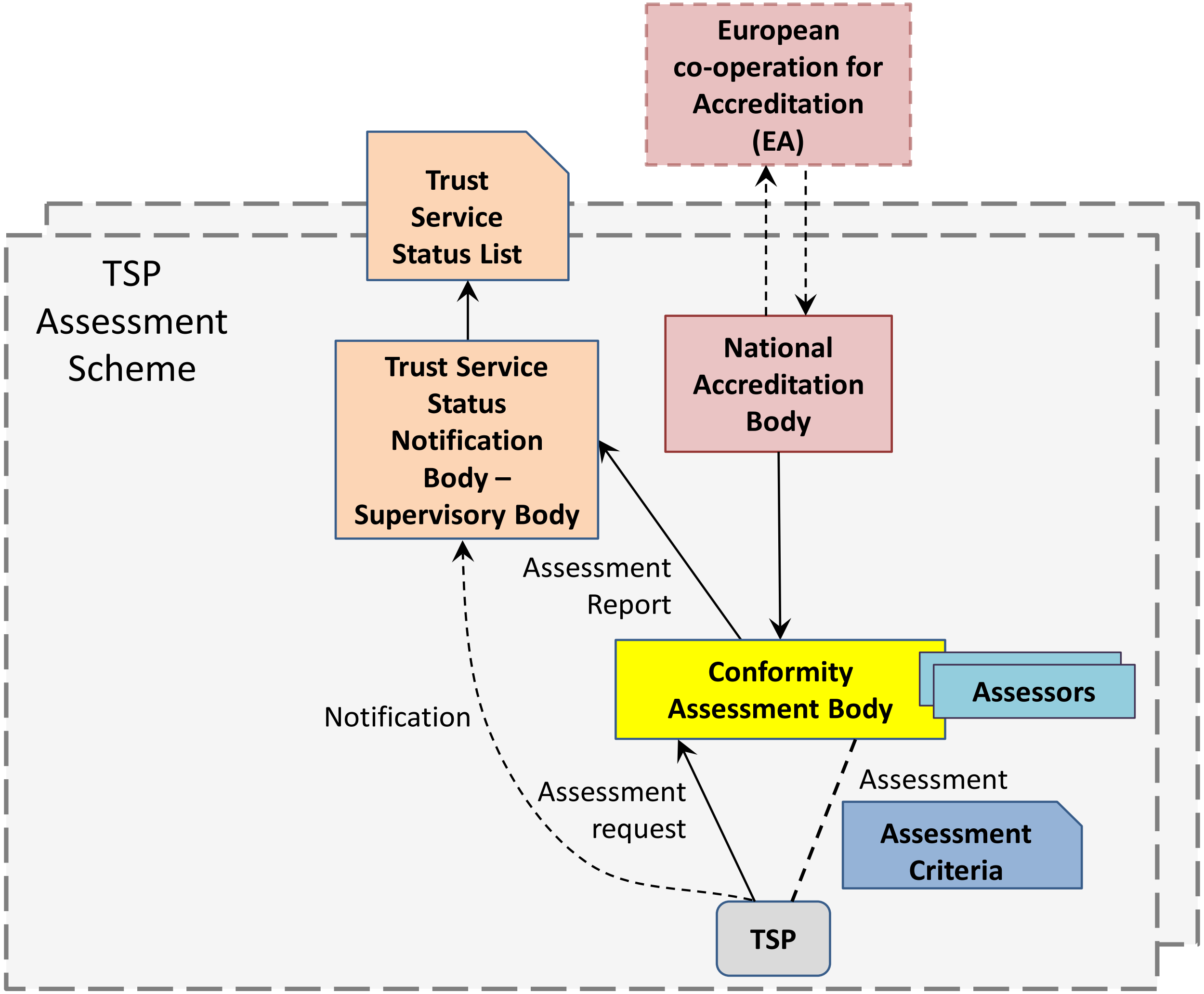
- •Made by CEN:
- •SSCDs (e.g. SC)
- HSMs & other SCDs

2 Signature Creation Devices

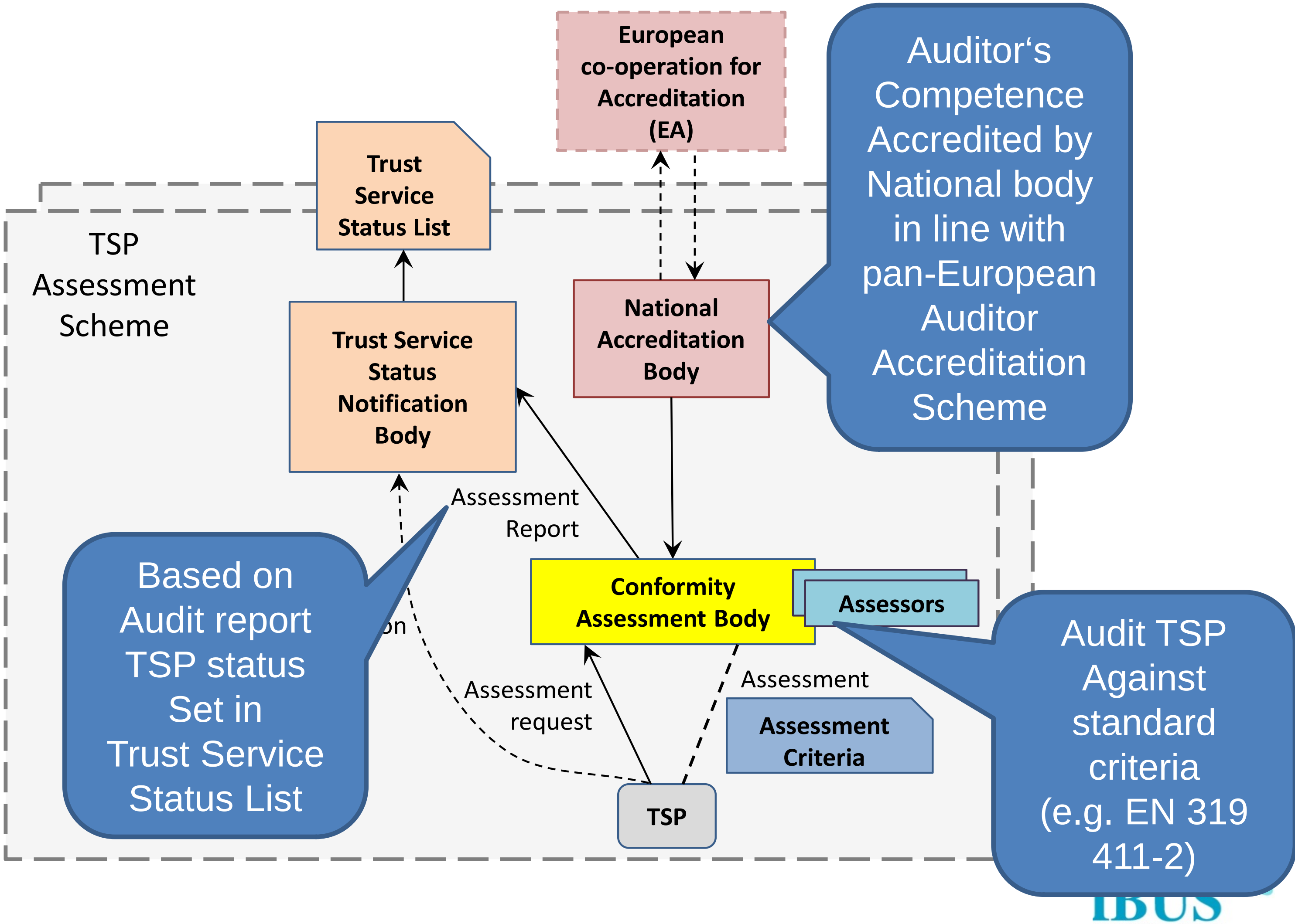
3 Cryptographic Suites

- Key generation
- Hash functions
- Signature algorithms
- Key lengths
- …

3.3 Trust Framework: Model for TSP Conformity Assessment


European co-operation for Accreditation (EA)
Trust Service Status List
TSP Assessment Scheme
Trust Service Status Notification Body – Supervisory Body
National Accreditation Body
Assessment Report
Conformity Assessment Body
Assessors
Notification
Assessment request
Assessment
Assessment Criteria
TSP

3.3 Trust Framework: TSP Conformity Assessment Model


European co-operation for Accreditation (EA)
Trust Service Status List
TSP Assessment Scheme
Trust Service Status Notification Body
National Accreditation Body
Assessment Report
Conformity Assessment Body
Assessors
Assessment request
Assessment
Assessment Criteria
TSP

Auditor's Competence Accredited by National body in line with pan-European Auditor Accreditation Scheme

Based on Audit report TSP status Set in Trust Service Status List

Audit TSP Against standard criteria (e.g. EN 319 411-2)

4. Next Steps

- In Spring 2013 EU Commission publish new 2nd draft regulation "on electronic identification and trust services for electronic transactions in the internal market".
- Under EU Mandate 460 (2013 to 2015) ETSI commissioned to produce
  - European Norm for TSP Conformity Assessment
  - European Norms for Best Practices (Policy Requirements)
    - Qualified Certificates for Personal Signing
    - Qualified Certificates for organisational "seals"
    - Qualified Time-stamping Services
    - Qualified Website Certificates (should be EN 319 411-4)
    - ………….
  - Option to operate as "Sector Specific" implementation of ISO 27001

NIMBUS Technologieberatung GmbH

5. Summary

- Existing national conformity assessment schemes (ISO/IEC 17021/17065) are a suitable and powerful framework for voluntary security assessments of TSPs (**Reactive Supervision**)
- ETSI criteria provide CP's and valuable requirements for the different types of conformity assessment activities
- Additional mandatory network security requirements and certified products will enhance the overall security level of TSPs significantly
- The new draft EU-Regulation will deliver a complete legal and trust framework for **Proactive Supervision** on "qualified level"
- ETSI standards will be a fundamental part in future EU legislation (delegating acts).
- but: "relying parties have to consume Trust"

NIMBUS Technologieberatung GmbH

Thank you !

- ETSI Download :

  http://pda.etsi.org/pda/queryform.asp

  Enter keyword / title / document number

- Draft EU Regulation:

  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:EN:PDF

Contact:

Arno Fiedler: STF 458 arno.fiedler@nimbus-berlin.com
Nick Pope: Lead STF 458 (TSP & e-Signature standards)
nick.pope@thales-esecurity.com