CA Compliance Info-Day
eIDAS and Trust Service Provider Conformity Assessment

Organizer: Bundesdruckerei, TÜVIT, ETSI STF 458
Date: Tuesday, 04.11.2014 from 10:00 AM to 05:00 PM
Venue: Bundesdruckerei, Berlin-Mitte, Conference Center, Kommandantenstraße 15 (**new entrance**)
Website: http://www.bundesdruckerei.de/de/kontakt/kontakt_anfahrt/index.html

Proposed Program: (Status 03.11.2014)

10:00	Welcome by Bundesdruckerei	Kim Nguyen, Bundesdruckerei, Chief Scientist Security, Managing Director, D-Trust	1
	Implementing eIDAS		
	eIDAS Regulation: State of play	Gerard Galler, EC	2
	First experiences with eIDAS	Riccardo Genghini, SNG	3
	Overview CEN/ETSI eSignature Standardisation	Nick Pope, Thales UK	4
	Role of accreditation in the Conformity Assessment Process	Kevin Belson, UKAS	5
	Implementing Conformity Assessment under eIDAS	Christoph Sutter, TÜVIT	6
	Q+A to speaker roundtable		
12:30	*Lunch*		
13:30	**The CA-View on eIDAS Regulation and other relevant policies**		
	CA/Browser Forum Developments	Ben Wilson, DigiCert	7
	Implementing Certificate Transparency:	Inigo Bareira, Izenpe	8
	New directions for signing: FIDO and beyond	Kim Nguyen, D-TRUST	9
	View from a Commercial CA	Robin Alden, Comodo	10
	Digital ID Challenges	Conny Enke, SwissSign	11
	A 10000 foot view on eIDAS from the outer edge of EU	Mads Henriksveen, BUYPASS	12
16:15	**Q+A to speaker roundtable and panel discussion**		
	Lessons learned, “paper-policies” and the actual threads? eIDAS: New business for TSP?	Moderator: Arno Fiedler ETSI STF 458 with Atilla Biler, TÜRKTRUST and Danilo Cattaneo, InfoCert	13 14
17:00-18:00	***Get together***		

eIDAS Regulation

Regulation (EU) N° 910/2014 of 23.7.2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

CA-Day

Berlin, 4.11.2014

Gérard GALLER
DG CONNECT, European Commission
eIDAS Task Force
gerard.galler@ec.europa.eu

Content of eIDAS Regulation

1. Mutual recognition of e-identification means

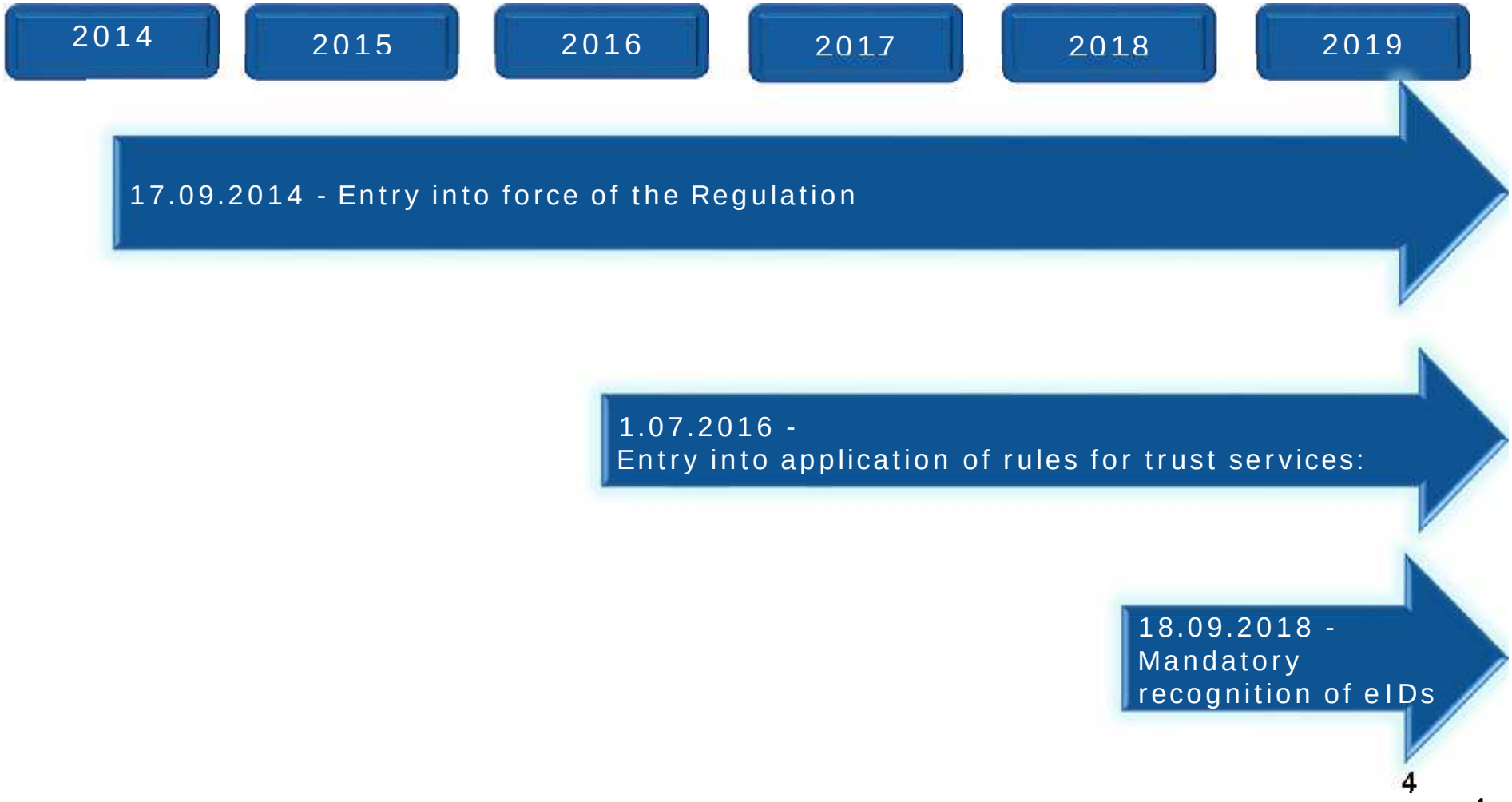
2. Electronic trust services:
   - Electronic signatures
   - Electronic seals
   - Time stamping
   - Electronic registered delivery service
   - Website authentication.

3. Assimilation of Electronic documents

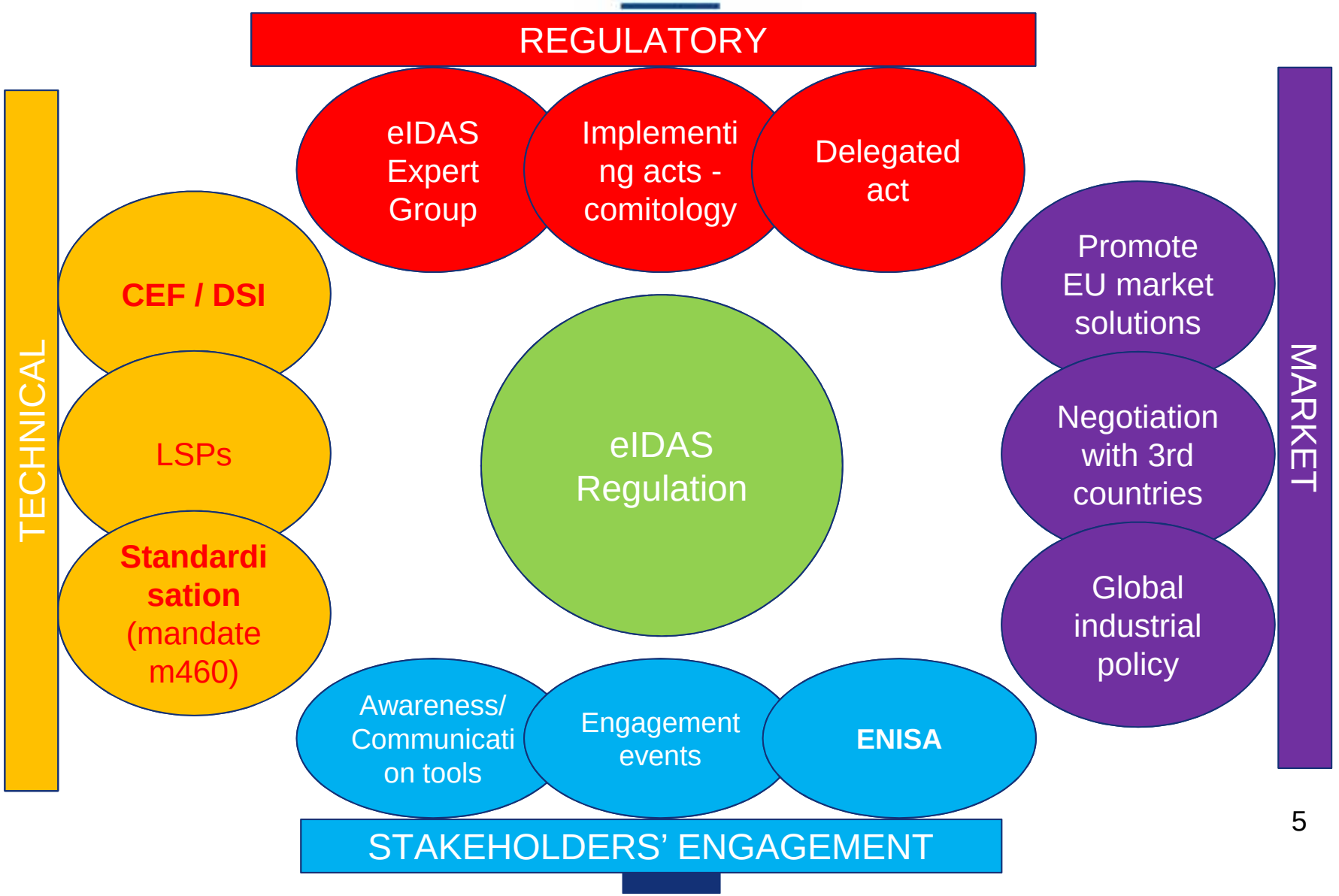
eIDAS – Key legal aspects

- Legal basis: **Art 114 TFEU** on internal market →
  * Free circulation of goods and services
- **One Regulation →**
  * Directly applicable in the 28 EU Member States
  * Also potentially to EEA members (NO, LI, IS)
- **77 recitals + 52 articles** + 4 annexes (42 pages)
- **Contains 28 provisions for implementing measures +1 for a delegated competency**
  - To further specify + complement the Regulation:
  - Most are **optional**: "*The Commission may adopt ….*"
  - Some are mandatory

eIDAS – Timeline of implementation



The full eIDAS picture:



Next steps:
mandatory implementing acts

7 implementing measures due within one year:

- Implementing acts on eID
  - EU Member States cooperation (art. 12.7)
  - Interoperability framework (art. 12.8)
  - eID levels of assurance (art. 8.3)

- Implementing acts on electronic trust services
  - Formats of eSignatures and eSeals for eGov (art. 27, 37)
  - Trusted list (art.22)
  - Trustmark (art.23)

Implementing act on EU Trust Mark for qualified services

Open competition:

You can vote online for your preferred logo!

Voting until 14.11.2014

https://ec.europa.eu/digital-agenda/en/news/e-mark-u-trust-competition-runners-online

Other implementing acts related to Trusted Services

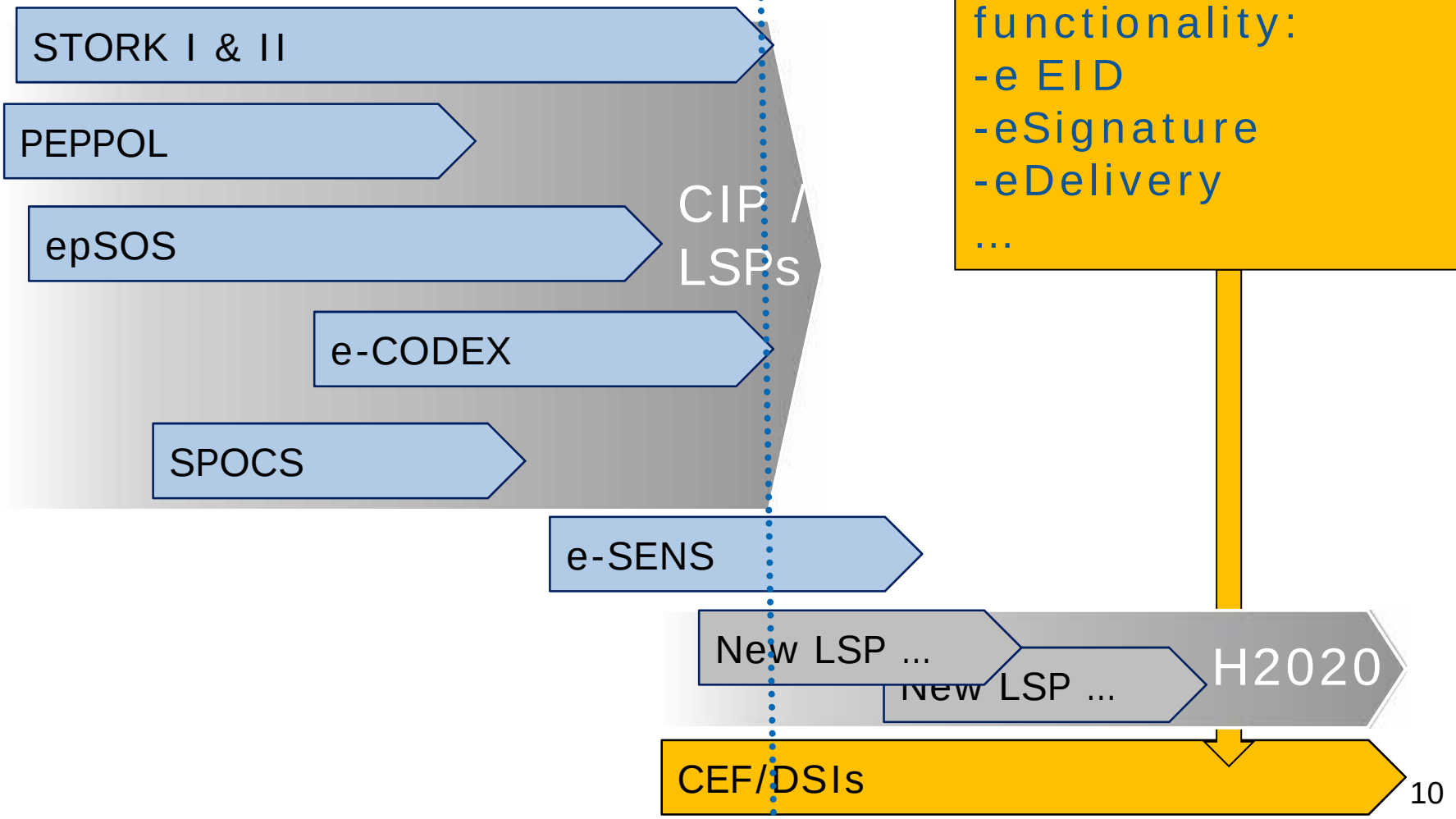
- **Supervisors yearly report** (art 17)
- **Qualified and Non-Q SP security measures** (art 19)
- **Security breaches reporting** (art 19)
- **Initiation of a Q trust service** (art 21)
- **QTSP trustworthy systems** (art 24)
- **QC for eSig, eSeals and Websites** (art 28, 38, 45)
- **Standards for QCSD security evaluation** (art 29, 30)
- **List of certified QCSDs** (art 31)
- **eSig/eSeal Validation** (art 32, 40)
- **Validation, preservation services** (art 33, 34, 40)
- **Timestamping, eDelivery services** (art 42, 44)

ENISA Support for eIDAS

- **Security measures for Trust Service Providers** (art 19):
  - 2012: **Report on implementing eIDAS ex-art. 15** (now art. 19)
  - 2013: **Guidelines for Trust Service Providers**
- **2014 onwards: Guidelines related to:**
  - Common audit scheme for trust services providers
  - Technical guidelines for auditors and supervisors
  - Guidelines for security breaches reporting

- **2015: Forum of SB, CABs and TSPs** (tbc)

Connecting Europe Facility (CEF)



Digital Service Infrastructures:

Provide basic functionality:
-e EID
-eSignature
-eDelivery
...

Open questions

Issue: availabity of accredited CABs by 1.7.2016

- What are priorities for SB, CABs and Q-TSP to be ready for eIDAS?
- What is / are the best option(s) for CAB accreditation?
  - national rules ?
  - "soft" EU guidelines ?
  - Implementing Act ?
- If implementing act: width of scope?
  - Template of Conformity Assessment Report
  - Generic standards (eg ISO 17065)
  - M460 Specific standards (19000 series)
  - .....
- If generic standard: ISO 17065 vs ISO 17021?

For further information and feedback

Web page on eIDAS
http://ec.europa.eu/digital-agenda/en/trust-services-and-eid

Text of eIDAS Regulation in all EU languages
http://europa.eu/!ux73KG

eIDAS functional mailbox
CNECT-TF-eIDAS-LT@ec.europa.eu

EU_eIDAS

CA Compliance Info-Day
eIDAS and TSP Conformity Assessment
Berlin – Nov 4th, 2014

First experiences with eIDAS

Riccardo Genghini
chairman of
ETSI TC-ESI
CEN-ETSI e-SIGN coordination group

Who is SNG?

Studio Notarile Genghini (SNG)
now
Studio Genghini & Associati (SG&A)
is a leading law firm for designing digitalization of the banking industry

BARCLAYS
BPM
CARIPARMA CRÉDIT AGRICOLE
Deutsche Bank
ING DIRECT La tua banca a conti fatti.
MEDIOLANUM GRUPPO MEDIOLANUM
UniBank
witness

SNG
and eWitness

SNG is also designing for eWitness SA,
signature environments, long term preservation facilities
and registered delivery components, in order to issue
cross border European Electronic Trust Services

Overview of this presentation

- SMEs, innovation and job creation
- TSP assessment and Member States
- Internal market and cooperation of TSPs from different Member States
- QeSCD certification and alternative procedures

SMEs, innovation and job creation

- new OECD work shows that, among small and medium-sized enterprises (SMEs, < 250 employees), young firms play a central role in creating jobs and enhancing growth and innovation
  - based on new data from OECD DynEmp project (2001 – 2011)
  - Criscuolo, Gal and Menon (2014), "The Dynamics of Employment Growth: New Evidence from 18 Countries", OECD Science, Technology and Industry Policy Papers no. 14, OECD Publishing http://dx.doi.org/10.1787/5jz417hj6hg6-en

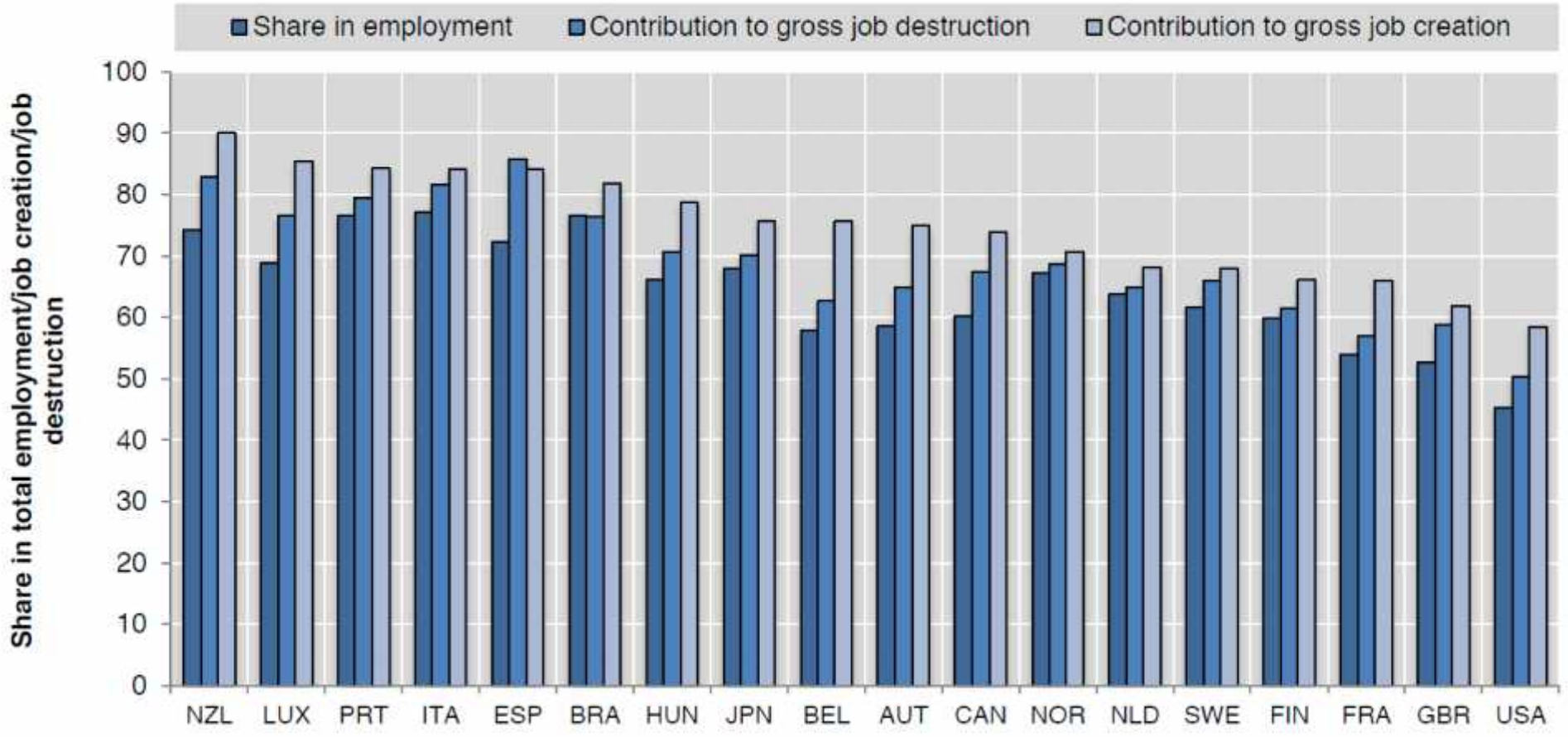
SMEs, innovation and job creation

- SMEs employ on average 65% of the workforce and account for
  - 75% of total gross job creation
  - 75% of the jobs destroyed
- most of SMEs are old or mature firms
- young (innovative) SMEs are the primary source of job creation
  - 42% of total job creation and 22% of total job destruction
  - young firms were hit the hardest by the crisis …
  - … but continue to create the most jobs

SMEs, innovation and job creation

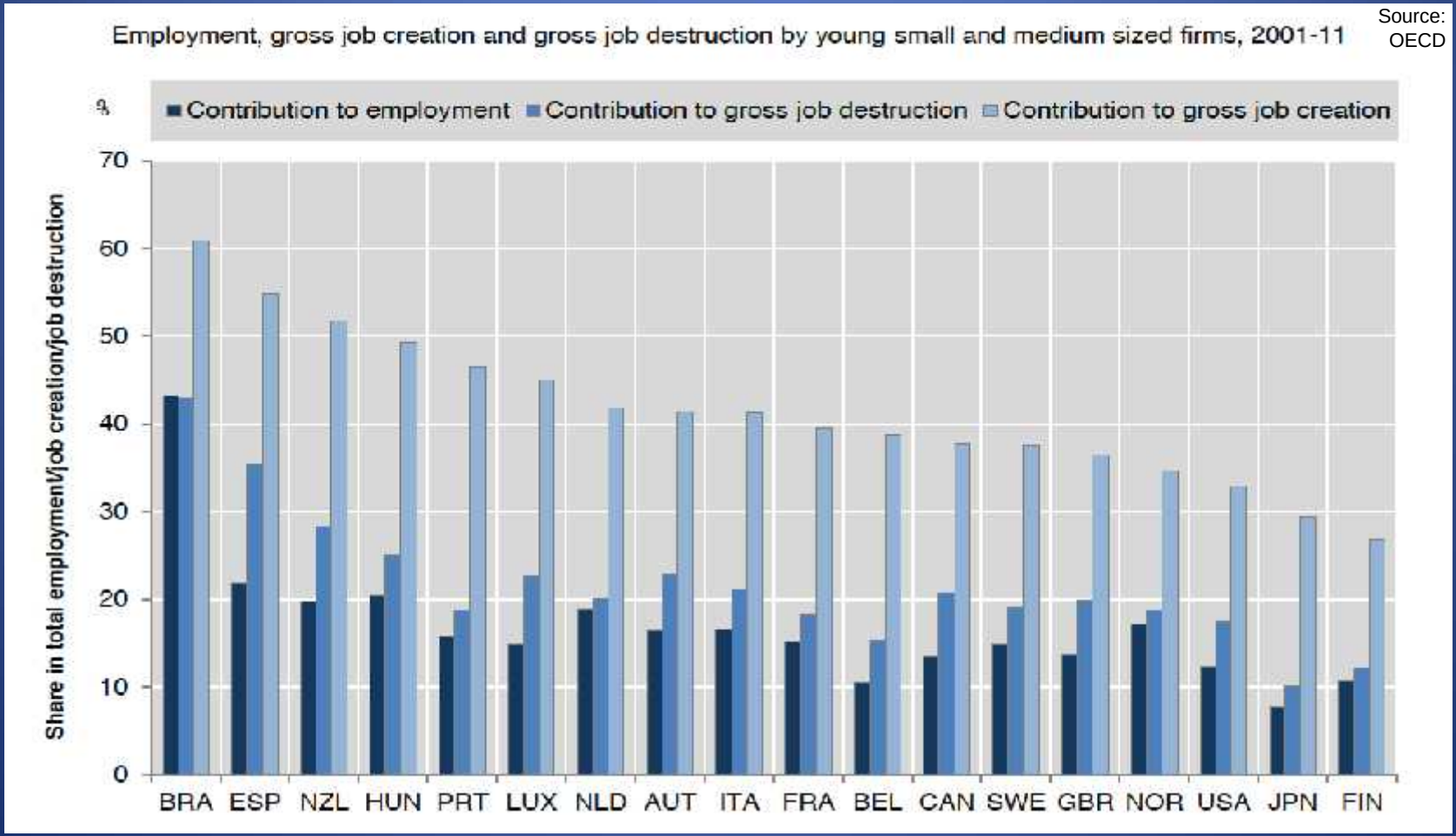
Averages over the 2001-2011 period for 18 countries

Source: OECD



SMEs, innovation and job creation

Source: OECD



TSP assessment and Member States

- TSPs that operate cross border and are assessed (i.e. supervised) at national level, will become the norm, like in banking industry
- As in banking industry, aviation, shipping, some legal and regulatory environments will prove more efficient: there will the most part of the EU Qualified TSPs have their registered offices
  - Where will it be? It depends on the choices of national supervision schemes. Great opportunity for some new EU Member States !!!!

TSP assessment and Member States

History (1997-2014) has proven that the real issue is NOT what is in theory the best possible security. In some EU member states with great technologic tradition, qualified signatures never took up ! What have we learnt ?

- that if supervision is too formal, costs for EU QTSP will soar, and only incumbents will be able to be part of the game, or even there will be no game at all;
- that is supervision fails, the whole system is at risk

Single market and TSP cooperation

- eIDAS Regulation builds on
  - the principle of the internal market (Art. 4)
  - the definition of Trusted Services (and of the related Providers) that extends the provisions on the Certification Service Providers as defined by the Directive 1999/93/EC
  - International cooperation (Art. 14)

Single market and TSP cooperation

- through these pillars, the eIDAS Regulation is strongly inducing Providers that are accredited, to develop an European strategy and to complete their offering of Trusted Services
  - from our observatory we see TSPs from different Member States cooperate for this objective
  - currently contractual agreements and due diligences are ongoing (no names ... privileged information!!!)

Single market and TSP cooperation

Regulation eIDAS - Article 30

- Paragraphs 1 & 2 state that
  - conformity of qualified electronic signature creation devices (QeSCD) with Annex II requirements must be certified by public or private bodies designated by Member States
  - Member States must notify to the Commission the names and addresses of such bodies
  - the Commission shall make this information available to Member States

Regulation eIDAS - Article 30

- When will paragraphs 1&2 come into force?
  - after publishing of Implementing Acts, even before 1st of July 2016 (logical interpretation)
  - On the 1st of July 2016 (formal interpretation)
- Read Art. 52 (2.a)…

Regulation eIDAS - Article 30

- paragraph 3 states that the conformity certification of QeSCD must follow one of these security evaluation processes
  - a process specified by a standard for the security assessment of IT products referenced by an Implementing Act (IA)
  - an alternative process (to be notified to the EC) that uses comparable security levels, if no referenced standard exists

Regulation eIDAS - Article 30

- When will paragraph 3 come into force?
  - after publishing of Implementing Acts (logical interpretation)
  - already in force (formal interpretation)
- Read Art. 52 (2.a)…

Conclusions

- There is a great opportunity in Reg. 910/2014/EU, the outcome depends on how it is implemented.
  - If the aim will be to create a single innovative market, it will be a success.
  - If the aim will be to protect national champions, it will fail.

MOST DEPENDS ON HOW SUPERVISION IS IMPLEMENTED AND HOW BIG DIFFERENCES IN ITS IMPLEMENTATION WILL BE !

Thank you for the attention!

Riccardo Genghini
ETSI ESI CHAIRPERSON
riccardo.genghini@ewitness.eu
www.riccardogenghini.eu

ETSI STANDARDS FOR TSP CONFORMITY ASSESSMENT - UPDATES FOR eIDAS

CA Day 4 Nov 2014 – eIDAS & TSP Conformity Assessment

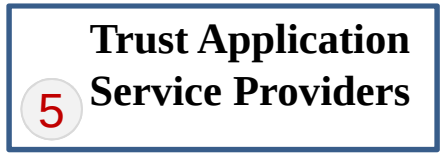
Topics

- Requirements of eIDAS
- ETSI Standards for TSP Conformity Assessment
- Time-scales

eSignature Standards Framework

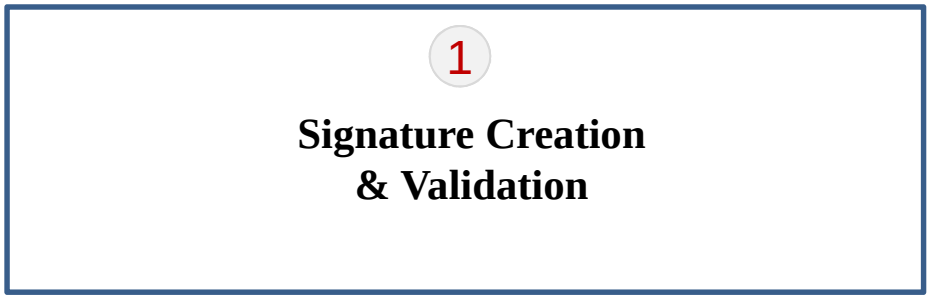
• List of TSP services approved (supervised) by National Bodies (e.g. Trusted Lists)

• Certificate Authority
• Time-stamping
• Signing Servers
• Validation Services



• Registered eMail
• Long term preservation

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



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

(CEN)
Common Criteria Protection profiles
• Smart Cards
• HSMs
• Signing services

• Key generation
• Hash functions
• Signature algorithms
• Key lengths
• ...

eIDAS Regulatory Main Requirements

- Requirements for all EU TSPs (excluding “closed” systems)
  - Liability (Article 13)
  - Security measures “commensurate to the degree of risk” (Article 19.1)
  - Reporting on security breaches (Article 19.2)

- Requirements for “qualified TSP”
  - Specific requirements TSPs practices (Article 24)
  - Specific requirements on Certificate Formats (Annex I, III and IV)
  - Bi-Annual Audit (Article 20)

ETSI Standard – EN 319 401 (TS 119 401) General Policy Requirements for TSPs

- EN 319 401 General Policy Requirements for TSPs
  - Based on Risk Assessment (e.g. ISO/IEC 27005)
  - Trust Service Practice Statement, Terms & Conditions, Security Policy
  - General requirements on TSP Management and Operation (e.g. 27002)

ETSI Standard – EN 319 411 (TS 119 411) Policy Requirements for TSPs issuing Certificates

- Part 1: General Requirements for Trust Service Providers issuing certificates
  - Based on CAB Forum Requirements
  - May be used for CAB Forum Conformance or other uses
  - References EN 319 401 for general requirements
  - References X.509 & EN 319 412 for certificate format
  - Equivalent to existing ETSI TS 102 042
- Part 2: Requirements for Trust Service Providers issuing qualified certificates
  - Meets specific requirements of eIDAS regulation for qualified TSPs
  - References EN 319 411-1 for general requirements for issuing certificates
  - Equivalent to existing ETSI TS 101 456

ETSI Standard EN 319 412 (TS 119 412) (X.509) Certificate Profiles

- Part 1: Overview & common data structures
- Part 2: certificates issued to natural persons
  - Includes variant for (eIDAS Annex I) qualified certificates
  - Equivalent to existing ETSI TS 102 280
- Part 3: certificates issued to legal persons
  - Includes variant for (eIDAS Annex III) qualified certificates
- Part 4: web site certificates issued to organisations
  - Based on CAB Forum requirements
  - Includes variant for (eIDAS Annex III) qualified certificates
- Part 5: Qualified certificate statements for qualified certificate profiles
  - Referenced from other parts qualified certificate requirements
  - Equivalent to existing ETSI TS 101 862

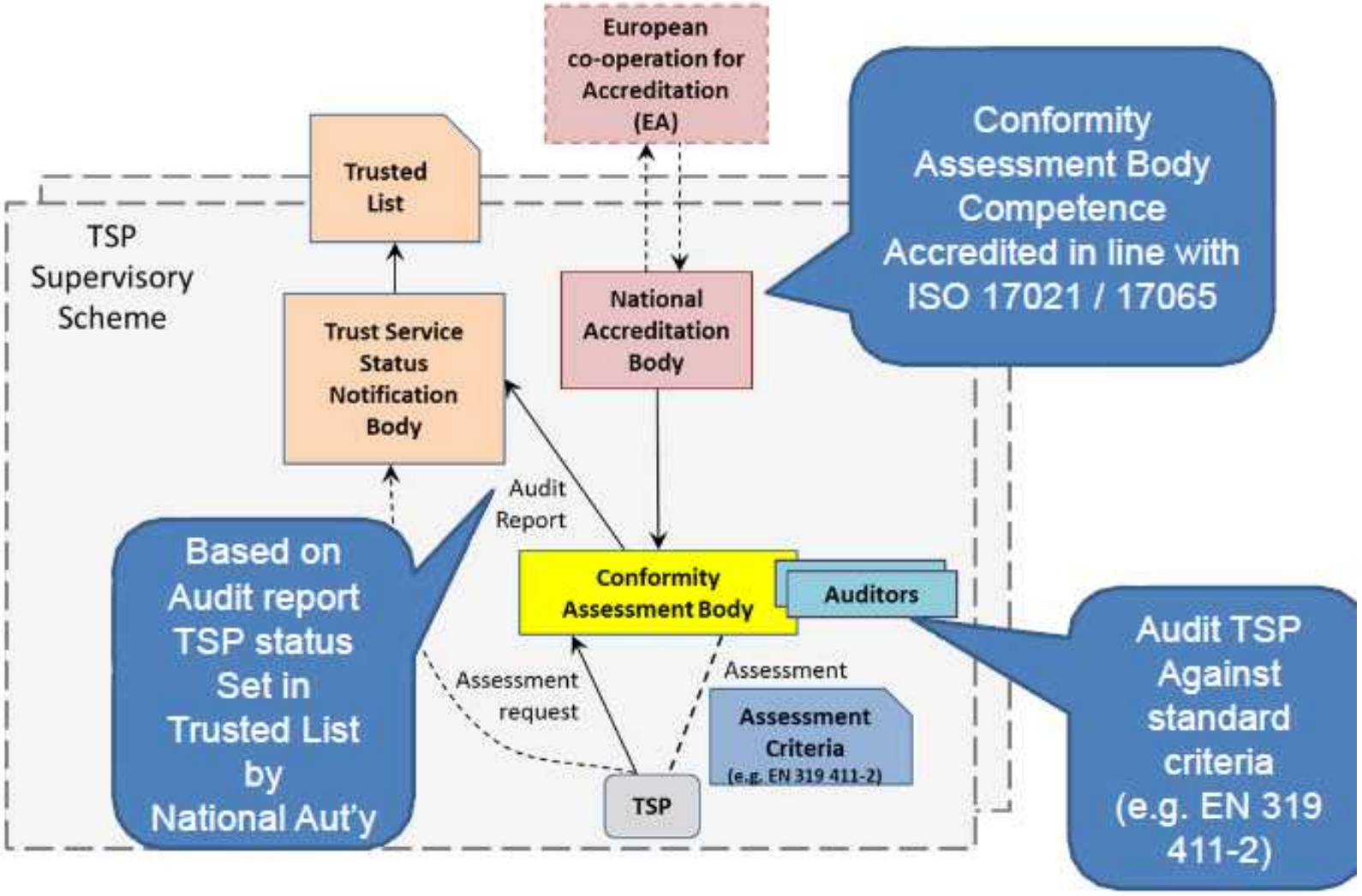
ETSI Standards - Time-stamping
EN 319 421 (TS 119 422) & 319 422 (TS 119 422)

- EN 319 421 – Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps
  - References EN 319 401 for general requirements
  - Equivalent to existing ETSI TS 102 023
  - Includes variant for qualified time-stamping
- EN 319 422 – Time-stamping protocol and electronic time-stamp profiles
  - Profiles RFC 3161
  - Equivalent to existing ETSI TS 101 861
  - Separate requirement for “Qualified” time-stamping statement

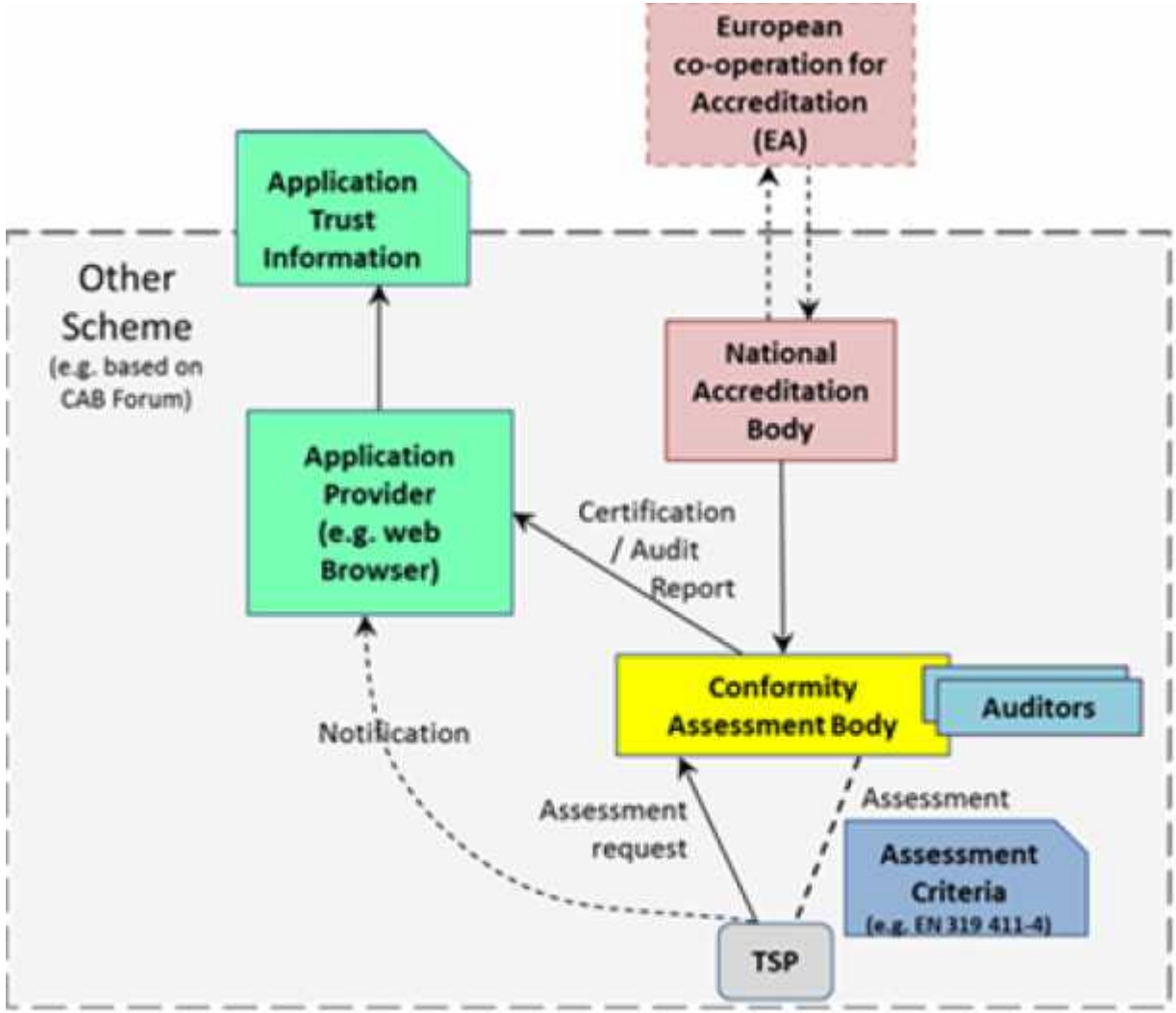
ETSI Standard EN 319 403 (TS 119 403)
TSP Conformity Assessment

- Specifies requirements on capabilities on “Conformity Assessment Bodies” and how they carry out audit
- Overseen by National Accreditation Bodies
- Aim to support both eIDAS and CAB Forum audit requirements

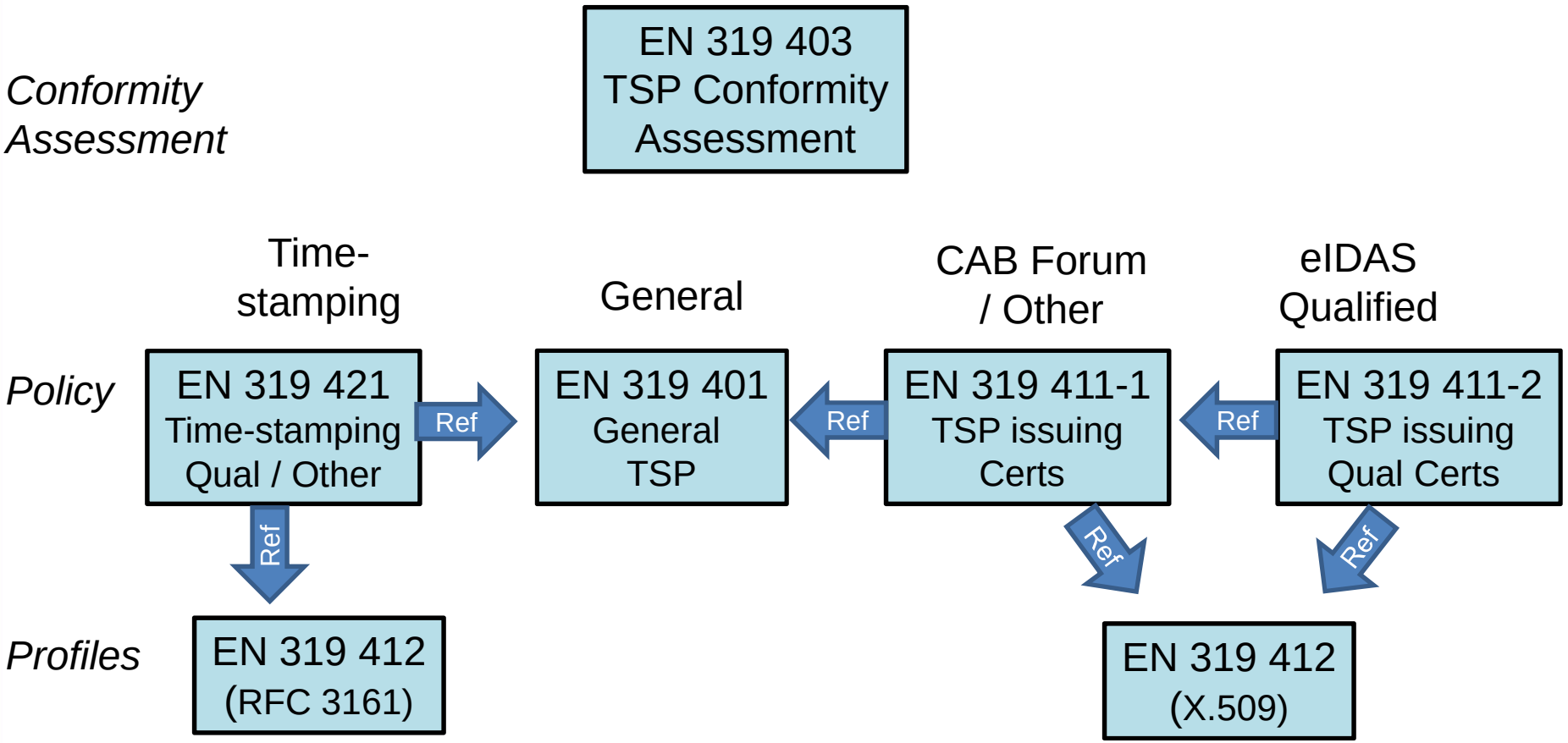
EN 319 403 TSP Conformity Assessment : Model: Regulatory Adoption



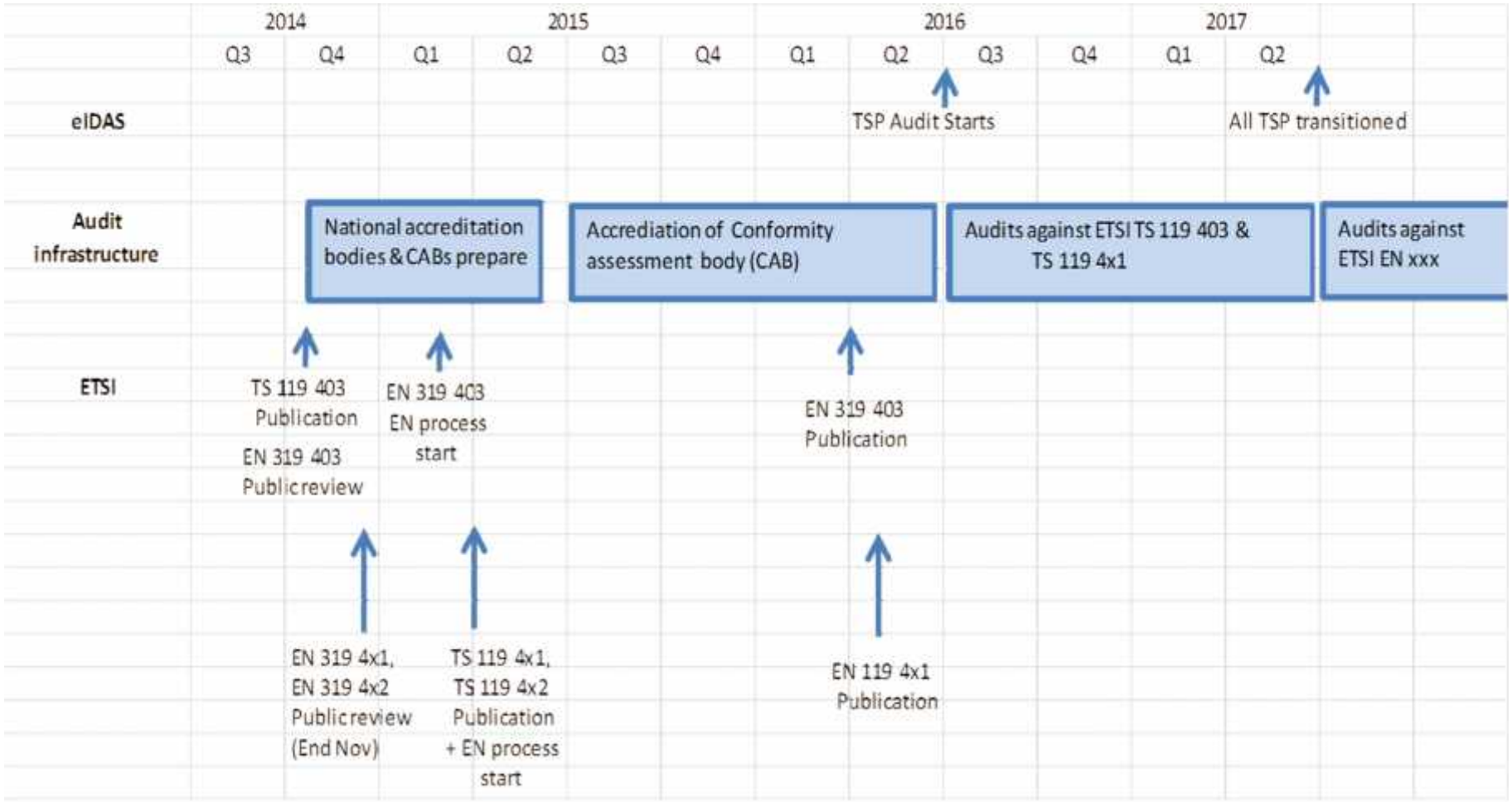
EN 319 403 TSP Conformity Assessment : Model: Non-Regulatory Adoption



ETSI TSP Standards Overview



ETSi TSP Standards Time-scale



Time-scale Key Points

- TSP Conformity Assessment
  TS Publication, EN formal review starts, Nov 2014
- TSP Policy Requirements and Profiles
  Public review Jan 2014
  TS Publication, EN formal review starts, April 2015
- Audit framework in place using TS versions – July 2016
- Migration to EN – Jul 2017

Thank you

Further Information:

- http://www.e-signatures-standards.eu/
- Subscribe to E-SIGNATURES_NEWS e-mail list
- http://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx

European co-operation for Accreditation

Trust Service Provider Conformity Assessment

The role of accreditation in the Conformity Assessment Process.

Presenter

Kevin Belson

- **Technical Manager – United Kingdom Accreditation Service (UKAS)**
- **Vice Chair EA Certification Committee**
- **Convenor – EA Task Force Group for ETSI**

European co-operation for Accreditation

A Brief Introduction to EA

The European co-operation for Accreditation (1)

- EA is **appointed by the European Commission** to **manage the accreditation infrastructure** within the EU, EFTA and candidate countries.
- EA is a **not-for-profit** association of nationally recognised accreditation bodies
- EA was **established** in 1997 and registered in NL in 2000
- 35 **full members** representing 35 European economies
- 13 **associate members**
- permanent **EA-Secretariat** of 5 persons

The European co-operation for Accreditation (2)

- EA is an active member of recognised international cooperations:

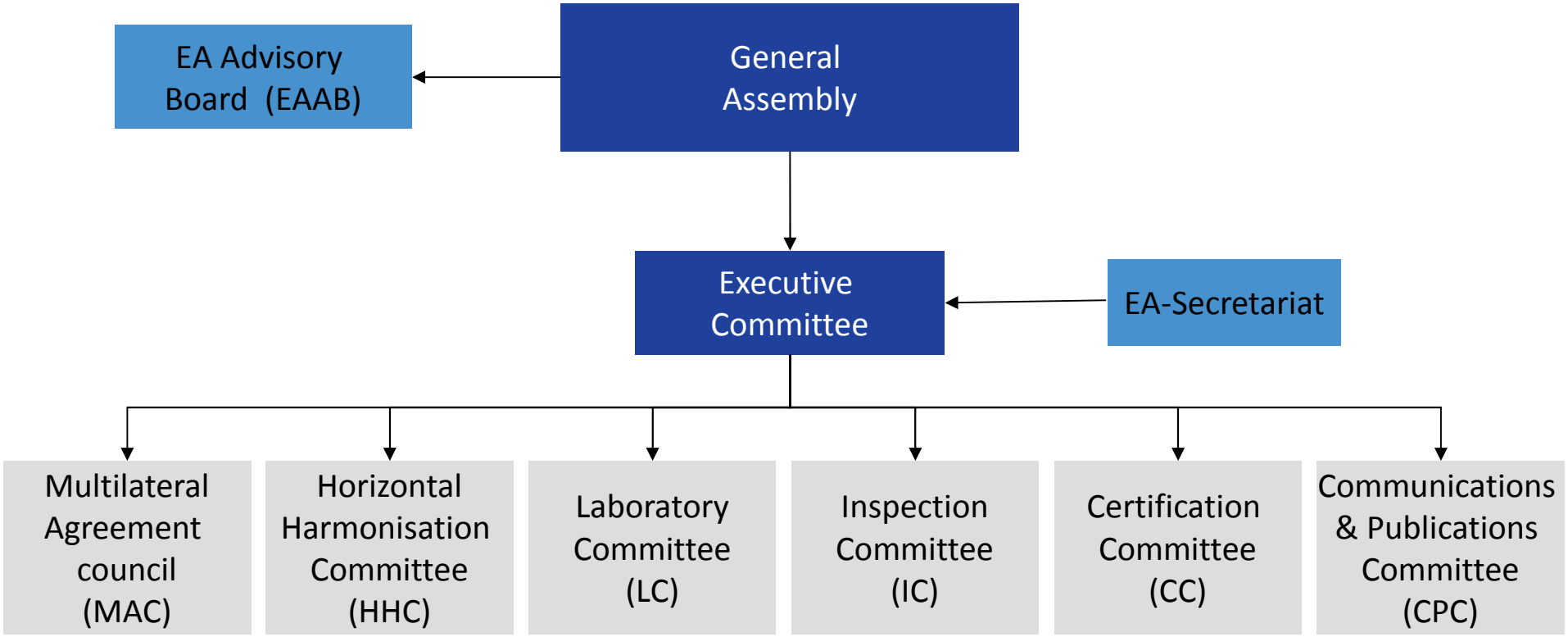
➢**ILAC**
(International Laboratory Accreditation Cooperation)

➢**IAF**
(International Accreditation Forum)

Purpose of EA

- Provide Europe with an **effective, reliable accreditation infrastructure**
- Develop accreditation criteria and guidelines supporting **harmonisation of practices**
- Operate a sound, robust, reliable **peer evaluation** process
- **Ensure equivalence** of accreditation and equal reliability of accredited results
- Cooperate with the **European Commission** and other European, international stakeholders

EA Organisational Structure



EA MLA Signatories

- EA MLA Signatories and the accreditations they grant are **internationally recognised** through the **ILAC and IAF Multilateral Agreements**.

- Each signatory is subject to routine rigorous evaluations by **peer evaluation** teams in order to verify continuing compliance with
  - the **Regulation 765/2008** and
  - the international standard for accreditation bodies (**ISO/IEC 17011**).

Standards for Accreditation (1)

Accreditation Body ← ISO/IEC 17011

Certification Bodies

EMAS Verifiers Council Regul. 1221/2009	ISO/IEC 17065 (EN45011)	ISO/IEC 17021	ISO/IEC 17024
Eco-Management Audit Scheme	Products	Management Systems	Persons




Standards for Accreditation (2)

Accreditation Body ← ISO/IEC 17011

Laboratories	**Inspection Bodies**
ISO/IEC 17025 ISO 15189	ISO/IEC 17020
Testing and Calibration	Inspection

EA MLA Signatories

33 Full Member accreditation bodies have signed the EA MLA, out of which 26 have signed for all accreditation activities covered by the EA MLA.

Full details of the scope for MLA Signatories can be found on the EA website

European co-operation for Accreditation

EN 319 103
The EA Role

EA Involvement

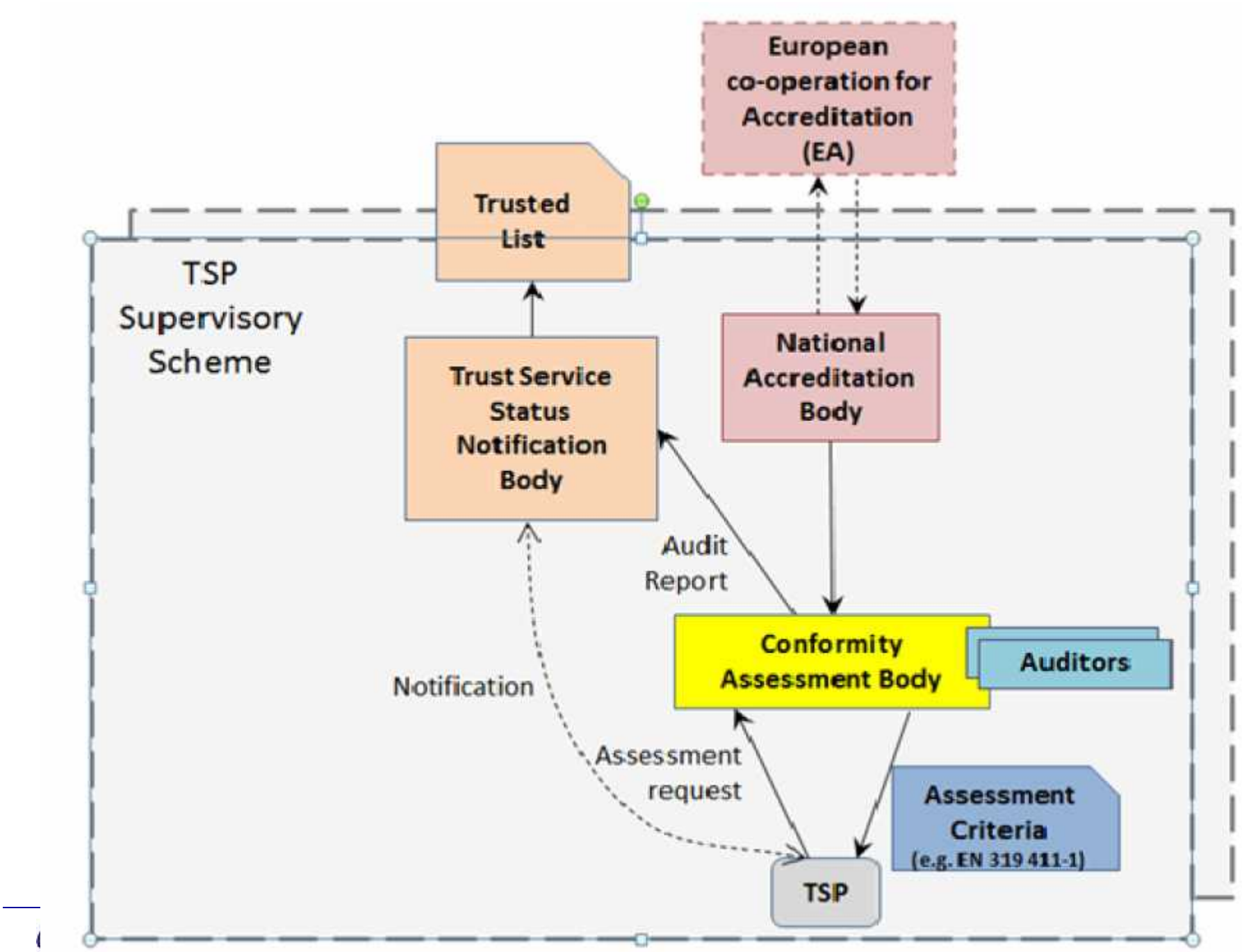
- Task Force Group (TFG) set up to advise on definition of the Conformity Assessment Requirements

- TFG consists of Accreditation Body representatives from UKAS; SWEDAC; COFRAC.

- TFG liaises between the ETSI drafting committee and the EA Certification Committee.

Main Role of the National Accreditation Body

To assess and accredit Certification Bodies as competent to assess to ETSI Conformity Assessment Requirements.


European co-operation for Accreditation (EA)
Trusted List
TSP Supervisory Scheme
Trust Service Status Notification Body
National Accreditation Body
Audit Report
Conformity Assessment Body
Auditors
Notification
Assessment request
Assessment Criteria (e.g. EN 319 411-1)
TSP

Conformity Assessment Requirements

- ISO/IEC 17065
- EN 319 403 (the scheme document)
- eIDAS regulation No 910/2014

Conformity Assessment Standard

ISO/IEC 17065

Conformity assessment — Requirements for bodies certifying products, processes and services.

Why ISO/IEC 17065?

Covers all aspects of the TSP conformity assessment requirements.

For example – clause 6.2.1:

"When a certification body performs evaluation activities, either with its internal resources or with other resources under its direct control, it shall meet the applicable requirements of the relevant International Standards and, as specified by the certification scheme, of other documents……."

Accreditation process

Initial Assessment

Surveillance

Reassessment

Accreditation process

Migration from existing schemes

"There are currently various schemes and programmes currently in place requiring accreditation to EN 45011; ISO/IEC 17021 for delivering certification according to ISO 27001 (in this case including fulfilling ISO 27006), or ISO 20000. In addition, a number of EU countries have assessed conformance to Directive 1999/93 (which the eIDAS regulation replaces), as well as a number of TSPs claimed conformance to the CAB Forum requirements, based on TS 102 042 and TS 101 456 which are replaced by EN 319 411-1 and 411-2. All existing arrangements will need to transition to accredited assessment against TS 119 403 and then EN 319 403. "

Implementing Conformity Assessment under eIDAS

Christoph Sutter

Outline

- What is required from eIDAS?
- How to audit compliance to eIDAS?
- When to start conformity assessment?
- Summary

eIDAS and Conformity Assessment

Objectives for conformity assessment

- confirm compliance to regulation of qualified TSP and services (every 24 month and ad hoc on demand of supervisory body)
- high level of security and legal certainty of trust services
- support of supervisory bodies (via report)
- use synergies of international schemes (reg. 765/2008) for conformity assessment of products and services

Conformity assessment (certification) of QSCD

- certification of qualified electronic signature / seal creation devices (QSCD) with respect to Annex II

Role of Conformity Assessment Report

- to be submitted from TSP to supervisory body from
  - existing CSP: asap but not later than 1 July 2017
  - new TSP / qualified trust service: together with notification
  - qualified TSP: every 24 month within 3 days after receipt
  - qualified TSP: ad hoc on request of supervisory body
- Support supervisory bodies
  - report analysis
  - mutual assistance between supervisory bodies
- possible additional contents
  - equivalent assurance of identification methods in terms of reliability to physical presence
  - equivalent signature/seal method concerning security and compliance for timestamps

TSP for qualified certificates - Requirements

- main requirements for qualified TSP for signatures
  - Article 15: Accessibility for persons with disabilities
  - Article 19: Security Requirements applicable to TSP
  - Article 20: Supervision of qualified TSP
  - Article 24: Requirements for qualified TSP
  - Article 28: Qualified certificates for electronic signatures
    - Annex I: Req. for qualified certificates for electronic signatures

6 Service Types for Trust Service Providers

1. qualified certificates for el. signatures (art. 28, Annex I)
2. qualified certificates for el. seals (art. 38, Annex III)
3. qualified validation service (art. 33, 32, 40)
4. qualified preservation service (art. 34)
5. qualified el. registered delivery service (art. 44)
6. qualified certificates for website authentication (art. 45, Annex IV)

Requirements from Article 19 “Security Incidents”

- take appropriate technical and organizational measures to manage the risks posed to security
- consider latest technological developments
- level of security is commensurate to degree of risks
- prevent and minimize impact of security incidents
- inform stakeholders of adverse effects of incidents
- notify incidents within 24 hours to supervisory body
- implementing acts for
  - appropriate technical and organizational measures
  - formats and procedures and deadlines for notification

Requirements from Article 24.1 “ID verification”

- verify identity by appropriate means and in accordance with national law:
  a. by physical presence
  b. remotely using electronic identification means ensuring
     - physical presence (prior to certificate issuance) and
     - assurance level substantial or high (cf. article 8)
  c. by means of a certificate of a qualified signature or seal issued in compliance to points a. or b.
  d. by use of other authentication methods recognized at national level with equivalent assurance in terms of reliability to physical presence
     - to be confirmed by conformity assessment body

Requirements from Article 24.2 “q-TSP” (1 / 3)

a. inform supervisory body about changes and intention to cease activities
b. employ qualified, experienced and reliable staff
c. maintain sufficient financial resources / appropriate liability insurance
d. publish terms and conditions for service use

Requirements from Article 24.2 “q-TSP” (2 / 3)

e. use trustworthy systems that are protected against modification and ensure technical security and reliability of processes supported by them

f. use TWS to store data provided to it in a verifiable form so that
   - retrieval only after consent of affected person
   - only authorised person can make entries / changes
   - data can be checked for authenticity

g. take appropriate measures against forgery and theft of data

Requirements from Article 24.2 “q-TSP” (3 / 3)

h. record and keep accessible relevant data for the purpose of legal proceedings and continuity of service for an appropriate period of time

i. have an up to date termination plan

j. ensure lawful processing of personal data

k. establish and keep update a certificate database

- implementing acts for
  - reference numbers of standards for TWS that comply with points e. and f.
  - formats and procedures and deadlines for notification

Requirements from Article 24.3/24.4 “revocation”

- register revocation in certificate database and publish revocation status of certificate in a timely manner
- at latest within 24 hours after receipt of request
- revocation becomes effective immediately after publication
- information shall be given to any relying party
  - at least on a per certificate basis *at any time* in an automated manner
  - *also beyond the validity of the certificate*
  - reliable, free of charge and efficient

How to audit compliance to Regulation 910/2014?

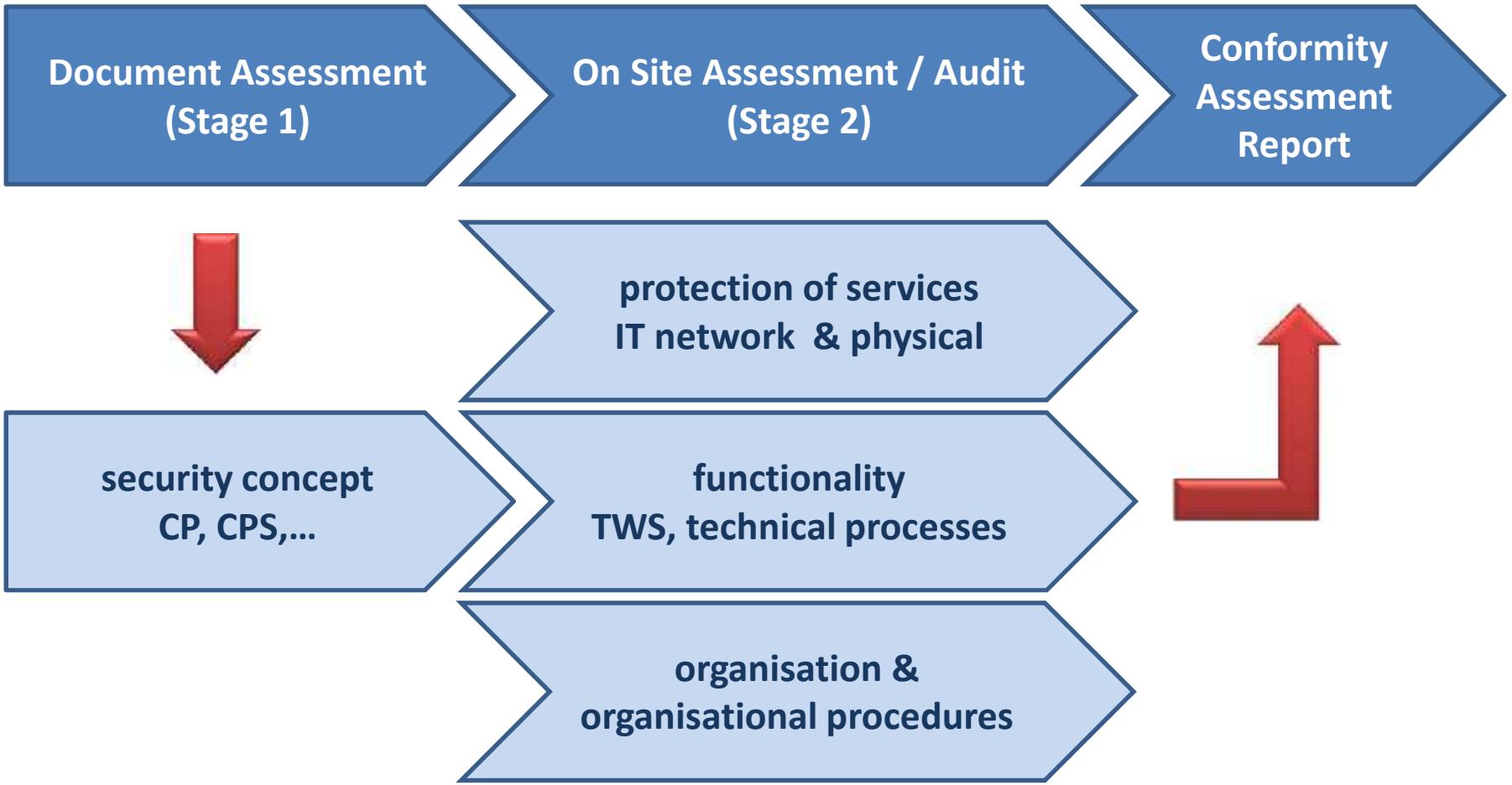
Main eIDAS requirement areas:

- protection of systems and services against attackers
  - physical and logical
- functional requirements, e. g.:
  - availability of service (certificate status)
  - certificate database and revocation
- organizational requirements, e. g.
  - identification of applicants
  - qualified, experienced and reliable staff
  - sufficient financial resources / liability insurance
  - communication with supervisory body

Principle elements of conformity assessment

- Descriptive Information (security concept)
  - all necessary technical, functional and organisational security measures and
  - their appropriateness for fulfilment of eIDAS requirements
- On-Site Audit
  - verify implementation of security measures
  - including technical and penetration testing
- Report with results
  - scope: identification of the TSP, service and policy
  - content and summary of conformity assessment activities
  - additional content as required by supervisory authority

TSP Conformity Assessment



Conformity Assessment Supporting Standards

For Conformity Assessment Bodies:

- EN 319 403: TSP Conformity Assessment

For Trust Service Providers:

- EN 319 401: General Policy Requirements
- EN 319 411: Policy Requirements for TSP issuing (qualified) certificates (parts 1 and 2)
- EN 319 421: Policy Requirements for TSP issuing electronic time-stamps
- EN 419 261: Security Requirements for Trustworthy Systems
- EN 319 412: Certificate Profiles (5 parts)

When to start conformity assessment?

- eIDAS is published -> start now is possible, but
  - (optional) implemented acts on
    - appropriate technical and organisational measures for TSP,
    - formats procedures and deadlines for breach notification
    - reference numbers for standards for TWS,
    - accreditation of conformity assessment bodies (CAB) and
    - requirements on conformity assessment reports may be published
  - final version of (supporting) ETSI standards need to be published
- recommendation: start at beginning of 2016 (1.5 year before deadline July 2017)

Summary

- eIDAS requirements on TSP and conformity assessment are published and can be applied
- supplementary, more detailed, requirements from implementing acts may follow
- ETSI and CEN standards will support TSP to implement requirements and CAB to perform audits
- Audit will focus on technical, functional and organisational security measures in two stages
  1. documents: security concept, CP, CPS, etc.
  2. onsite: protection, functionality, organisation
- Audits should start beginning of 2016

Thank you very much for your attention!

TÜV Informationstechnik GmbH
Member of TÜV NORD GROUP

Dr. Christoph Sutter
IT Infrastructure & IT Quality

Langemarckstr. 20
45141 Essen, Germany

Phone: +49 201 8999 – 582
Fax: +49 201 8999 – 555
E-Mail: C.Sutter@tuvit.de
URL: www.tuvit.de