eIDAS – 47 pages of

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Presented by Arno Fiedler based on a presentation from Andrea Servida in June 2014.

eIDAS - What is the ambition?

Strengthen EU Single Market by boosting TRUST and CONVENIENCE in secure and seamless cross-border electronic transactions

Submitting a tax declaration

E-Transactions workflow

Website

authentication: check if the website you enter is really linked to the tax authority.

eID: identify (or authenticate) yourself using, for instance, an eID means

Creation of the tax declaration

E-signature / e-seal: Signing or Sealing the tax declaration

Time stamp: Proof of submission of the tax declaration in due time

E-registered delivery: Tax authority sends acknowledgement of receipt

Preservation: storage of the tax declaration and acknowledgment of receipt

The eIDAS Regulation

Mutual recognition of e-identification means

Electronic trust services:

- Electronic signatures
- Electronic seals
- Time stamping
- Electronic registered delivery service
- Website authentication.

Electronic documents

eIDAS – Key legal aspects

- Art 114 TFEU on internal market as the legal basis
- One Regulation for eID and trust services directly applicable in the 28 MS
- 28 implementing acts and 1 delegated act to further specify the technical aspects of the Regulation:
  - ✓eID: 4 implementing acts
  - ✓eTS: 24 implementing acts and 1 delegated act

eIDAS breaks new ground (1/2)

*Provides **legal certainty** and **fosters the usage** of eID means for online access ("world première") → never regulated at EU level before*

*Addresses **all the stages** of a generic e-transaction, from the authentication of a web site to preservation*

*Provides the legal framework for a comprehensive "**toolbox**" of mechanisms and services to boost trust and confidence in electronic transactions*

eIDAS breaks new ground (2/2)

Takes a risk management perspective, not based on normative rules but on principles:

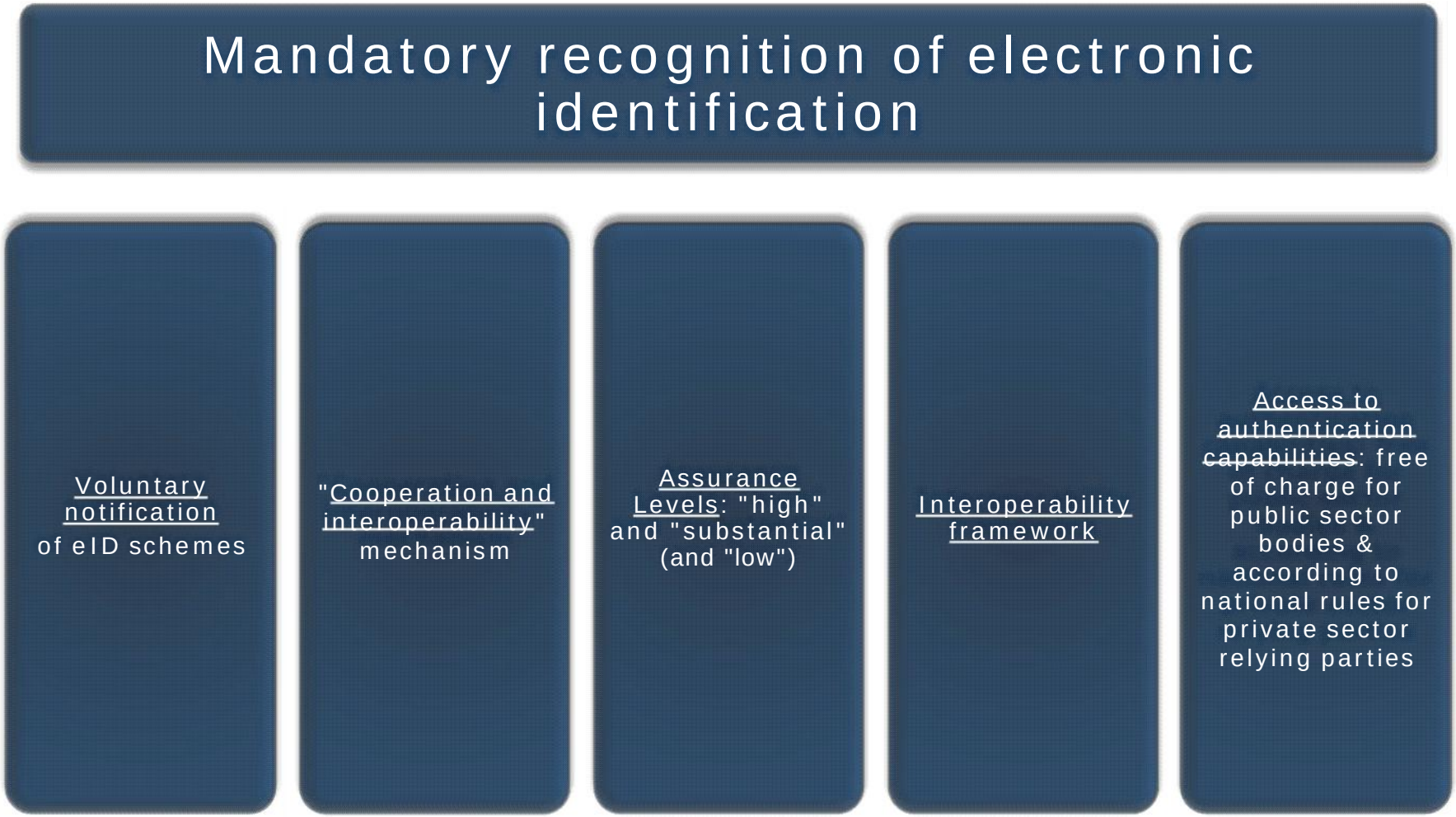
- **Transparency and accountability: well-defined minimal obligations for TSPs and liability**
- **Trustworthiness of the services together with security requirements for TSPs**
- **Light-touch reactive monitoring for TSPs *vs.* full-fledged supervision for QTSPs**
- **Technological neutrality: avoiding requirements which could only be met by a specific technology**
- **Market rules and building on standardisation**

Provides one set of rules directly applicable across all EU MS →

Regulation (including 1 DA and 28 IA)

eIDAS Regulation Part II

eIDAS – Mutual recognition of eIDs



eIDAS - eID

- Mutual recognition (Art 6)
  - MS must recognise eID means issued under 'notified' eID schemes from other Member States for cross-border access to its public services requiring e-identification based on the reciprocity principle (art.6)

Notification (Art 9)

- MS may 'notify' to European Commission the 'national' electronic identification scheme(s) used at home for, at least, access to public services (art.9)

- ➢ Implementing acts may be adopted by the Commission on circumstances, formats, and procedures of the notification (art.9.4)

eID assurance levels (Art 8)

- Notified eID schemes shall specify the assurance level of the eID means (art.8.1)
  - ✓ Assurance <u>level low</u> ➔ recognition is voluntary (art.6.2)
  - ✓ Assurance <u>level substantial</u> ➔ recognition is mandatory (art.6.1(b))
  - ✓ Assurance <u>level high</u> ➔ recognition is mandatory (art.6.1(b))

➢ Implementing acts to be adopted by the Commission to set out minimum technical specifications, standards, and procedures for assurance levels low, substantial and high by 12 months after the entry into force of the Regulation (art.8.3)

eIDAS - eID

- Interoperability of notified eID schemes (art.12)
  - ensured through an interoperability framework
  - Implementing act to be adopted by the Commission on the interoperability framework by 12 months after the entry into force of the Regulation (art.12.8)

- Authentication (art 7(f))
  - MS must provide cross-border online eID authentication capabilities (art.7(f))
  - The cross-border authentication shall be free of charge where in relation to a service online provided by a public sector body (art.7(f))
  - MS may allow the private sector to use authentication capabilities: the regime applicable to national private sector shall apply to private sector established in a different MS (principle of non-discrimination) (art.7(f))

- Cooperation and interoperability (art 12)
  - MS must exchange good practices and experience (art.12)
  - Implementing act to be adopted by the Commission to specify the procedural modalities for the cooperation between MS by 6 months after the entry into force of the Regulation (art.12.7)

- Liability (art 11)
  - Liability of MS, eID providers & authentication operators is foreseen (art.11)

eIDAS Regulation Part III

eIDAS – Trust services

eIDAS – General principles for trust services

- Liability regime for Q & non-QTSPs (art.13)
  - Liability for damages caused intentionally or negligently
  - Reversal of the burden of the proof only for QTSPs
  - Possible limitations of liability for the use of the service by the TSP subject to clear information to customers
  - Applicability of national rules on liability
- Recognition of 3rd countries TSPs (art.14)
  - Only through international agreements between the Commission and a third country or international organisation
  - Principle of reciprocity
- Accessibility for persons with disabilities (art.15)

(37) This Regulation should provide for the liability of all trust service providers. In particular, it establishes the liability regime under which all trust service providers should be liable for damage caused to any natural or legal person due to failure to comply with the obligations under this Regulation. In order to facilitate the assessment of financial risk that trust service providers might have to bear or that they should cover by insurance policies, this Regulation allows trust service providers to set limitations, under certain conditions, on the use of the services they provide and not to be liable for damages arising from the use of services exceeding such limitations.
Customers should be duly informed about the limitations in advance. Those limitations should be recognizable by a third party, for example by including information about the limitations in the terms and conditions of the service provided or through other recognisable means. For the purposes of giving effect to those principles, this Regulation should be applied in accordance with national rules on liability. Therefore, this Regulation does not affect those national rules on, for example, definition of damages, intention, negligence, or relevant applicable procedural rules.

Article 24
2. A qualified trust service provider providing qualified trust services shall:
with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;

Article 14 International aspects

1. Trust services provided by trust service providers established in a third country shall be recognised as legally equivalent [to qualified trust services provided by qualified trust service providers established in the Union] where the trust services originating from the third country are recognised under an agreement concluded between the Union and the third country in question or an international organisation in accordance with Article 218 TFEU.

eIDAS – Role of the Supervisory body

- Light touch ex post reactive monitoring of non-qualified TSPs vs. Full-fledged ex ante and ex post supervision of qualified TSPs (art.16)
- Detailed tasks of the Supervisory body (art.16.4)
  - Analyse conformity assessment reports
  - Report to the Commission about main activities
  - Carry out audits / Request conformity assessments
  - Inform data protection authorities where appropriate
  - Grant and withdraw qualified status
  - Inform national body responsible for trusted lists
  - Require (Q)TSPs to remedy any failure to fulfil the requirements
  - …

eIDAS – Obligations of TSPs

Minimum security requirements for + notification of significant security breaches by all TSPs (art.18)

- Specific requirements to be met by QTSPs (art.24):
  - staff,
  - trustworthiness of their systems,
  - liability insurance scheme,
  - identification of the certificate owner,…
- Conformity assessment of QTSP (art. 19 & 21):
  - Ex ante (prior authorisation scheme – art.21) ➔ SB may grant the qualified status in a given timeframe ➔ Inclusion in the Trusted Lists
  - ex post (every 24 months & ad hoc – art. 19) ➔ May withdraw the qualified status
  - building upon Regulation 765/2008 conformity assessment scheme

eIDAS – Supporting tools

Trusted lists for QTSPs and QTSs (art.22)

EU trust mark for qualified trust services (art.23)

- ✓Usage by QTSP after qualified status has been indicated in the TLs
- ✓Trustmark indicates in a simple, recognisable, and clear manner the qualified status of a trust service
- ✓Link to the relevant TL has to be ensured by the QTSP

➢ Implementing act to be adopted by the Commission by 01 July 2015 to specify the form of the EU trust mark (in particular presentation, composition, size, design)

eIDAS - Electronic signature and seals

- Non-discrimination as evidence in legal proceedings (art.25.1-34.1)
- Legal effect (art.25.2-34.2)
  - e-signature:
    - ✓ only for natural persons
    - ✓ Assimilation to handwritten signature
  - e-seal:
    - ✓ only for legal persons
    - ✓ Integrity of the data and correctness of the origin
- Recognition in all MS of a qualified electronic signature /seal based on a qualified certificate issued in one MS (art.25.3-34.3)

eIDAS – Validation & Long time preservation of e-signature and e-seals

- Validation of e-signatures and seals (art.31 & 32-38)
  - ✓ Requirements for the validation of qualified e-signatures / seals (art.31.1-38)
  - ✓ Requirements for qualified validation services for qualified e-signatures / seals
    - Meeting the requirements set in article 31.1 (art.32.1-38)
    - Allow relying parties to receive the results (art.32.1-38):
      - ❖ in an automated process which is reliable and efficient
      - ❖ bearing the advance electronic signature / seal of the provider of the Q-validation service
- Long term preservation of e-signatures and seals (art.33-38)

eIDAS - Electronic time stamp

- Non-discrimination as evidence in legal proceedings (art.39.1)
- Legal effect (art.39.2)
  - ✓ Accuracy of the date and time it indicates
  - ✓ Integrity of the data to which the date and time are bound
- Requirements for qualified e-time stamp (art.40)
  - ✓ Binds the date and time to data in such a manner as to reasonably preclude undetectable changes to the data
  - ✓ Based on accurate time source linked to UTC
  - ✓ Signed with an AeS or sealed with an AeSeal of the QTSP – or by some equivalent method

eIDAS - Electronic registered delivery service

- Non-discrimination as evidence in legal proceedings (art.41.1)
- Legal effect (art.41.2)
  - ✓ Integrity of the data sent and received
  - ✓ Accuracy of the date of the data sent and received
- Requirements for qualified e-registered delivery service (art.42)
  - ✓ To be provided by one or more QTSPs
  - ✓ Ensure with high level of confidence identification of the sender
  - ✓ Before delivery of the data: ensure identification of the addressee
  - ✓ Sending and receiving of data have to be secured by AeS or AeSeal of the QTSP
  - ✓ Needed changes to data have to be clearly indicated
  - ✓ The date and time of sending, receipt and changes have to be indicated with a Qualified e-time stamp

eIDAS – Website authentication

- Requirements for qualified certificates for website authentication (art.43)
- Website authentication certificate (SSL, TSL, …) TSPs are subject to supervision (QTSPs) or monitoring (non-QTSPs)
- Website authentication certificate TSPs have to match minimum security requirements as well as to notify significant security breaches
- Website authentication certificate TSPs are subject to the liability regime

(67)Website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website. Those services contribute to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated.

The provision and the use of website authentication services are entirely voluntary. However, in order for website authentication to become a means to boosting trust, providing a better experience for the user and furthering growth in the internal market, this Regulation should lay down minimal security and liability obligations for the providers and their services.
To that end, the results of existing industry led initiatives, for example the **Certification Authorities / Browsers Forum - CA/B Forum,** have been taken into account.

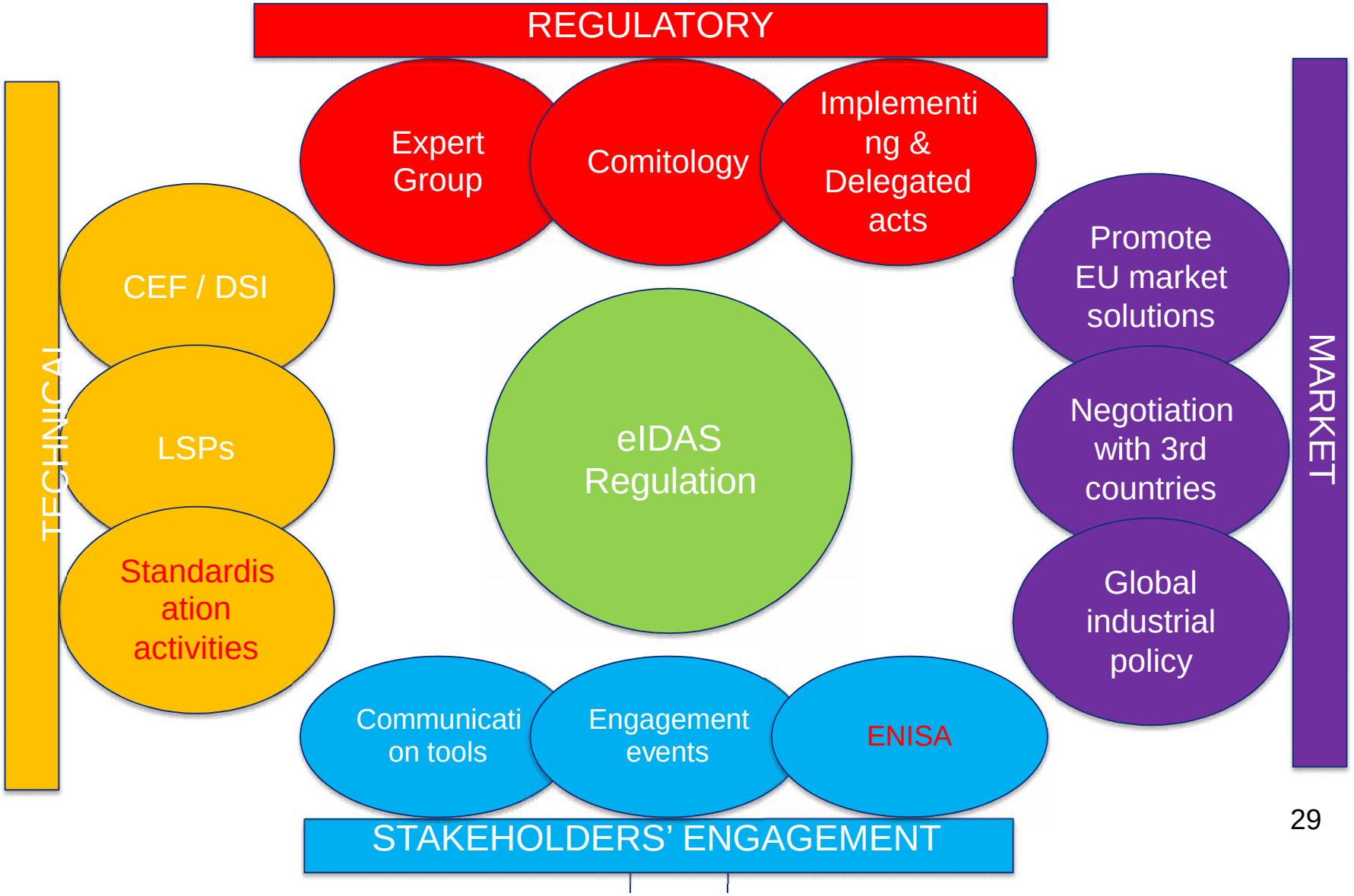
In addition, this Regulation should not impede the use of other means or methods to authenticate a website not falling under this Regulation nor should it prevent third country providers of website authentication services from providing their services to customers in the Union.

However, a third country provider should only have its website authentication services recognised as qualified in accordance with this Regulation, if an international agreement between the Union and the country of establishment of the provider has been concluded.

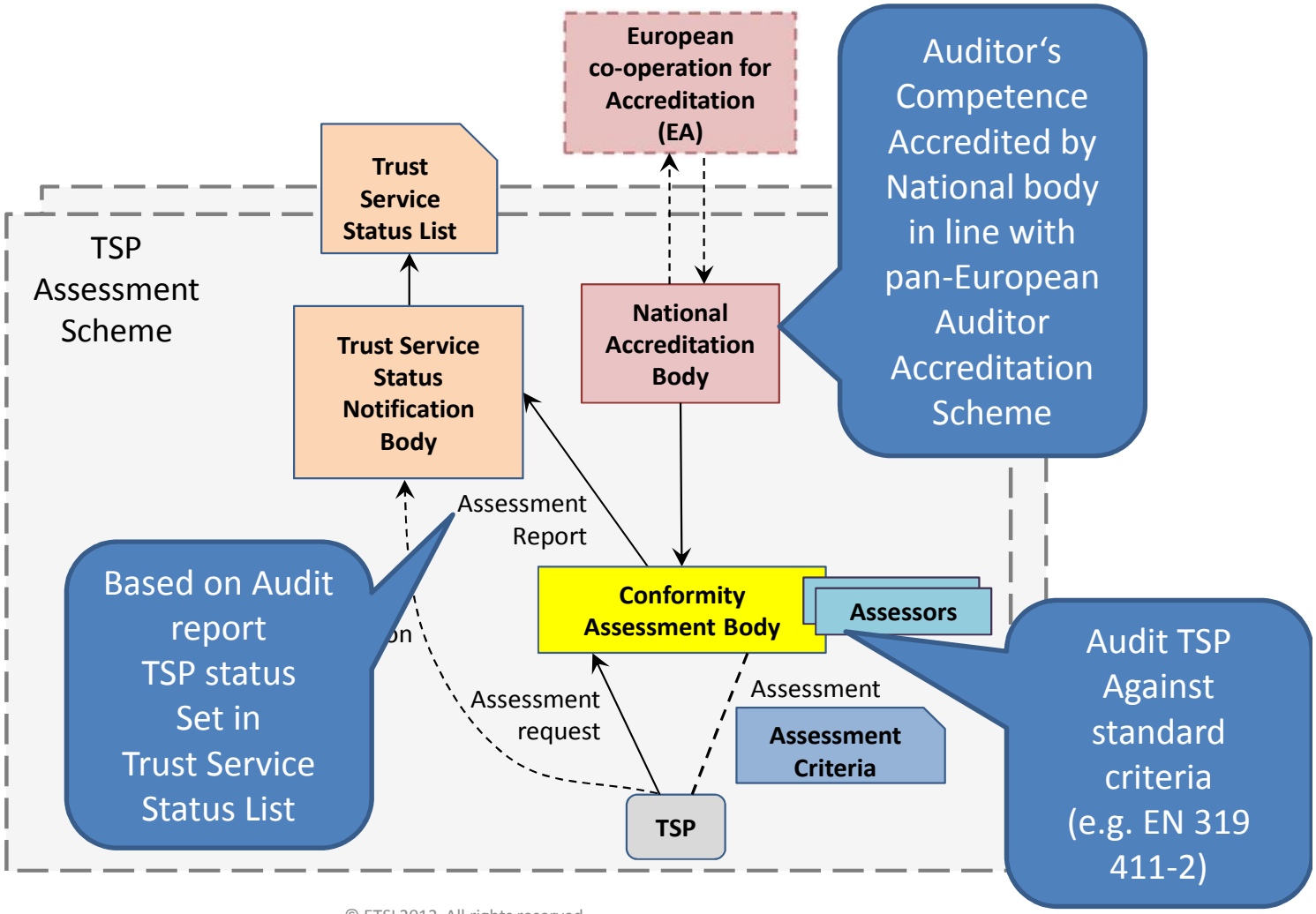
eIDAS - Electronic documents

Non-discrimination of electronic documents vis-à-vis paper documents as evidence in legal proceedings (art.44)

- ✓Ensures validity and legal certainty of cross-border electronic transactions through the impossibility for Courts to reject a document on the grounds that it is in electronic form

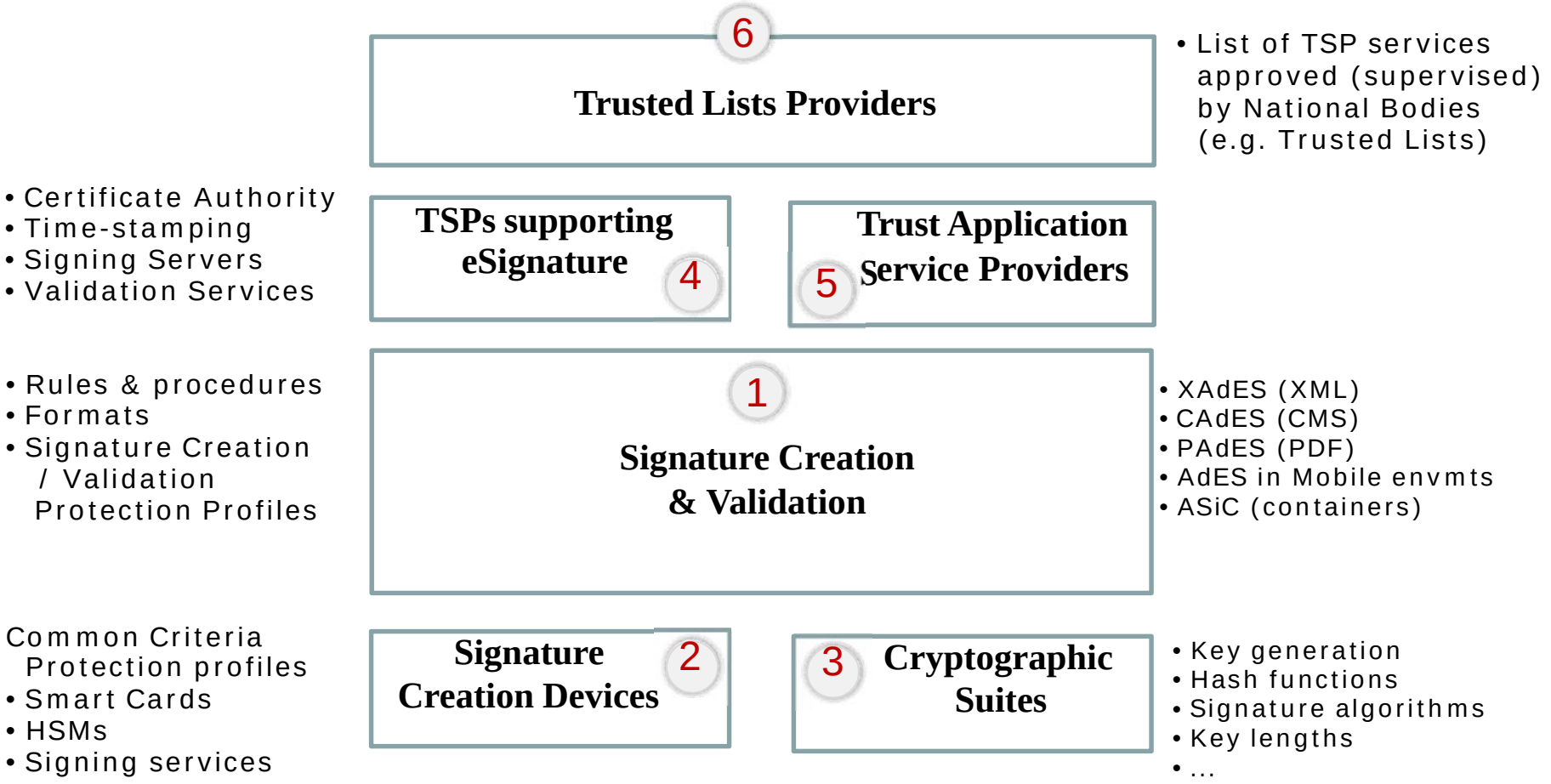

REGULATORY
Expert Group
Comitology
Implementing & Delegated acts
TECHNICAL
CEF / DSI
LSPs
Standardisation activities
eIDAS Regulation
MARKET
Promote EU market solutions
Negotiation with 3rd countries
Global industrial policy
Communication tools
Engagement events
ENISA
STAKEHOLDERS' ENGAGEMENT

TSP Conformity Assessment Model



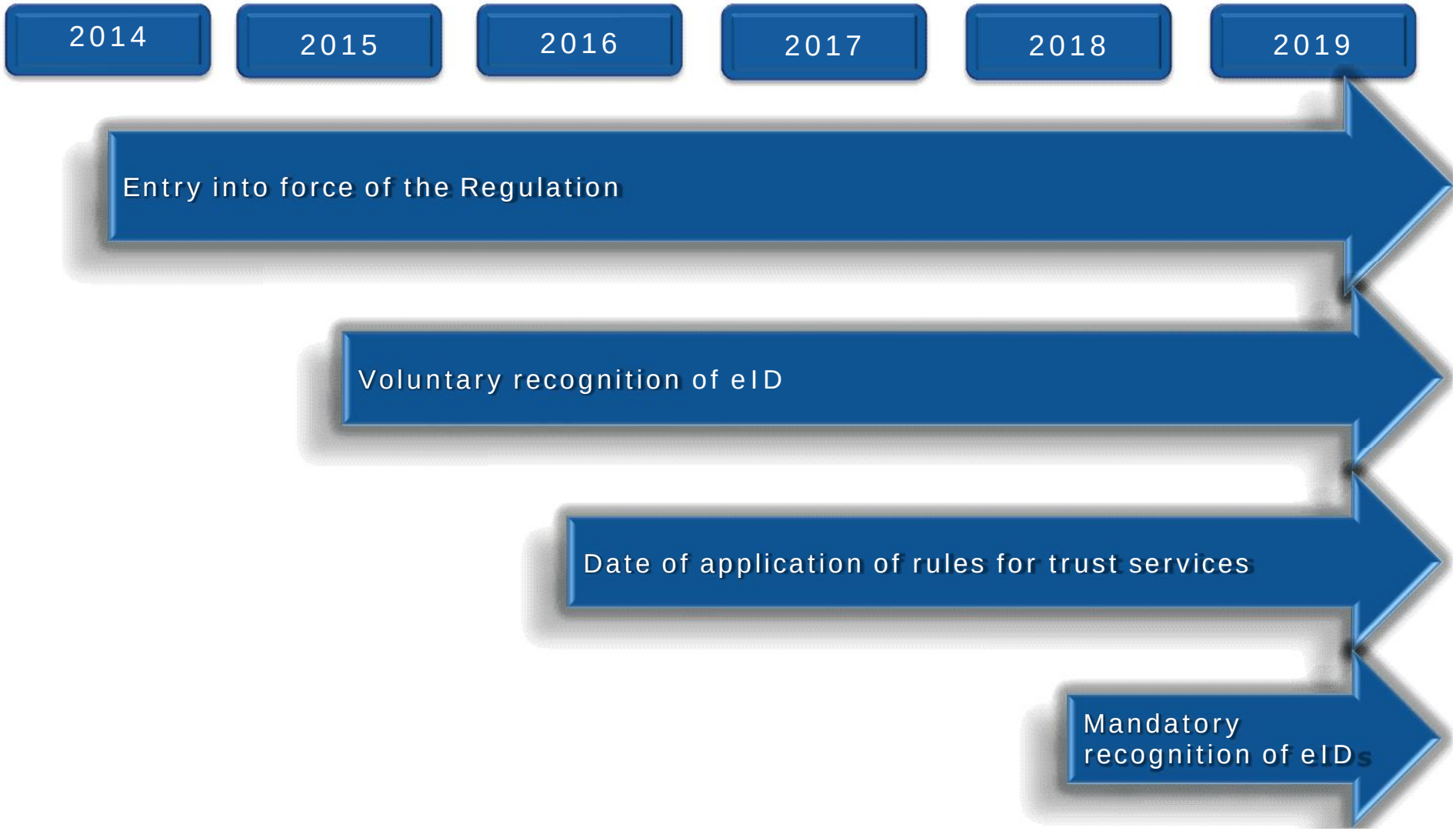
Standardisation mandate

by CEN and ETSI



http://www.e-signatures-standards.eu

eIDAS – Timeline of implementation



For further information and feedback

http://ec.europa.eu/digital-agenda/en/trust-services-and-eid

eIDAS Regulation –
published in O.J. on 28.08.2014

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

EU_eIDAS