European Commission's proposal for a

Regulation on Electronic identification and trust services for electronic transactions in the EU internal market

Gérard GALLER
Policy Officer
European Commission - DG ConNECT
Gerard.galler@ec.europa.eu

Problem statement – example #1

Elisa, a Belgian student wants to enrol <u>online</u> to a University in Italy.

Albeit she has an eID card,

it does not work

because her Belgian eID

IS NOT RECOGNISED in Italy

European Commission

Problem statement – example #2

- **A French SME wants to do business electronically with an Italian counterpart.**
- **What about the respective requirements for trust services like e-signatures, seals, documents, time stamps, delivery?**
- **Are cross-border services technically feasible? May be…**
- **Will they be legally recognised?**

- **Result:**

Where do we stand in EU?

- **EU legal** framework for **eSignatures:** Directive 1999/93/EC of 13.12.1999
- **No** EU legal framework for **electronic trust services ancillary** to eSignature (ex. time stamping)
- Excellent but incomplete **EU standards framework** on eSignature and ancillary electronic trust services
- **No** EU legal framework for **eID**
- Few widely adopted **standards on eID**
- Large **EU Member States + industry investments**

European Commission

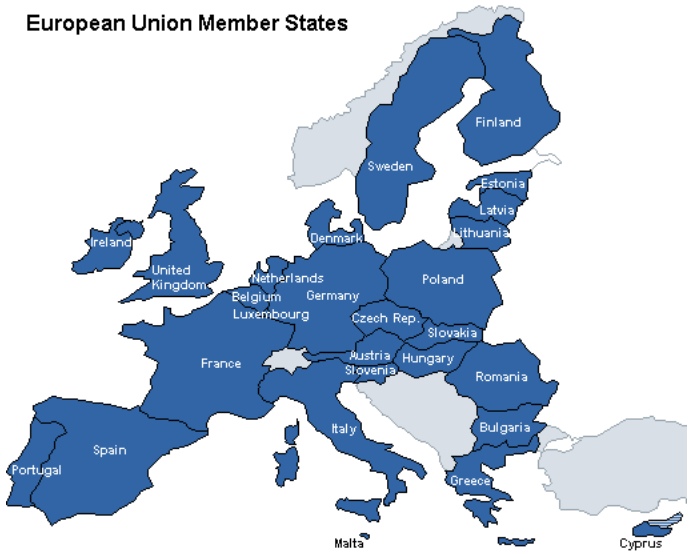
What is the legislative proposal's ambition?

- **To strengthen EU Single Market by boosting TRUST and CONVENIENCE in cross-border and cross-sector electronic TRANSACTIONS**

European Commission

How?

1. **By ensuring that <u>people</u> and <u>businesses</u> can use their national eIDs to access online services in other EU countries.**



European Commission

How?

2. **By removing the barriers to seamless eSignatures and related trust services across borders**

→

i.e. by ensuring that trust services have the <u>same legal value</u> as in traditional paper-based processes.

European Commission

What is the scope of the proposed Regulation?

1. Mutual recognition of **electronic identification**

2. **Electronic trust services**:
   - **Electronic signatures** interoperability and usability
   - **Electronic seals** interoperability and usability
   - Cross-border dimension of:
     1. **Time stamping**,
     2. **Electronic delivery service**,
     3. **Electronic documents admissibility**,
     4. **Website authentication**.

European Commission

What is foreseen for electronic trust services?

Common Principles:

- **Technological neutrality**
- Mutual recognition of «**qualified**» electronic trust services (including non EU countries)
- Strengthens and harmonises **national supervision** of qualified trust service providers and trust services
- Reinforces **data protection** + obligation for **data minimisation**
- Uses **secondary legislation** to ensure flexibility vis-à-vis technological developments and best practice

European Commission

What is foreseen for electronic trust services?

eSignature

- Builds on existing eSignature infrastructure and clarifies concepts related to eSig. (**natural** persons)
- Introduces **eSeals** (**legal** persons)
- Allows for full reference to standards
- Clarifies validation of qualified eSignatures
- Ensures long term preservation
- Allows «server / remote» and «mobile» signing

European Commission

Ch. 3. Trust services
Section 2. TSP and TS Supervision (1/2)

- **Art 13, 14: Supervision**
  - **National or «regional» supervision authority**
  - Common essential supervision requirements **of Q-TSPs**
  - **Cooperation between Supervisors:**
    - Mutual supervision assistance
    - Yearly supervision report
    - Collection of market statistics from Q-TSPs and Supervisors
    - Exchange of good practices between Supervisors (🡐 FESA)
  - **MS to ensure long term availability of trust data of Q-TSPs**

European Commission

Ch. 3. Trust services
Section 2. TSP and TS Supervision (2/2)

- **Art 15: Requirements on Q and non Q-TSPs:**
  - Obligation of security due diligence for Q and non Q-TSPs
  - Security breach notification obligation for Q and non Q-TSPs
  - Binding instructions by Supervisors to Q and non Q-TSPs
- **Art. 16: Supervision of Q-TSPs**
  - Q-TSP subject to at least yearly audit
  - Supervisor can issue binding instructions to Q-TSP. Supervisor can remove “Qualified” status.
- **Art. 17: Initiation of Q-Trust services**
  - Mandatory notification to Supervisor
  - No prior authorisation
- **Art. 18: Trusted Lists:**
  - EU trusted lists of Q-TSs and Q-TSPs (← SD Decision 2009/767/EU)
- **Art. 19: Requirements for Q-TSPs:**
  - **Issuance certificates**: face-to-face OR remotely using «notified» eID
  - Mandatory on-line standardised certificate status info (ex. OCSP)
  - Other reliability and professionalism requirements similar to ex-Annex II

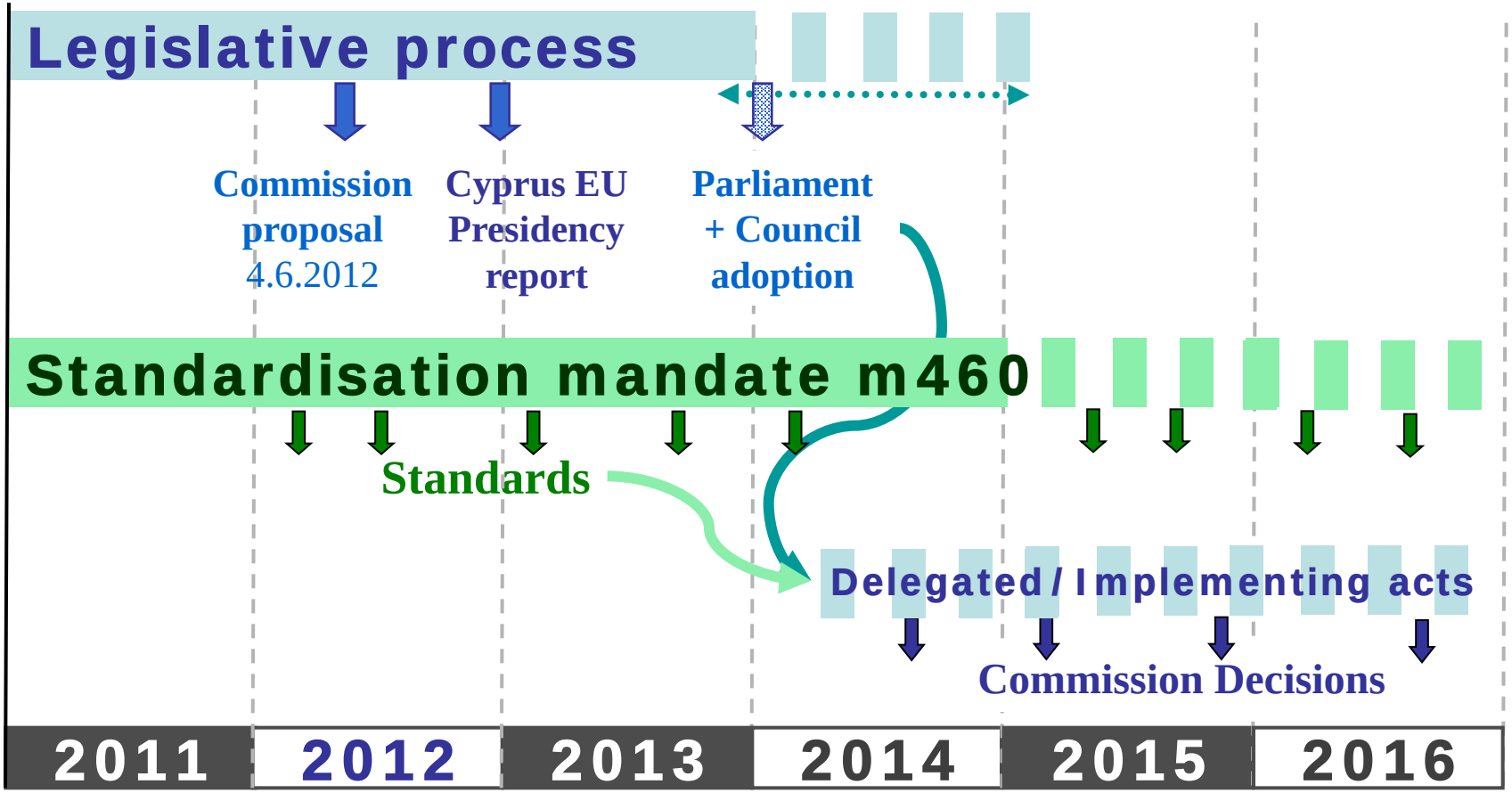
European Commission

Why will it make a difference?

- **Creates confidence in electronic trust services:**
  - Effective state **supervision**
  - Systematic usage of "**trusted lists**“
  - *De facto* «trustmark» for EU qualified services
  - Comprehensive “toolbox” of trust building instruments
  - One single legislation across EU
- **Easy eSignature:**
  - Harmonisation power of **Regulation**
  - **Full eSig specification** via secondary legislation **+** standards
- **Related trust services:**
  - Address clear market needs: eSeals, eDelivery, eDocuments, …
  - Harmonise national legislation: time stamping, eDelivery
  - eDocument admissibility: « big bang » for de-materialisation
  - Website authentication is an implicit expectation of the citizens

European Commission

Indicative timeline



NB. Dates are indicative

For further information

- **Website:**
  http://ec.europa.eu/information_society/policy/esignature

- **Draft Regulation:**
  - European Commission's "*Proposal for a Regulation of the European Parliament and Council on electronic identification and trust services for electronic transactions in the internal market*", COM(2012)238, 4.6.2012
    http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation
  - Impact assessment report: SWD(2012)135 and SWD(2012)136

European Commission

Provisions of the proposed Regulation

- **Ch 1: General Provisions**
- **Ch 2: Electronic identification**
- **Ch 3: Trust services**
  - *Sec 1: General Provisions*
  - *Sec 2: Supervision*
  - *Sec 3: Electronic signature*
  - *Sec 4: Electronic seals*
  - *Sec 5: Electronic time stamp*
  - *Sec 6: Electronic documents*
  - *Sec 7: Qualified electronic delivery service*
  - *Sec 8: Website authentication*
- **Ch 4: Delegated acts**
- **Ch 5: Implementing acts**
- **Ch 6: Final provisions**
- **Annexes I, III, IV: Qualified certificates**
- **Annex II: Qualified eSig creation devices**

European Commission

Ch 1. General Provisions

- **Legal basis:** Art 114 TFEU (internal market)
- **Art 1, Art 2: Subject matter and scope**
  - Cover mutual recognition & acceptance of
    - "notified" eID
    - "electronic trust services" (eSig, eSeals, eDoc, time stamping, eSig/eSeal long term preservation service, certificates, website authentication)
  - « Toolbox » of trust services: usage is NOT mandatory
- **Art 3: Definitions**
  - Trust services do not encompass eID (subsidiarity)
  - **Qualified** = matching the requirements of the Regulation
  - Qualified trust service providers (QTSP) and trust services (QTS)
  - **eSig creation device**: SW or HW used to create an eSig
- **Art 4: Internal market**
    - Free “movement” of trust services and related products
    - Mutual recognition and acceptance of trust services

European Commission

Ch 2. Electronic identification

- Art 5: **Legal effect:**
  - Mutual recognition and acceptance of “notified” e-identification schemes
  - Natural and legal persons
- Art 6, Art 7: **Notification mechanism:**

  A Member State:

  1. May ‘**notify**’ to Commission the ‘national’ electronic identification scheme(s) used at home, at least, for access to public services;
  2. Must recognise and accept ‘notified’ eIDs of other Member States for cross-border access to its online services requiring e-identification under its national laws;
  3. Must provide online free ID data **authentication** facility;
  4. Is **liable** for unambiguous identification of persons and for authentication;
  5. May allow the **private sector** to use ‘notified’ eID
- Art 8: **Coordination mechanism** between Member States to ensure eID means interoperability and enhance security

European Commission

Ch. 3. Trust services (TS)
Section 1. General provisions

- **Art 9: Liability:** TSP is liable for what it does (similar to e-sign Dir)
- **Art 10: International aspects**:
  - Mutual recognition of QTS and Q-certificates
  - Mutual recognition only via international agreements
  - 3rd country TS must comply with EU data protection, security and supervision levels
- **Art 11: Data processing and protection**
  - Stronger and unlimited reference to data protection directive
  - Obligation of data minimisation
- **Art 12: Accessibility for disabled persons**
  - Services and products «accessible» whenever possible
- **Generic three-pronged approach**:
  - Technologically neutral definition (non discrimination)
  - "Qualified" secure level (with legal effect)
  - Presumption of compliance (if voluntary standards are matched)

European Commission

Ch. 3. Trust services
Section 2. TSP and TS Supervision (1/2)

- **Art 13, 14: Supervision**
  - **National or «regional» supervision authority**
  - Common essential supervision requirements **of Q-TSPs**
  - **Cooperation between Supervisors:**
    - Mutual supervision assistance
    - Yearly supervision report
    - Collection of market statistics from Q-TSPs and Supervisors
    - Exchange of good practices between Supervisors (🡐 FESA)
  - **MS to ensure long term availability of trust data of Q-TSPs**

European Commission

Ch. 3. Trust services
Section 2. TSP and TS Supervision (2/2)

- **Art 15: Requirements on Q and non Q-TSPs:**
  - Obligation of security due diligence for Q and non Q-TSPs
  - Security breach notification obligation for Q and non Q-TSPs
  - Binding instructions by Supervisors to Q and non Q-TSPs
- **Art. 16: Supervision of Q-TSPs**
  - Q-TSP subject to at least yearly audit
  - Supervisor can issue binding instructions to Q-TSP. Supervisor can remove “Qualified” status.
- **Art. 17: Initiation of Q-Trust services**
  - Mandatory notification to Supervisor
  - No prior authorisation
- **Art. 18: Trusted Lists:**
  - EU trusted lists of Q-TSs and Q-TSPs (← SD Decision 2009/767/EU)
- **Art. 19: Requirements for Q-TSPs:**
  - **Issuance certificates**: face-to-face OR remotely using «notified» eID
  - Mandatory on-line standardised certificate status info (ex. OCSP)
  - Other reliability and professionalism requirements similar to ex-Annex II

European Commission

Ch. 3. Trust services
Section 3: eSignatures (1 / 2)

- **Art. 3 (definitions): eSignature:**
  - eSig. = “data in e-form attached to or logically associated with other e-data and which are used by the signatory to sign”
  - Natural persons only
  - Advanced eSig. (AeS): adapted to allow server signing and make « sole control » manageable
- **Art. 20: Legal effects and acceptance of eSignatures**
  - Qualified eSig. (QeS) has “equivalent legal effect” to handwritten signature
  - Mutual recognition and acceptance of QeS
  - Allows for classification of eSignatures with security assurance levels < QeS
  - Security of AeS may be defined via standards
  - Security assurance requirements higher than QeS are forbidden for public services

European Commission

Ch. 3. Trust services
Section 3: eSignatures (2/2)

- **Art. 21 and Annex I: Qualified Certificates for eSignature**
  - Fully defined in Annex I: exact mandatory content
- **Art 3.17, 22-24: Qualified signature creation devices** Q-SCD
  - Extended scope of creation devices: HW or SW to create an eSig.
  - Certification of Q-SCD (ex. ISO 15408 “Common criteria)
  - European positive list of certified Q-SCD
- **Art 25-26: Validation**
  - Defines when a QeS is valid
  - Defines Q-validation service provider (new)
- **Art 27: Preservation of eSignatures**
  - Defines Q-long term preservation service (new)
- **Art 34.4: eSig formats** for public services:
  - Administrations to accept a minimum common set of standardised eSig formats (= SD Decision 2011/130/EU: CAdES, XAdES, PAdES)

European Commission

Ch. 3. Trust services

- **Section 4. eSeals**
  - Legal persons only
  - Instrument for document authentication: "data in e-form attached to or logically associated with other e-data to ensure origin and integrity of the associated data"
  - «mutatis mutandis» like eSignature
- **Section 5. Time stamping**
  - Legal existence of time stamps
  - Defines qualified time stamps («*date certaine*»)
- **Section 6. eDocuments**
  - Non discrimination «paper vs e-documents»
  - Presumption of authenticity and integrity of Q-signed/sealed eDocuments

European Commission

Ch. 3. Trust services

- **Section 7. eDelivery**
  - Legal effect: certainty of cross-border electronically delivery
  - Establishes qualified eDelivery services
  - NB. Assumes national legislation will establish equivalence of e-delivery and paper «lettre recommandée»

- **Section 8. Website authentication**
  - Only establishes legal existence of qualified website authentication certificates

European Commission

Ch 4 and 5. Secondary legislation

- **Ch 4: Delegated acts**
  - Art. 38: Standard provision for delegated acts

- **Ch 5: Implementing acts**
  - Art 39: Standard provision for implementing acts:
    - “Examination procedure”
    - Qualified majority

European Commission

Ch 6. Final provisions

- **Art 40: reporting** every four years
- **Art 41: Repeal Directive 1999/93/EC**
  - SSCDs already certified as SSCDs become QSCDs
  - Existing Q-Certificates will remain valid max. five years
- **Art 42: Immediate entry into force**
  - 20 days after official publication following adoption by European Parliament and Council by the «ordinary procedure» (ex-codecision)

European Commission