Introduction to EU Trustmodel

Mark Erlich
08. October 2021

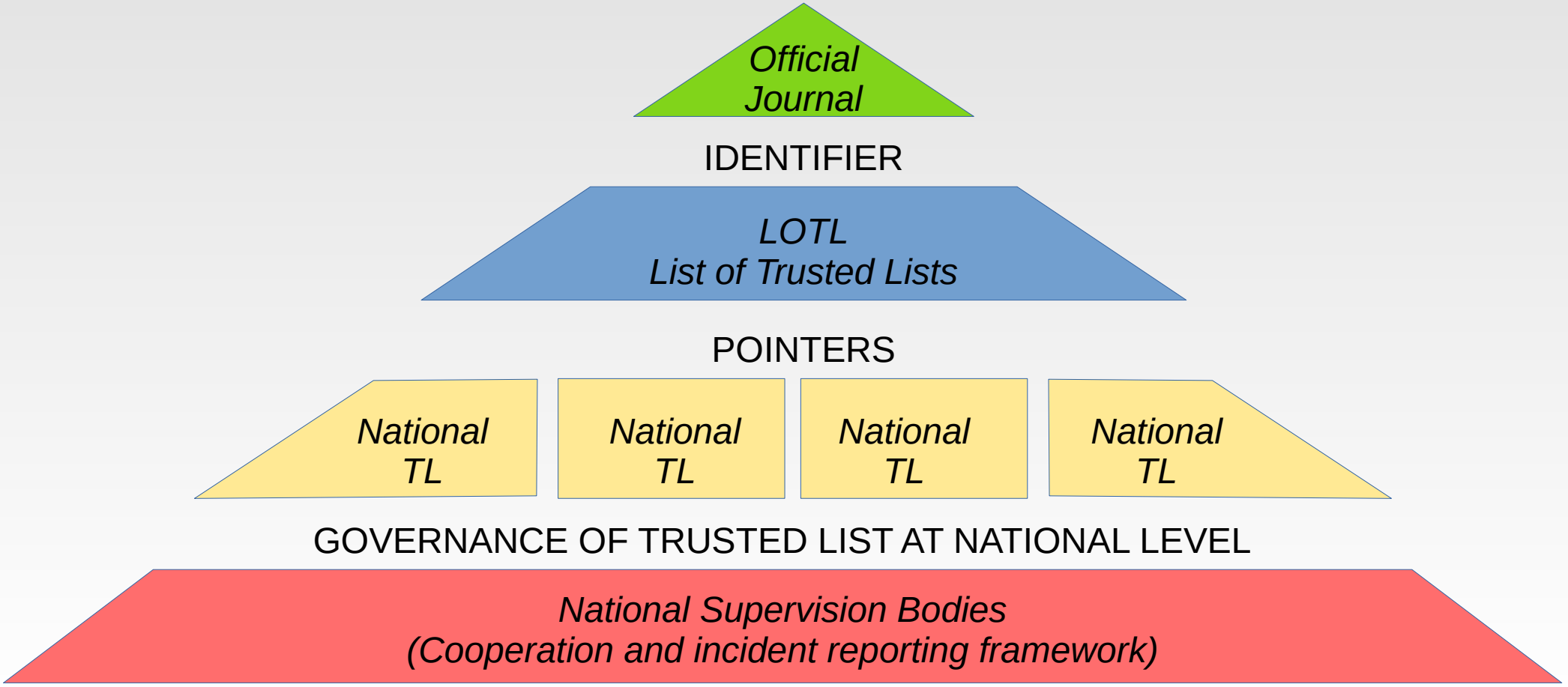
Trust List as Trustanchor (1)

- Before eIDAS: local trust/offline trust
  - Bilateral trust model: trust for application or partner
  - Change of status required manual local updates
- Since eIDAS: global online trust framework
  - Common assesment and supervision model (clear liability rules)
  - Federated trust chain with pointers to locally trusted nodes (no need for bilateral trust)

Trust List as Trustanchor (2)

- eIDAS - Trustmodel with Fundamental Requirements
  - Requirements for the Trust Services and Trust Service Providers
  - Requirements for Trust and Mutual Recognition
    - Rules for Supervision
    - Incident reporting and cooperation on risk mitigation
    - Equal treatment of Trust Services disregarding country of origin
  - Using framework of international standards
- eIDAS works as model and set of requirements even outside of EU

Trust List as Trustanchor (3)



Trust List Related Standards

- X19 6xx Series
  - TR 119 600 Guidance on the use of standards for trust service status lists providers
  - TS 119 612 Trusted Lists
  - TS 119 614-1 Specifications for testing conformance of XML representation of Trusted Lists
  - TS 119 615 Procedures for using and interpreting European Union Member States national trusted lists
- Indirect relation: EN 319 412-5 QCStatements

Usecases

- Trust on signature validation
- Trust on timestamp source
- Trust on e-Delivery source
- Additional level of trust on Website

Supervision and Liability (1)

- NAB - National Acreditation Body
  - Accredits Auditor’s competence according ETSI EN 319 403
    - ISO 17065 - Requirements for bodies certifying products, processes and services
    - ISO 17021 - Requirements for bodies providing audit and certification of management systems
    - ETSI TS 119 403-2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates
    - ETSI TS 119 403-3: Additional Requirements for CABs Assessing QTSPs against the eIDAS Regulation Requirements

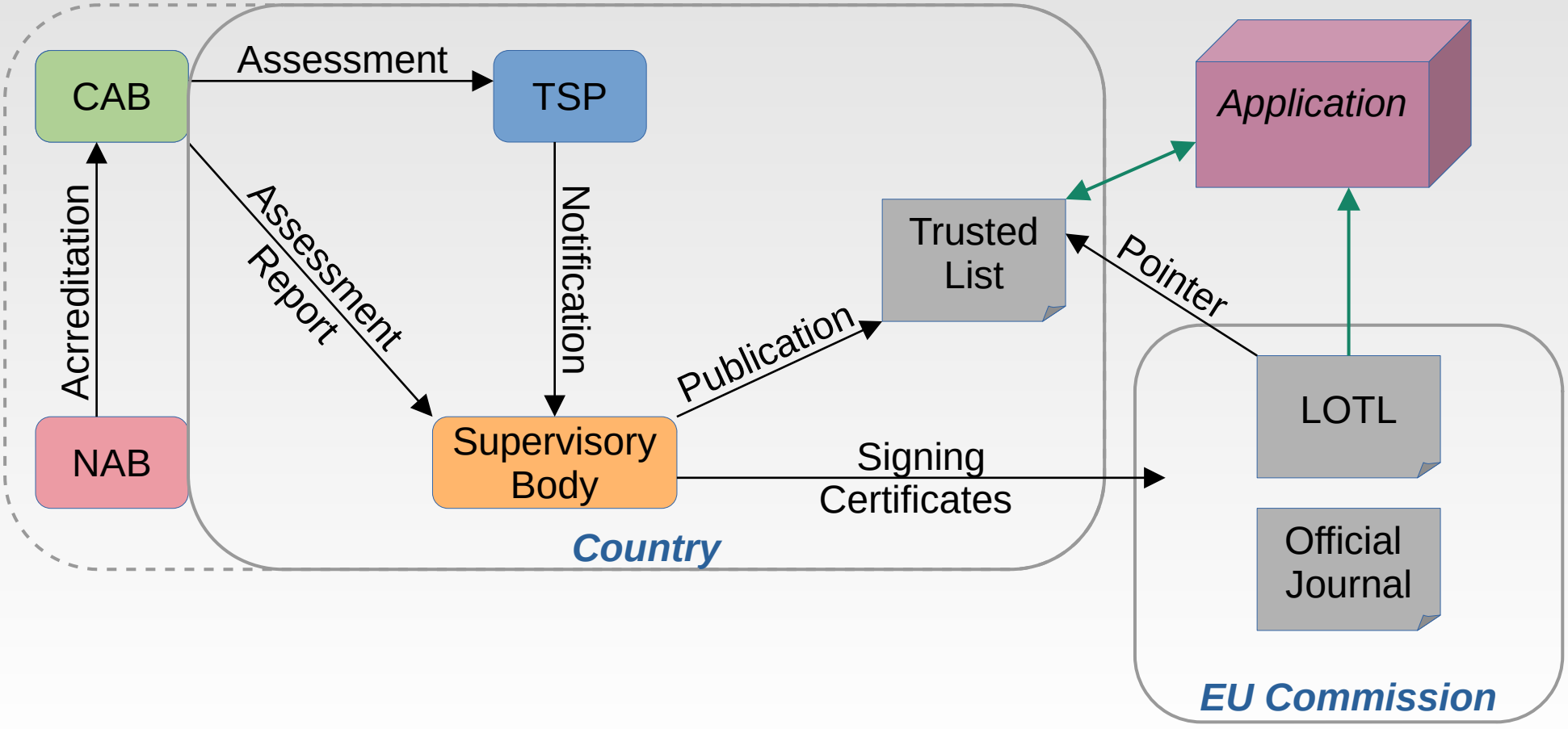
- CAB – Comformity Assessment Body
  - Audits TSP (Trust Service provider) organization and services
    - For CA service ETSI EN 319 411 - policy and security requirements for Trust Service Providers issuing certificates
  - Provides Assessment Report: describing status of comformance with requirements

Supervision and Liability (2)

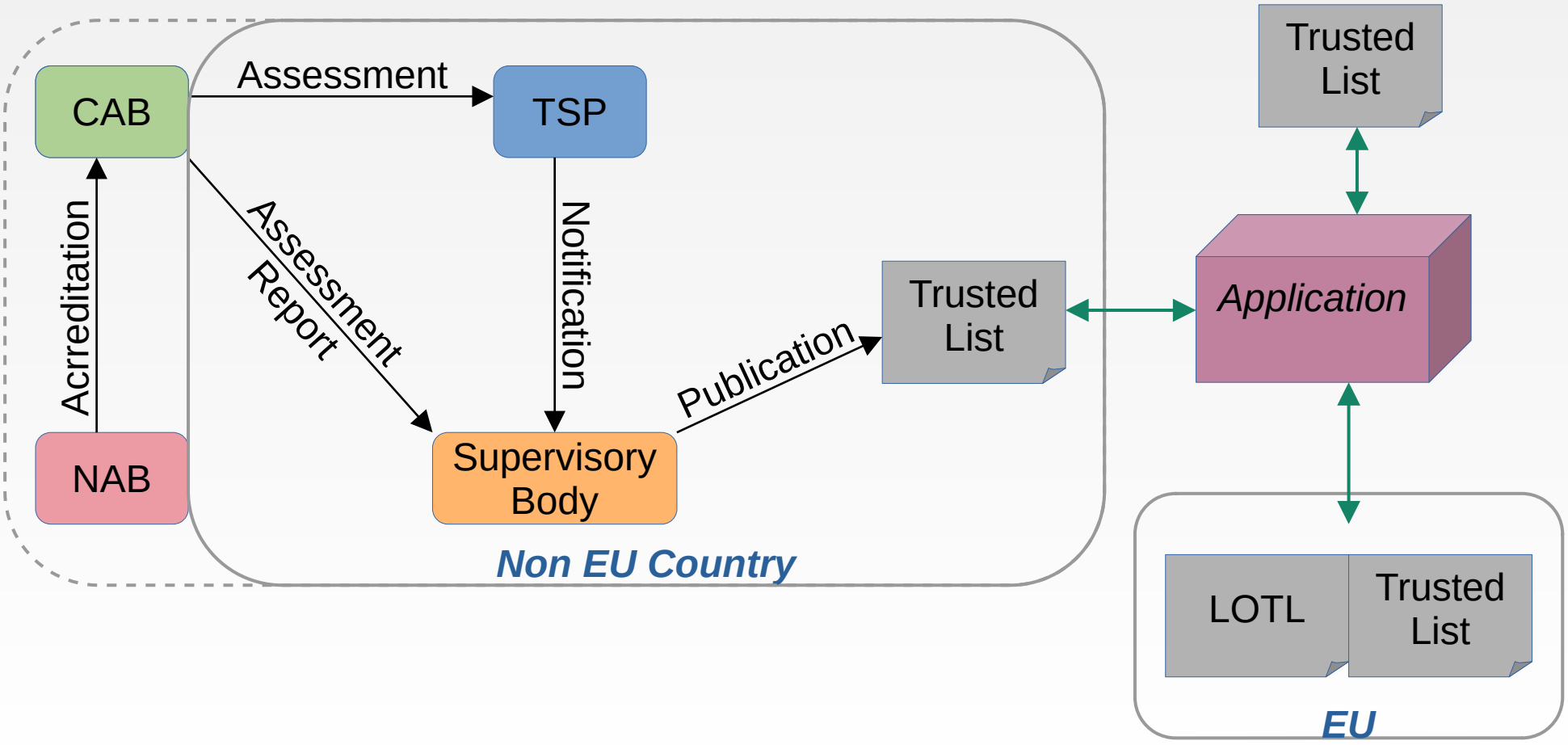
- TSP - Trust Service Provider
  - Qualified status grants a „place” in Trusted List
    - Regular/annual audits on services and organization
    - Liability insurance required
    - High level of trust and open market
  - Non-Qualified status doesnt require regular audits
    - Low trust level
    - Limited market

- Supervisory Body
  - Assessment of TSP Policy conformance with regulation and service status requirements
  - Maintanance of National Trusted List
  - Providing national Trust Anchor information (TL signing certificates and official contacts)
  - Trust and Security Cooperation with other National Supervisory Bodies
    - Incident reporting and experience exchange.

Summary: in EU



Summary: Global model



Qualified Status Application

- TSP submitts Application for Qualified status
  - Including Audit reports and relevant documentation
  - Administrative fee has to be paid
- Supervisory Body
  - Technical bureaucracy
    - Documentation
    - Taxes and fees
  - Check of conformity assessment report
    - Standards
    - Results
    - Conformance With eIDAS regulation Article 13 (p1, p2); Article 20; Article 24 (p2, e,f,g,k); and National Law (Liability and responsibility; regulation; no criminal records)

Supervision of Qualified TSP

- TSP incident reporting
  - According eIDAS Articke 19
  - Within 24 hours
- Change reports
  - Information Change:
    Any change related to the information in Trust List
  - Trust service change:
    Any change related to the trust service internal procedures or technology
    - A new comformity assessment and QTSP status appligation might be required

Qualified TSP “end of life”

- Service will lose its qualified status
- All certificates must be revoced
- TSP must have regulation for ending of providing service
  - All clients and partners must be informed
  - Procedures for destruction of private keys
  - Procedures for hardware destruction
- Trust Service logs, data and related documentation has to be preserved in 10 years.
  - On ending the business, the material is given to the supervisory body

Links and References

- Information about Trust List and Trust Services
  https://sr.riik.ee/en.html
- National Law
  https://www.riigiteataja.ee/en/eli/527102016001/consolide
- Implementing Act
  https://www.riigiteataja.ee/akt/128102016017

Time for Questions and Discussions

Thank You!