Electronic Identity

Mark Erlich

Senior Expert

eGA.ee

e-Facts about Estonia

- Population: ~1.4 M
- 3 types of eID sccepted in both Public and Private sector:
  - Smartcard
  - SIM-card
  - Splitkey
- 99% of population have eID
- 99% of public services are online
- ~1 daily transactions per user
- e-Signatures saves ~2% of GDP

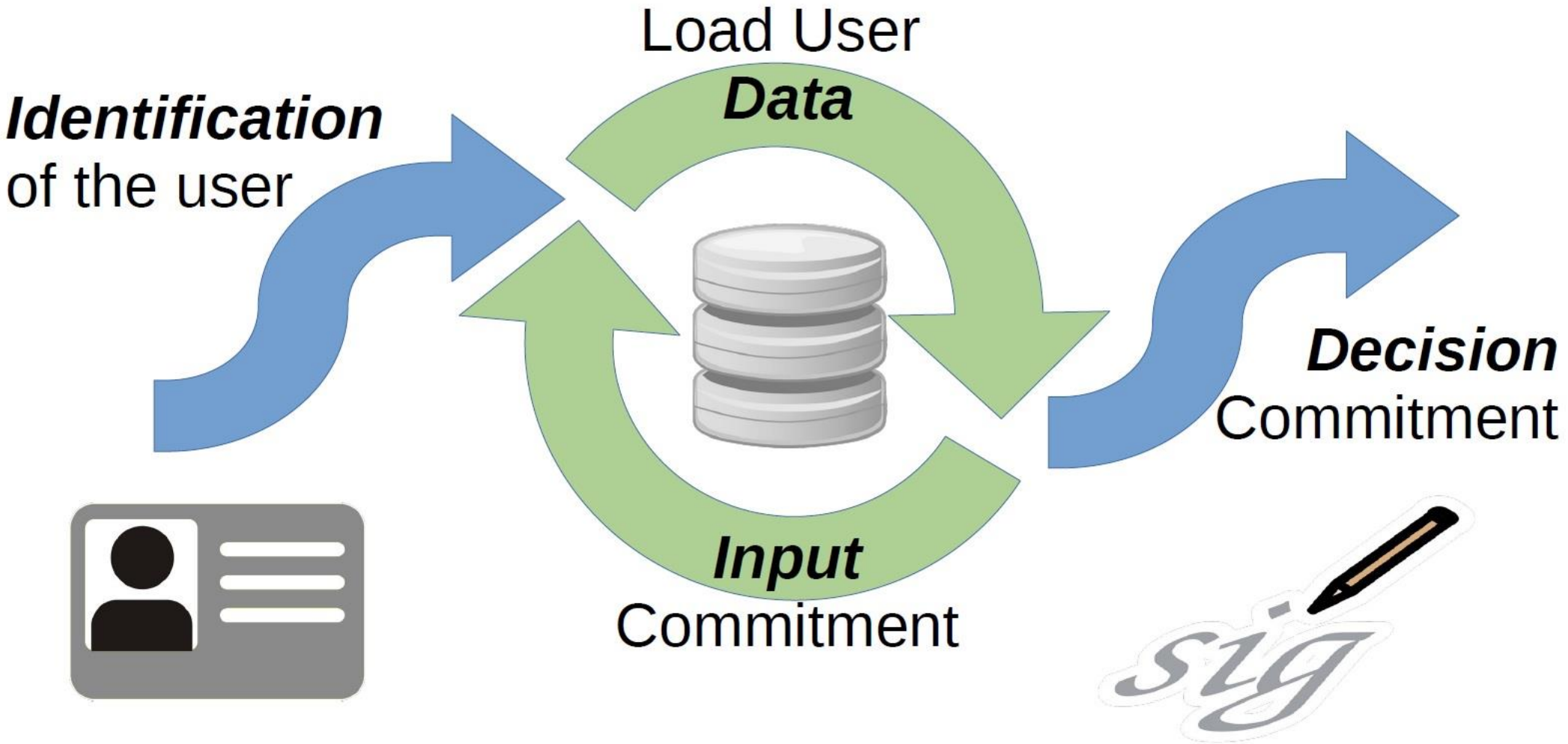
eGA.ee

eID use cases

- **Authentication** (no authorization)
  - Identifying the natural person only. Roles and rights are in registries
- Legally binding **e-Signature** of a natural person
  - Qualified e-Signature: equal with handwritten signature
- Legally binding **e-Stamp** (e-seal) of a legal entity
  - Same as for natural person but with legal entity certificate
  - Replaces rubber stamp from paper world
- File **encryption / decryption** for secure data / information delivery

eGA.ee

Service – s set of processes



Estonian ID Code

- Personal Identification Code
  xYYMMDDyyyz
  x – century and sex
  YYMMDD – date of birth
  yyy – localization and sequence number at the registration day
  z – control number

- Population Registry
  All records are available since birth (but with limited access)

- ID-Card as a mandatory ID document from age of 15
  ...but since it is in a convenient format and valid as a travel document, even newborn babies use to have one.

eGA.ee

Government issued ID Documents

- It is considered to be most reliable evidence of identity
  - Has legal value
  - Accepted by all
  - Physical presence required

- No room for risks
  - National security
  - Democracy and independence

Identity and its uniqueness

- The government issued identity is in most cases based on Biometrics:
  - At least the picture is collected and compared with historical
  - Physical face is compared to known picture
  - In some cases same happens with fingerprints

- Persons biometric data are in 99,9% unique, but
  - Some similarities make it impossible for human eye to detect difference
  - Machine algorithms are fine tuned to use on a specific group of people
  - Even machines have difficulties in specific cases

1-2-3 Factor identification & Biometrical Data

- 3 Factors, each with own risks:
  - (1) „Something I Know" – **I can control**
  - (2) „Something I Have" – **I probably can control**
  - (3) „Something I Am" – **I can't control**
- Authentication based solely on biometrics is not reliable
  - Only one factor and weakest of them all
- Authentication based on 2-F with biometrics is weak
  - 3rd factor is for strengthen 2-F and not for replacement of another factor
- Single point of failure – end user device:
  - as single source of truth is a bad practice
  - can not be trusted: it can be manipulated

eGA.ee

Remote identification & Biometrical Data

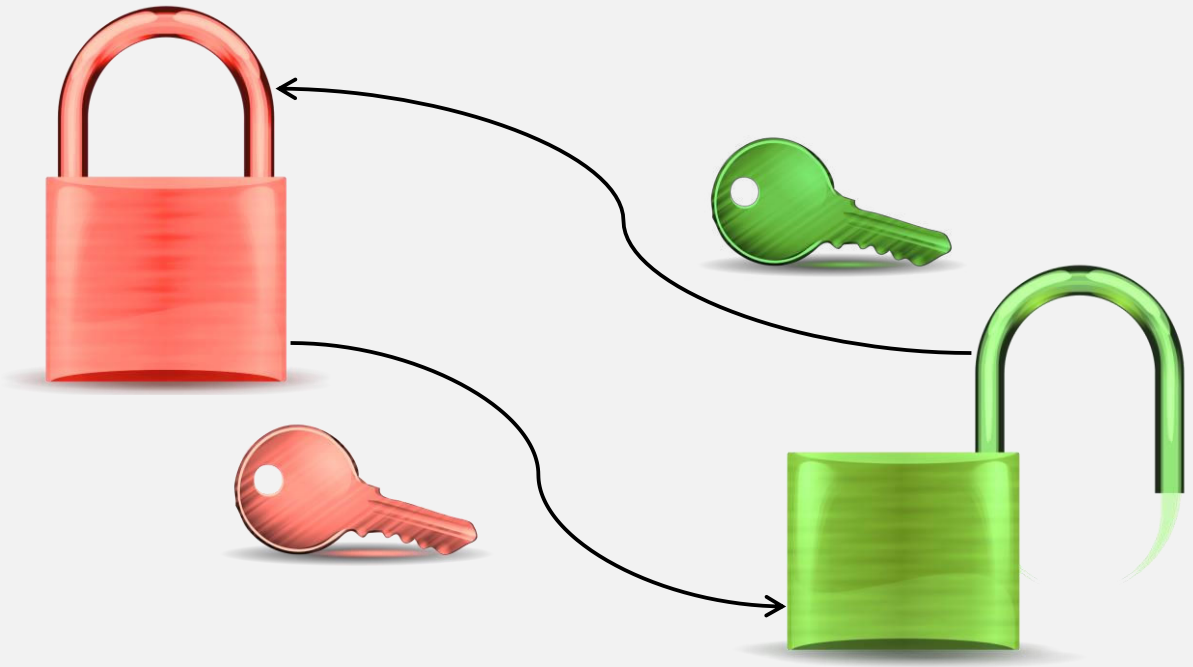
- Authentication based solely on biometrics is not reliable today:
  - by using other means in addition makes solution non-user-friendly

- Physical presence can be replaced with biometrical identification:
  - by using sole control mechanisms
  - e.g. Roll-Out procedure, extension of validity, etc.

eGA.ee

PKI Based Solutions

- Public and Private key
  - Public key identifies
  - Private key verifies
- Public key is distributed with certificates
- Private key
  is under **sole control** of the user
  - User in possession of the Chip with the Secure element
  - Keys are generated in the secure element
  - Private key is stored in the secure element



eGA.ee

eID Technology in Estonia

- PKI with X.509 certificates
  - Estonian Government Root
  - Maintained and issued by Qualified Trust Service Provider
- Certificate contains minimum personal data:
  - First name, Last name, personal identifier
- All other personal data and authorization information:
  - Different registries in owned by different institutions
  - Unique identifier is a Foreigner Key for record matching
  - Authorized control at institutional level

eGA.ee

ID-Card and Smartcards

- Issued by Estonian Police
- Technically same for ID-Card, Residence Permit Card, Digi-ID and eResidence Card, Diplomatic ID
- 2 pairs of keys with corresponding X.509 certificate:
  - Authentication: SSL/TLS and/or OpenID Connect is used.
  - Signing: Middleware software with end user application and web browser plugins
- Validity: 5 years

eGA.ee

Mobile-ID on SIM-card

- Special SIM card with PKI eID chip
  - SIM Toolkit application
  - SMS service for data exchange
- 2 pair of keys with corresponding X.509 certificate
  - Private keys in secure module on SIM
  - Certificate stored in public repository only
- Central M-ID Service instead of middleware

Mobile-ID Technology

- M-ID central service provided by Trust Service provider
  - Access control for known customers
  - Message center
- SIM toolkit application
  - Calculates control number
  - Protects use of private keys

eGA.ee

Split Key Technology

- Since we can’t trust user device solely, we need additional trusted component from the third party
- Challenges:
  - how to assure that device connected is under sole control of the user (?)
  - how to ensure that this is an original device and it is not compromised (?)

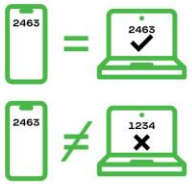
The full 6K bit virtual key never exists in the whole. It’s composed of two 3K bit shares.

The key’s shares are generated and stored by independent entities. Protection doesn’t rely on a single device.

No reference data on user’s phone. Offline brute forcing is impossible.

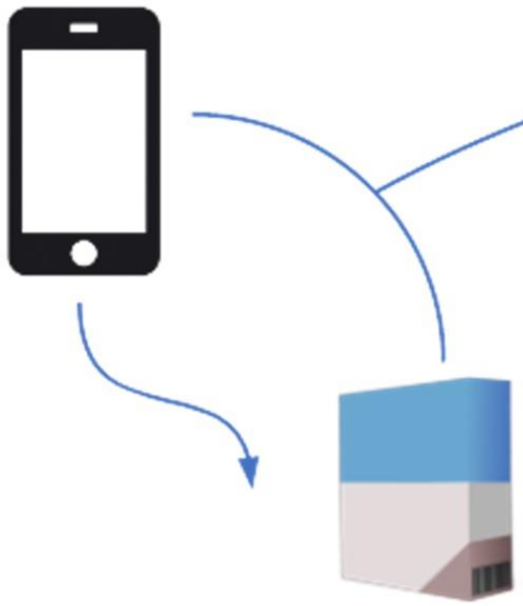
Signature creation is an interactive process. User has technical control of their signing.

A transaction-gererated code is present on the web browser and smartphone. Defence against phishing/MitM.



PIN verification takes place online. Multiple incorrect PIN attempts will result in a locked key.

Smart-ID with Split Key



Smart-ID
Application

Phone DNA = an Unique account
based on HW, SW and Smart-ID application

+ encrytion with ½ Key

Second ½ generated key
Stored in HSM bound to
Phone DNA Account

SMART-ID

User journey (UX):

- Same as with Mobile-ID
- But instead of Telecom, the internet with secure channel is used

Comparison on Mobile Phone eID

- **Mobile-ID**: SIM card PKI

+ Simple Sole Control mechanism
+ Works on old 2G phones
+ Low roaming costs (no need for internet)
+ No app security and maintenance issues

– Depending on hardware availability
– Complicated issuance process (many parties)

…

- **Smart-ID**: Split Key (App and remote PKI)

+ No special hardware is needed
+ Easy issuance process
+ Fast and user friendly

– Higher App and security maintenance costs
– Works only on updated smartphones with support
– Higher roaming costs when travel (need internet)

…

Why we need additional eID

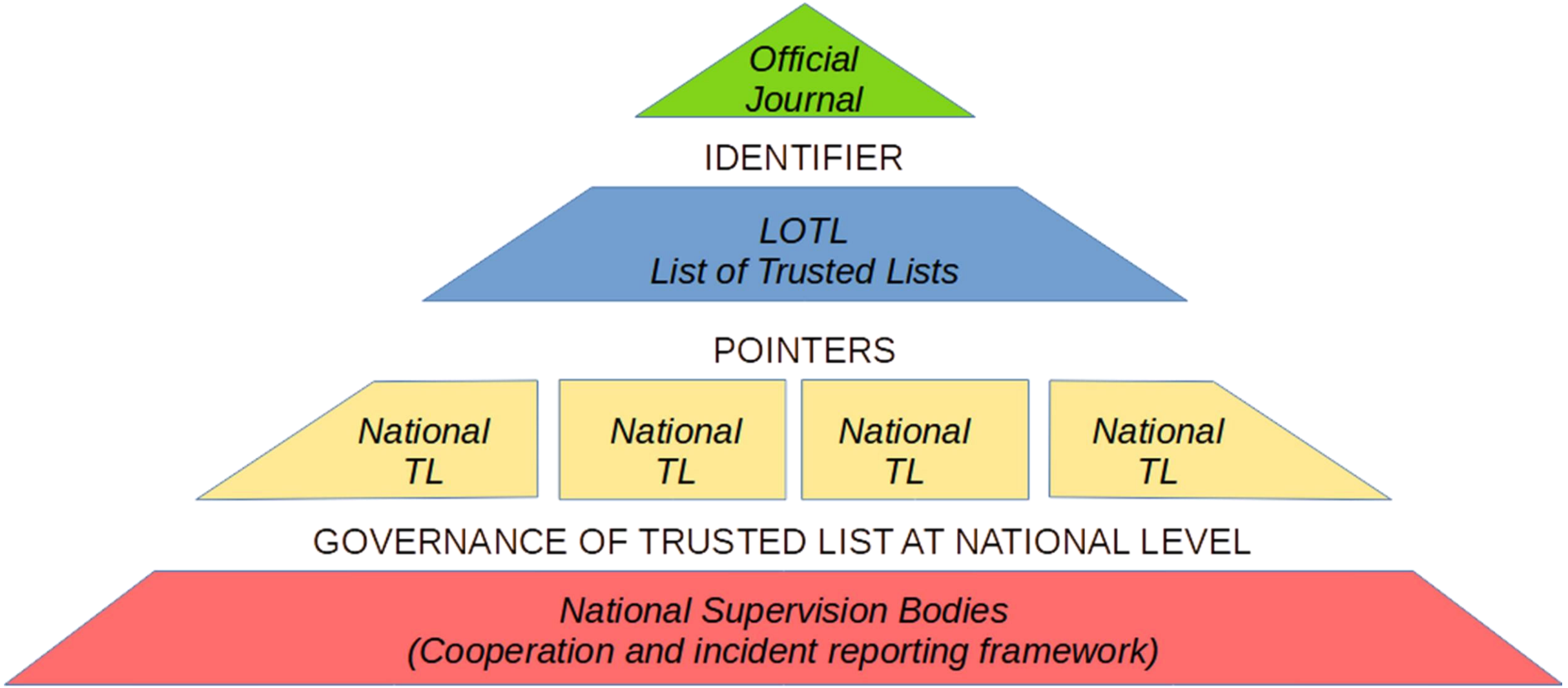
- eID is used as working tool
  - Must be able to leave the tool at work
  - Hazardous environments – can't take thing out from facility
- Alternative for traveling people
  - Roaming costs
  - Can't use own environment
- Emergency switch
  - In case one system fails, the alternative solution can be used
  - Can't keep all eggs in the same basket

What is a Trust Service

- 7 types of Trust Services:
  - 4 directly e-Signature/Seal related: Creation; Verification; Validation; Preservation
  - Time-stamping service
  - Electronic Delivery service
  - Web-page identification service

- A Service provided by a Third Party
  - Provides and Commits legal statement with its Key
  - Has Liability responsibility

EU Trust Model



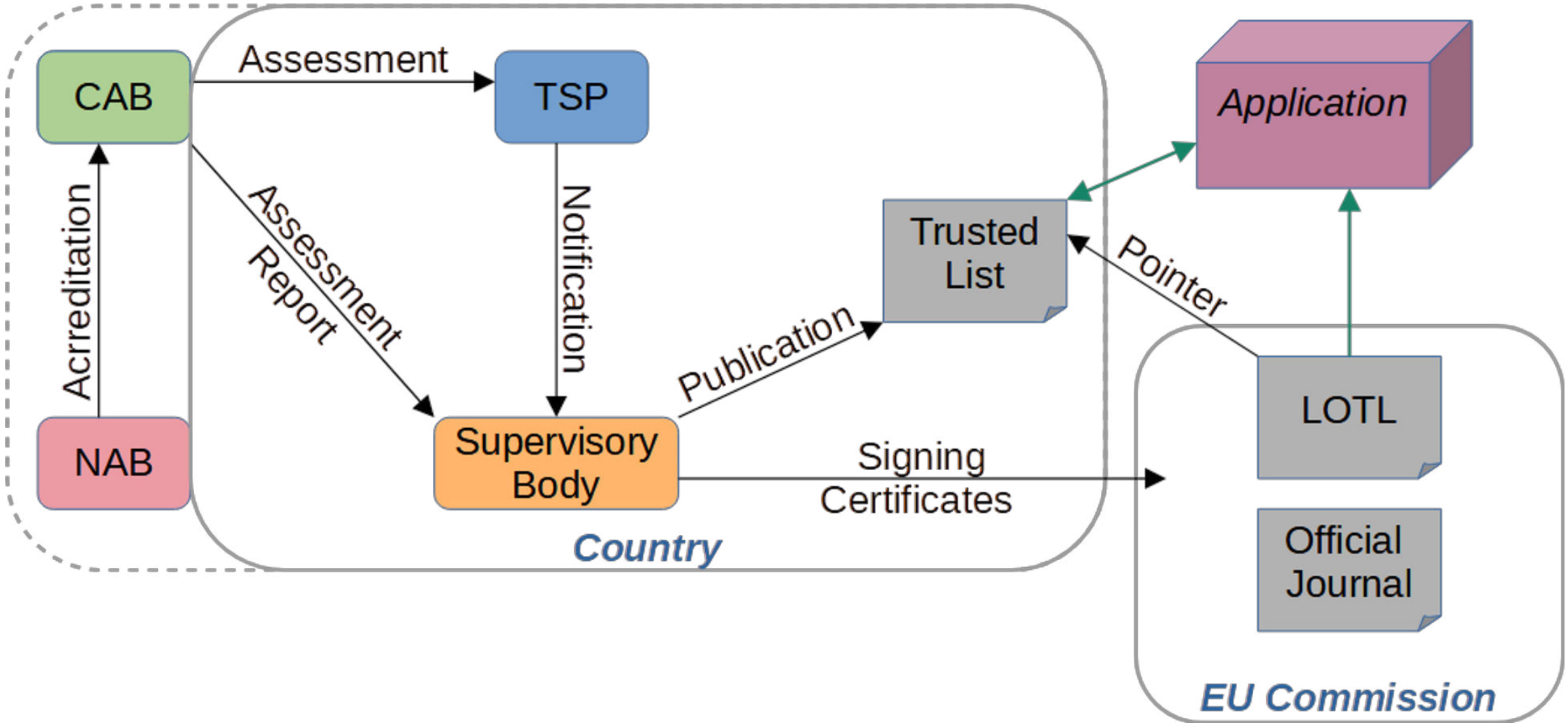
Supervision and Liability (NAB/CAB)

- 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 conformance with requirements

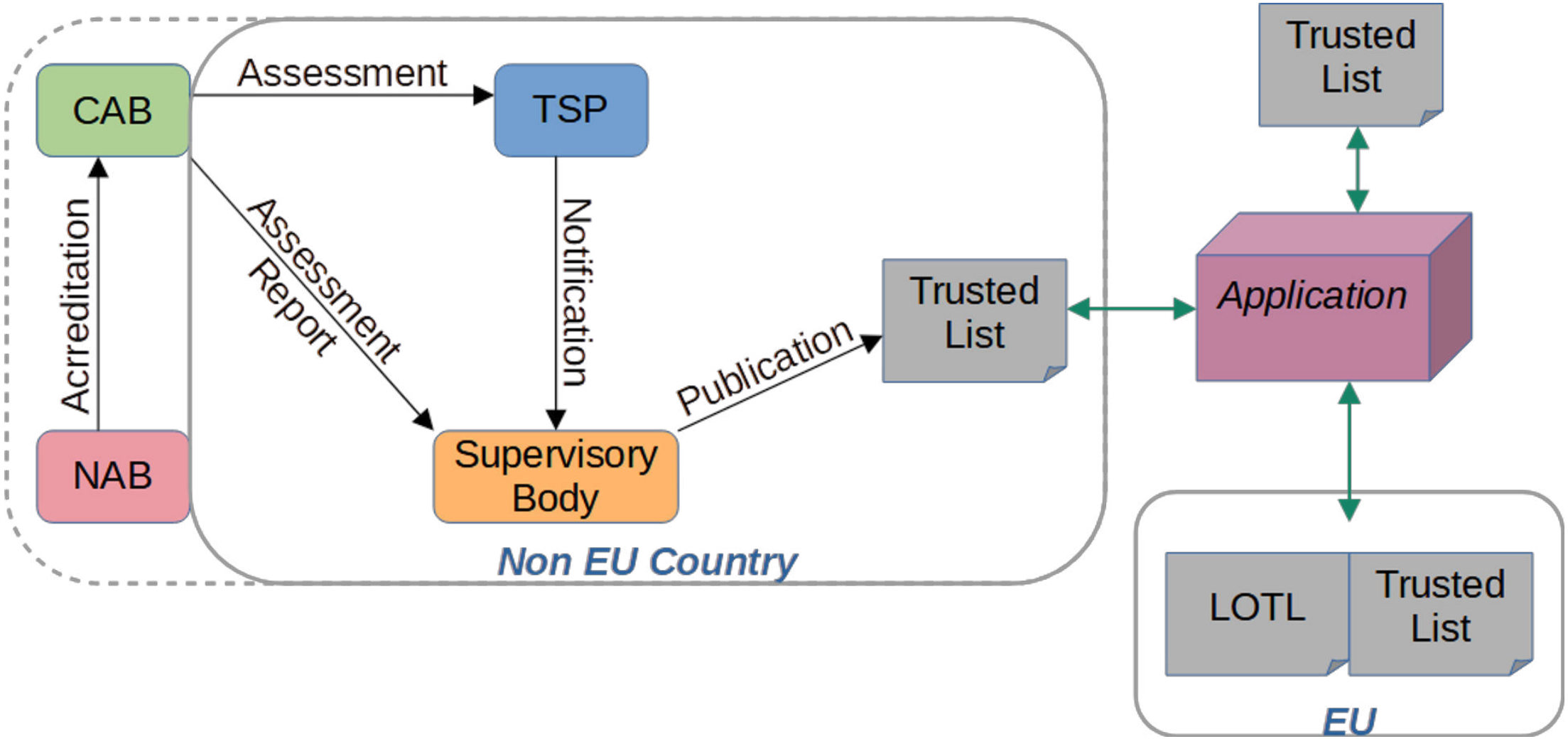
Supervision and Liability (TSP/SB)

- 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 doesn’t require regular audits
    - Low trust level
    - Limited market
- SB – Supervisory Body
  - Assessment of TSP Policy conformance with regulation and service status requirements
  - Maintenance of National Trusted List
  - Providing national Trust Anchor information (TL signing certificates and official contacts)

Roles in EU Trust Model



Trust Model for non-EU Country



eIDAS AdES and QES requirements

- **AdES** – Personal Certificate (not "on behalf of")
- **AdES QC** – Qualified status assures about real identity
- **QES** – AdES QC + QSCD (Equal with handwritten signature)
  - The **QSCD** assures about persons presence at signing action
  - In addition, the signature must fulfill following criteria:
    - Certificate had QC status **at time of signing** (Trust List)
    - Certificate was valid at **time of signing** (OCSP)
    - Signing token had QSCD status **at time signing** (Certificate + Trust List)

eGA.ee

ETSI Standards in a nutshell

- Baseline profile:
  - Basic (-B): only signed data and corresponding certificate are required
  - Time (-T): Basic level + Time to assure that signature existed at certain time
  - Long term (-LT): Time level + validation material, for long term validation. Usually it’s OCSP
  - Archival (-LTA): Long term + annual timestamp
- Validation data: Timestamps and Certificate revocation information

eGA.ee

e-Signature file formats

- **In Baltics**: To sign and seal any data in any format
- **Container** based signature file using PKI for signing
  - XAdES and ASiC
  - eSignatures and eStamps (e-seal)
- **PDF** (?)
  - Limited use only
  - Poor User interface – problem with trust and understanding of signature level
  - PDF document format security issues (e.g. https://www.pdf-insecurity.org/)

eGA.ee

Estonian Legal Framework

- eIDAS implementation Act: https://www.riigiteataja.ee/en/eli/ee/527102016001/consolide/current
  - Replaces old Digital Signature Act
  - Defines processes, roles and tasks for organisations (supervision, notification etc.)
  - Defines eIDAS QES as „Digital Signature” (all other legal acts already use „Digital Signature”)
- Identity document Act
  - Regulates identification, identity document lifecycle and defines roles and tasks for organisations.

Summary
- Key Takeout

- All processes are regulated
- Keep the process that works
  - Automate as much as possible, even decision making
  - Eliminate bottle necks – Human intreraction within process
- Key tool for the process
  - eID – Authentication Triggers the process
  - e-Signature Ends or Starts next process

Time for Questions

Mark.Erlich@ega.ee

Follow us: **egovacademy**