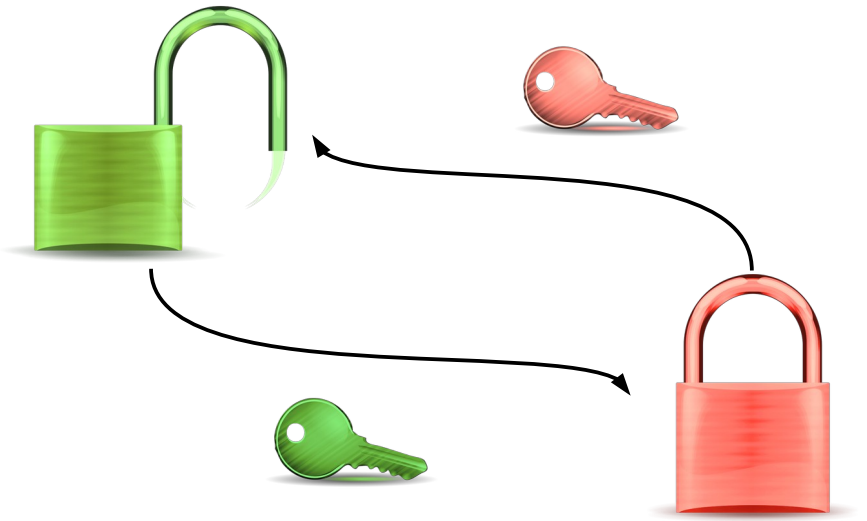
REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Strong and Secure Mobile eID

Mark Erlich
Business Architect

2022-June-06

PKI based solutions

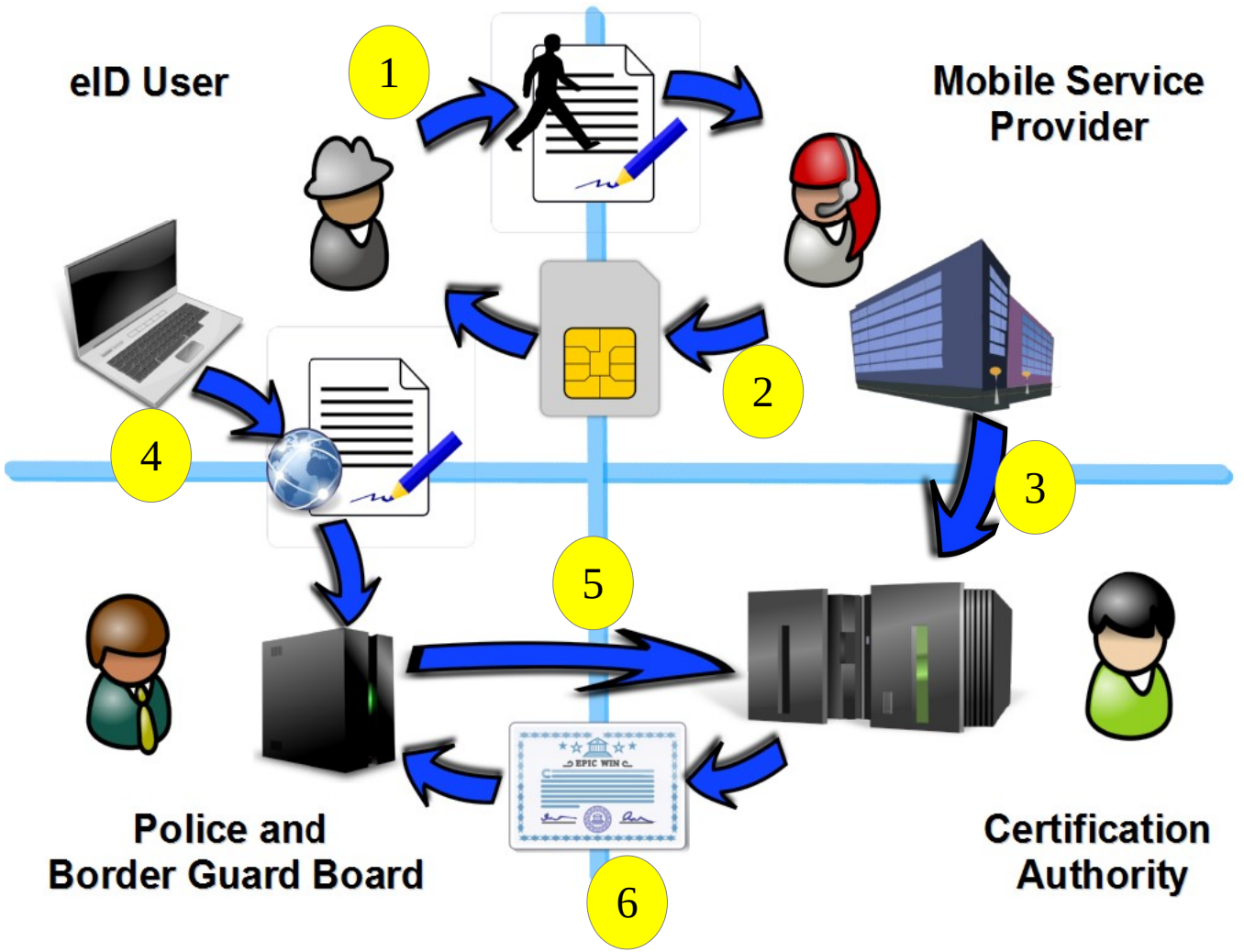


- Public and Private key
  - Public key identifies
  - Private key verifies
- Public key is distributed with certificates
- Private key is under **sole control** of the user
  - User in possession of the Chip with the Secure element
  - Keys are generated in the secure element
  - Private key is stored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

Mobile ID

- 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
- Validity: 5 years

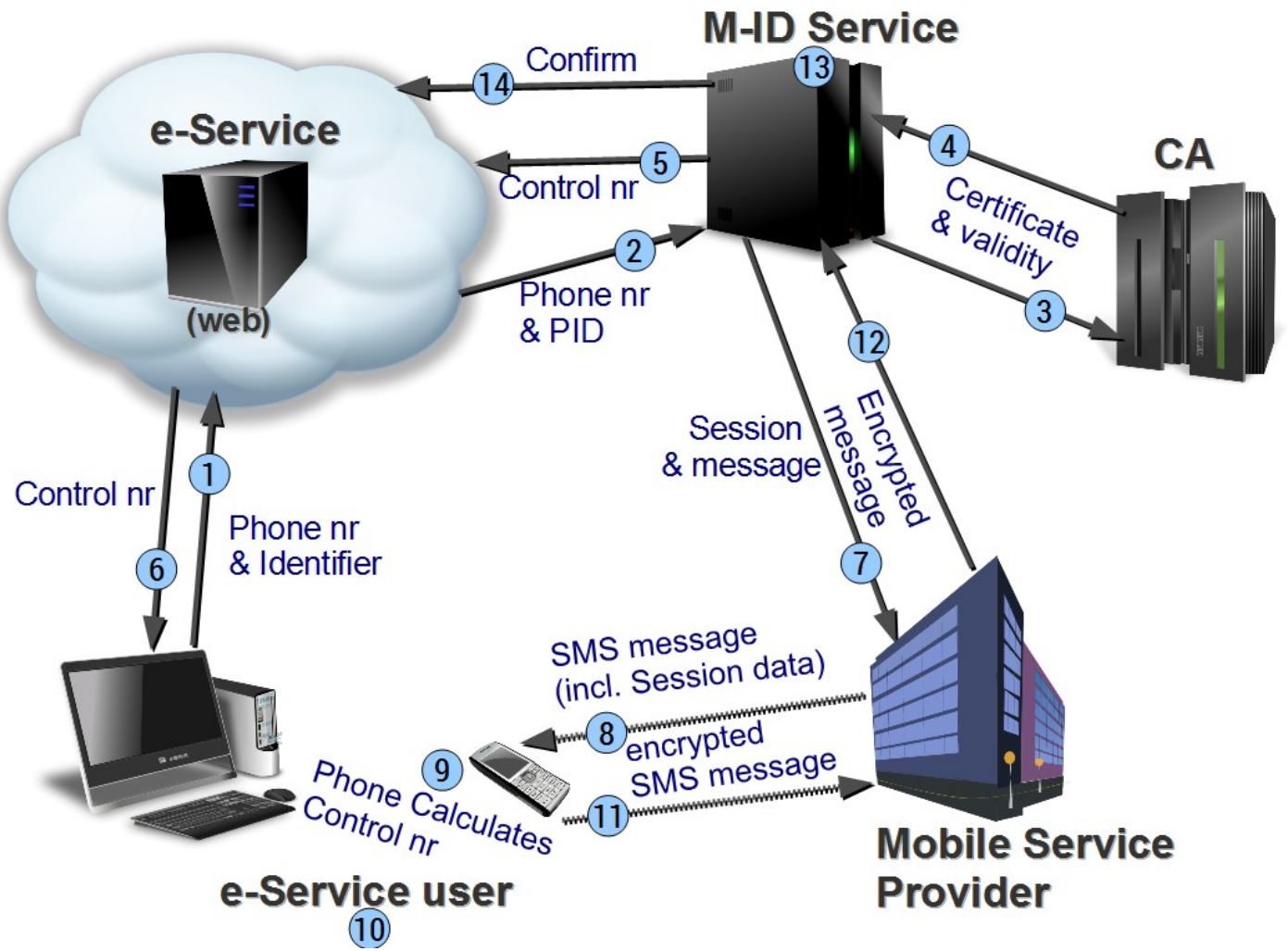
Mobile-ID: issuing process



Mobile-ID: issuing process description

(1) User applies for mobile-ID service at Telecom service desk
 - physical person identification is done
(2) User receives special SIM card with cryptographic chip
 - PKI based eID token
(3) Telecom company sends information about user (his unique identifier), phone number SIM card identifier and public key to CA
(4) User logs in to Police web service, using his national ID-card (primary eID token) and sign electronically prefilled mobile-ID application
(5) Police information system sends information about user to CA for issuing certificates
(6) If data from Police and Telco matches, the certificates will be issued/activated.

Mobile-ID: system



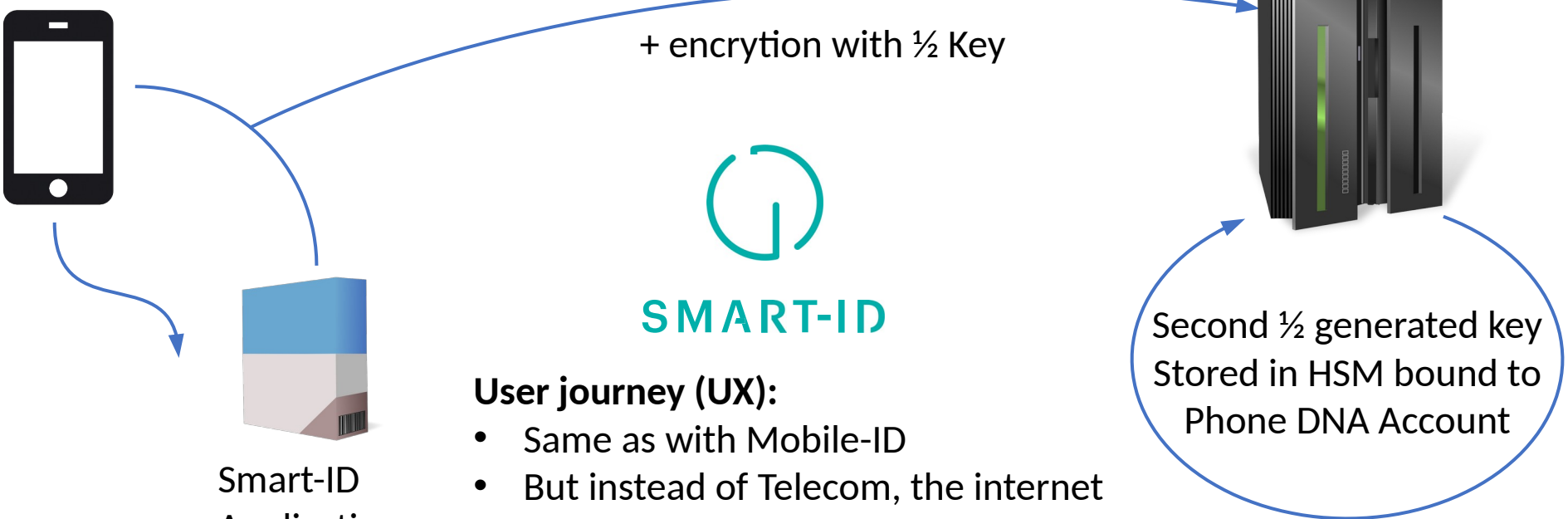
Mobile-ID: system process description

(1) On web page user fills in phone number and identifier in login field
(2) e-Service sends users ID and phone nr to central M-ID Service
(3-4) M-ID Service (M-IDS) checks if claimed person has mobile-ID connected to given phone nr and request certificate validity from CA
(5) If certificate is valid, the request message is created and control nr is calculated (out of message) by M-IDS. Control nr is sent to e-Service.
(6) e-Service webpage shows control number to the user
(7-8) M-IDS sends request message to user phone (SIM toolkit message)
(9) SIM application calculates control number out of received message.
(10) If control numbers shown on phone and on the web matches, the user can accept login and enter PIN for encryption with private key.
(11-12) Encrypted message is sent M-IDS.
(13-14) If positive result (decryption of message with users public key), then M-IDS will confirm user authenticity

Smart-ID

- Private sector initiative
  - Solving eID security issues for Banks
  - Popular among the users
- Techincally equal to Gov issued eID
  - PKI based solution
  - Private keys splitted between server and App
- Supported by Gov. e-services
  - Based on Gov. Issued ID/eID
  - Assurance level (High) recognized by government.

Smart-ID: Split Key Technologie



User journey (UX):

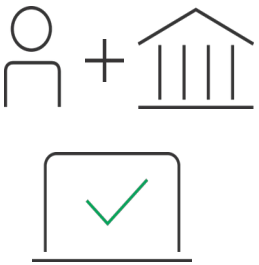
- Same as with Mobile-ID
- But instead of Telecom, the internet with secure channel is used

CYBERNETICA

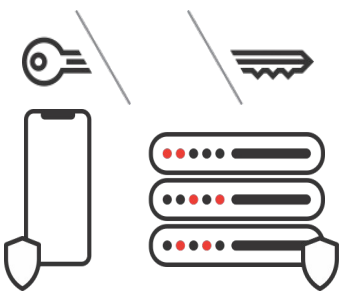
The important parts of SplitKey

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

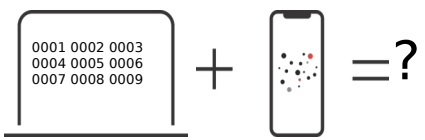
The key's shares are generated and stored by independent entities. Protection doesn't rely on a single device.



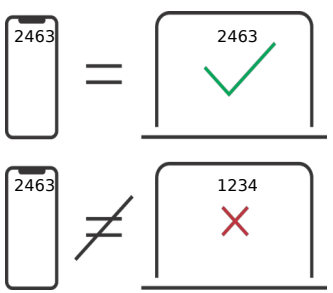
No reference data on user's phone. Offline brute forcing is impossible.



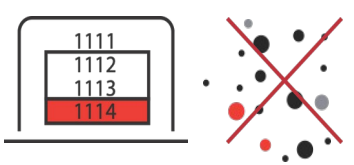
Signature creation is an interactive process. User has technical control of their signing.



A transaction-generated 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.



How to compare these two mobile technologies

- 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: 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)

REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Thank You!