Cloud-based provisioning of qualified certificates for the German ID card

September 11th 2013

Open Identity Summit 2013, Kloster Banz

Marcel Selhorst

Agenda

- **Overview: the German eID card (nPA)**
- **Post Issuance Process**
- **Security Goals and Measures**
- **Status quo and future developments**
- **Live-Demo**

Overview: The German ID Card

- provides „classic" visual identification as well as online authentication
- secured by EAC 2.0
- Three applications on smartcard:

ePass (ICAO compliant - sovereign use only)

- fast electronic access to id data by sovereign agencies within the European Union
- contains MRZ data, image and optionally fingerprints

eID (Application for electronic identification - *optional*)

- online- and offline-Identification
- pseudonym Login-Functionality
- anonymous age and place verification

eSign (Application for qualified electronic signatures - *optional*)

- legally binding signatures for electronic documents (QES)
- online and offline usable
- initially inactive

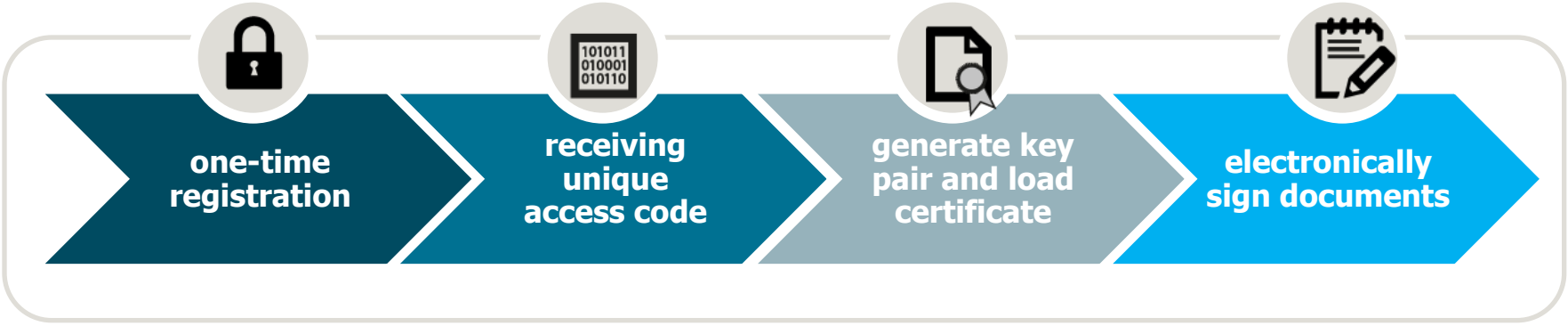
BUNDESDRUCKEREI

Using the German ID card as a secure signature creation device (SSCD)

- Legally equal to personal signature
- Full control by the citizen
- Signature key is generated and stored on ID card
- Immediate online transmission of the generated certificate to the ID Card
- Deletion of the generated signature key under control of the citizen
- Unlimited (re-)generation of signature keys possible
- Different certificate validity periods possible (e.g., < 1 year up to 10 years)
- All advantages of digital signatures in existing business processes are maintained

sign-me and the new ID Card enable for the first time on-the-fly post-issuance key generation and certification on an SSCD!

Signature Process from the citizen's point of view:



All advantages at a glance

one-time registration
for all certificates
→ requires eID to read personal data

easy handling
identic layout independent of the service provider selling the certificates

uncomplicated workflow
users are guided through the necessary steps to ease the overall loading process

grouping of processes
one solution for many processes by grouping the required components into one online application

offline signature creation
already 5 different signature application components available supporting sign-me

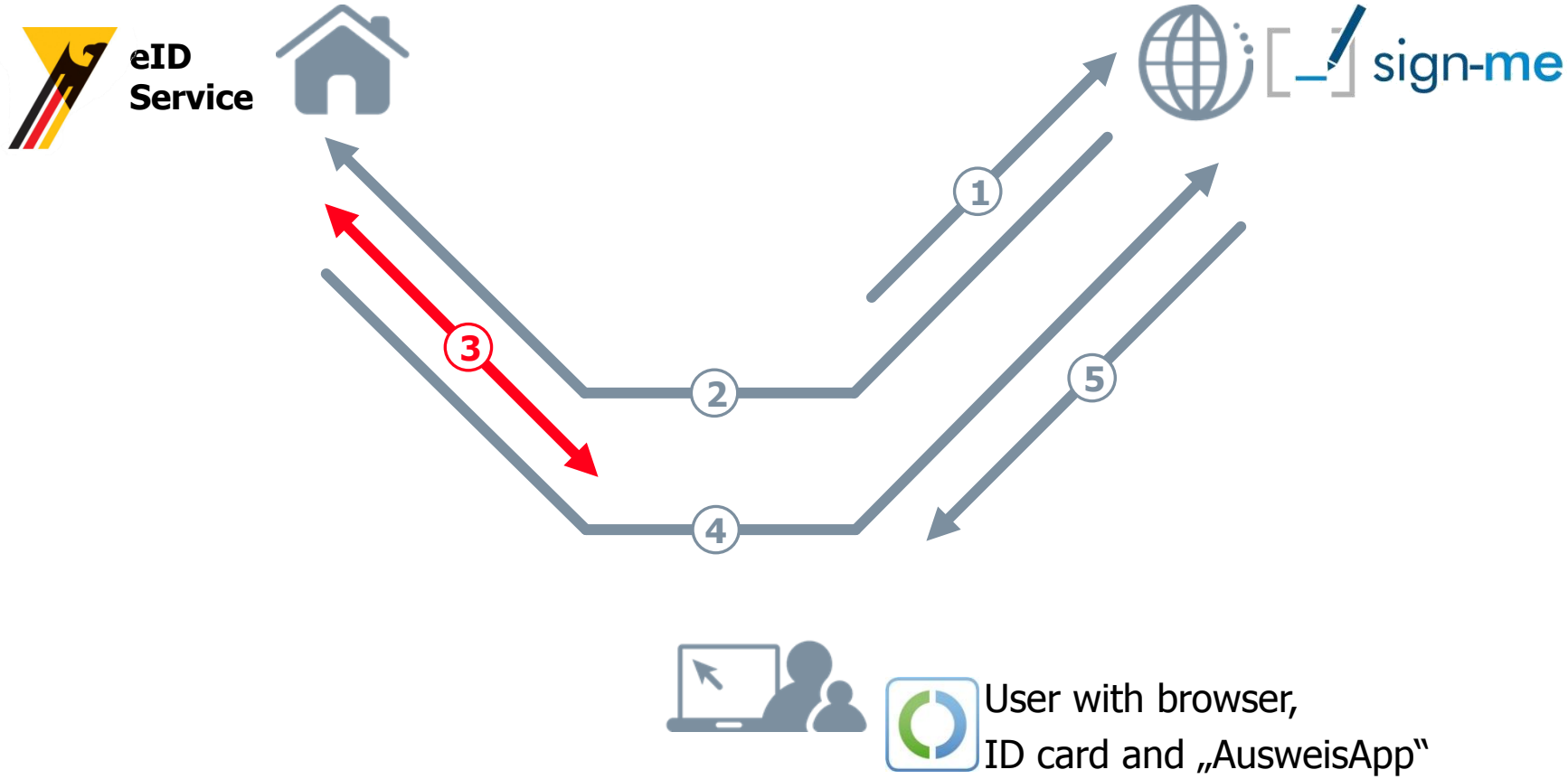
The following preparations are required *before* starting the certification process:

1. **Buy a Comfort Reader**: Standard reader with display, keypad and **security module** for secure key storage
   → required for signature PIN management
   → required for generation of qualified signatures

2. **Buy a certificate from an affiliated online shop**
   Certificates are not sold by the Bundesdruckerei directly but rather by affiliated online shops
   (currently: card reader manufacturer Reiner SCT)

3. **Register online to obtain a re-usable authorization code**
   Ensures that even in case of theft only the legitimate card holder can initiate the certification process.

Registration using eID

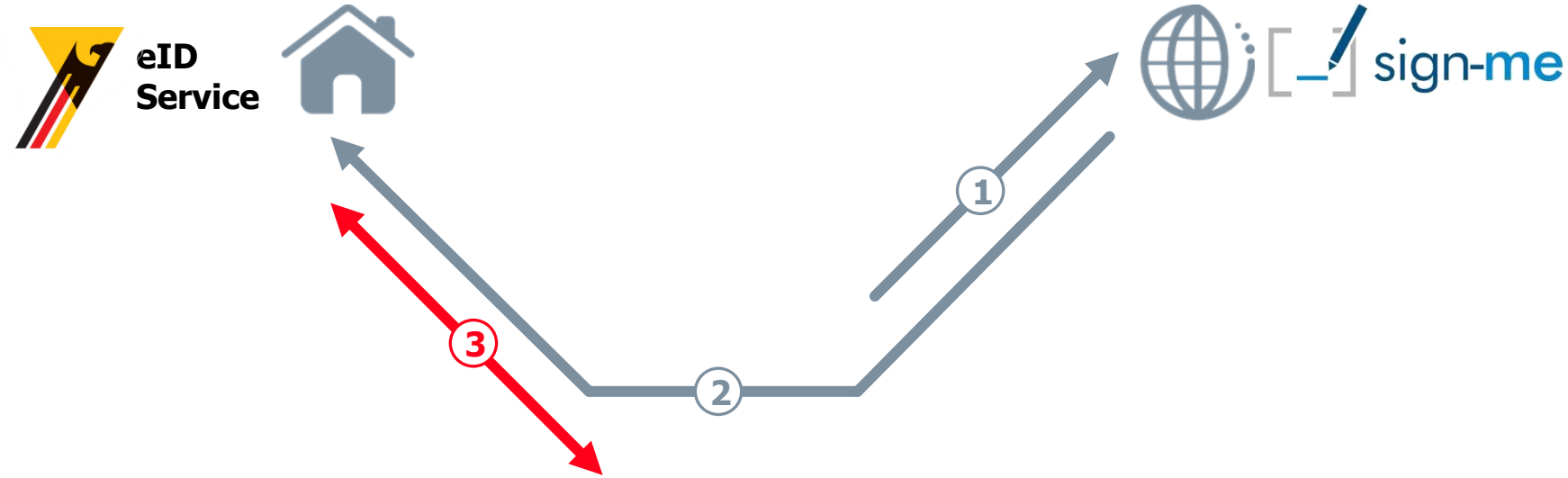


BUNDESDRUCKEREI

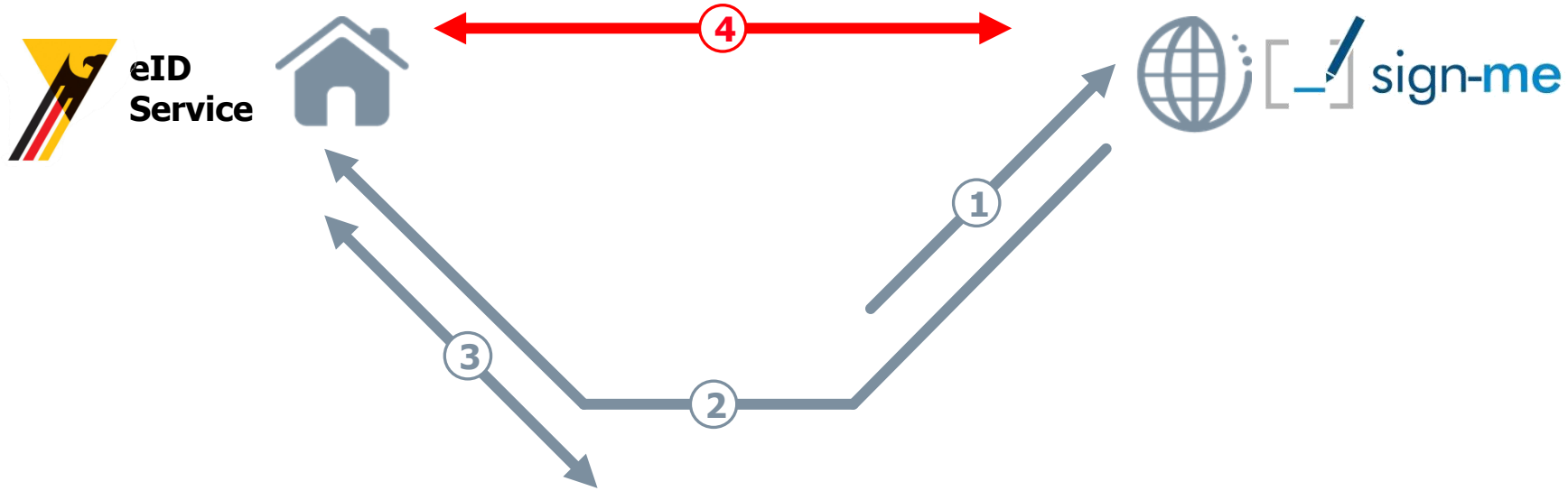
The Post-Issuance process consists of

1. entering the authorization code (received upon registration)
2. setting the signature PIN
3. selecting a revocation password (for the hotline)
4. loading the certificate in an enhanced eID session (including key generation)
5. confirming reception of the certificate (required by German signature law)

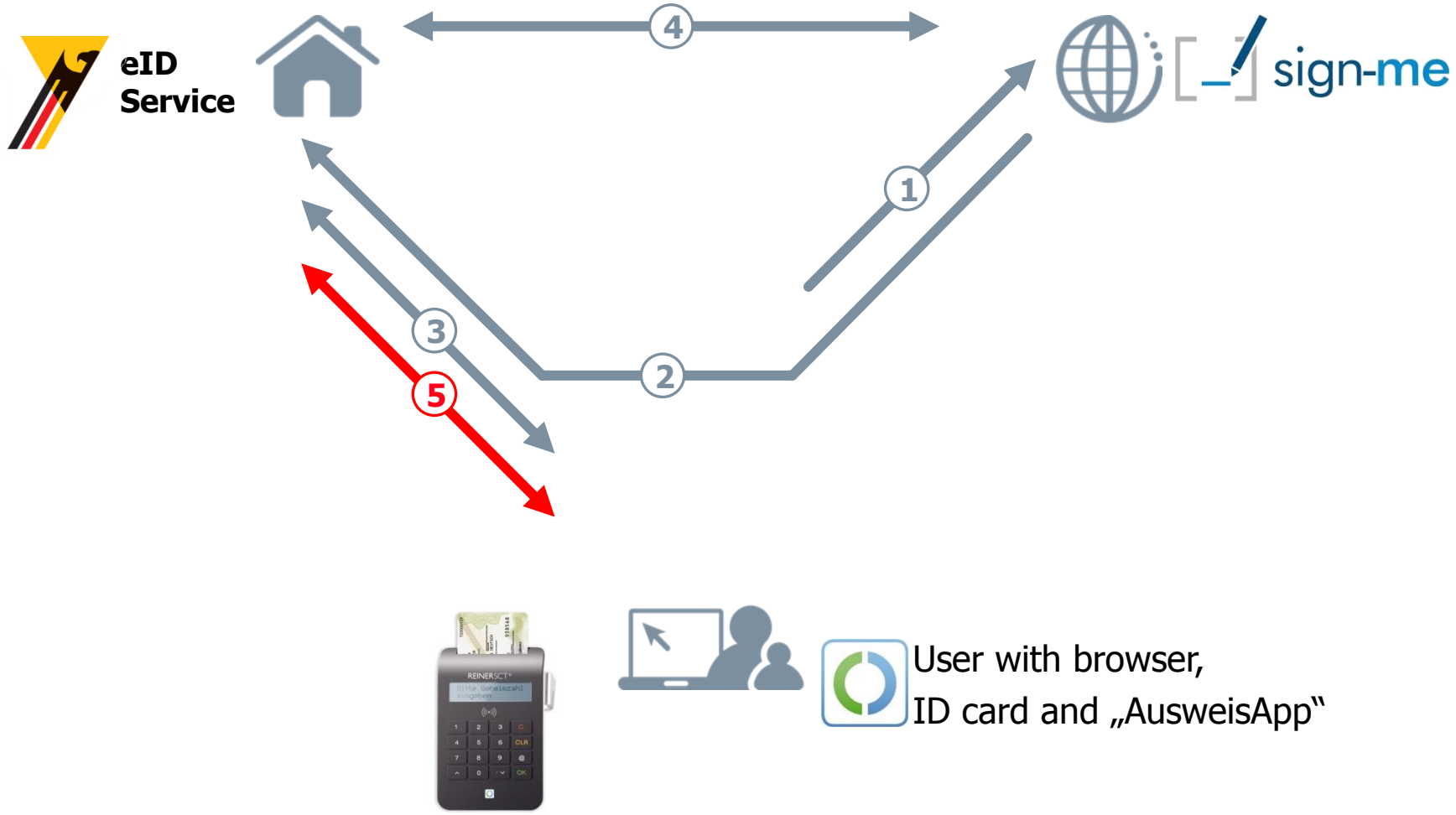
Post-Issuance Certification Process

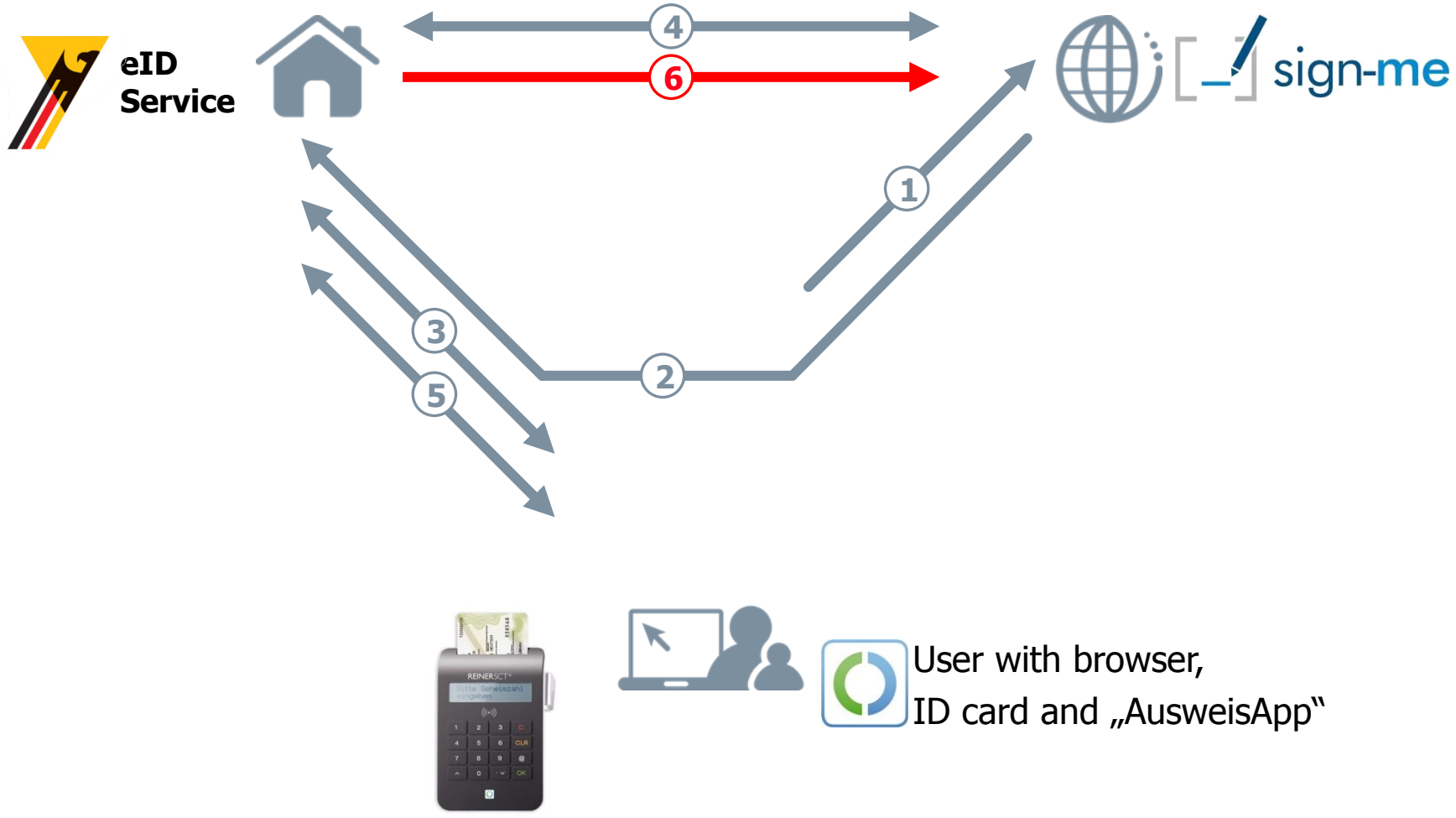


User with browser,
ID card and „AusweisApp"

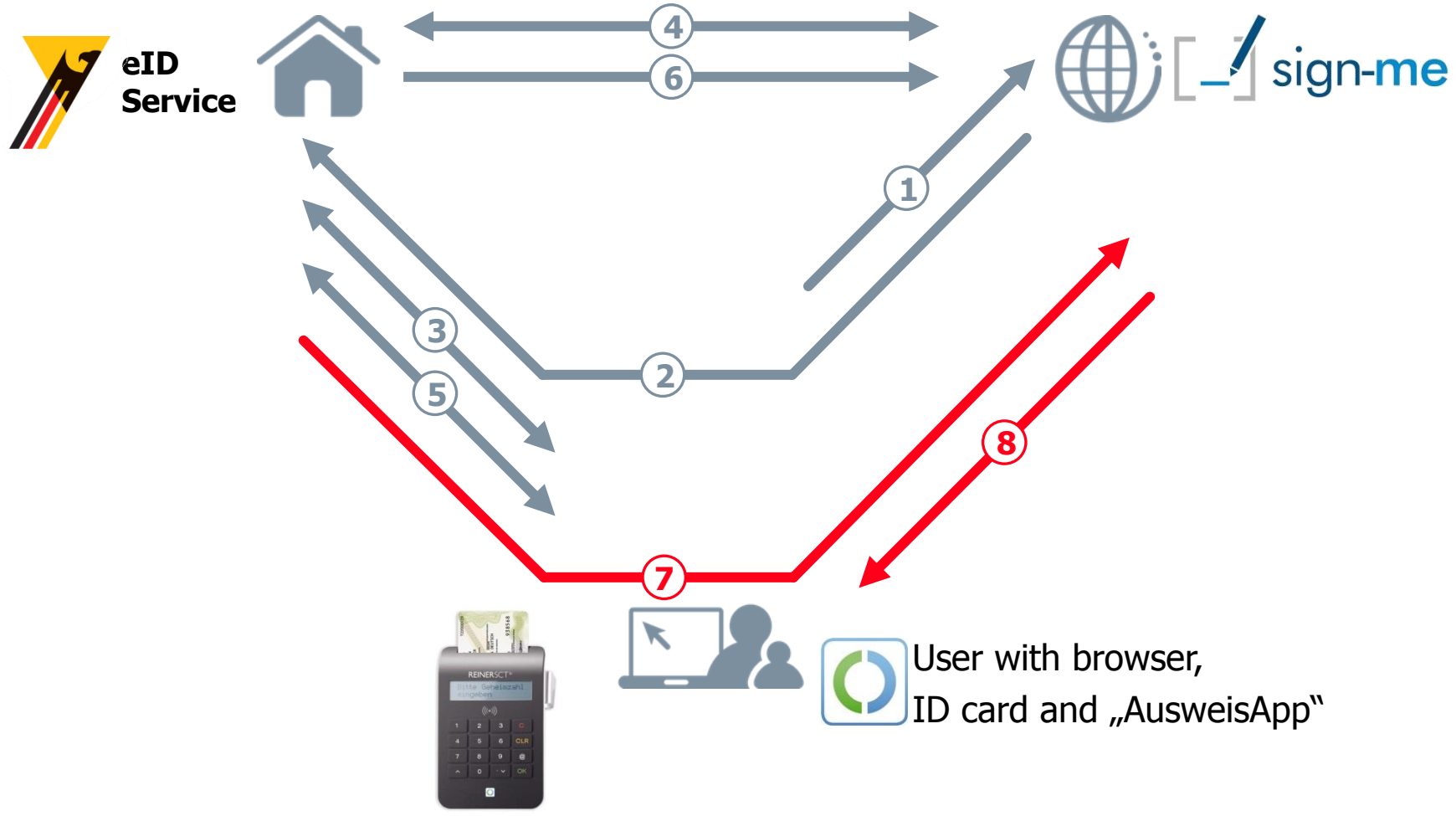


User with browser,
ID card and „AusweisApp"


eID
Service
4
1
2
3
5
sign-me
User with browser,
ID card and „AusweisApp“


eID
Service
4
6
1
2
3
5
sign-me
User with browser,
ID card and „AusweisApp“

Post-Issuance Certification Process



BUNDESDRUCKEREI

- Protection against malicious chip access
  - Mutual authentication between chip and terminal
- Protection against eavesdropping or manipulation of communication
  - PACE: Password Authenticated Connection Establishment
  - establishment of shared secret by EC-DH via PIN, CAN or MRZ
  - establishment of a symmetric encrypted channel using AES
- Protection against unauthorized access to stored data
  - Access Rights are granted by Federal Office of Administration (BVA)
  - fine granular access rights to dedicated data groups and applications
  - can be further limited by the citizen upon each access
- Assurance of Authenticity of the service provider
  - Short lived certificate
  - Authentication Certificate is provided to the eID Card
  - Contains terminal‘s access rights
- Data avoidance and data economy

- **stolen ID cards can be revoked temporarily or permanently**
  - certificates are revoked automatically
  - certificates expire along with ID card

- **the card's authenticity and the citizen's identity are checked before generating the certificate**

- **using one single eID session for**
  - key generation
  - export of signature verification key
  - certificate generation and storage on card

  → **ensures a strong binding between *certificate*, *public key* and *ID card***

- **Signing Key Pair Algorithm: ECDSA with Brainpool P256r1 curve**

- **System is currently in pilot phase**
- **Operational phase starting 2014**

- **Currently in development: signature portal for**
  - Post-issuance certification
  - quick and easy signing of electronic documents
  - workflow easily integrable for companies (very little development required)

Thank You → Live-Demo

Marcel Selhorst
Software Architect

Bundesdruckerei GmbH

Telefon: +49 30 2598 3243
E-Mail: marcel.selhorst@bdr.de