Selected Topics IT-Security 1 (E-Government)

Austrian E-Government Infrastructure

kevin.theuermann@egiz.gv.at
Kevin Theuermann

Graz, 20.11.2019

Citizen Card Concept

Personal Identifiers

Infrastructure

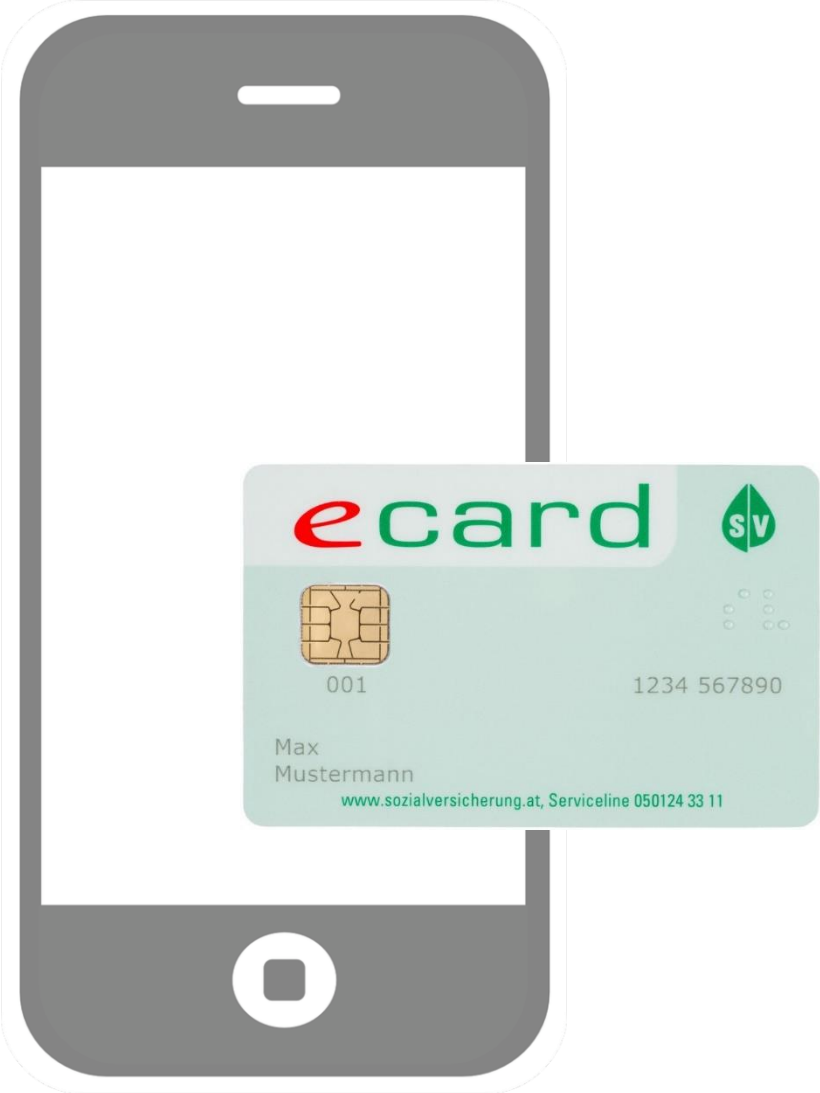
Registers

Electronic Record (ELAK)

Photo by: Michael Hull

CITIZEN CARD Concept

… there was a card-based solution.



CITIZEN CARD

denotes a

CONCEPT

not a technology

Citizen Card is used for…

1.

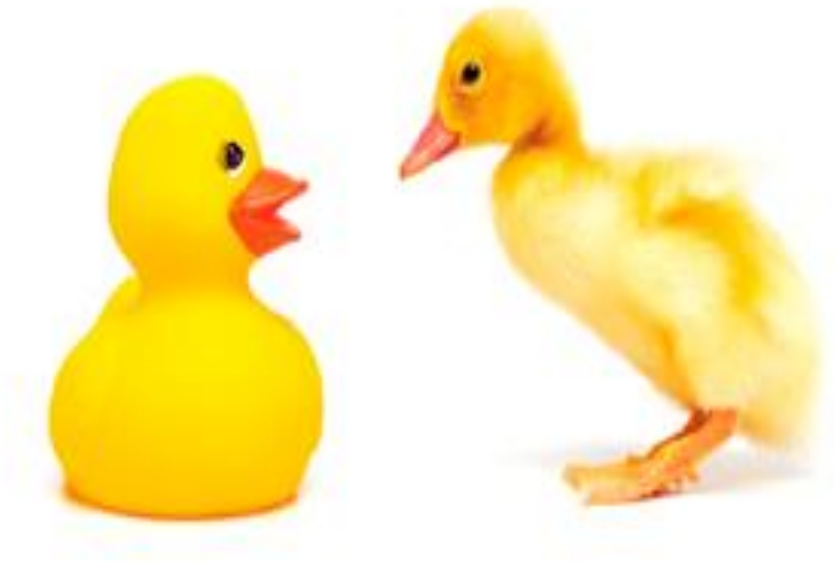
proving unique

IDENTITY

Citizen Card is used for…

2.

…and Authenticity



For instance for **signing** Documents **electronically**

CITIZEN CARD

may be implemented

Using a **smart card** or

other technology like

the **mobile phone**

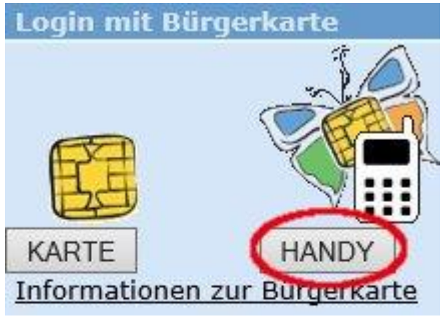
Signature.

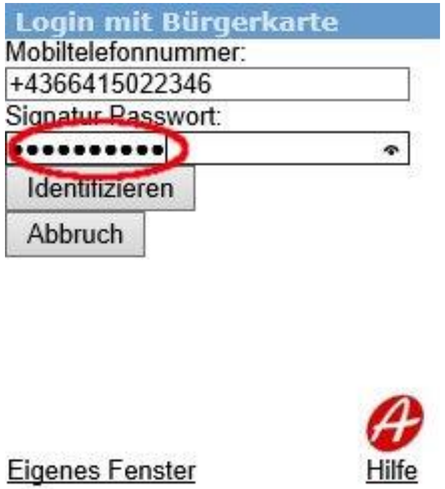
Electronic
Identity document

Signature
on the Internet

CITIZEN CARD

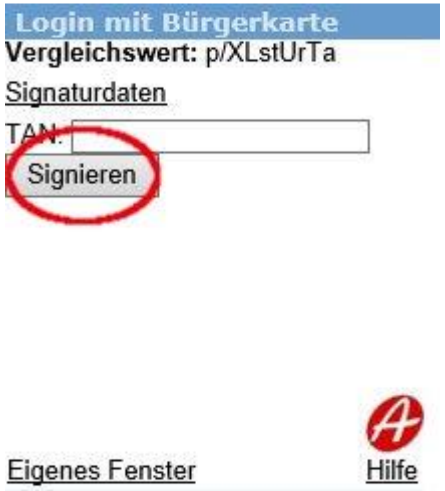
Mobile Phone Signature


Login mit Bürgerkarte


Login mit Bürgerkarte

Mobiltelefonnummer: +4366415022346

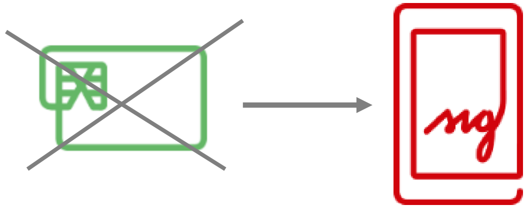
Signatur Passwort: ••••••••••


Login mit Bürgerkarte

Vergleichswert: p/XLstUrTa

Signaturdaten

TAN:



What is stored on the citizen card?

1. **Electronic Certificate**

2. Person Identity Link:

- First name
- Surname
- Date of birth
- sourcePIN

Person Identity Link

An integral part of the **Citizen Card Concept.**

http://www.buergerkarte.at/konzept/personenbindung/spezifikation/20050214/Index.en.html

Identity Link
example

sourcePIN

Personal data
(name, birthday)

Public key
(from qualified certificate)

Signature from the SRA

```
...
<saml:SubjectConfirmationData>
  <pr:Person xsi:type="pr:Physical
      <pr:Identification>
      <pr:Value>123456789012 </pr:V
<pr:Type>http://reference.e-g
    </pr:Identification>
  <pr:Name>
    <pr:GivenName>Max</pr:GivenName>
    <pr:FamilyName>Mustermann</pr:FamilyName>
  </pr:Name>
...
<saml:Attribute
AttributeName="CitizenPublicKey"
... <dsig:RSAKeyValue>
<dsig:Modulus>snW8OLCQ49qNefems
...
<dsig:Siganture>
...
```

https://www.buergerkarte.at/konzept/personenbindung/
spezifikation/20050214/Personenbindung-20050214.en.pdf

Foto by: Thomas Martinsen

Citizen Card Concept

Personal Identifiers

Infrastructure

Registers

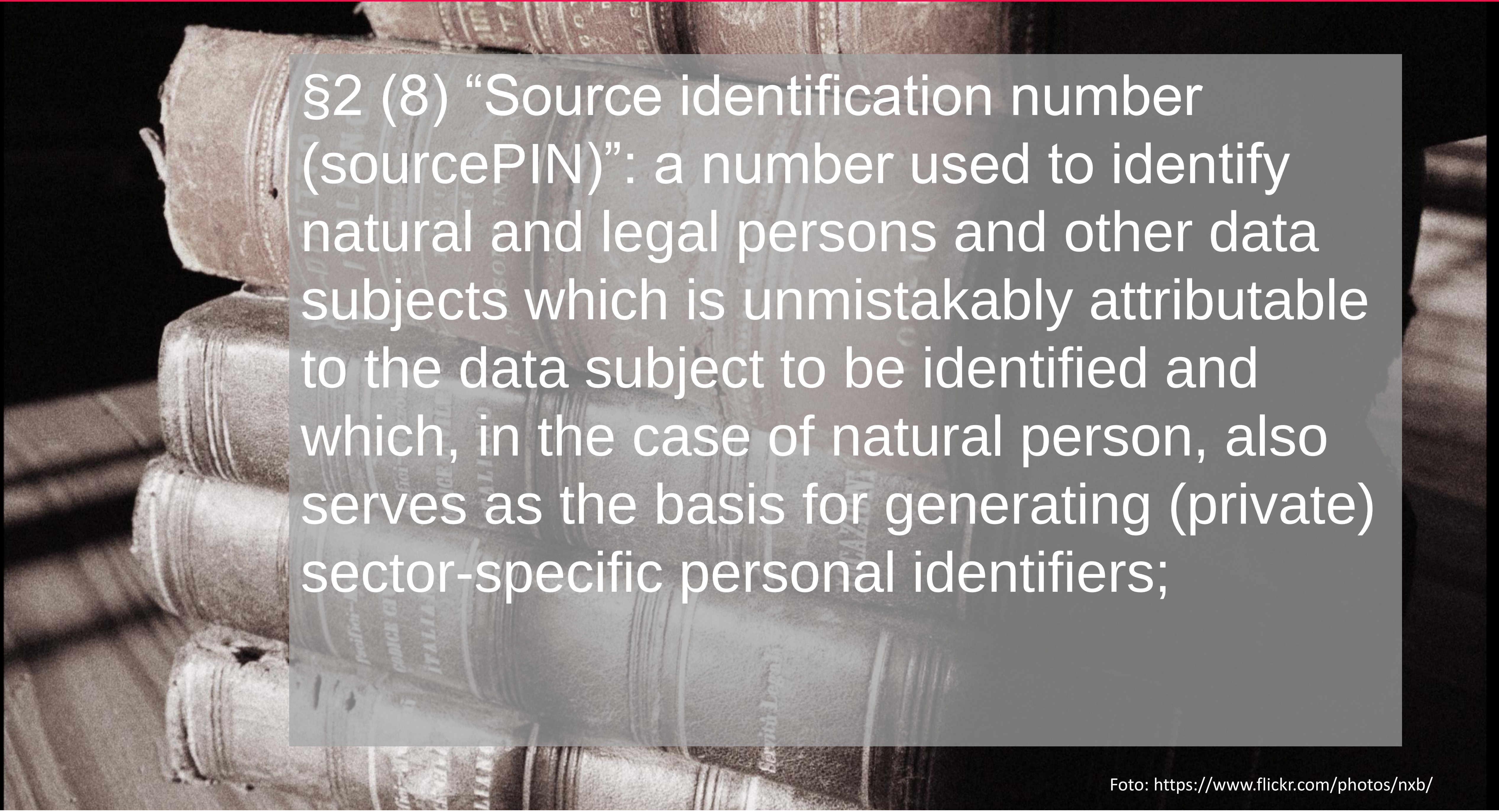
Electronic Record (ELAK)

Photo by: Michael Hull

source personal Identifier

(sourcePIN)

Qq03dPrgcHsx3G0lKSH6SQ==



§2 (8) “Source identification number (sourcePIN)”: a number used to identify natural and legal persons and other data subjects which is unmistakably attributable to the data subject to be identified and which, in the case of natural person, also serves as the basis for generating (private) sector-specific personal identifiers;

Foto: https://www.flickr.com/photos/nxb/

sourcePIN

Algorithm

1. Base number (12 decimals) (BN)

2. Convert to hexadecimal representation (5 bytes)

3. Expand the calculation basis to 128 bit (16 byte) using the format:
   BN|Seed|BN|BN
   Seed is a secret, constant, 8-bit value which is only known to the SRA

4. This value is encrypted using Triple-DES.
   The secret key is only known to the SRA.

5. The result is encoded as BASE64

sourcePIN calculation example

Base number: 000247681888
(E.g.: CRR-number, 12 decimals)

Hexadecimal representation: 00 0E C3 53 60
(5 Byte, hexadecimal representation)

Expand to 128 bit: 00 0E C3 53 60 FF 00 0E C3 53 60 00 0E C3 53 60
(16 Byte, Seed value set to e.g. 0xFF)

Triple-DES encryption, hexadecimal:
42 AD 37 74 FA E0 70 7B 31 DC 6D 25 29 21 FA 49 (16 Byte)

Source PIN, BASE64: Qq03dPrgcHsx3G0lKSH6SQ== (24 digits)

sourcePIN
usage

sourcePIN stored

on the Citizen Card

may be read by an agency but

only for the calculation

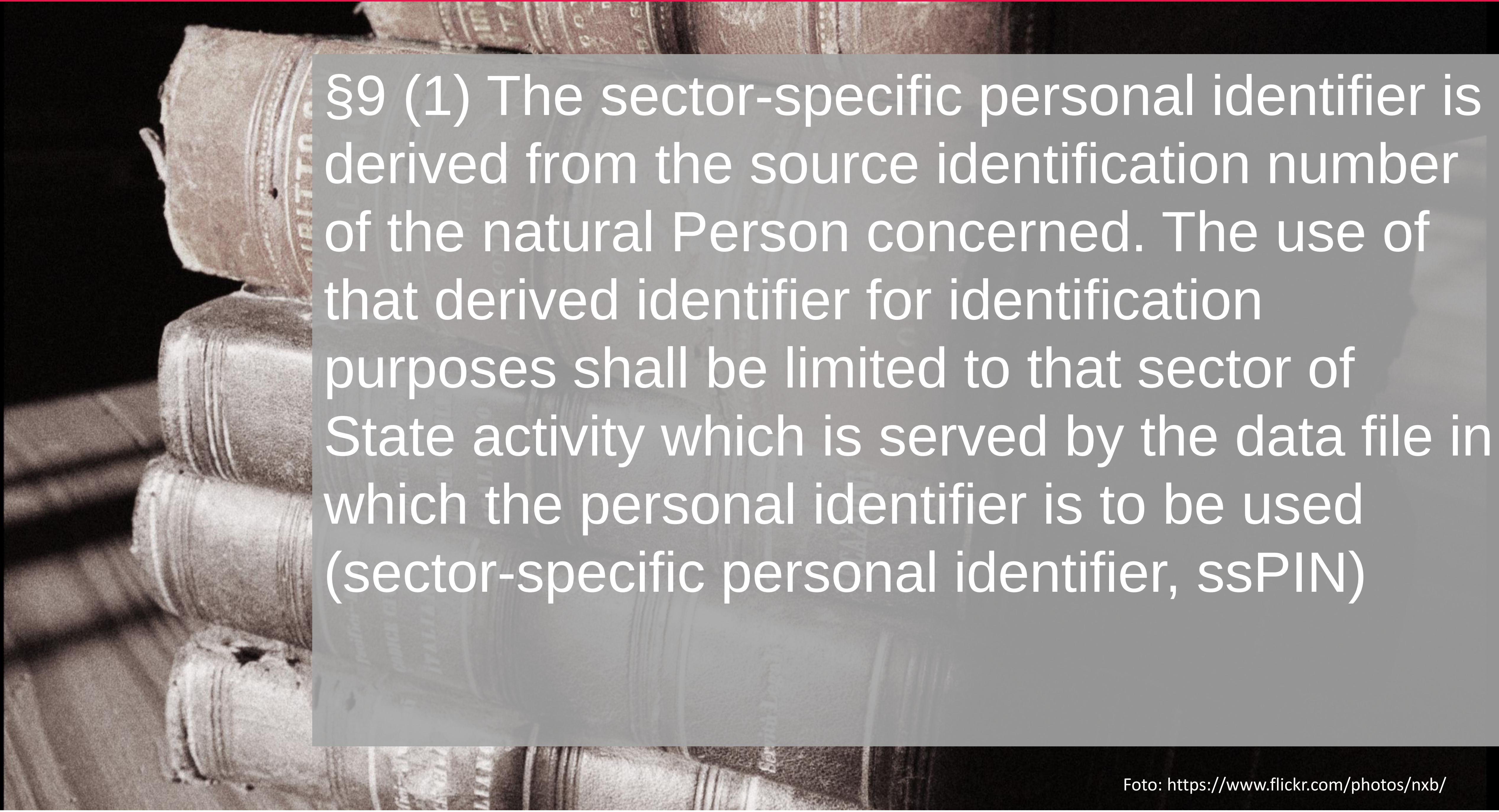
of the sector specific personal identifier (ssPIN)

NO STORAGE! (§ 12 EGovG)

sector-specific Personal Identifier

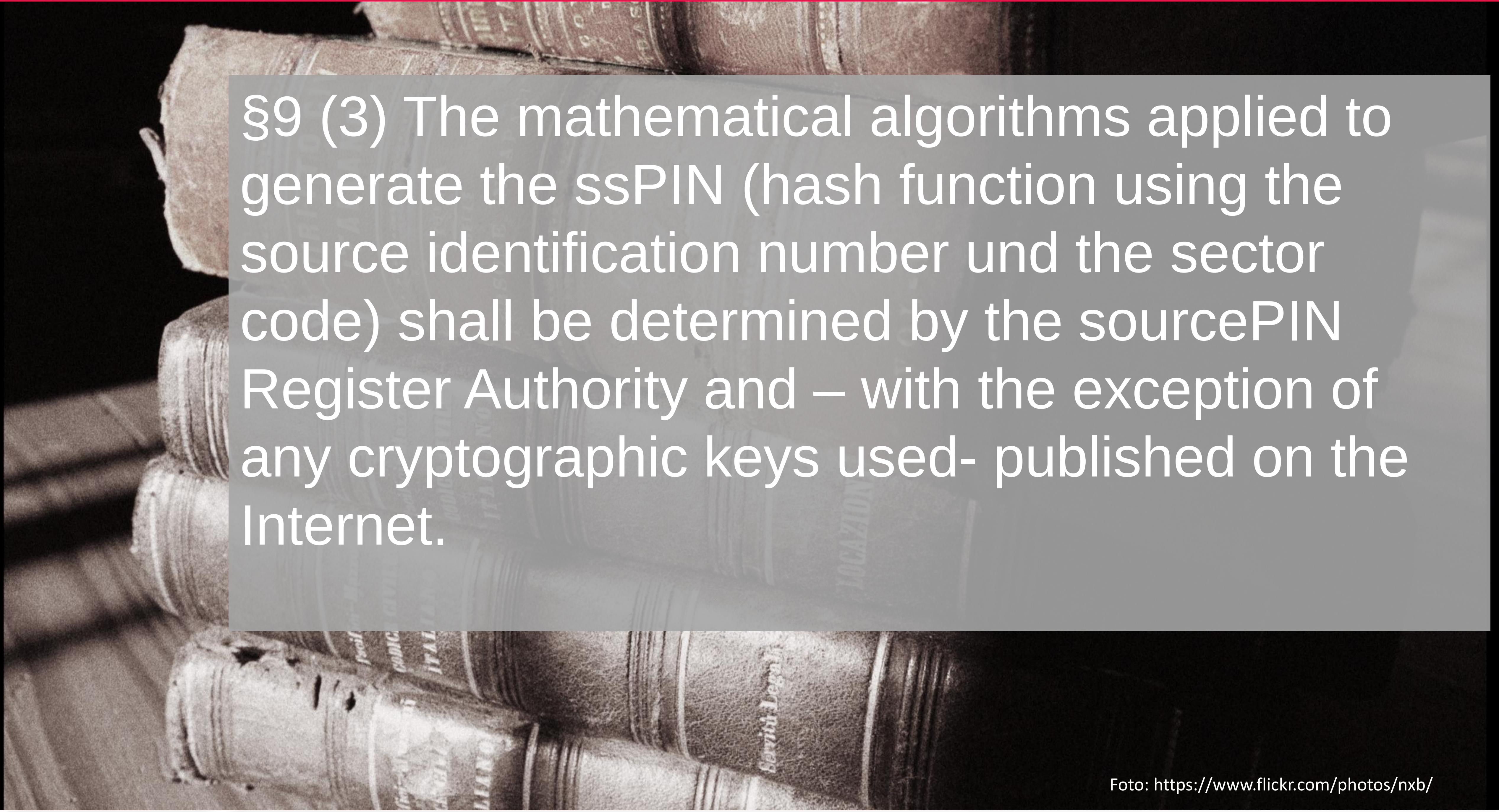
(ssPIN)

j/NxdRQhp+tNyE9WhHdBSYuy3hA=



§9 (1) The sector-specific personal identifier is derived from the source identification number of the natural Person concerned. The use of that derived identifier for identification purposes shall be limited to that sector of State activity which is served by the data file in which the personal identifier is to be used (sector-specific personal identifier, ssPIN)

Foto: https://www.flickr.com/photos/nxb/



§9 (3) The mathematical algorithms applied to generate the ssPIN (hash function using the source identification number und the sector code) shall be determined by the sourcePIN Register Authority and – with the exception of any cryptographic keys used- published on the Internet.

Foto: https://www.flickr.com/photos/nxb/

ssPIN

Algorithm

1. Starting point

   sourcePIN, base64 encoded

   Sector code:

   character string representing the sector according to the "Bereichsabgrenzungsverordnung" of the federal chancellery of Austria

2. Build the string: sourcePIN | '+' | URN-prefix[1] and the sector code.

[1] URN-Prefix := "urn:publicid:gv.at:cdid+"

ssPIN

Algorithm

3. Calculate the SHA-1 hash value

4. The resulting 160 bit number may be used for calculations within the application. If the number is needed in written form or forwarded via the Internet it has to be base64 encoded.

ssPIN

calculation

example

sourcePIN, Base64

Qq03dPrgcHsx3G0lKSH6SQ== (24 chars)

Sector code

BW (ISO-8859-1, E.g.: Bauen und Wohnen)

Input data for hash value calculation

Qq03dPrgcHsx3G0lKSH6SQ==+urn:publicid:gv.at:cdid+BW

Hash value

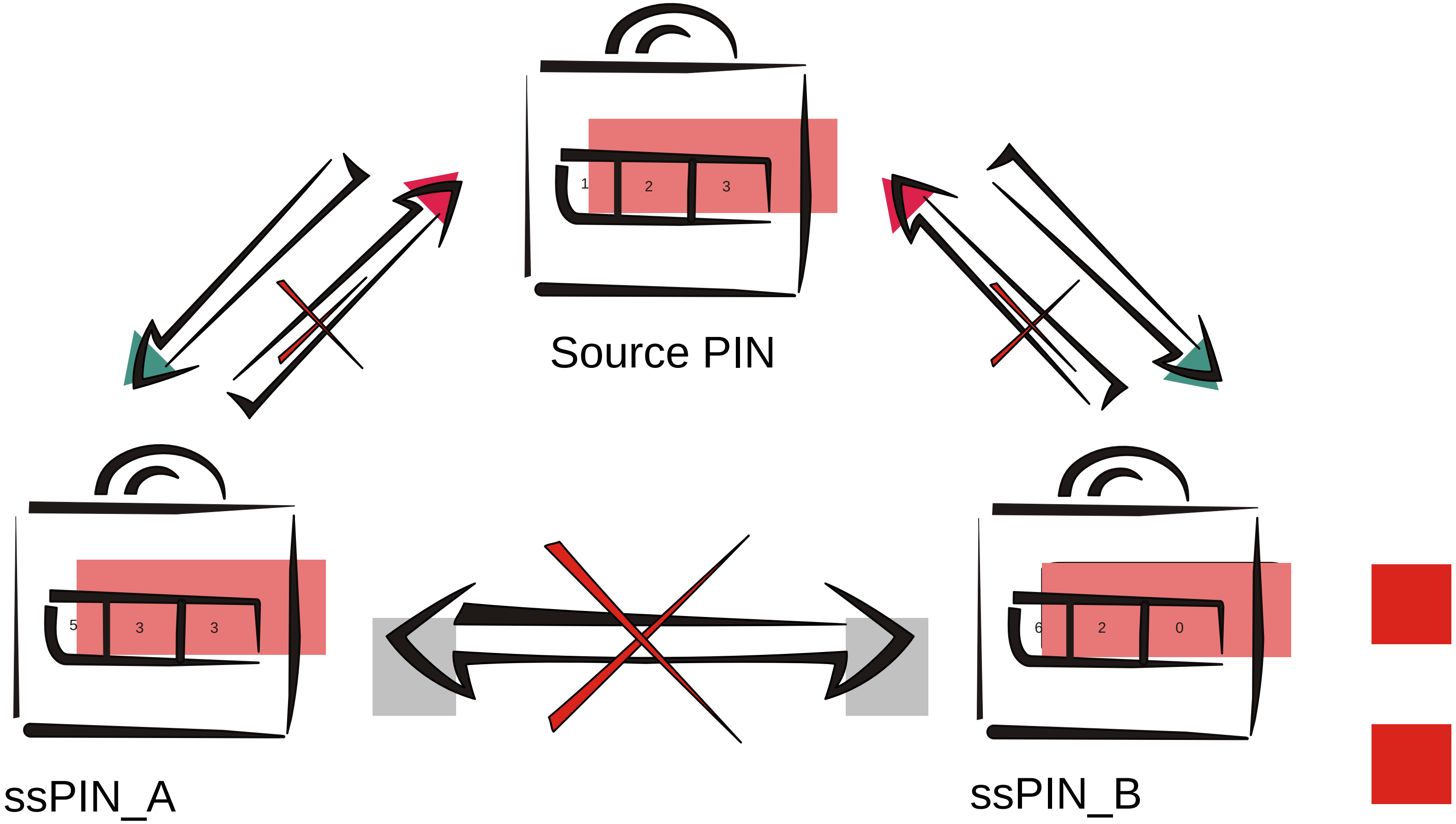
8FF3717514 21A7EB4DC8 4F56847741 498BB2DE10

(5 x 32bit; hexadecimal representation)

ssPIN, Base64

j/NxdRQhp+tNyE9WhHdBSYuy3hA= (28 chars)

ssPIN
generation



Not Invertible!

Can we use the

Citizen Card

Functions

for the

Private Sector?

Yes!

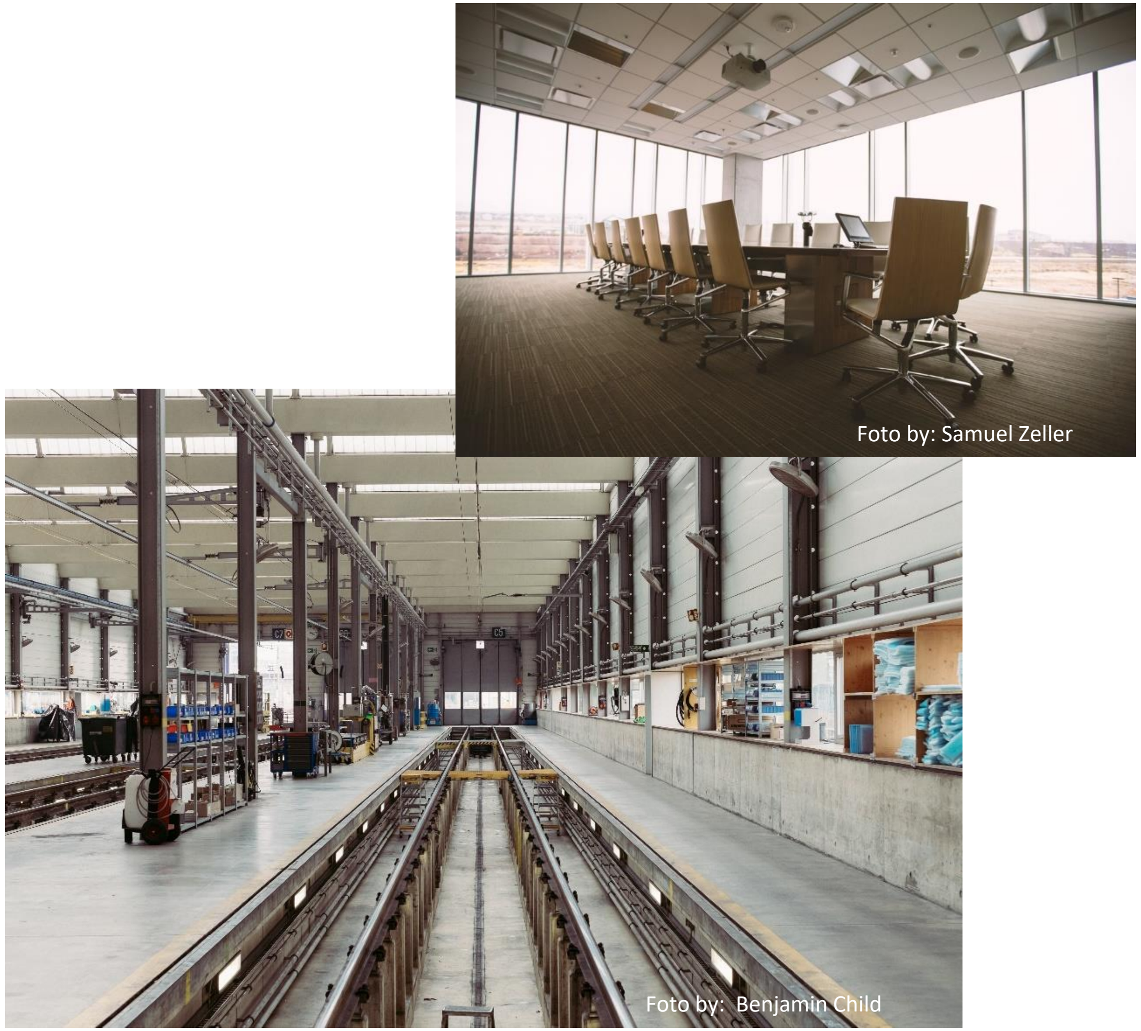


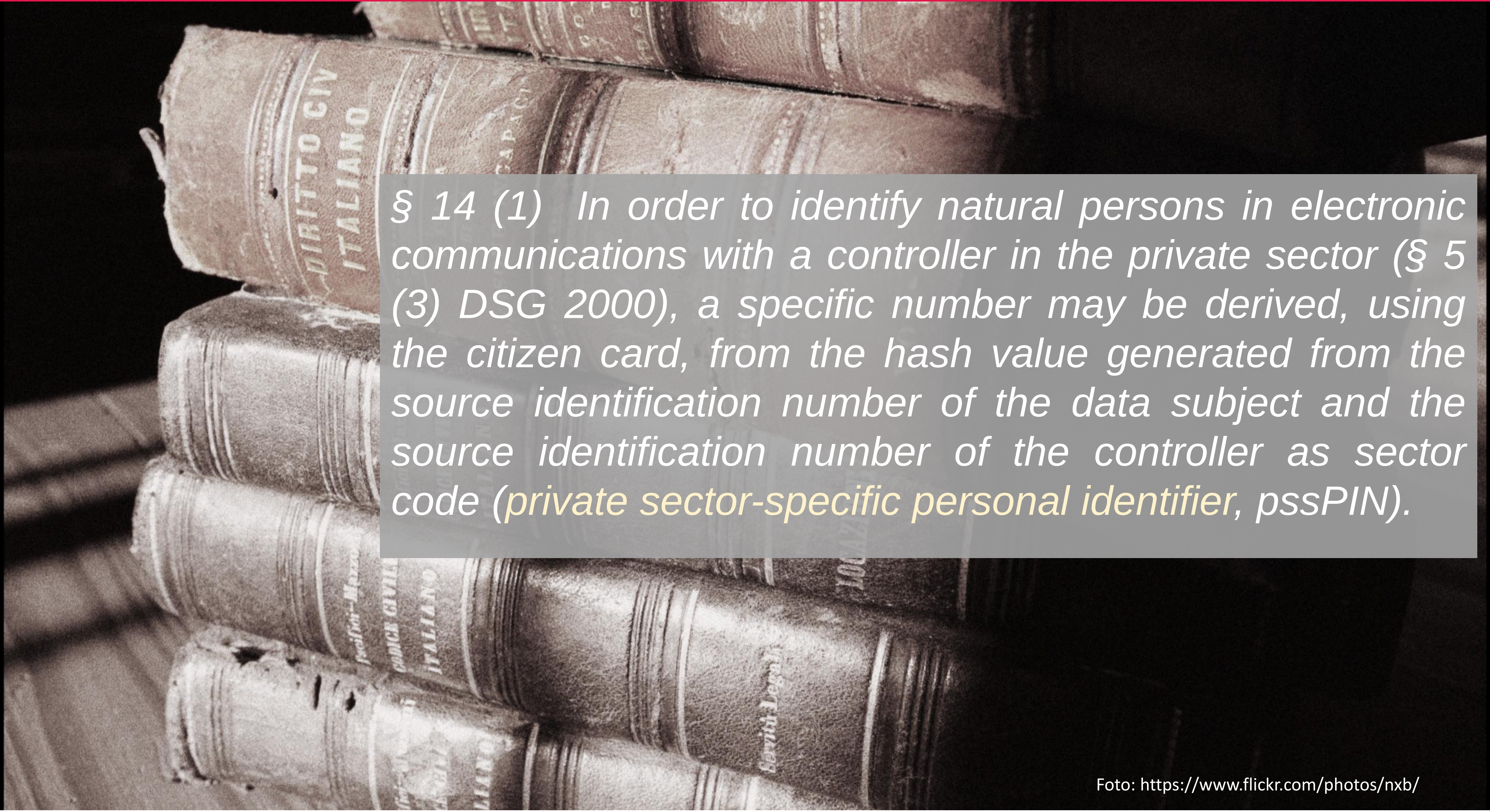
Foto by: Samuel Zeller

Foto by: Benjamin Child

private sector-specific Personal Identifier

(pssPIN)

Q7hIWrVqP+VZRiTilm3+mioIK5w=



§ 14 (1) In order to identify natural persons in electronic communications with a controller in the private sector (§ 5 (3) DSG 2000), a specific number may be derived, using the citizen card, from the hash value generated from the source identification number of the data subject and the source identification number of the controller as sector code (private sector-specific personal identifier, pssPIN).

Foto: https://www.flickr.com/photos/nxb/

pssPIN Algorithm

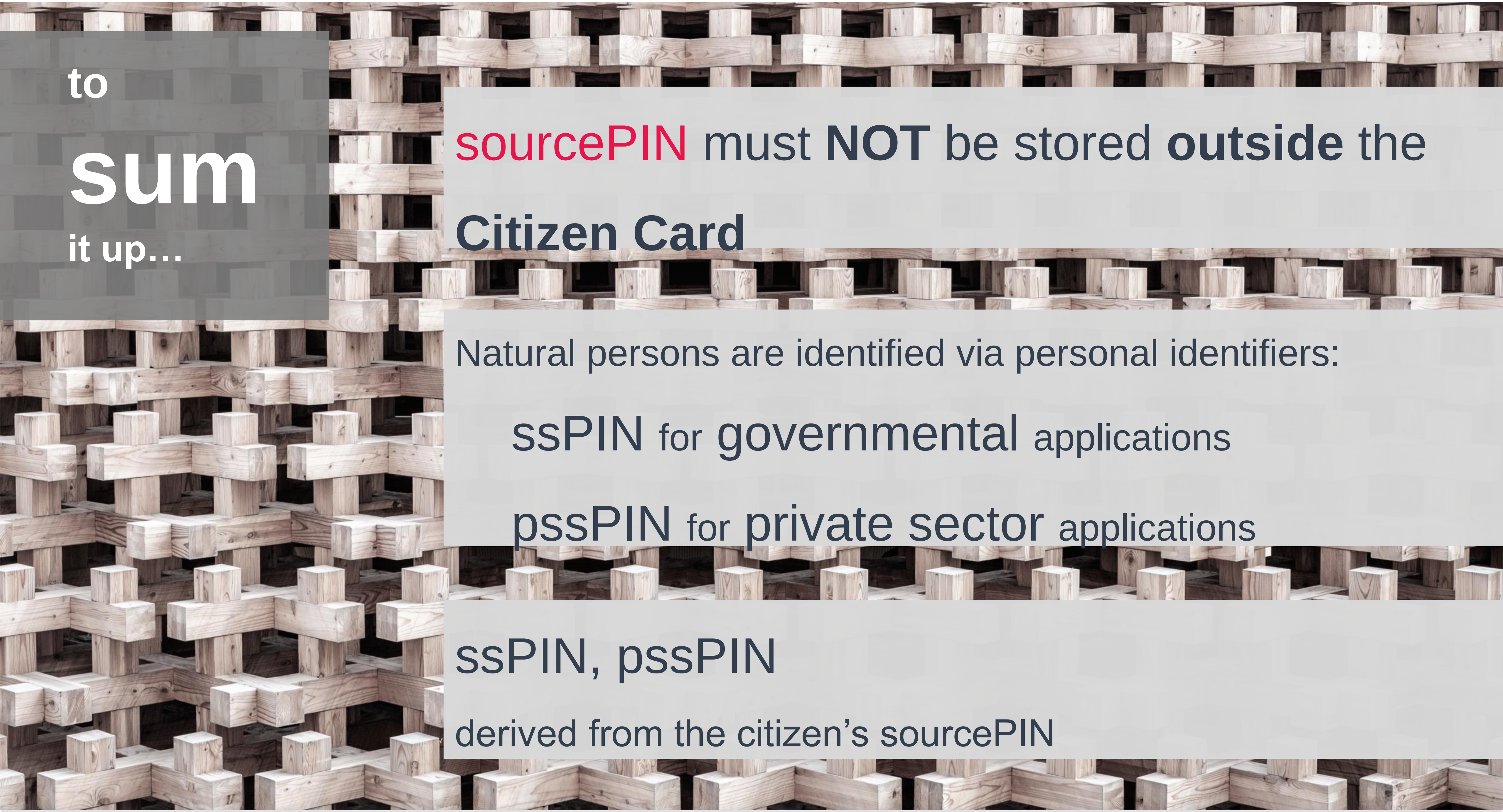
1. Base data:

    sourcePIN of the natural person, base64 encoded
    sourcePIN of the initiator (Auftraggeber) as sector code

2. Building the character string as concatenation of the natural person’s sourcePIN | ‘+’ | URN-prefix and the sourcePIN of the initiator.

    URN-prefix := "urn:publicid:gv.at:wbpk+XXX+“ where ‘XXX’ will result in the following values, if the sourcePIN of the initiator is:
    a companies register number: ‘FN’
    a associations register number (Vereinsregisternummer): ‘VR’
    a number within the supplementary register (Ergänzungsregister) for natural persons: ‘ERJ’
    a sourcePIN belonging to a natural, reportable person: ‘CPR’
    a sourcePIN belonging to a natural person that is registered within the supplementary register: ‘ERN’

Step 3 and 4 same as for ssPIN



to **sum** it up…

sourcePIN must **NOT** be stored **outside** the **Citizen Card**

Natural persons are identified via personal identifiers:

- ssPIN for governmental applications
- pssPIN for private sector applications

ssPIN, pssPIN

derived from the citizen’s sourcePIN

Citizen Card Concept

Personal Identifiers

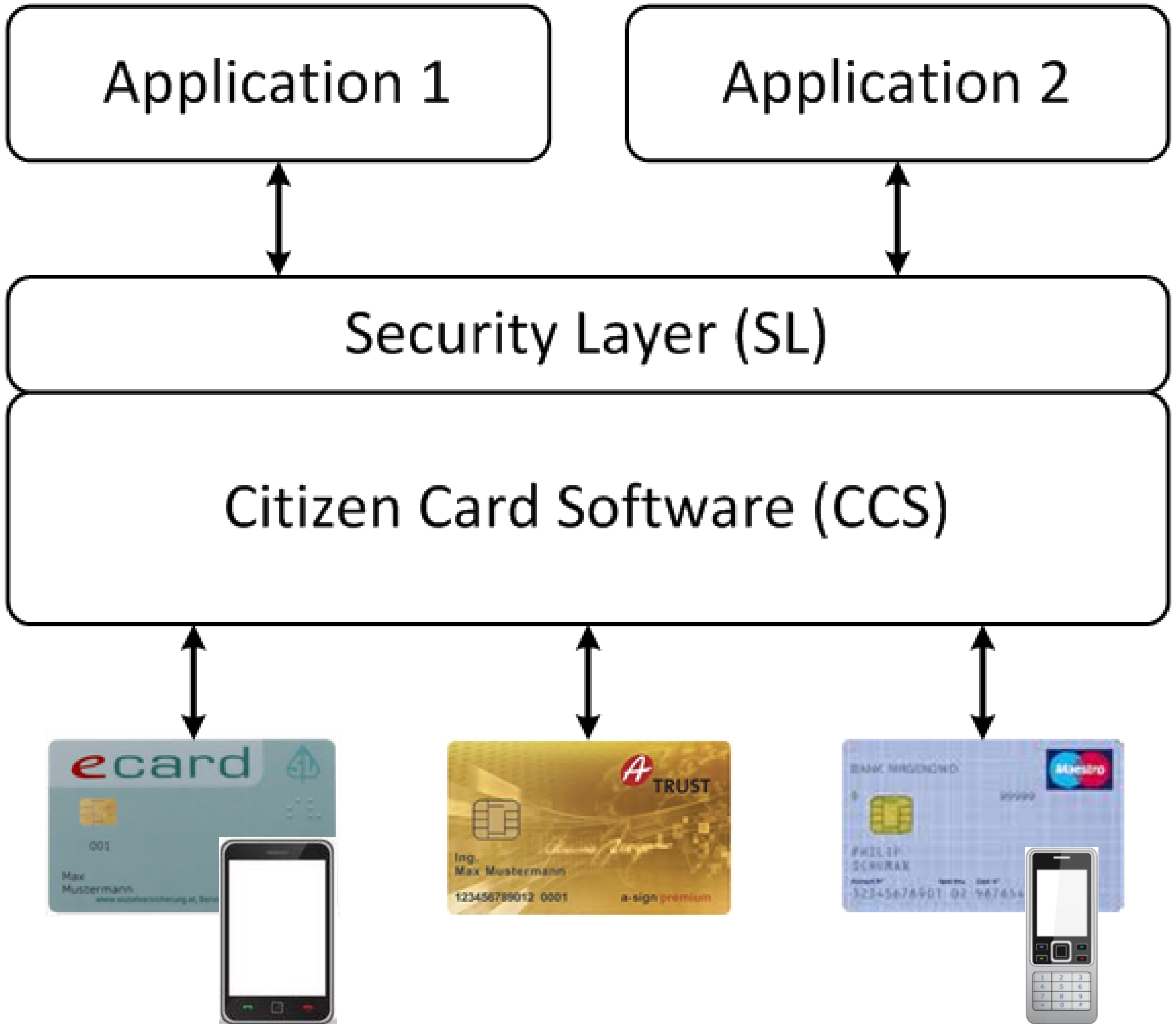
Infrastructure

Registers

Electronic Record (ELAK)

Photo by: Michael Hull

Citizen Card
Infrastructure



Infrastructure | Security Layer (1)

- Represents the interface to
  - Communicate with the Citizen Card and applications
  - Use the Citizen Card Concept in a technology-neutral manner
- XML based protocol on application layer
- Transport layers are
  - TCP
  - HTTP
  - HTTPS

Infrastructure | Security Layer (2)

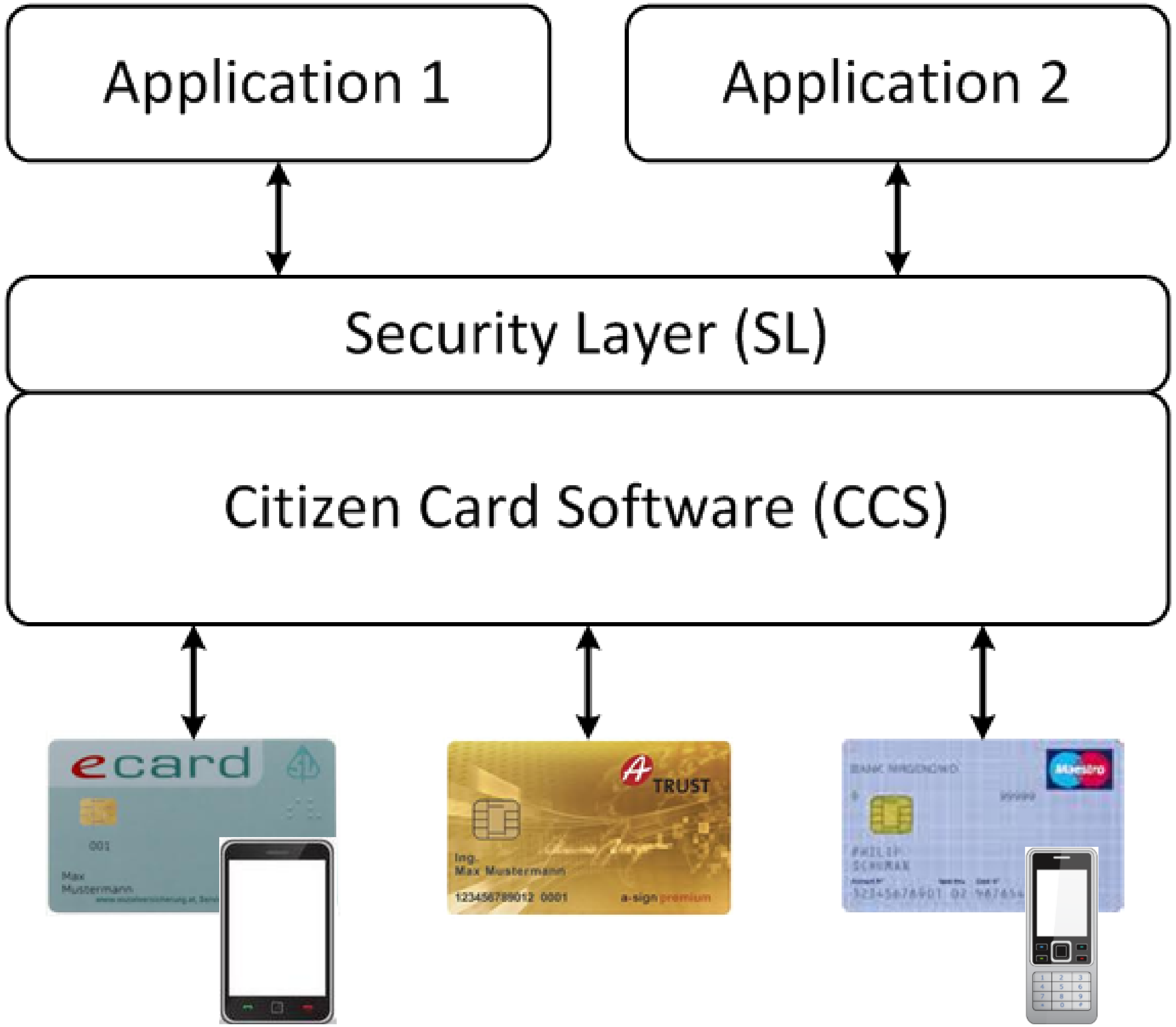
- Provides the possibility to interact with the Citizen Card:
  - XML (XAdES)/CMS (CAdES) signatures
    - Creation
    - Verification
  - Read info boxes (Identity Link, certificates)

https://www.buergerkarte.at/konzept/securitylayer/spezifikation/20140114-en/tutorial/Tutorial.en.html

Foto by: Thomas Martinsen

Citizen Card

Infrastructure



Application 1

Application 2

Security Layer (SL)

Citizen Card Software (CCS)

Smart card Implementation

If smart card implementation is used for the citizen card concept, a middleware for card communication is needed (Citizen Card Environment)

Citizen Card Environment…

Implements SL

Provides the smart card communication
(via PC/SC)

Ensures that the authentication classes are observed

Default display format for signature data

- Requirement for signature creation devices for creating qualified signatures

Local CCE

- CCE is executed on the citizen’s computer
- SL requests are sent to a local endpoint
  - http://127.0.0.1:3495/*
  - https://127.0.0.1:3496/*

Implementations

- MOCCA
- A-Sign Client
- BDC Hotsign
- …

Infrastructure| Mobile Phone Signature

Foto by: Alejandro Escamilla

Mobile Phone Signature

Implements the Citizen Card concept using a mobile TAN or smartphone app

Provided by A-Trust
www.handy-signatur.at

Mobile Phone Signature

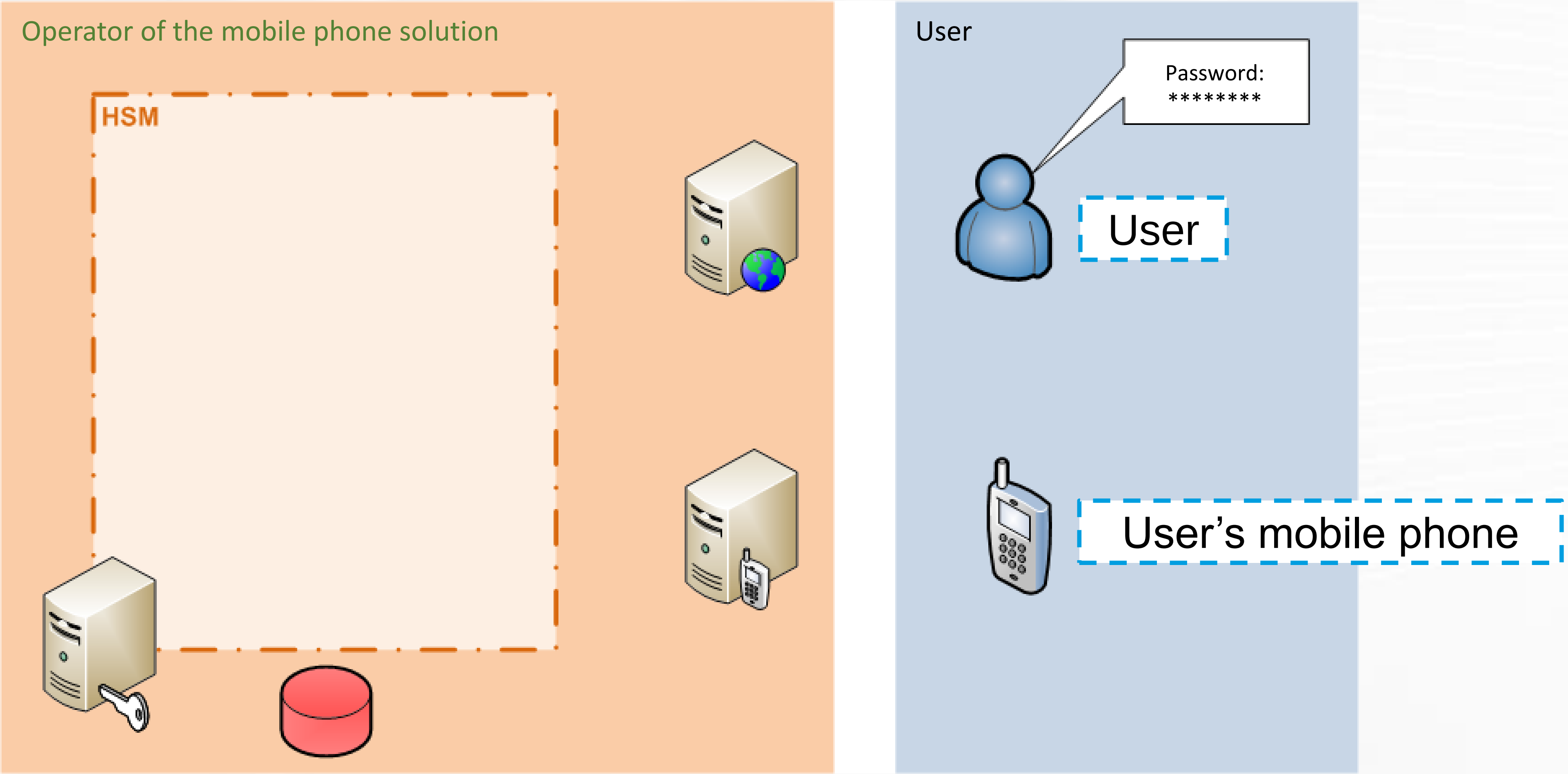
Identity link and asymmetric key are stored by A-TRUST and protected by a hardware security module (HSM)

For the signature creation a TAN is sent to the citizen via SMS or via app

This TAN must be entered during the signature creation process

Alternatively, a QR code is generated and scanned via the smartphone app

Mobile Phone Signature | Components

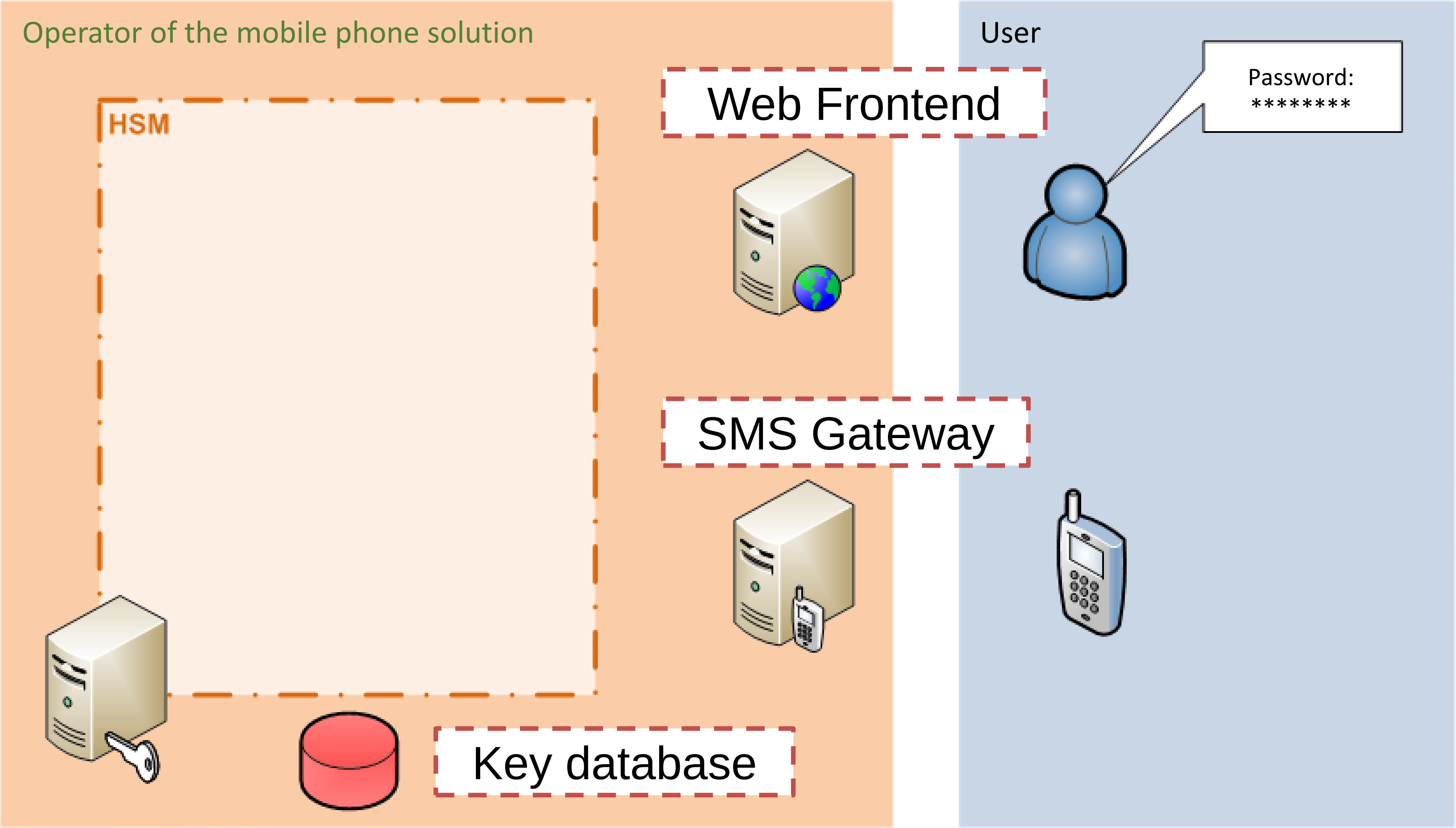


Mobile Phone Signature | Components

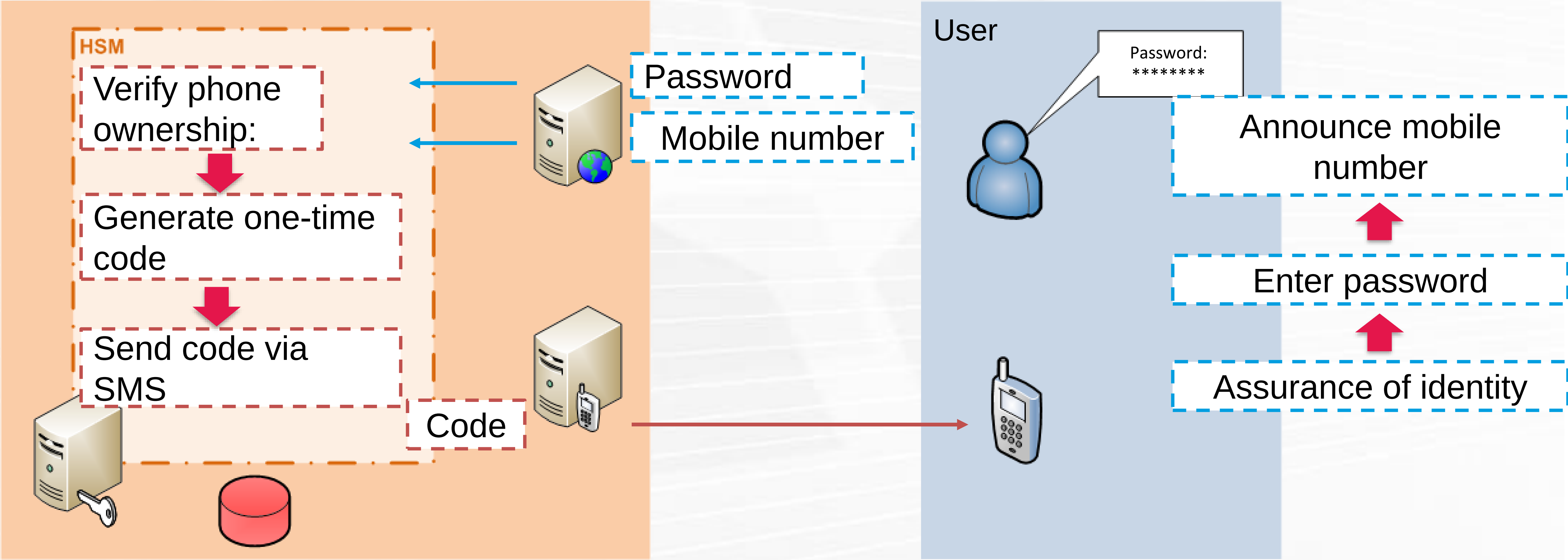
HSM
- Creation of signature creation data
- Decryption of stored signature creation data
- Creation of qualified electronic signatures

Key database

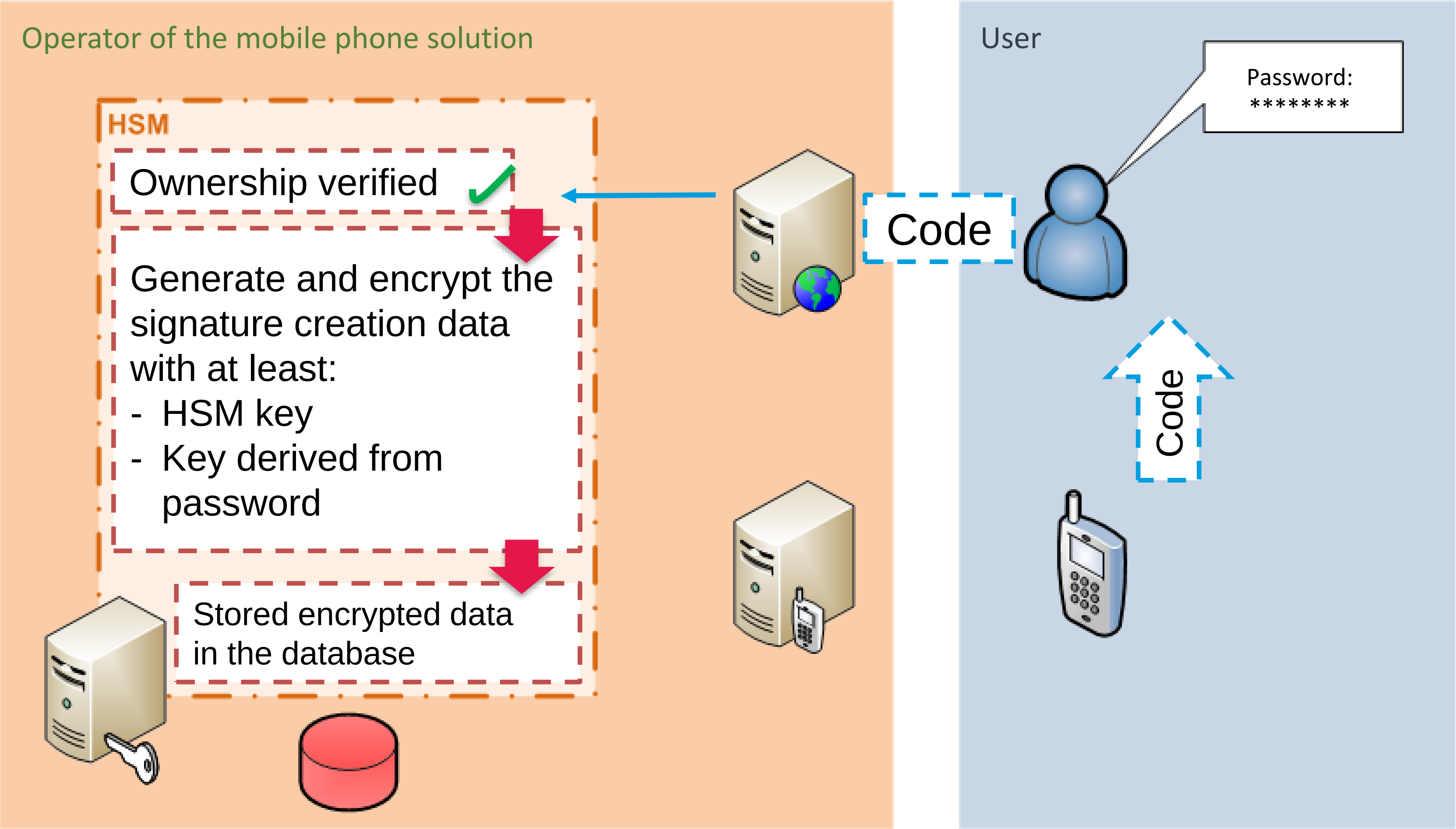
Signature creation data is encrypted using a key consisting of at least:
- Secret password
- Secret HSM key



Registration Process | Step 1 Announce mobile number and pw



Registration Process | Step 2 Ownership vrification



Operator of the mobile phone solution

HSM

Ownership verified ✓

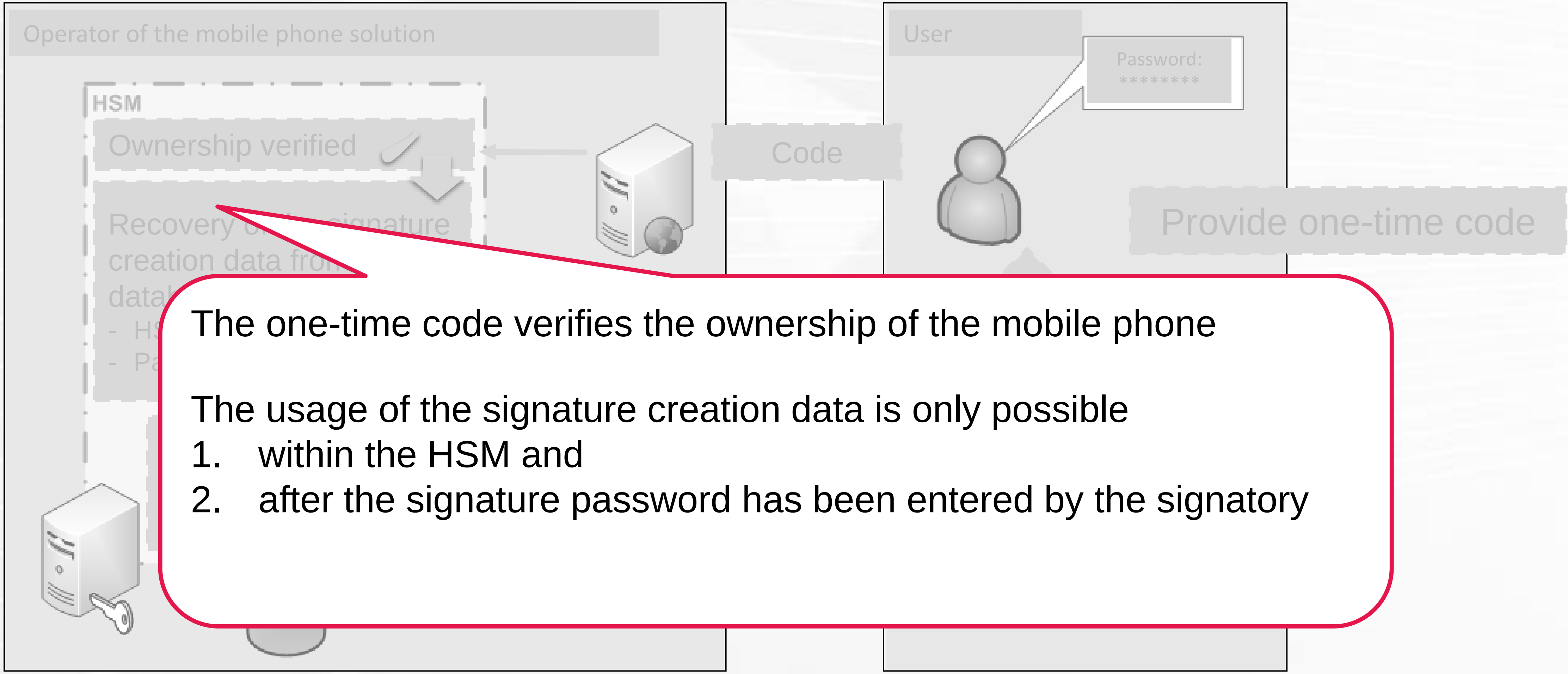
Generate and encrypt the signature creation data with at least:
- HSM key
- Key derived from password

Stored encrypted data in the database

User

Password: ********

Mobile Phone Signature | Signature Process



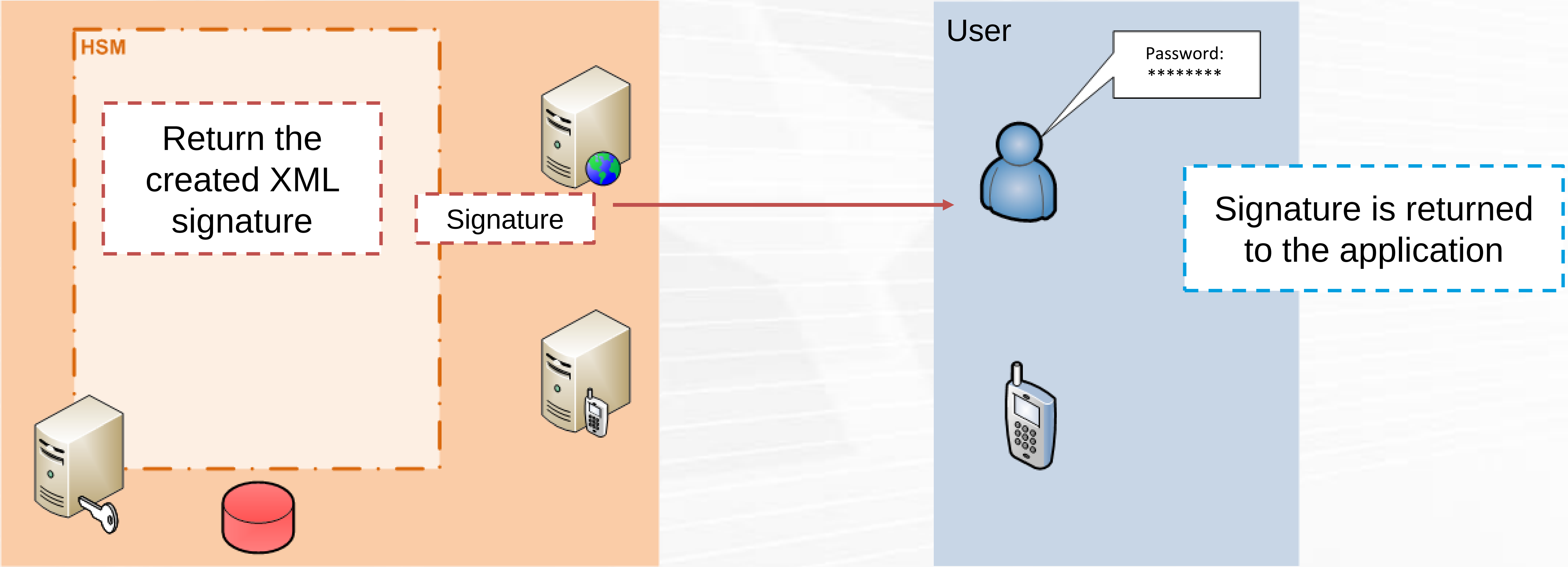
Operator of the mobile phone solution
HSM
Ownership verified
Recovery of the signature creation data from database
- HS
- Pa
Code
User
Password: ********
Provide one-time code

The one-time code verifies the ownership of the mobile phone

The usage of the signature creation data is only possible

1. within the HSM and
2. after the signature password has been entered by the signatory

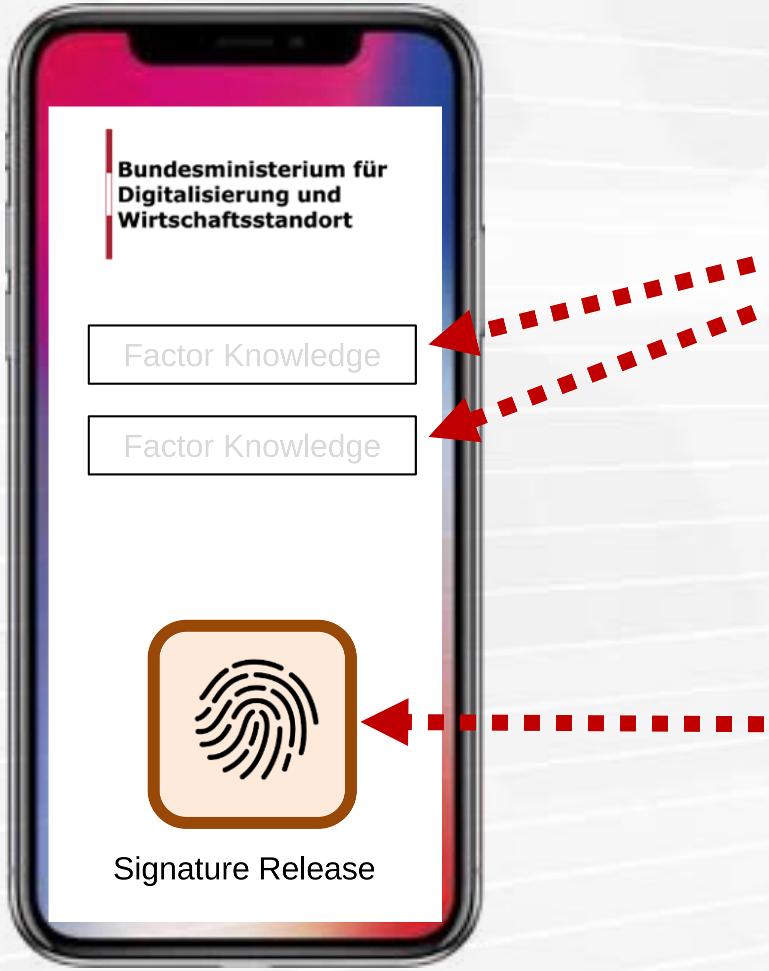
Signature Process | Step 4 Return signed data


HSM
Return the created XML signature
Signature
User
Password: ********
Signature is returned to the application

Infrastructure| Mobile Phone Signature 2.0

Foto by: Alejandro Escamilla

New Mobile Phone Signature



Bundesministerium für Digitalisierung und Wirtschaftsstandort

Factor Knowledge

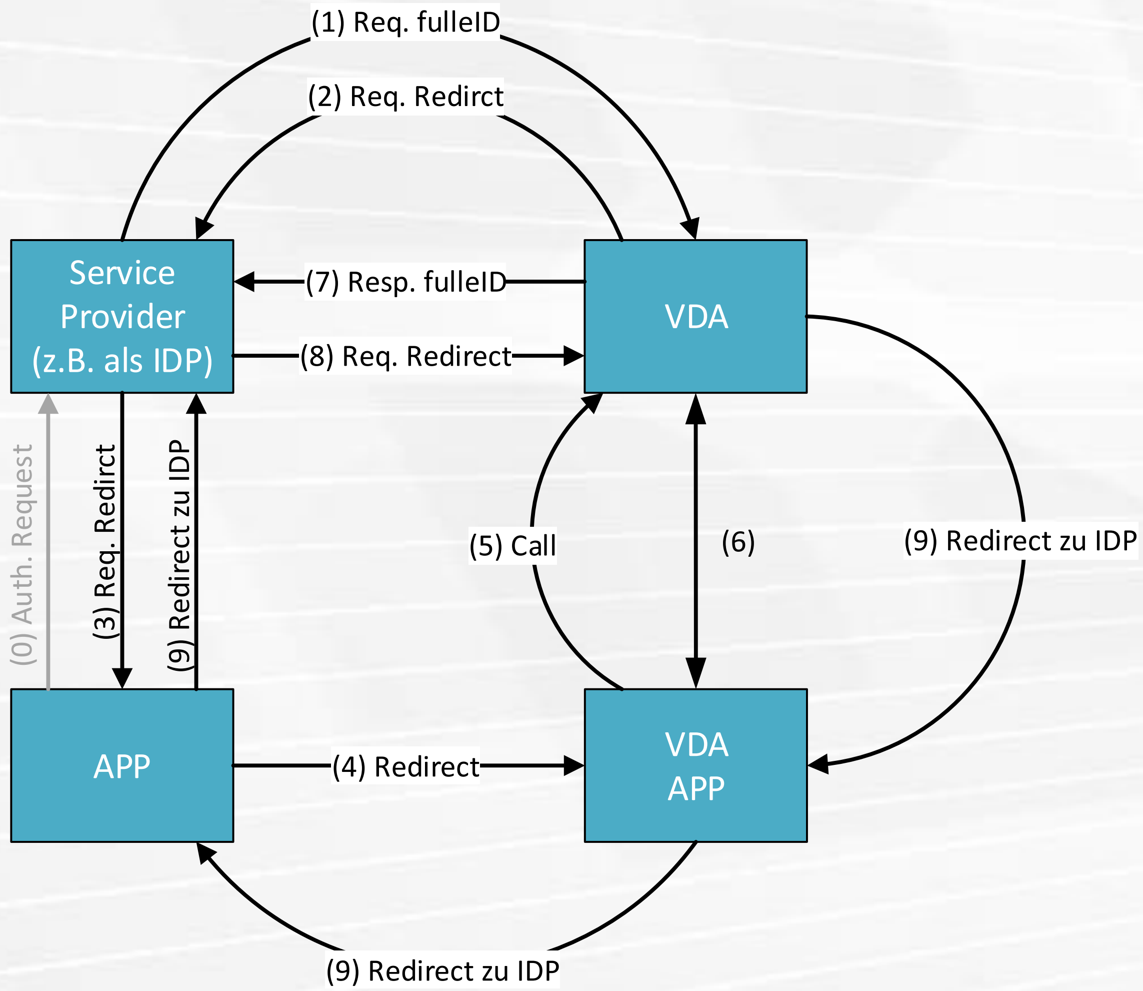
Factor Knowledge

Signature Release

Factor Knowledge: Generic implementation

Factor Possession: Possession of cryptographic key material in Keystore/Keychain, which is protected against unautorized access through a fingerprint

Security Layer 2.0



Adaptation of Security Layer needed

Security Layer 2.0 based on JSON Web Tokens

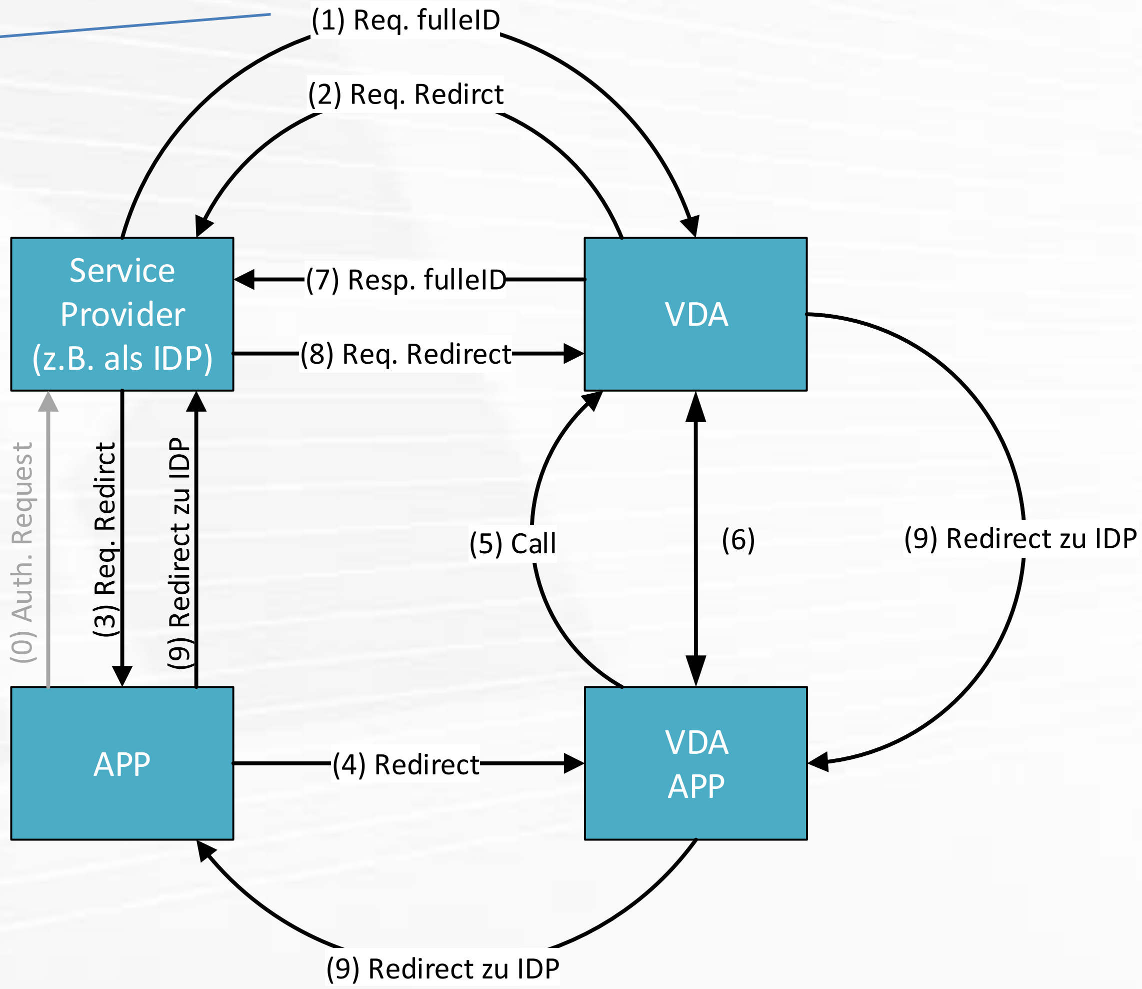
Complex routing of Communication Interfaces

Security Layer 2.0 Request

1) IDP -> VDA: {"v":"10","reqID":"79728758-5d1a-4235-a5b1-ea7192a27e21","signedPayload":"eyJhbGciOiJSUz…. "}

signedPayload = {"alg":"RS256","cty":"application/sl2.0;command", "x5c":"MIIC9zCCAd8CB….}

{"name":"qualifiedeID","params":{"authBlockTemplateID":"authblock_DE","dataUrl":"http://localhost:8080/idp/dataurl","attributes":[{“ServiceProvider":"http://localhost:8080/idp"},{"MANDATE-REFERENCE-VALUE":"da421273-c830-4a3d-a527-324046686d49"}]}}



Communication Interfaces of SL2.0

Application Interface:

The interface with which a service provider communicates with the VDA to use functions provided by the VDA.

Service Provider Interface:

Interface via which an application software communicates with a service provider. This interface MUST be based on http.

Authentication Interface:

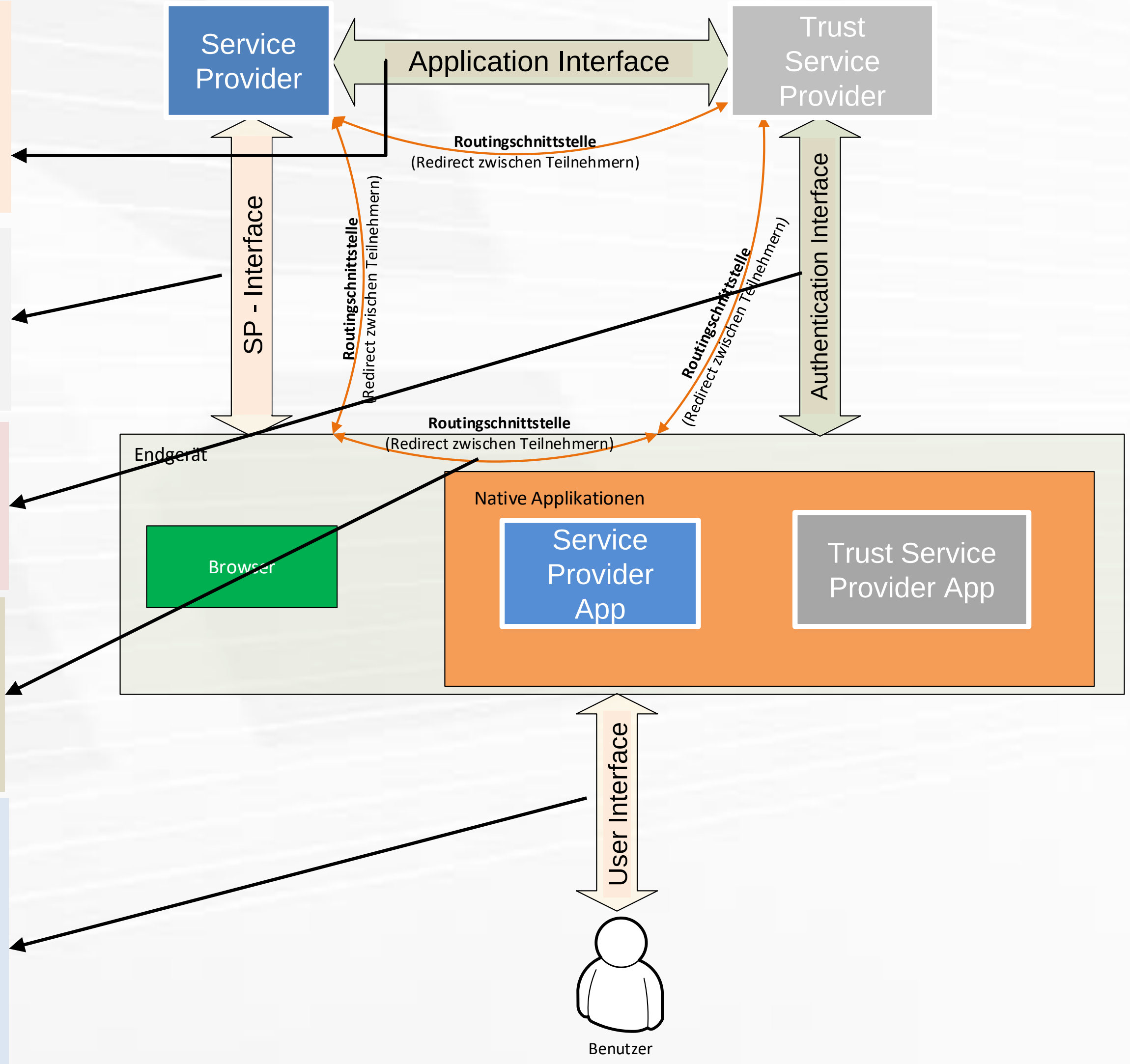
That interface used by the VDA for authenticating a user.

Routing Interface:

Generic interface of the security layer 2.0 system which specifies basic requirements and general functions.

User Interface:

Via this interface, the user interacts with the end device used by him and the application software installed on it in order to use functions of the service provider and to authenticate himself to the VDA.



Citizen Card Concept

Personal Identifiers

Infrastructure

Registers

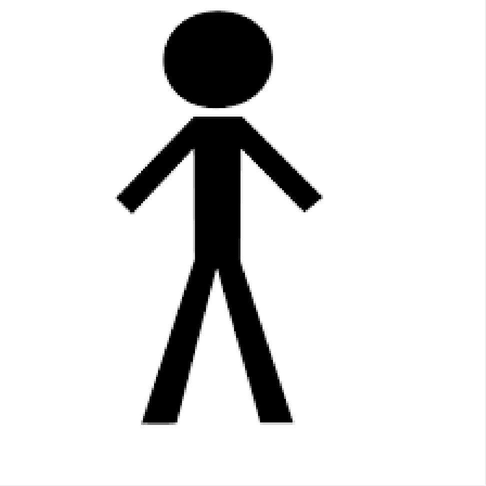
Electronic Record (ELAK)

Photo by: Michael Hull

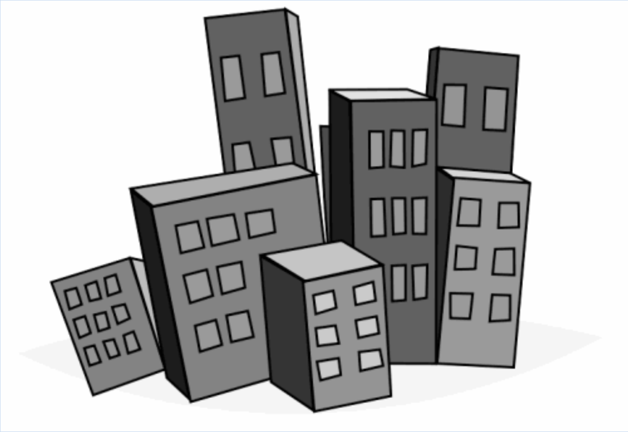
Registers

https://www.flickr.com/photos/kulturarvsprojektet/

Natural Persons

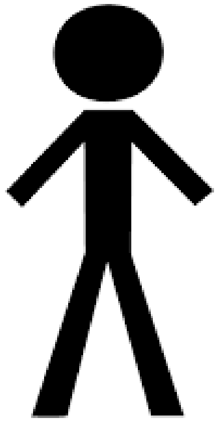


Legal Persons



Person Registers

Natural Persons



Central population register (CPR)

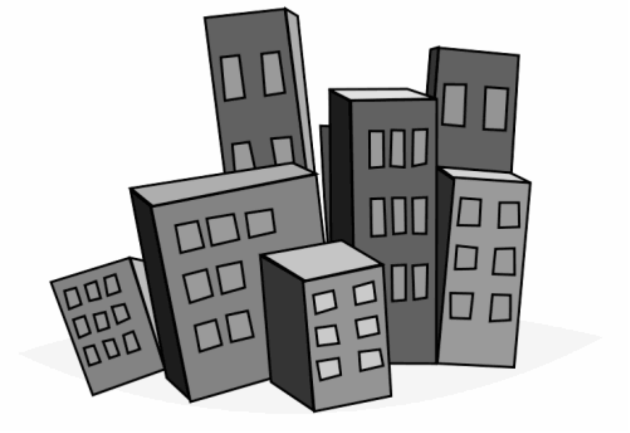
Supplementary register for natural persons (SRnP)
(Persons concerned that are not recorded in the CPR)

overview registers for natural persons

Name	Competence	Amount
Central Population Register (CPR)	BM.I	8,4 Mio
Supplementary Register for natural Persons (ERnP)	DSK	12.000
Source PIN Register	BM.I	
Central Register for Weapons (ZWR)	Weapons Office	230.000
Criminal Record Register	BPD Wien	206.000
Register of births, marriages and deaths - Zentrales Personenstandsregister (ZPR)	BM.I	

Not natural persons („companies“)

Legal Persons



Companies register (FB)

Register of associations (ZVR)

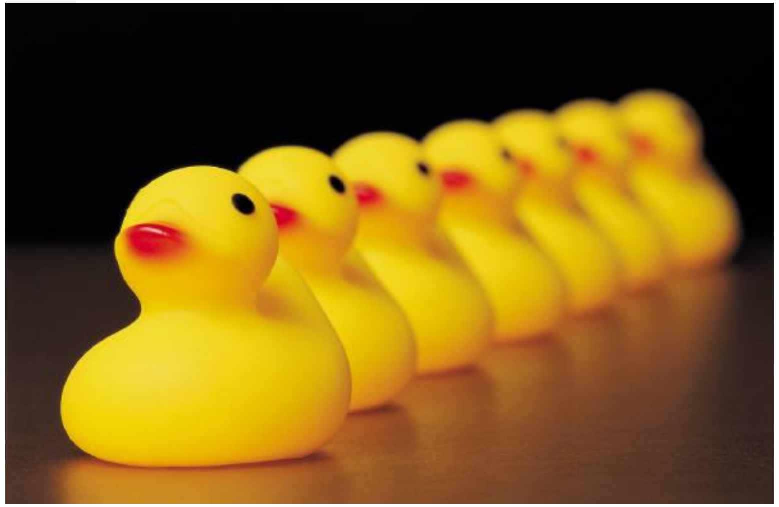
Supplementary register for other persons concerned (ERsB)
Persons concerned that don’t have to be listed within the FB or ZVR
(e.g. University)

overview registers for
legal persons

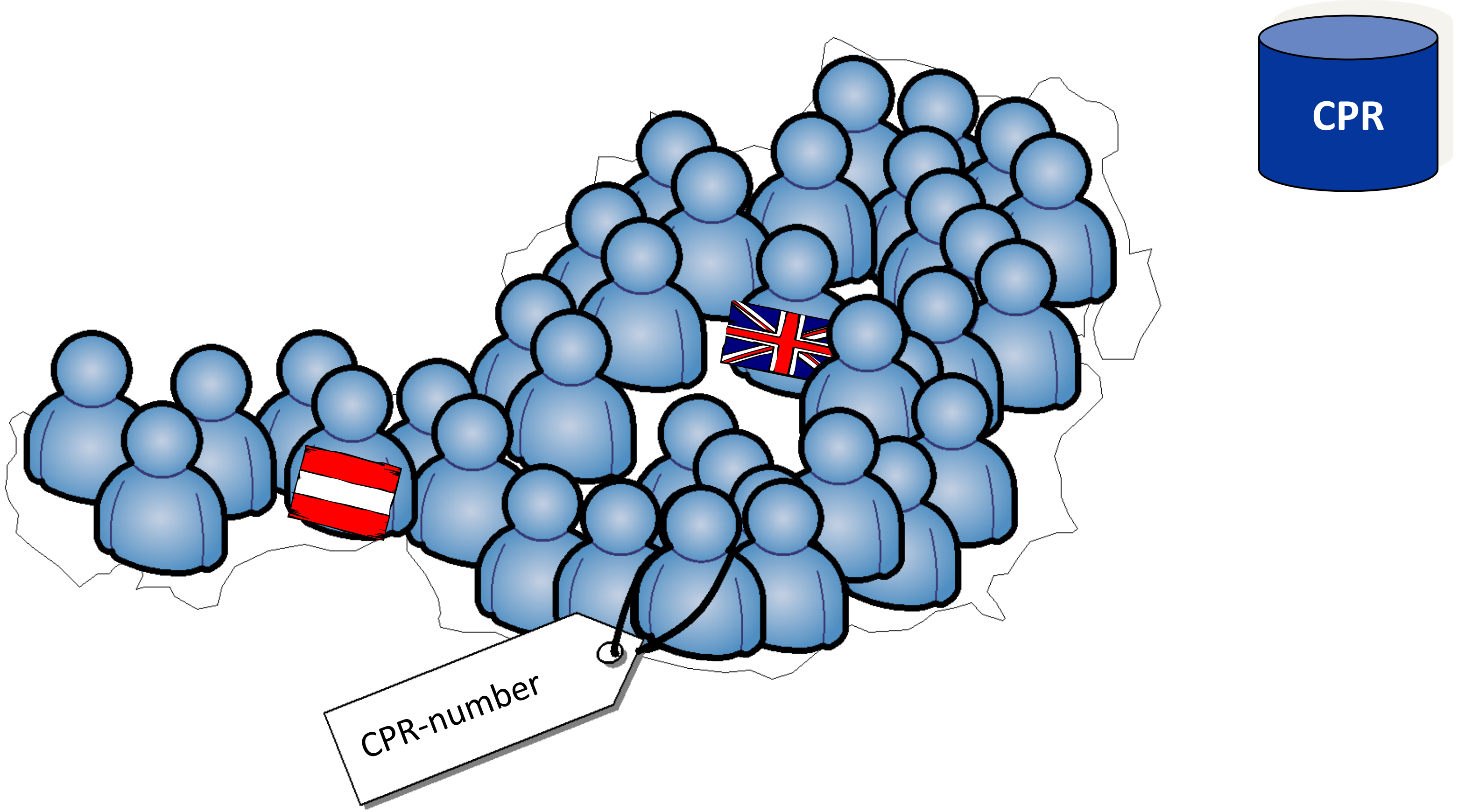
Name	Competence	Amount
Companies register (Firmenbuch)	BMJ	220.000
Register of associations (Vereinsregister)	BM.I	120.000
Central professional register (Gewerberegister)	BMWFJ	720.000
Supplementary register for other persons concerned (ERsB)	BKA	?

Central Population Register

(Zentrales Melderegister)



Central Population Register



Central Population Register

Included data:

First Name

Last Name

Date of birth

Gender

Citizenship

Address

CPR-number

May contain references to documents concerning civil status and citizenship

Provider:

Federal Ministry of the Interior (Bundesministerium für Inneres - BMI)

source PIN Register

(Stammzahlenregister)

sourcePIN Register

Calculation of the

Identity Link (sourcePIN)

Sector specific personal identifier (ssPIN)

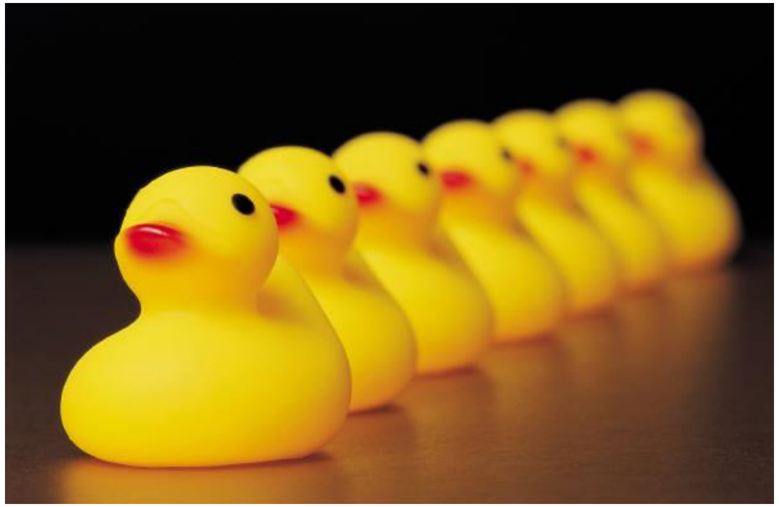
NO STORAGE of sourcePIN

Provider:

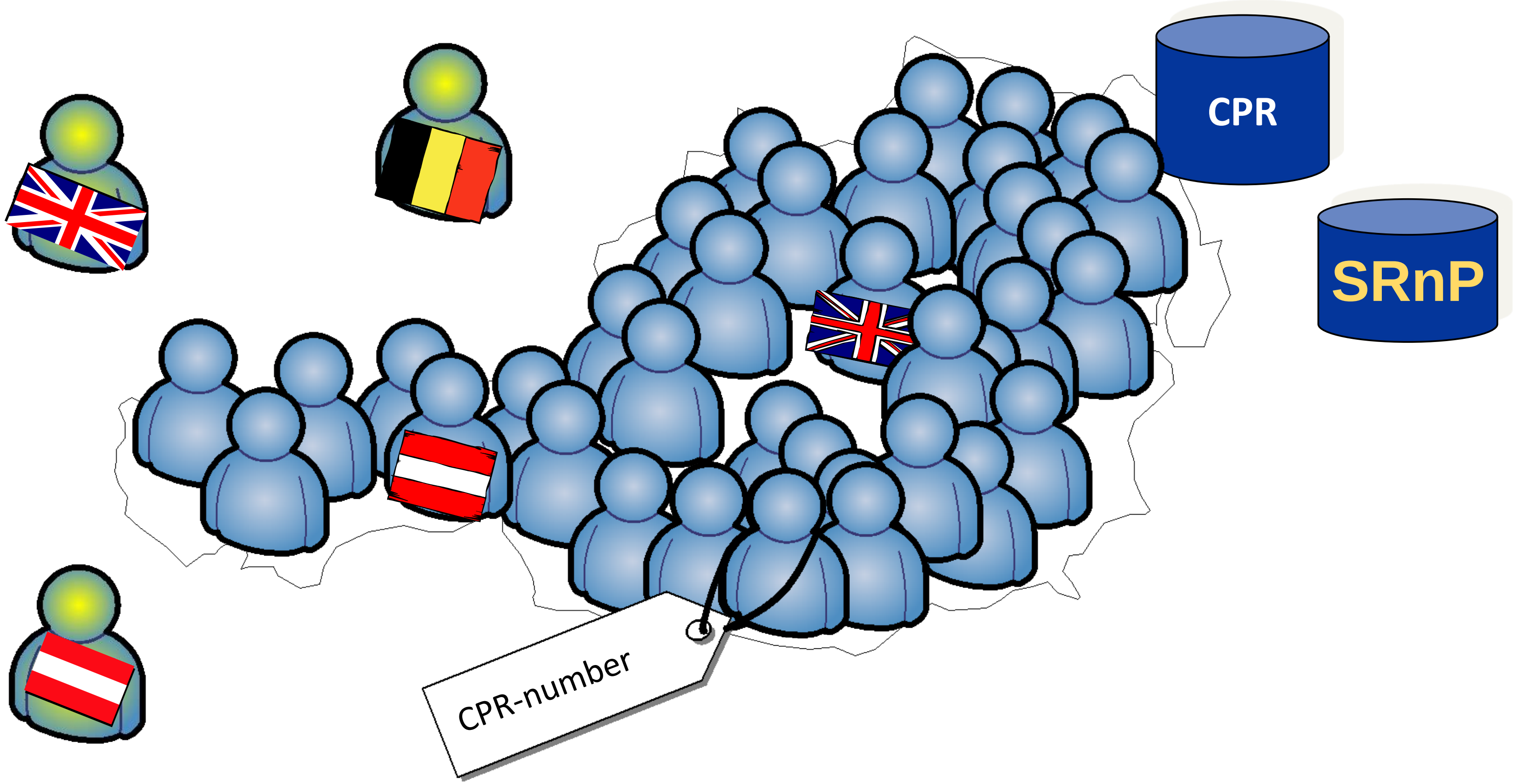
- SourcePIN register authority (SRA) at the data commission

Supplementary Register for natural Persons

(Ergänzungsregister für natürliche Personen)



Base Registers for natural Persons



Supplementary Register for natural Persons

Contains natural persons not included within the CPR

If a person is not found in the CPR and SRnP
(e.g. Austrian expatriates) during the citizen card creation process, she/he may request the entry into the SRnP.

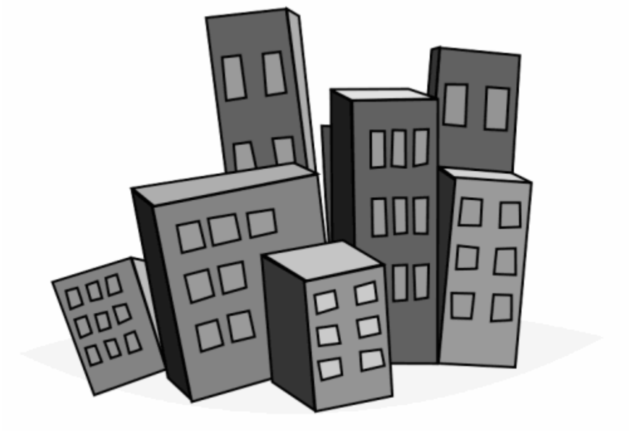
Included data:

- Name
- Date of birth
- Gender
- Citizenship
- Address
- Place of birth

Provider:

sourcePIN Register Authority

Register of Company Names
Included data



Identification

Legal form

Address

Organs

Power of representation

Person data

Financial resources

Legal facts

Since 2001 –
 electronic annual balance sheet

Since 2005 –
 electronic record of documents

Register for Associations

Included data:

Identification

Address

Foundation date

Constitutions, articles

Organs (Identification, ssPIN, function)

Provider:

BMI

No fees

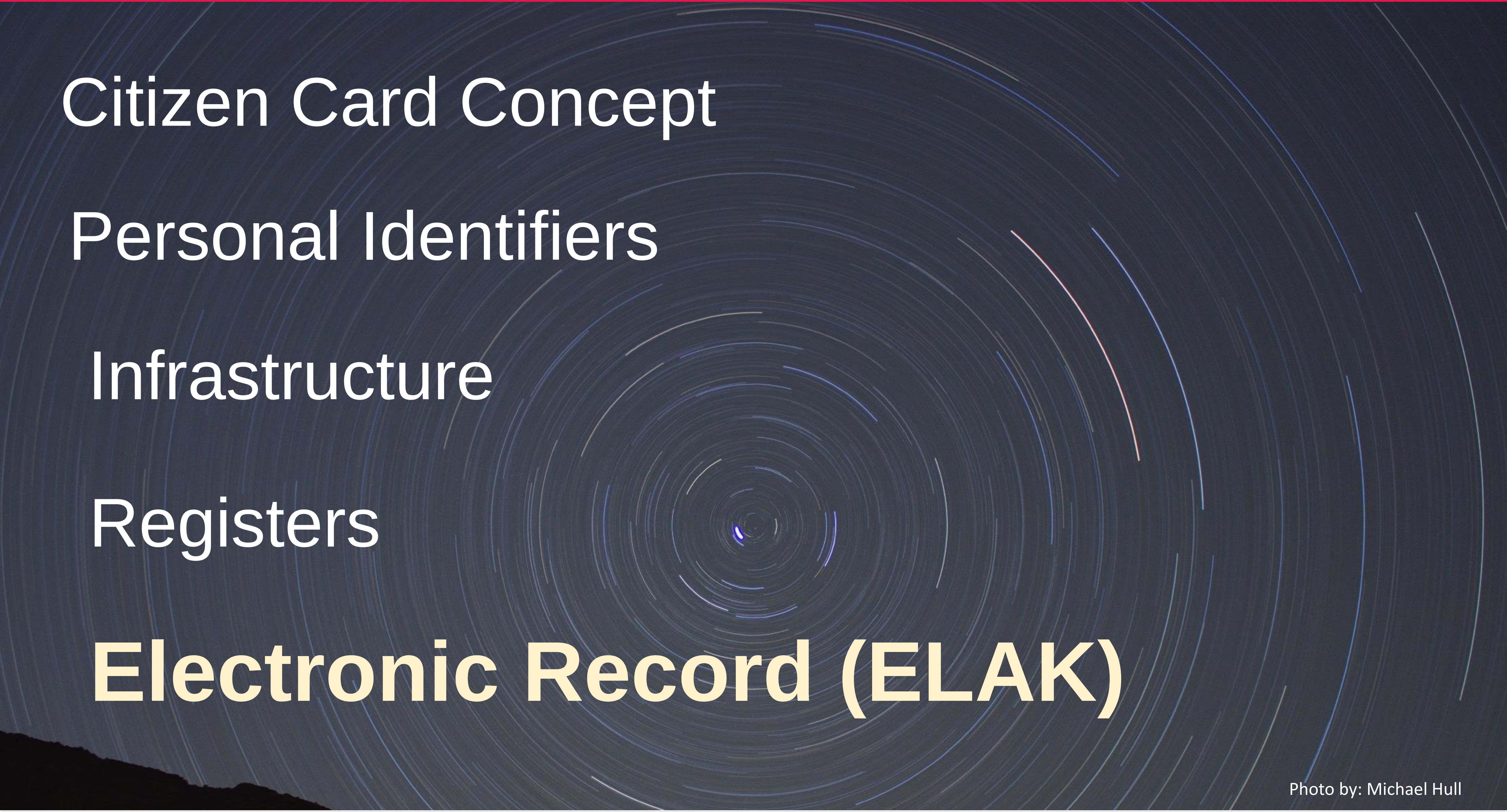
http://zvr.bmi.gv.at/Start

Supplementary Register for others concerned

Identification
Address
Legal form
Authorized representative (Organwalter)
Reference number (Ordnungsnummer)

Provider:

sourcePIN Register Authority (at BMI)



Citizen Card Concept

Personal Identifiers

Infrastructure

Registers

Electronic Record (ELAK)

Photo by: Michael Hull

Electronic Record

ELAK
(Elektronischer **AK**t**)**

- Document management
- Electronic record processing workflow

Why **ELAK?**

modern

E-Government

Continuous,

electronic

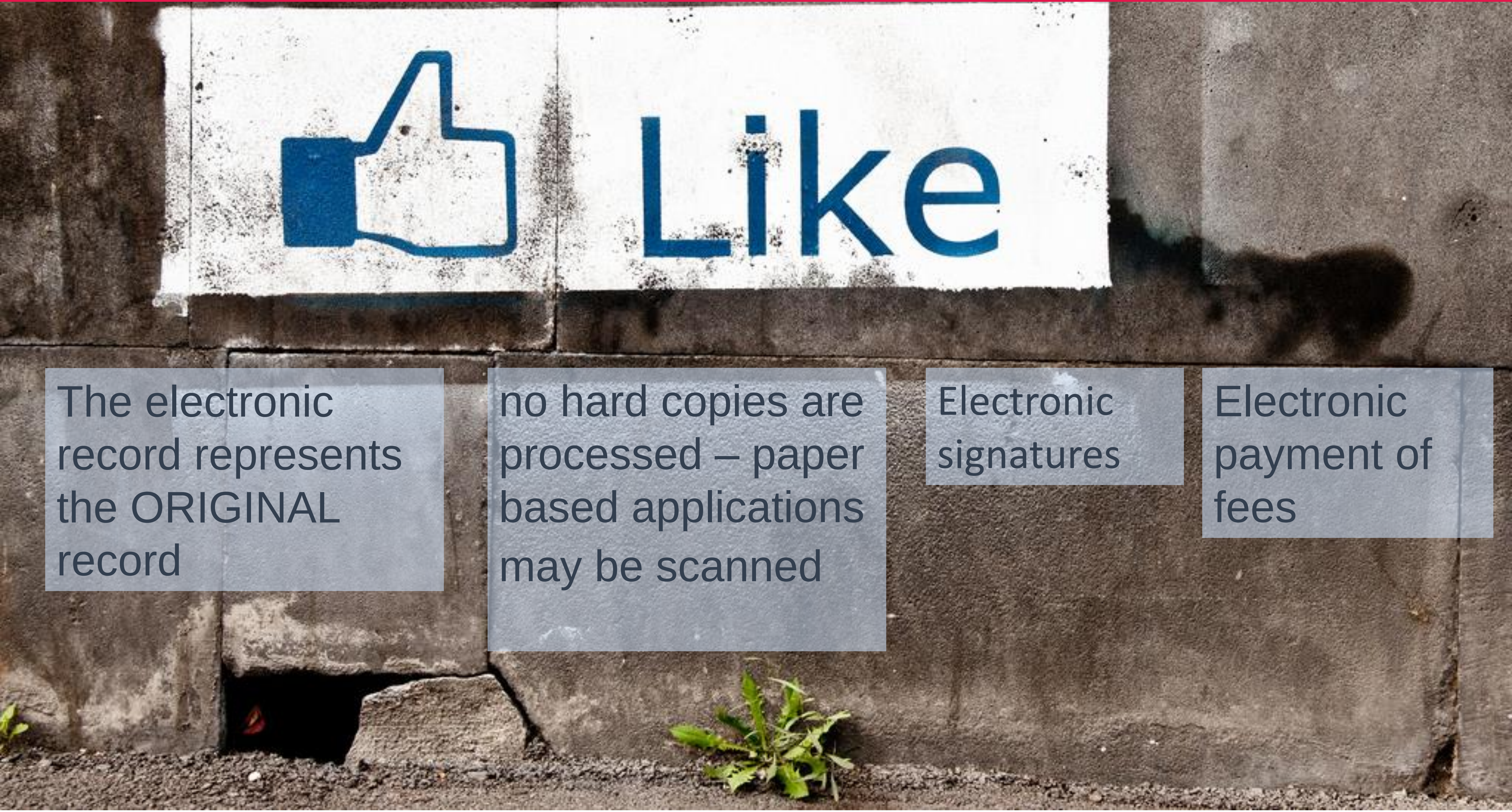
governmental

process

Why ELAK?

beginning of E-Government

- Form Server: Electronic web forms for citizens
- EPS Interface: Electronic Payment Interface
- Electronic Delivery



The electronic record represents the ORIGINAL record

no hard copies are processed – paper based applications may be scanned

Electronic signatures

Electronic payment of fees

- Automated processing
- Employee independent processing
- Full-text search within the records
- Reduction of cycle time up to 20%

Austrian E-Government Infrastructure

Kevin.Theuermann@egiz.gv.at
Kevin Theuermann

Graz, 20.11.2019

EGIZ
E-Government Innovationszentrum

Control Questions

- Explain and draft on ½ sheet of paper the basics of the Austrian Citizen Card.
- Explain the usage of Citizen Card Environment. What is the Security Layer?
- What is an Identity Link? How does it work?
- What do you know about Austrian Electronic Records (ELAK)?
- What is the difference between sourcePIN and sector specific source PIN (ssPIN)? What is ssPIN used for?
- Where is the sourcePIN stored?