Federal Office
for Information Security

# Identities Go Mobile

## The Future of Electronic Identification

Dr. Dennis Kügler
Federal Office for Information Security (BSI)

# History of Identification Documents

From paper to plastic

… to mobile.

# Evolution of Identity Documents

# Evolution of Identity Documents

1829

Wir Friedrich Wilhelm von Gottes Gnaden König von Preussen ꝛc. ꝛc.

Ersuchen hiermit, unter dem Versprechen einer vollkommenen Erwiederung, alle Militair- und Civil-Behörden auswärtiger Staaten, Unsern sämmtlichen Militair- und Civil-Bedienten aber befehlen Wir ausdrücklich, auf Vorzeigung dieses, [illegible] gebürtig aus [illegible] wohnhaft in [illegible] welche [illegible] von [illegible] über [illegible] mit [illegible] reist, und durch [illegible] als unverdächtig legitimirt ist, frei und ungehindert reisen, und von dort hieher zurückreisen, auch nöthigen Falls ihm Schutz und Beistand angedeihen zu lassen.

Signalement des Paß-Inhabers

Alter [illegible]
Größe [illegible] Fuß [illegible] Zoll
Haar [illegible]
Stirn [illegible]
Augenbraunen [illegible]
Augen [illegible]
Nase [illegible]
Mund [illegible]
Bart [illegible]
Kinn [illegible]
Gesicht [illegible]
Gesichtsfarbe [illegible]
Statur [illegible]

Besondere Kennzeichen:

Unterschrift des Paß-Inhabers

Der gegenwärtige Paß muß aber von der Polizei-Behörde nicht blos des Grenz-Orts, sondern, ohne Unterschied zwischen Stadt und plattem Lande, eines jeden Orts, an welchem der Inhaber länger, als Vier und zwanzig Stunden sich aufhält, visirt und ihr zu dem Ende vorgelegt werden.

Gegeben [illegible] 18[illegible]

Auf Seiner Königlichen Majestät allerhöchsten Special-Befehl.

Der Minister des Innern und der Polizei.

Reise-Paß

gültig auf [illegible]

Source:
Wikipedia /
Katalog "Stuttgarter Antiquariatsmesse 2007"

# Evolution of Identity Documents

1829

Wir Friedrich Wilhelm von Gottes Gnaden König von Preussen ꝛc. ꝛc.

Ersuchen hiermit, unter dem Versprechen einer vollkommenen Erwiederung, alle Militair- und Civil-Behörden auswärtiger Staaten, Unsern sämmtlichen Militair- und Civil-Bedienten aber befehlen Wir ausdrücklich, auf Vorzeigung dieses, [redacted] gebürtig aus [redacted] wohnhaft in [redacted] welche [redacted] von [redacted] über [redacted] gut [redacted] reist, und durch [redacted] als unverdächtig legitimirt ist, frei und ungehindert reisen, und von dort hieher zurückreisen, auch nöthigen Falls ihm Schutz und Beistand angedeihen zu lassen.

Der gegenwärtige Paß muß aber von der Polizei-Behörde nicht blos des Grenz-Orts, sondern, ohne Unterschied zwischen Stadt und plattem Lande, eines jeden Orts, an welchem der Inhaber länger, als Vier und zwanzig Stunden sich aufhält, visirt und ihr zu dem Ende vorgelegt werden.

Gegeben [redacted]

Auf Seiner Königlichen Majestät allerhöchsten Special-Befehl.

Der Minister des Innern und der Polizei.

Reise-Paß

gültig auf [redacted]

Signalement des Paß-Inhabers

Alter [redacted]
Größe [redacted] Fuß [redacted] Zoll
Haar [redacted]
Stirn [redacted]
Augenbraunen [redacted]
Augen [redacted]
Nase [redacted]
Mund [redacted]
Bart [redacted]
Kinn [redacted]
Gesicht [redacted]
Gesichtsfarbe [redacted]
Statur [redacted]

Besondere Kennzeichen:

Unterschrift des Paß-Inhabers

Source: Wikipedia / Katalog "Stuttgarter Antiquariatsmesse 2007"

Erstein, den 14.12. 1917

Der Kreisdirektor
J. V.

Source: “Der Passexpedient”

1917

# Evolution of Identity Documents

1829

Wir Friedrich Wilhelm von Gottes Gnaden König von Preußen etc. etc.

Ersuchen hiermit, unter dem Versprechen einer vollkommenen Erwiederung, alle Militair- und Civil-Behörden auswärtiger Staaten, Unsern sämmtlichen Militair- und Civil-Bedienten aber befehlen Wir ausdrücklich, auf Vorzeigung dieses, den ... gebürtig aus ... wohnhaft in ... welche ... von ... über ... gut ... reist, und durch ... als unverdächtig legitimirt ist, frei und ungehindert reisen, und von dort hieher zurückreisen, auch nöthigen Falls ihm Schutz und Beistand angedeihen zu lassen.

Der gegenwärtige Paß muß aber von der Polizei-Behörde nicht blos des Grenz-Orts, sondern, ohne Unterschied zwischen Stadt und plattem Lande, eines jeden Orts, an welchem der Inhaber länger, als Vier und zwanzig Stunden sich aufhält, visirt und ihr zu dem Ende vorgelegt werden.

Gegeben ...

Auf Seiner Königlichen Majestät allerhöchsten Special-Befehl.

Der Minister des Innern und der Polizei.

Reise-Paß

gültig auf ...

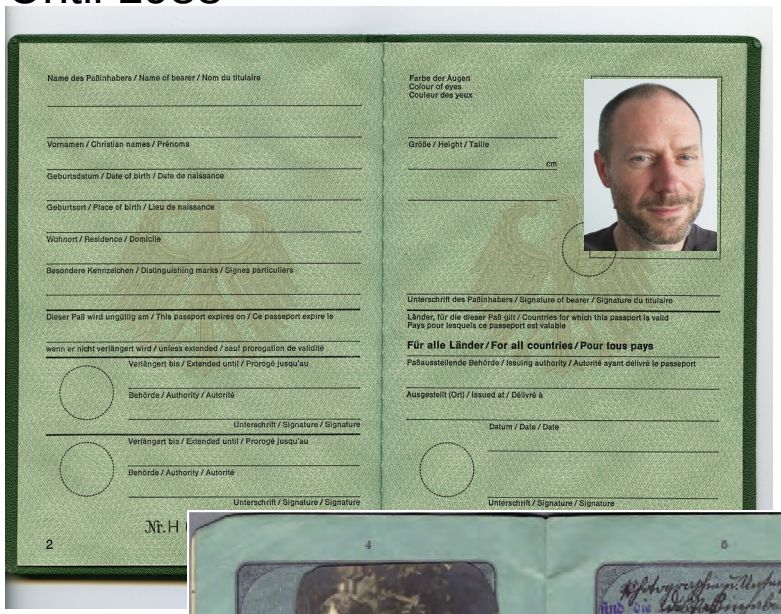
Signalement des Paß-Inhabers

Alter ... Größe ... Fuß ... Zoll. Haar ... Stirn ... Augenbraunen ... Augen ... Nase ... Mund ... Bart ... Kinn ... Gesicht ... Gesichtsfarbe ... Statur ...

Besondere Kennzeichen:

Unterschrift des Paß-Inhabers

Until 1988





Source: Wikipedia / Katalog "Stuttgarter Antiquariatsmesse 2007"

Source: “Der Passexpedient”

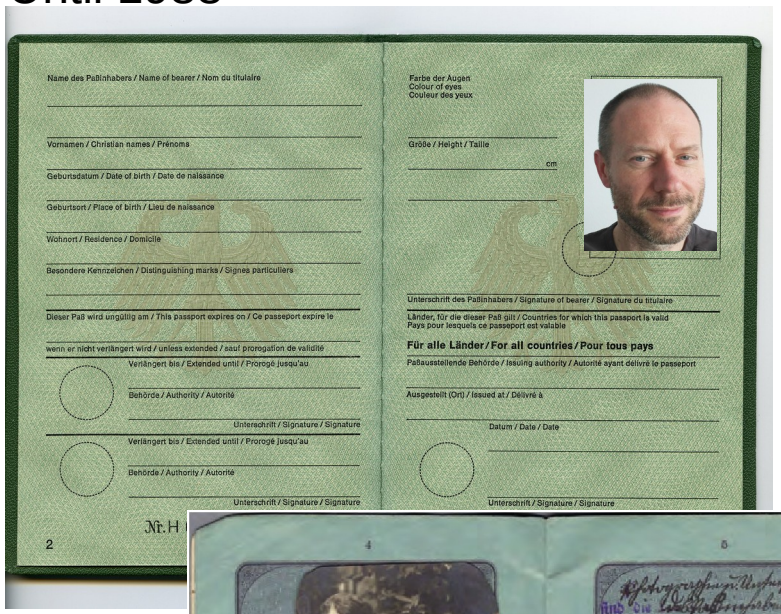
1917

# Evolution of Identity Documents

1829


Source: Wikipedia / Katalog "Stuttgarter Antiquariatsmesse 2007"

Until 1988





Source: “Der Passexpedient”

1917

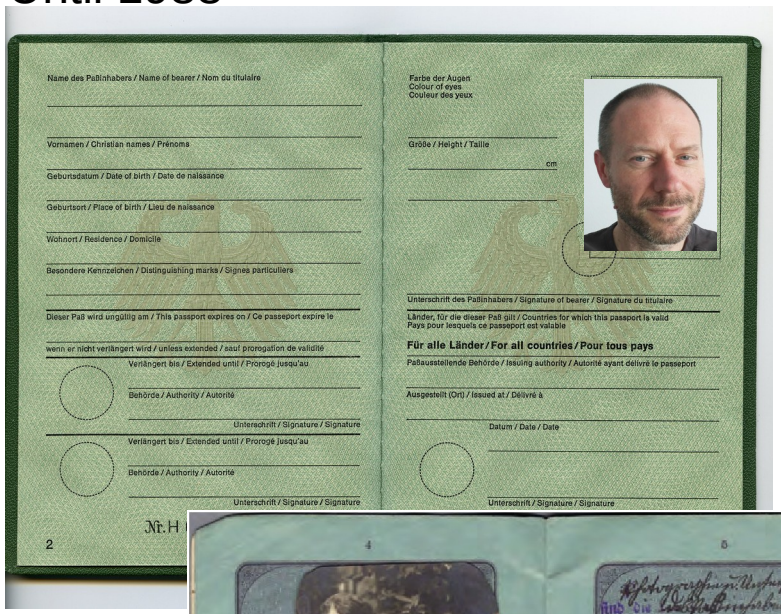
1988-2005

# Evolution of Identity Documents

1829


Source: Wikipedia / Katalog "Stuttgarter Antiquariatsmesse 2007"

Until 1988



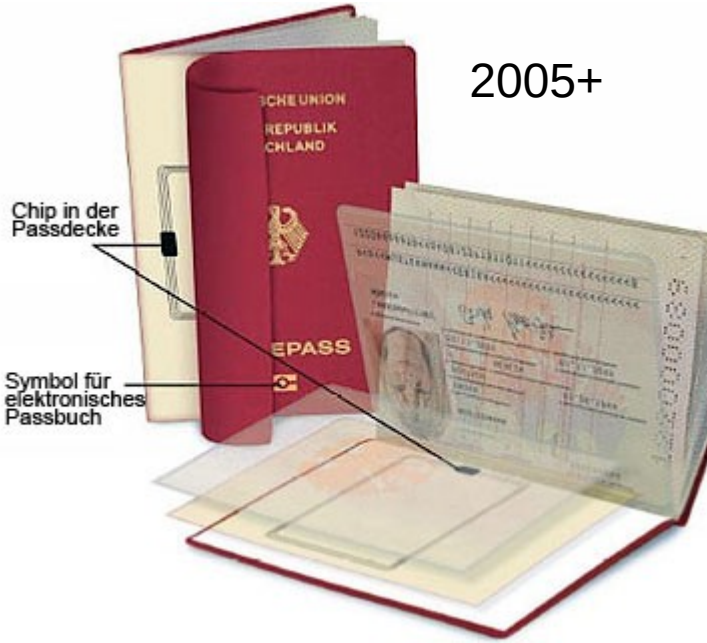


Source: “Der Passexpedient”

1917

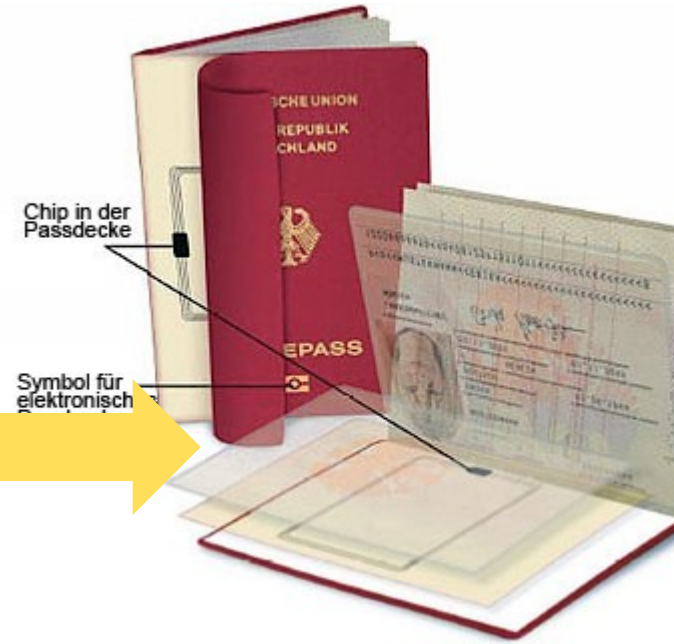
1988-2005


2005+



# Evolution of Identity Documents

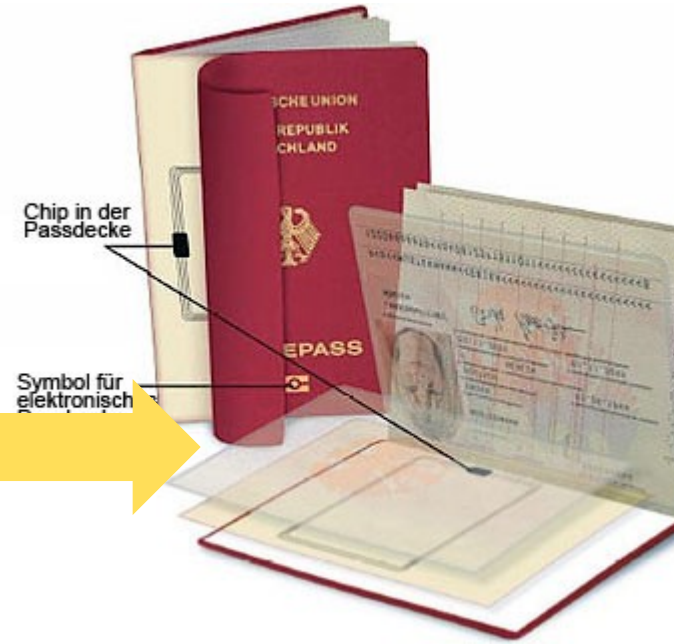



Federal Office for Information Security

# Evolution of Identity Documents



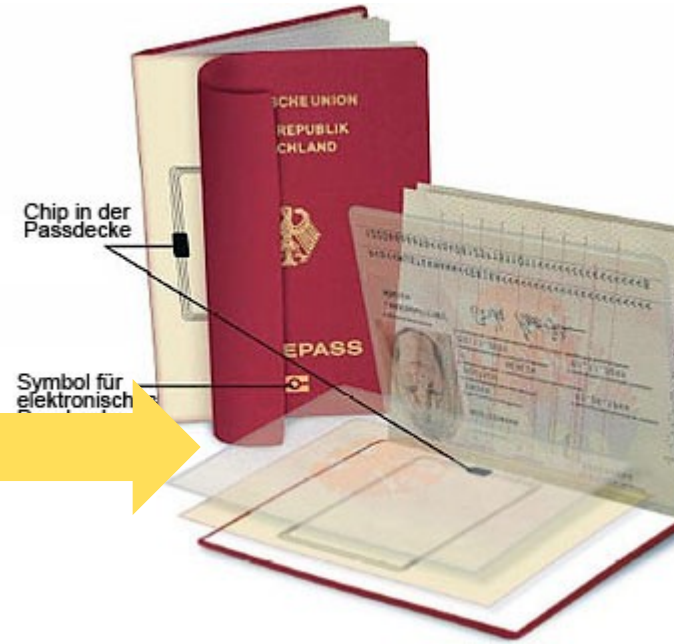




Possession

# Evolution of Identity Documents

Possession


Possession

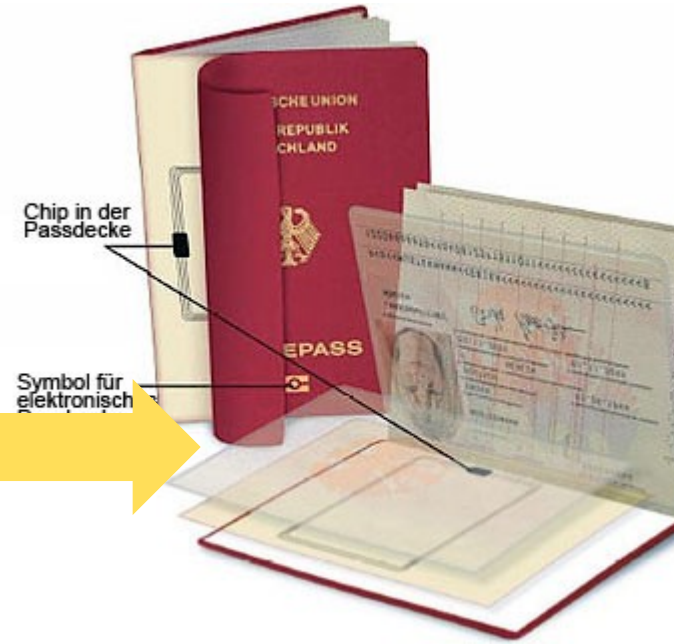




Federal Office for Information Security

# Evolution of Identity Documents


Possession


Possession
Facial Image

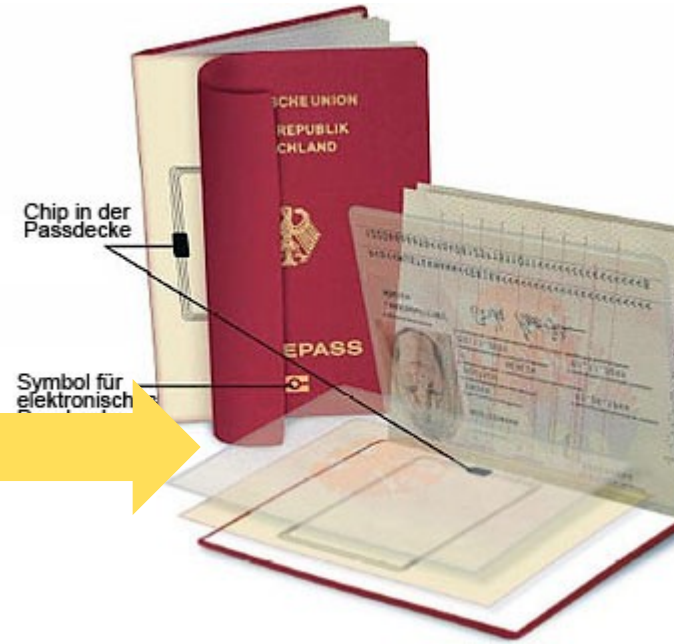

Federal Office
for Information Security

# Evolution of Identity Documents

Possession


Possession
Facial Image


Possession



# Evolution of Identity Documents

Possession


Possession
Facial Image

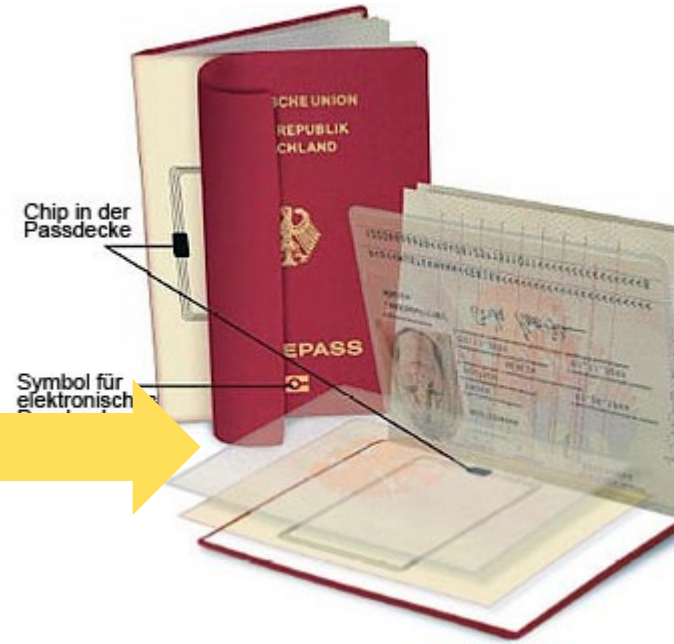

Possession
Facial Image

# Evolution of Identity Documents

Possession

Possession
Facial Image


Possession
Facial Image
Machine Readable



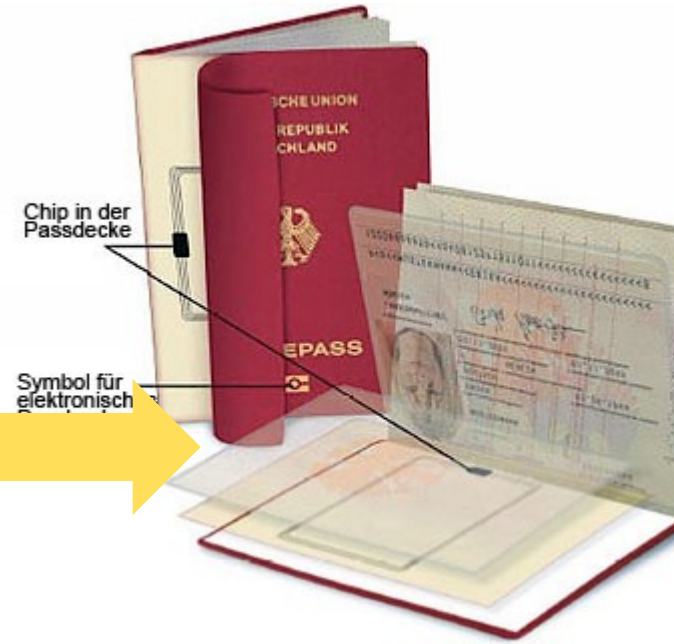

Federal Office
for Information Security

# Evolution of Identity Documents

Possession

Possession
Facial Image


Possession
Facial Image
Machine Readable



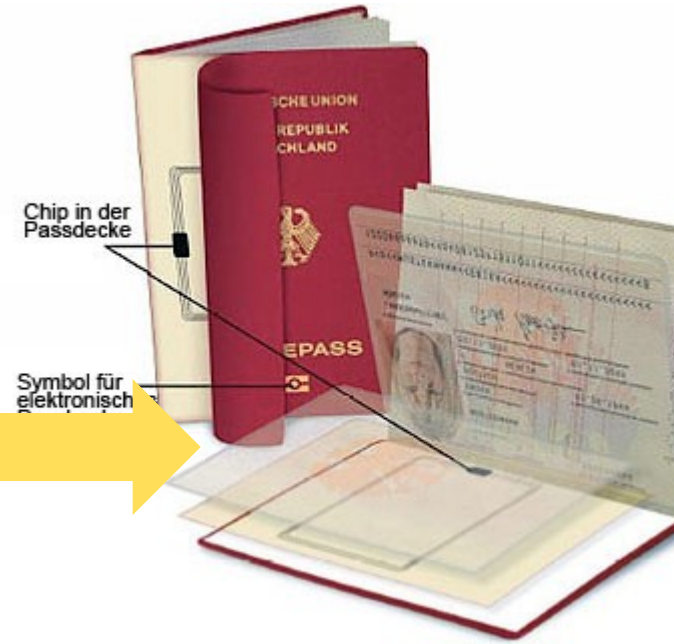

Possession

# Evolution of Identity Documents

Possession

Possession
Facial Image


Possession
Facial Image
Machine Readable




Possession
Facial Image

# Evolution of Identity Documents

Possession


Possession
Facial Image


Possession
Facial Image
Machine Readable

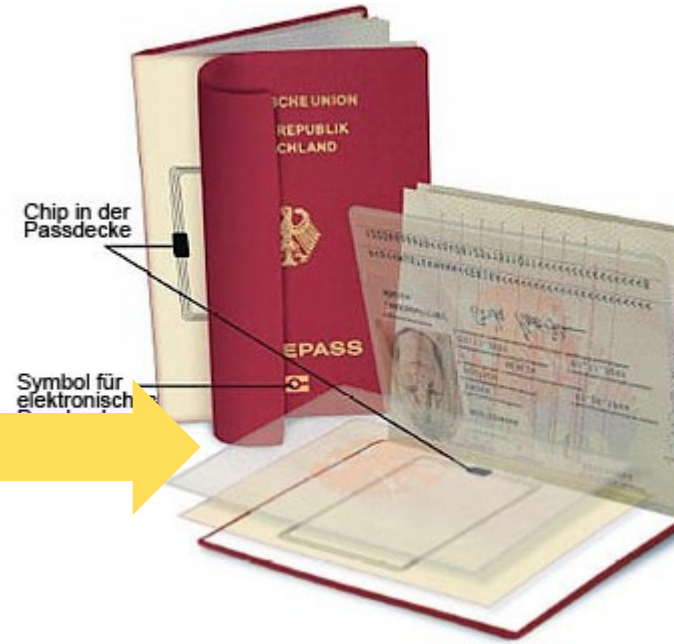

Possession
Facial Image
Biometrics

# Evolution of Identity Documents

Possession

Possession
Facial Image


Possession
Facial Image
Machine Readable



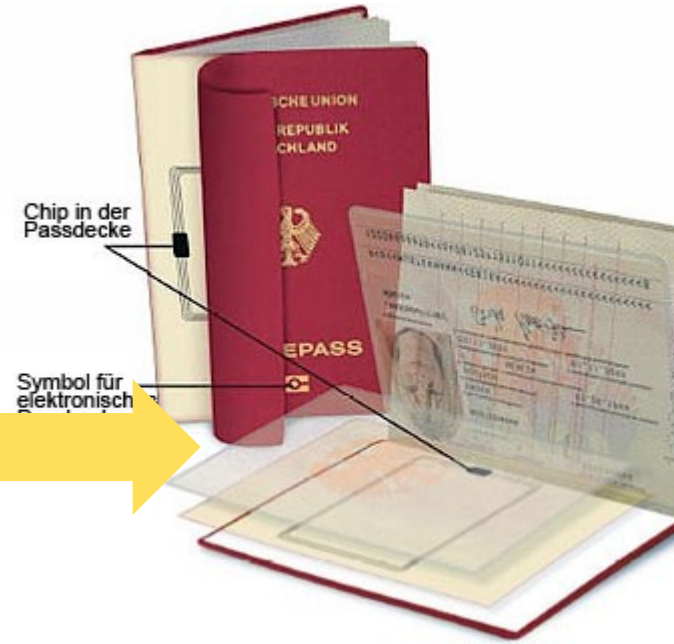

Possession
Facial Image
Biometrics
Machine Readable

# Evolution of Identity Documents

Possession

Possession
Facial Image


Possession
Facial Image
Machine Readable




Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

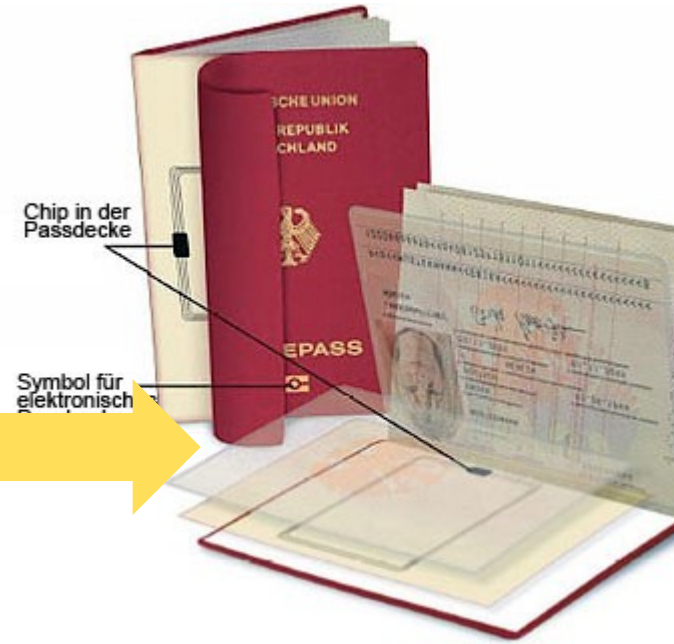
Federal Office
for Information Security

# Evolution of Identity Documents

Possession


Possession
Facial Image


Possession
Facial Image
Machine Readable




Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

Rubber Stamps

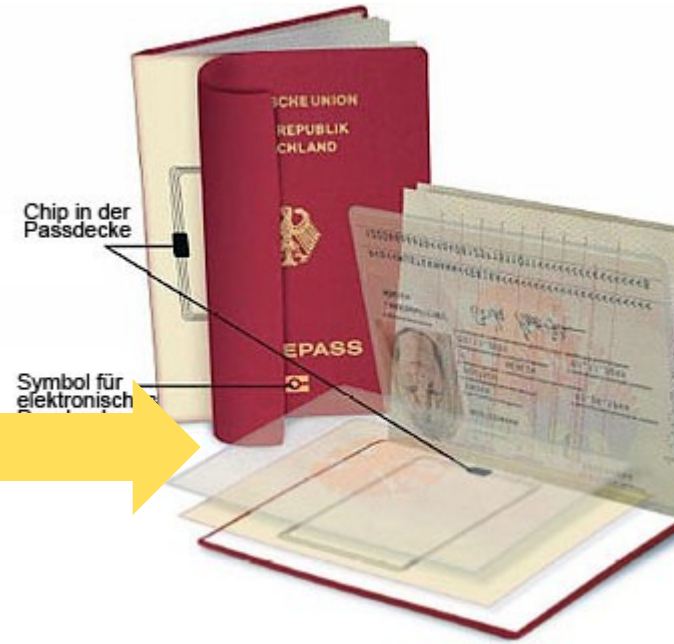
# Evolution of Identity Documents

Possession

Rubber Stamps

Possession
Facial Image


Possession
Facial Image
Machine Readable




Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

Holograms etc.

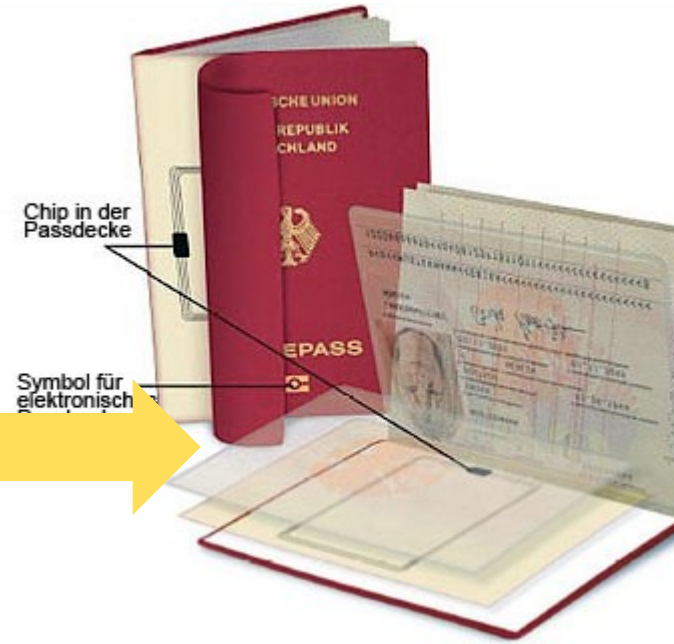
Federal Office
for Information Security

# Evolution of Identity Documents

Possession

Possession
Facial Image


Possession
Facial Image
Machine Readable




Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

Rubber Stamps

**Increased (Physical) Security**

Holograms etc.

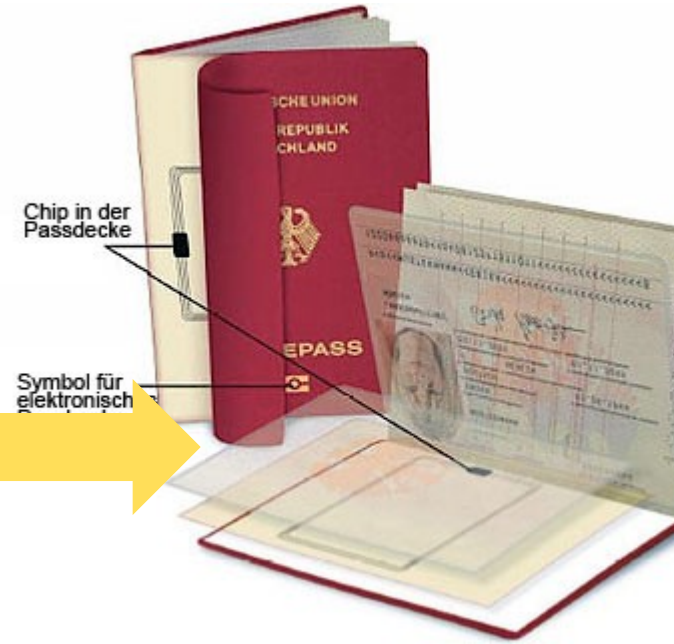
Federal Office
for Information Security

# Evolution of Identity Documents

Possession

Possession
Facial Image


Possession
Facial Image
Machine Readable




Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

Rubber Stamps
Single-Factor-Identifcation

**Increased (Physical) Security**

Holograms etc.

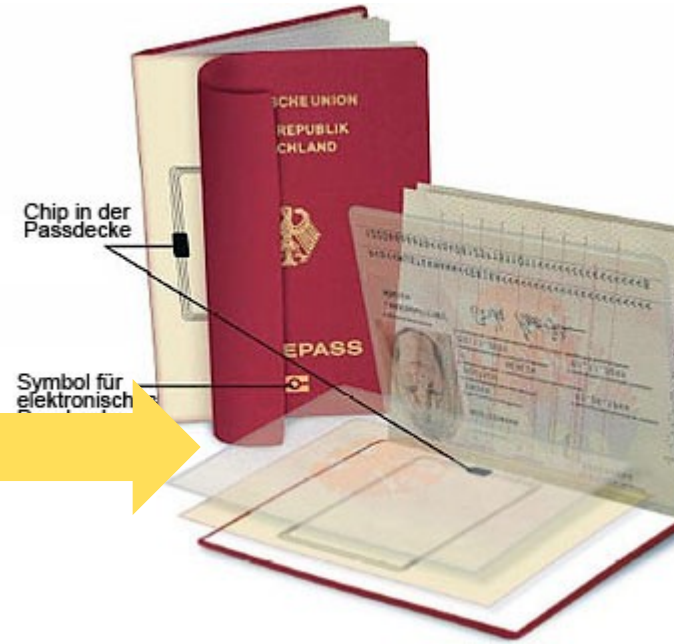
Federal Office
for Information Security

# Evolution of Identity Documents

Possession

Possession
Facial Image


Possession
Facial Image
Machine Readable




Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

Rubber Stamps
Single-Factor-Identifcation

**Increased (Physical) Security**

Holograms etc.
Two-Factor-Identification

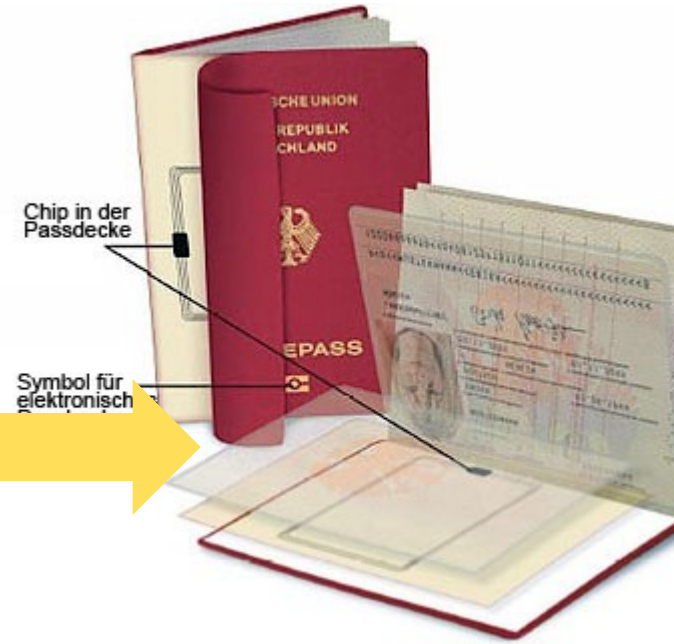
Federal Office
for Information Security

# Evolution of Identity Documents

Possession

Possession
Facial Image


Possession
Facial Image
Machine Readable




Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

Rubber Stamps
Single-Factor-Identifcation

**Increased (Physical) Security**
**Improved Binding**

Holograms etc.
Two-Factor-Identification

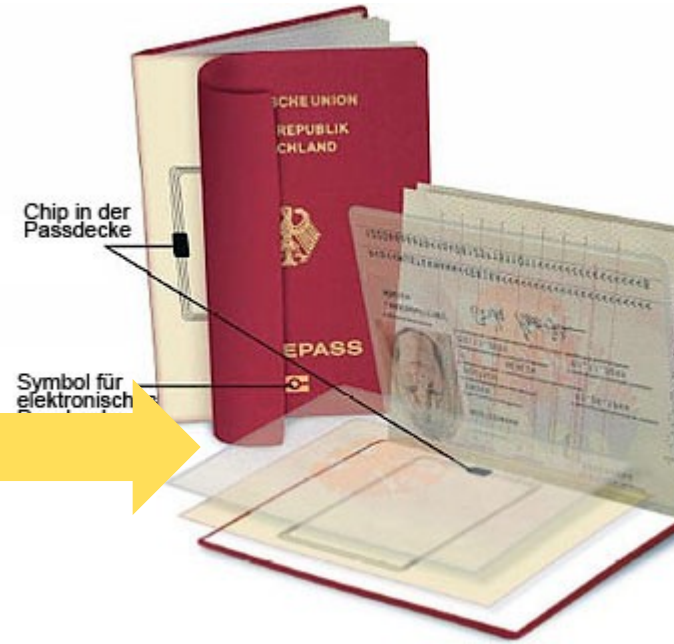
Federal Office
for Information Security

# Evolution of Identity Documents

Possession

Possession
Facial Image


Possession
Facial Image
Machine Readable




Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

Rubber Stamps
Single-Factor-Identifcation
“Analogue” Security

**Increased (Physical) Security**
**Improved Binding**

Holograms etc.
Two-Factor-Identification

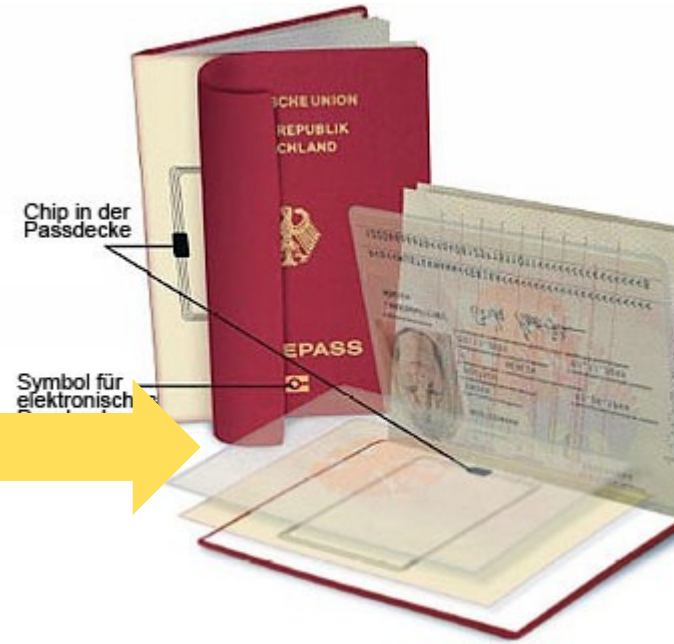
Federal Office
for Information Security

# Evolution of Identity Documents

Possession

Possession
Facial Image


Possession
Facial Image
Machine Readable




Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

Rubber Stamps
Single-Factor-Identifcation
“Analogue” Security

**Increased (Physical) Security**
**Improved Binding**

Holograms etc.
Two-Factor-Identification
Digital Security

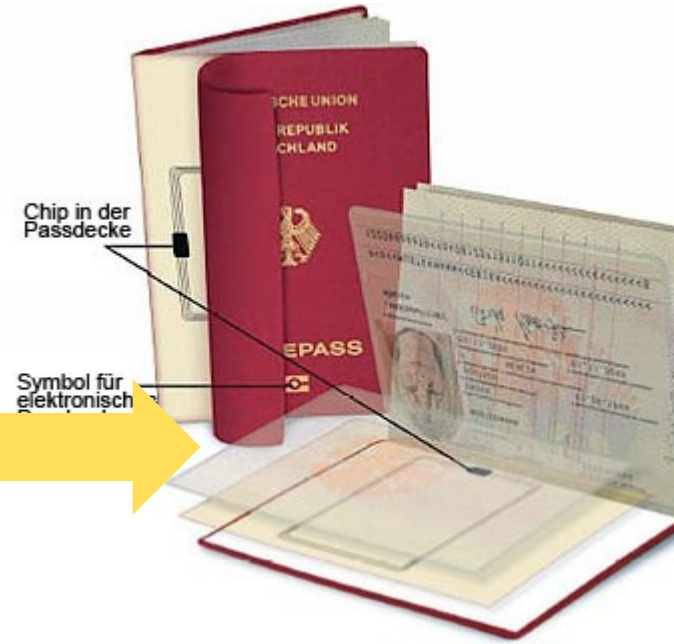
Federal Office
for Information Security

# Evolution of Identity Documents

Possession

Possession
Facial Image


Possession
Facial Image
Machine Readable




Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

Rubber Stamps
Single-Factor-Identifcation
“Analogue” Security

**Increased (Physical) Security**
**Improved Binding**
**Digitization**

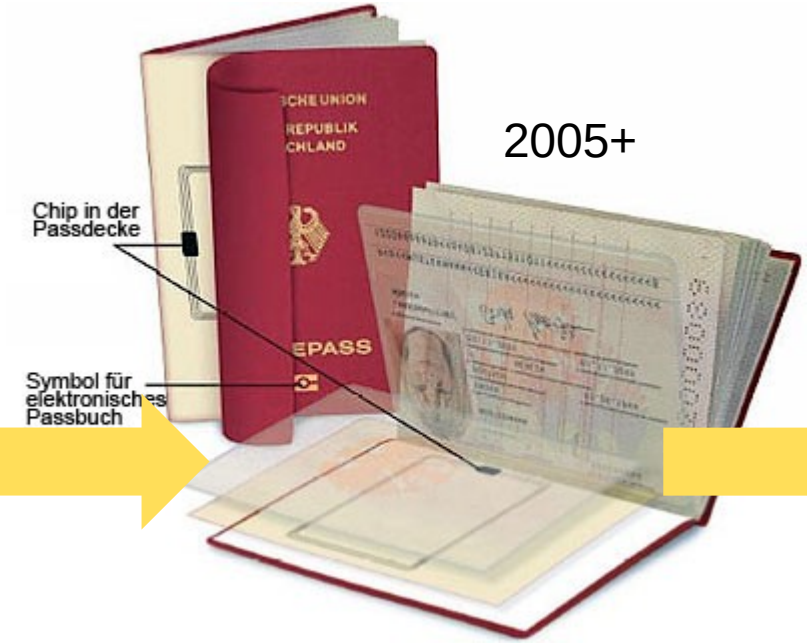
Holograms etc.
Two-Factor-Identification
Digital Security

Federal Office
for Information Security

# “Beyond the Book”

1988-2005


2005+



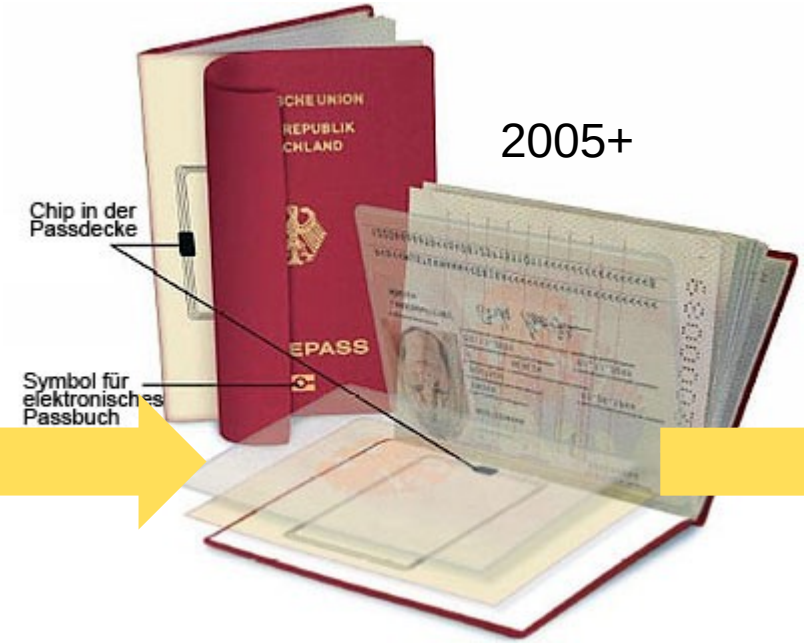

Possession
Facial Image
Machine Readable

Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

# “Beyond the Book”

1988-2005


2005+




20??

?

Possession
Facial Image
Machine Readable

Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

# “Beyond the Book”

1988-2005


Possession
Facial Image
Machine Readable

2005+


Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

20??

**“Digital”**

# “Beyond the Book”

1988-2005


2005+


20??

Possession
Facial Image
Machine Readable

Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

**“Digital”**
*Possession*

# “Beyond the Book”

1988-2005


Possession
Facial Image
Machine Readable

2005+


Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

20??

**“Digital”**
*Possession*
~~Facial Image~~

# “Beyond the Book”

1988-2005


2005+


20??

?

Possession
Facial Image
Machine Readable

Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

**“Digital”**
*Possession*
~~Facial Image~~
Biometrics

# “Beyond the Book”

1988-2005


2005+


20??

Possession
Facial Image
Machine Readable

Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

**“Digital”**
*Possession*
~~Facial Image~~
Biometrics
Machine Readable

# “Beyond the Book”

1988-2005


2005+


20??

Possession
Facial Image
Machine Readable

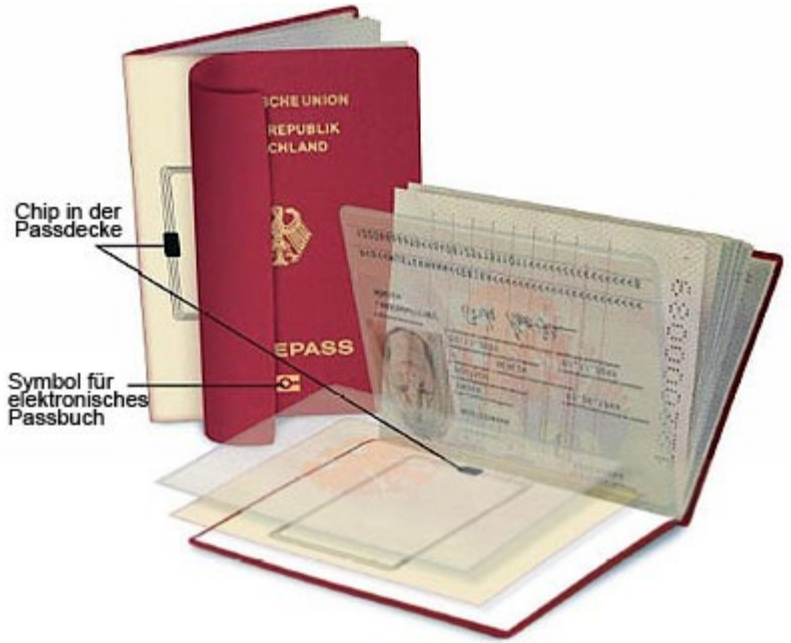
Possession
Facial Image
Biometrics
Machine Readable
Machine Verifiable

**“Digital”**
*Possession*
~~Facial Image~~
Biometrics
Machine Readable
Machine Verifiable

# Securing electronic Identities

- **Integrity:** (biographic) data must be authentic
  - Established by the issuer and remain unmodified
  - ~~Physical security: render counterfeiting difficult~~
  - Digital security: data is digitally signed

- **Binding:** identity must be bound to the holder
  - Identity must not be transferable to any other person
  - **Possession** of the physical document
    - ~~Physical security: render copying difficult~~
    - Digital security: hardware protected private key
  - **Biometrics** of the holder



# Example

Counterfeiting a Liechtenstein ePassport

# What Would We Loose?
# Example: Liechtenstein Specimen ePassport

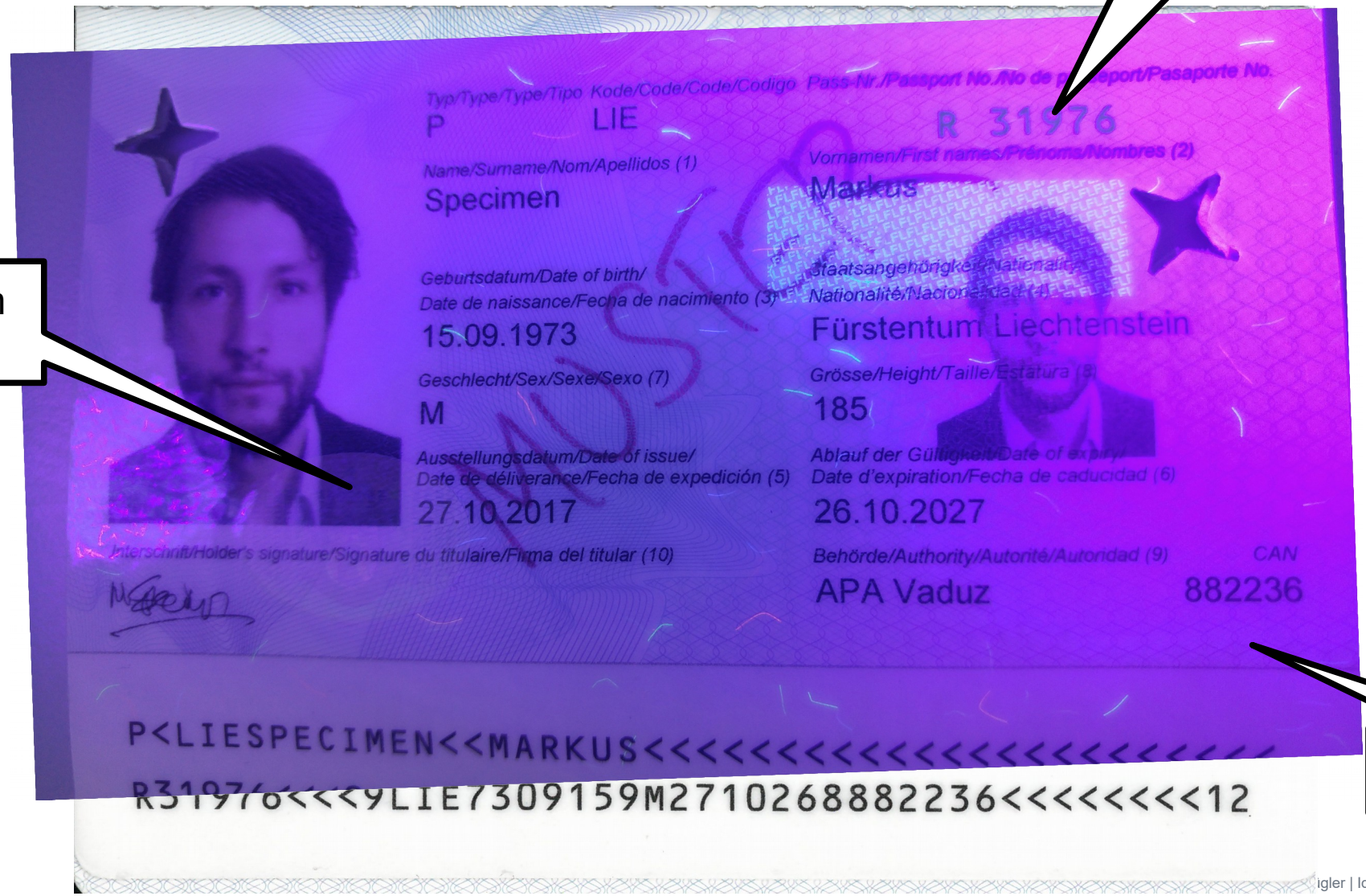
# What Would We Loose?
# Example: Liechtenstein Specimen ePassport


Laminated Paper

# What Would We Loose?
# Example: Liechtenstein Specimen ePassport

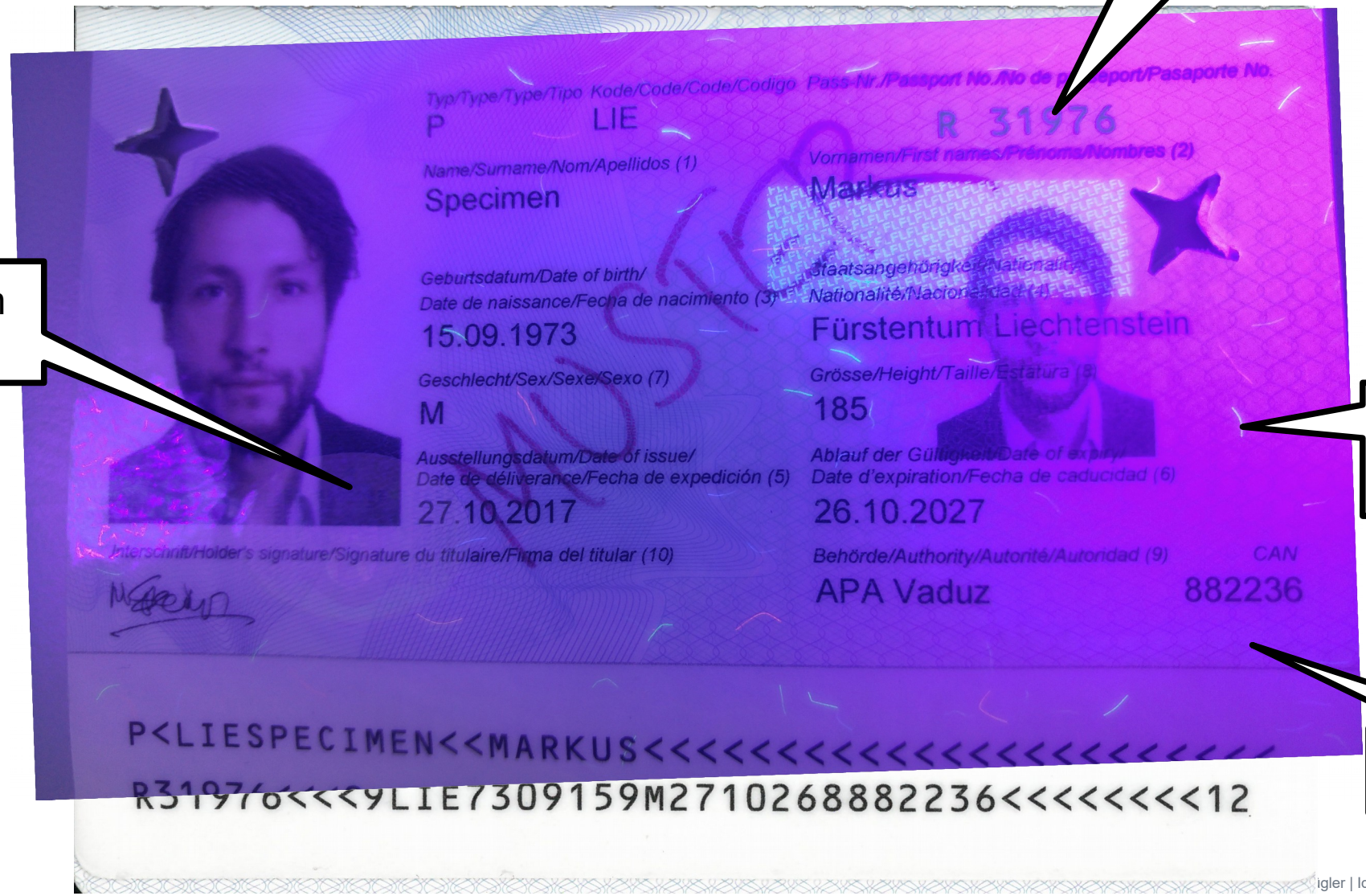
# What Would We Loose?
# Example: Liechtenstein Specimen ePassport

# What Would We Loose?
# Example: Liechtenstein Specimen ePassport




Federal Office for Information Security

# What Would We Loose?
# Example: Liechtenstein Specimen ePassport




Tactile

Hologram Sticker

UV-Fluorescent Fibers

Laminated Paper

Federal Office for Information Security

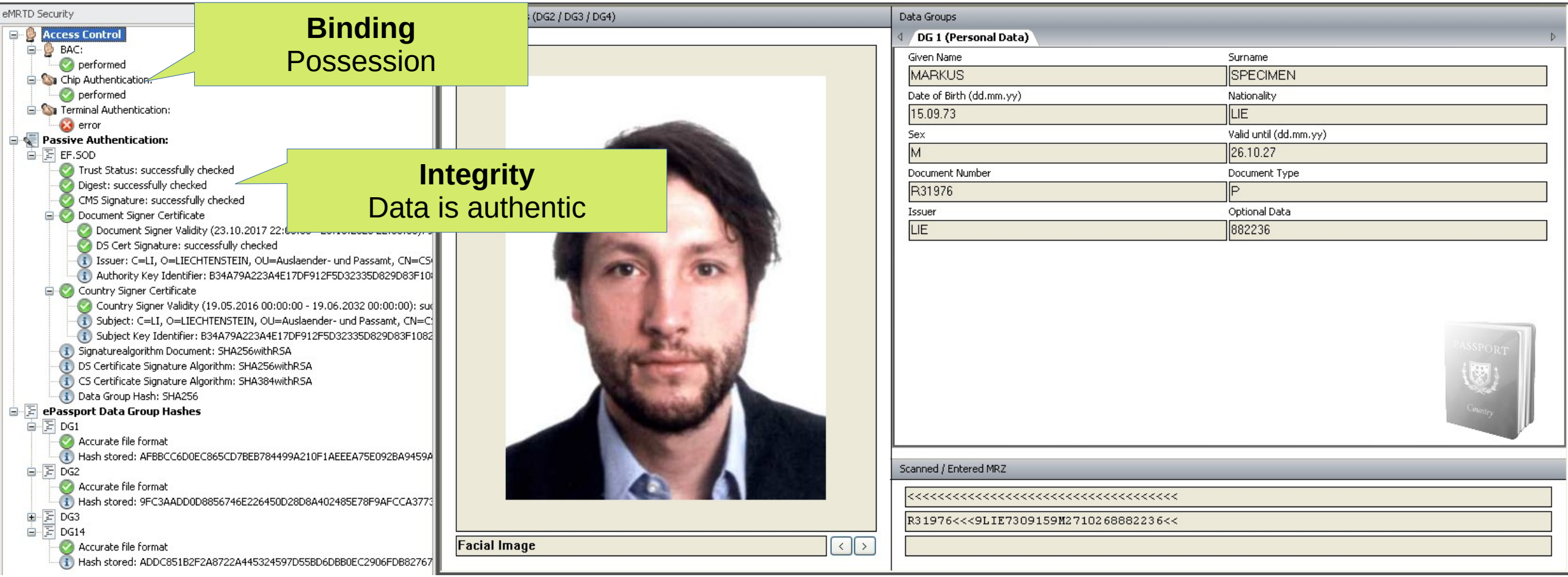
# What Would We Loose?
# Example: Liechtenstein Specimen ePassport

# Example: Liechtenstein ePassport – Chip Content

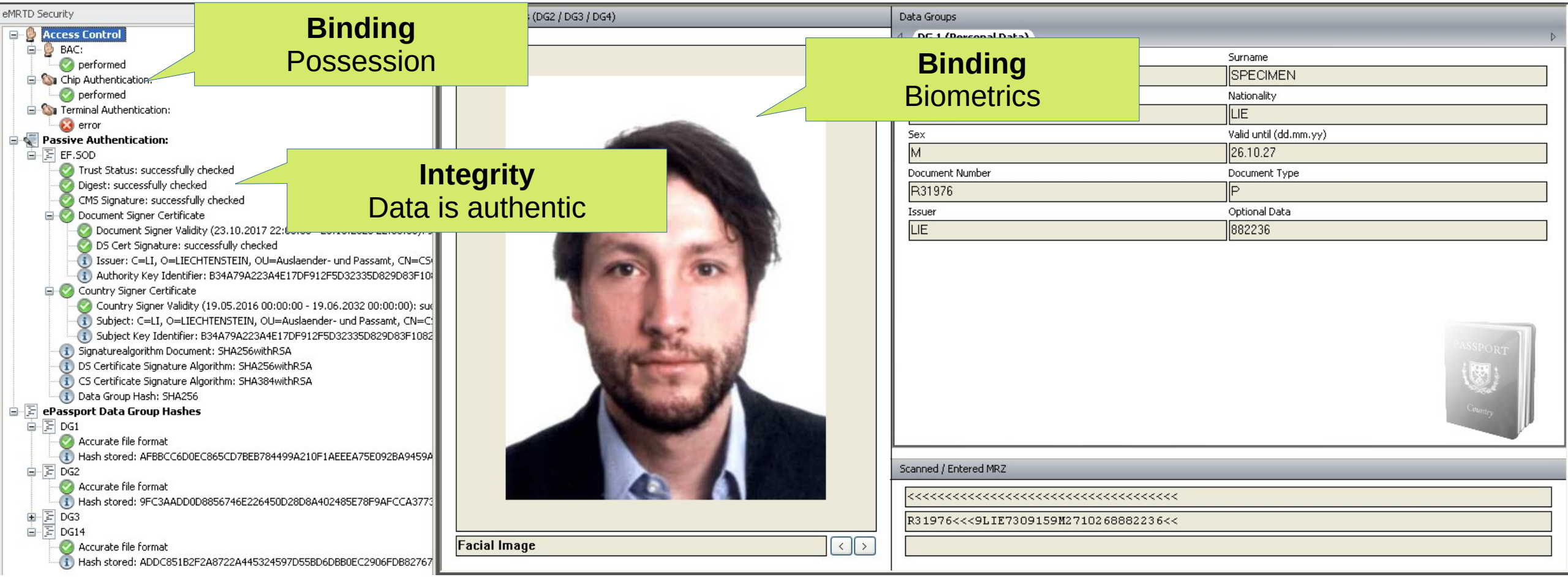

Federal Office
for Information Security

# Example: Liechtenstein ePassport – Chip Content

# Example: Liechtenstein ePassport – Chip Content

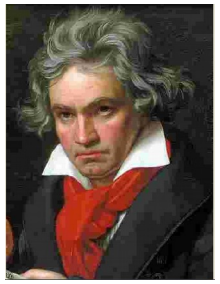


# Example: Liechtenstein ePassport – Chip Content

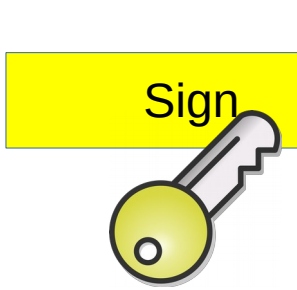



Federal Office
for Information Security

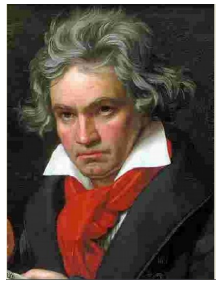
# Liechtenstein – Electronic Counterfeit



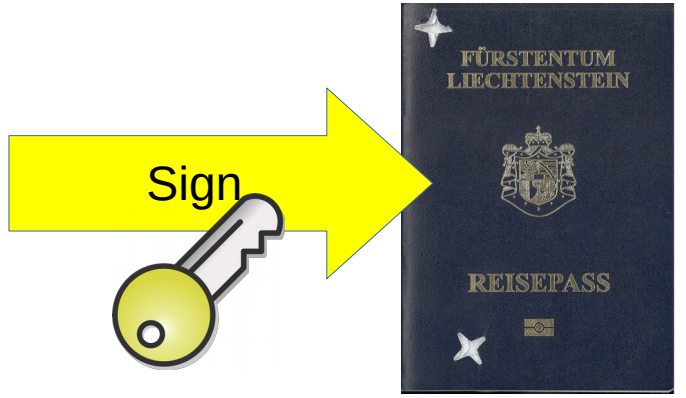
Ludwig Fun Beethoven




# Liechtenstein – Electronic Counterfeit



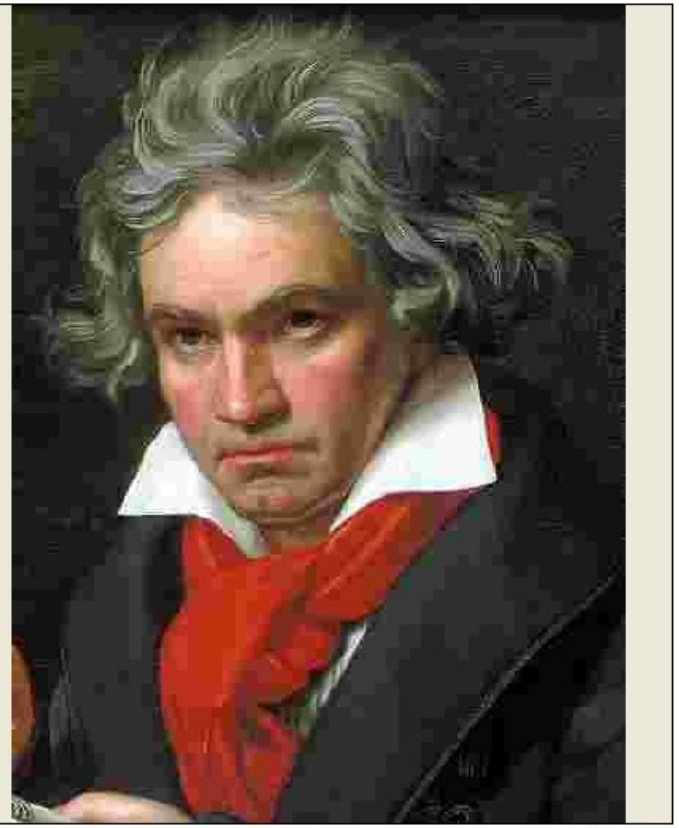
Ludwig Fun Beethoven




eMRTD Security

- **Access Control**
  - BAC:
    - performed
- **Passive Authentication:**
  - EF.SOD
    - Trust Status: successfully checked
    - Digest: successfully checked
    - CMS Signature: successfully checked
    - Document Signer Certificate
      - Document Signer Validity (29.04.2015 00:00:00 - 29.05.2026 00:00:00): s
      - DS Cert Signature: successfully checked
      - Issuer: C=LI, O=LIECHTENSTEIN, OU=Auslaender- und Passamt, CN=CS
      - Authority Key Identifier: F11121061CB05027BCE9CC060AF2C1C63FF717
    - Country Signer Certificate
      - Country Signer Validity (17.05.2011 17:00:55 - 01.09.2026 17:00:55): suc
      - Subject: C=LI, O=LIECHTENSTEIN, OU=Auslaender- und Passamt, CN=C
      - Subject Key Identifier: F11121061CB05027BCE9CC060AF2C1C63FF717D6
    - Signaturealgorithm Document: SHA256withRSA
    - DS Certificate Signature Algorithm: SHA256withRSA
    - CS Certificate Signature Algorithm: SHA256withRSA
    - Data Group Hash: SHA256
- **ePassport Data Group Hashes**
  - DG1
    - Accurate file format
    - Hash stored: 2AB209E7CEFA085561171C46A5CD760EDC7FDA11A3FE0E4DA
  - DG2
    - Accurate file format
    - Hash stored: 77A8ECA9CA5C59755B948C16F03F8D45C0A2BC090E5A17A5F

Biometric Pictures (DG2 / DG3 / DG4)



Facial Image

Data Groups

DG 1 (Personal Data)

| Given Name | Surname |
|---|---|
| LUDWIG | FUN BEETHOVEN |
| Date of Birth (dd.mm.yy) | Nationality |
| 17.12.70 | LIE |
| Sex | Valid until (dd.mm.yy) |
| M | 16.10.20 |
| Document Number | Document Type |
| TESTTEST2 | P |
| Issuer | Optional Data |
| LIE | |

Scanned / Entered MRZ

```
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
TESTTEST22LIE7012174M2010164<<<<<<<<
```

# Secure electronic Identities require MUCH more than storing data on a chip

## Electronic Identification

As simple as possible

but **not** simpler!

The Sydney Morning Herald
INDEPENDENT. ALWAYS.

January 22 2017

# 'World first': Government moves to radically overhaul Australia's international airports

International passengers would be whisked through immigration and customs without stopping or even encountering humans, while passport scanners and paper cards would be a thing of the past, under a radical overhaul of Australia's airports due to start this year.

The Department of Immigration and Border Protection has sought technology that would abolish incoming passenger cards, remove the need for most passengers to show their passports and replace manned desks with electronic stations and automatic triage.

# Biometrics-only is single-factor identification

**Electronic Identification**

based on open standards

not on patents

(19) **United States**

(12) **Patent Application Publication**

**Sibert et al.**

(10) **Pub. No.: US 2017/0213211 A1**

(43) **Pub. Date: Jul. 27, 2017**

(54) **DOCUMENT IMPORTATION INTO SECURE ELEMENT**

(71) Applicant: **Apple Inc.**, Cupertino, CA (US)

(72) Inventors: **Herve Sibert**, San Francisco, CA (US); **Onur E. Tackin**, Sunnyvale, CA (US); **Matthias Lerch**, Septemes les vallons (FR); **Ahmer A. Khan**, Milpitas, CA (US); **Franck Rakotomalala**, Sunnyvale, CA (US); **Oren M. Elrad**, San Francisco, CA (US)

(21) Appl. No.: **15/415,467**

(22) Filed: **Jan. 25, 2017**

**Related U.S. Application Data**

(60) Provisional application No. 62/286,944, filed on Jan. 25, 2016.

**Publication Classification**

(51) **Int. Cl.**

| | |
|---|---|
| ***G06Q 20/38*** | (2006.01) |
| ***G06Q 20/40*** | (2006.01) |
| ***G06Q 20/32*** | (2006.01) |
| ***H04L 9/32*** | (2006.01) |
| ***H04L 29/06*** | (2006.01) |

(52) **U.S. Cl.**

CPC ..... ***G06Q 20/3829*** (2013.01); ***H04L 9/3263*** (2013.01); ***H04L 63/0428*** (2013.01); ***G06Q 20/3278*** (2013.01); ***G06Q 20/40145*** (2013.01); *G06Q 2220/00* (2013.01)

(57) **ABSTRACT**

Techniques are disclosed relating to authenticate a user with a mobile device. In one embodiment, a computing device includes a short-range radio and a secure element. The computing device reads, via the short-range radio, a portion of credential information stored in a circuit embedded in an identification document issued by an authority to a user for establishing an identity of the user. The computing device issues, to the authority, a request to store the credential information, the request specifying the portion of the credential information. In response to an approval of the request, the computing device stores the credential information in the secure element, the credential information being usable to establish the identity of the user. In some embodiments, the identification document is a passport that includes a radio-frequency identification (RFID) circuit storing the credential information, and the request specifies a passport number read from the RFID circuit.

# EIDAS Regulation

The European Perspective on Interoperating eIDs

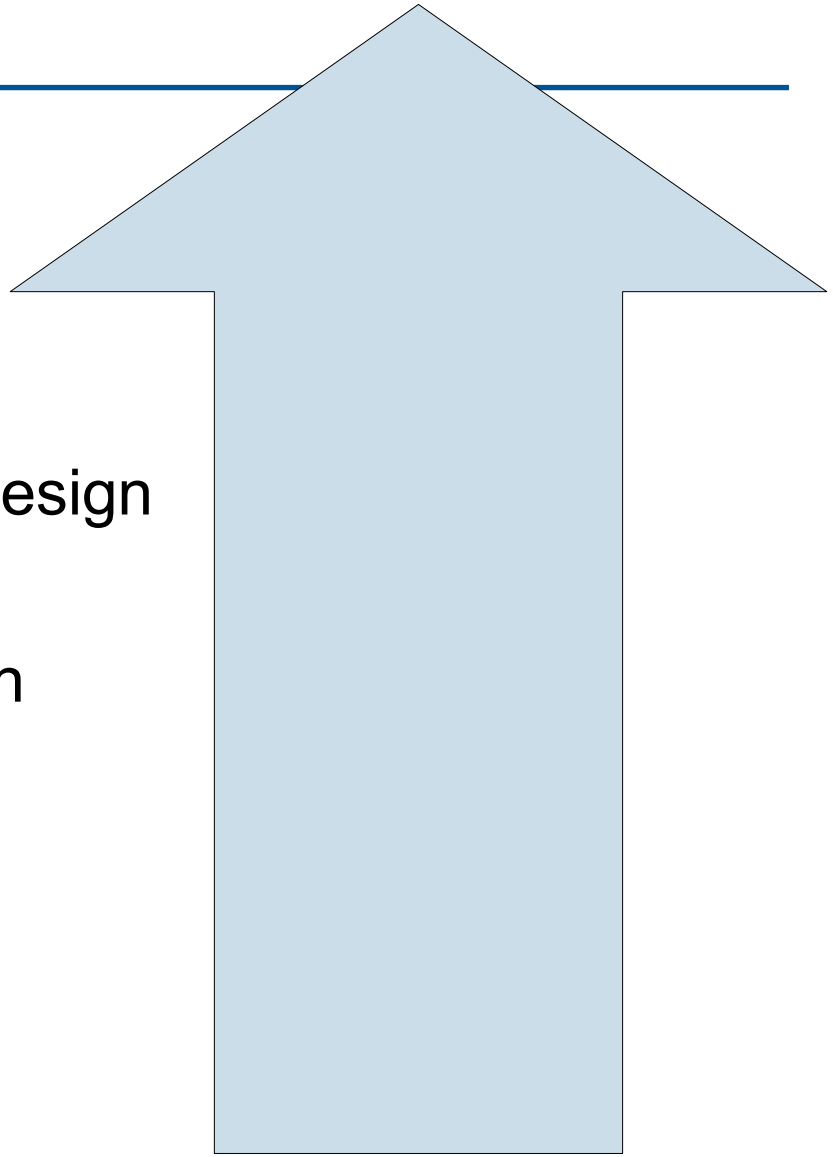
Federal Office
for Information Security

# eIDAS Level of Assurance

- Enrollment
- Identification Means Management
  - Identification means characteristics & design
  - Issuance, delivery and activation
  - Suspension, revocation and reactivation
  - Renewal and replacement.
- ***Authentication***
- Management & Organization

Federal Office
for Information Security

# eIDAS Level of Assurance

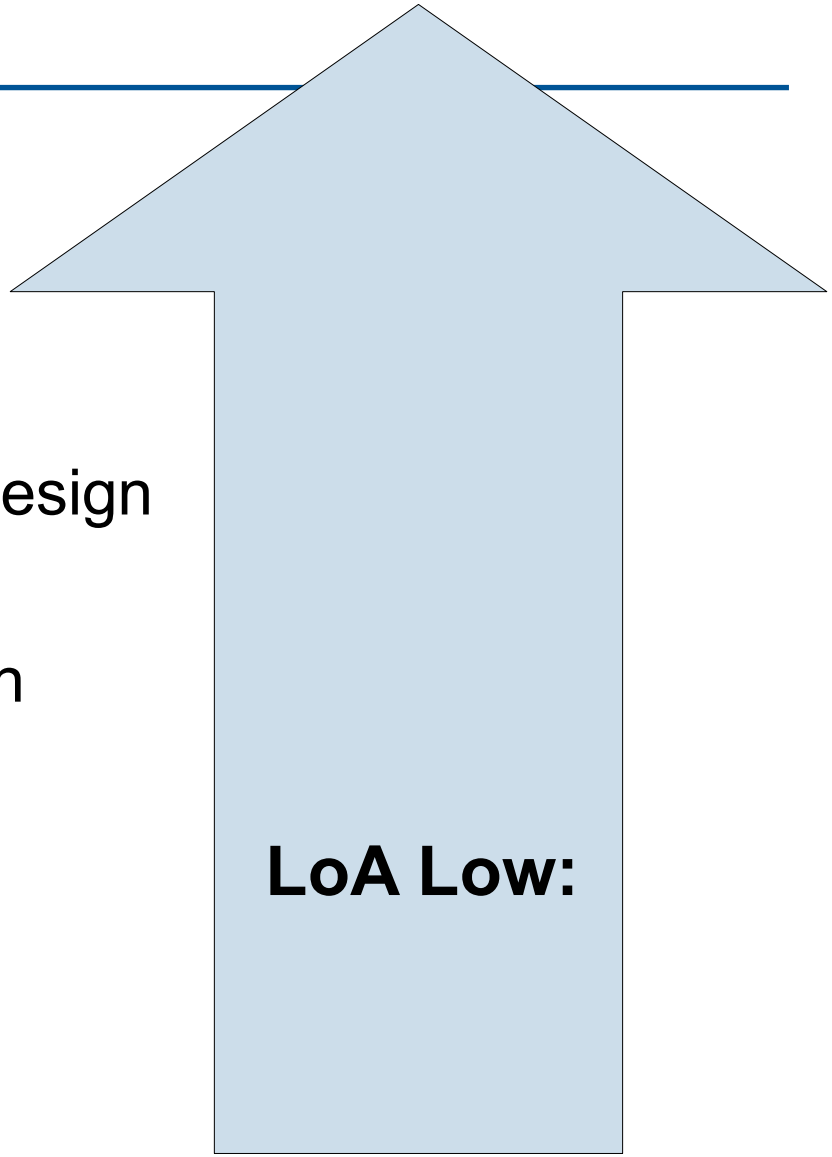


- Enrollment
- Identification Means Management
  - Identification means characteristics & design
  - Issuance, delivery and activation
  - Suspension, revocation and reactivation
  - Renewal and replacement.
- ***Authentication***
- Management & Organization

Federal Office
for Information Security

# eIDAS Level of Assurance

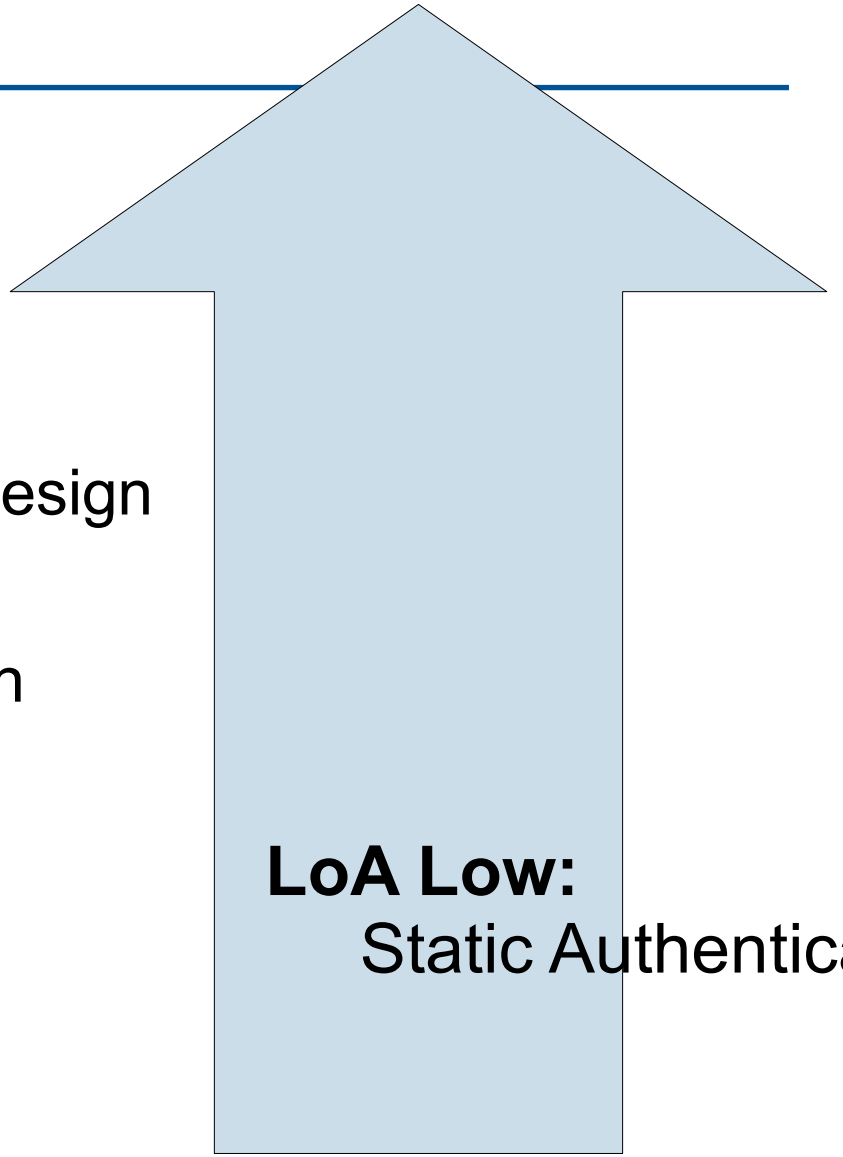
- Enrollment
- Identification Means Management
  - Identification means characteristics & design
  - Issuance, delivery and activation
  - Suspension, revocation and reactivation
  - Renewal and replacement.
- ***Authentication***
- Management & Organization



Federal Office
for Information Security

# eIDAS Level of Assurance

- Enrollment
- Identification Means Management
  - Identification means characteristics & design
  - Issuance, delivery and activation
  - Suspension, revocation and reactivation
  - Renewal and replacement.
- ***Authentication***
- Management & Organization

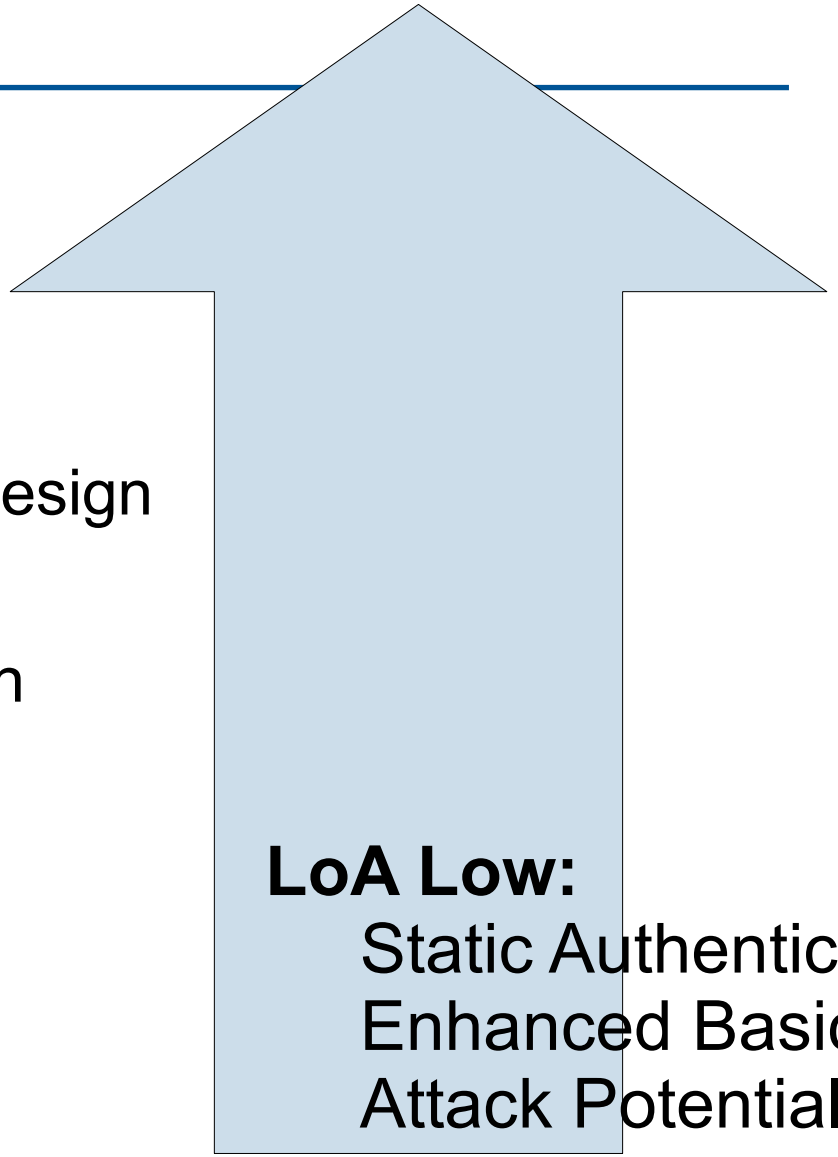


**LoA Low:**
Static Authentication

Federal Office
for Information Security

# eIDAS Level of Assurance

- Enrollment
- Identification Means Management
  - Identification means characteristics & design
  - Issuance, delivery and activation
  - Suspension, revocation and reactivation
  - Renewal and replacement.
- ***Authentication***
- Management & Organization



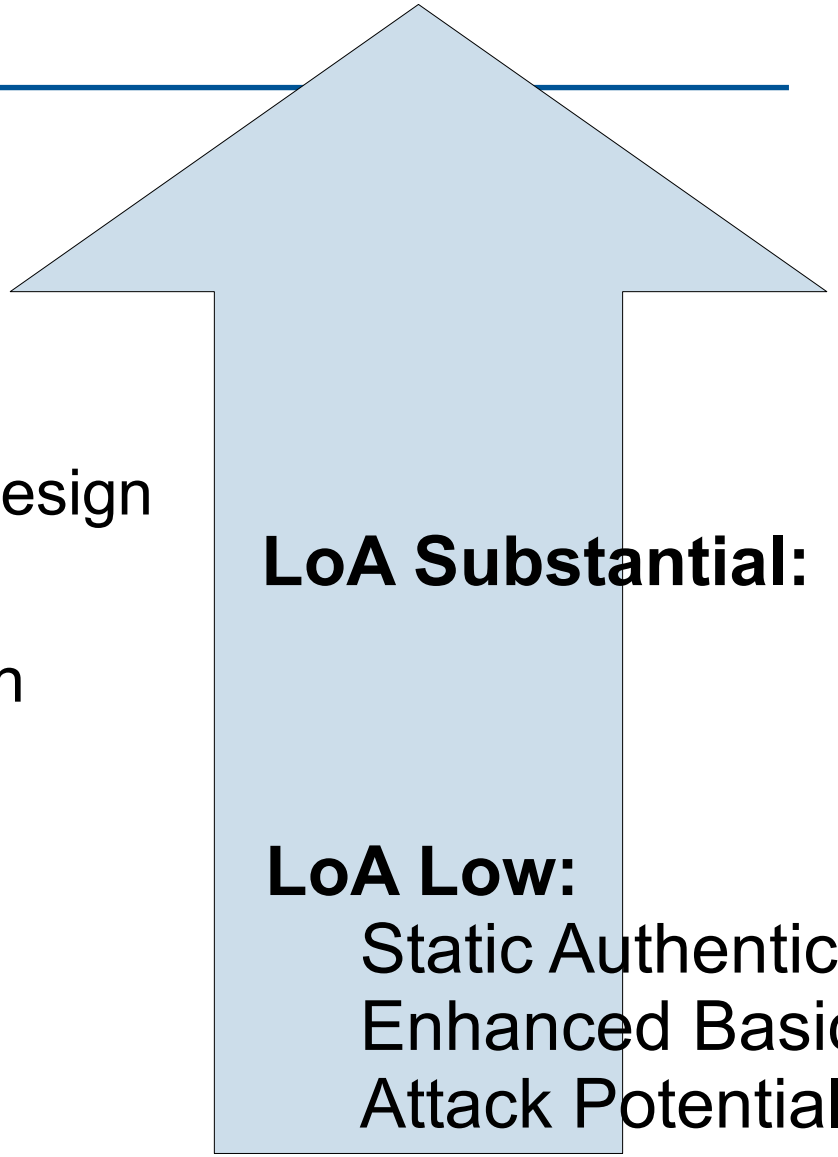
**LoA Low:**

Static Authentication
Enhanced Basic
Attack Potential

Federal Office
for Information Security

# eIDAS Level of Assurance

- Enrollment
- Identification Means Management
  - Identification means characteristics & design
  - Issuance, delivery and activation
  - Suspension, revocation and reactivation
  - Renewal and replacement.
- ***Authentication***
- Management & Organization



**LoA Substantial:**

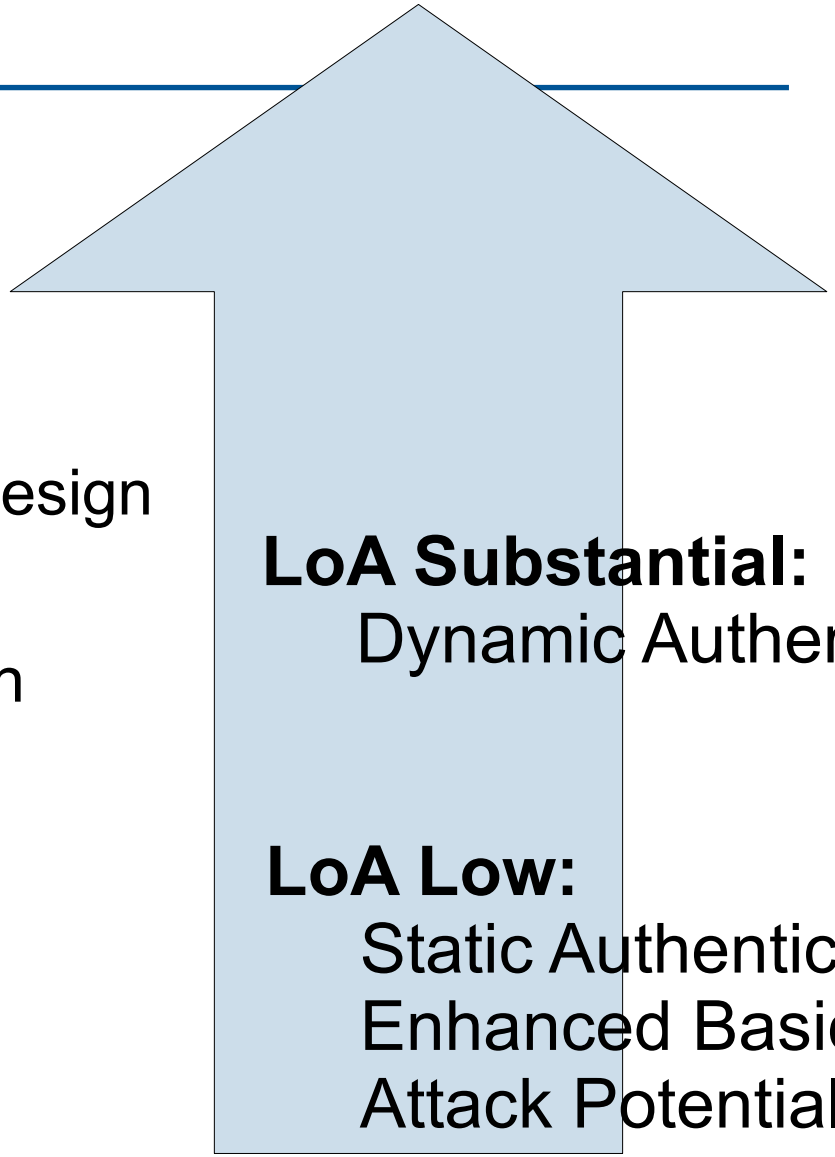
**LoA Low:**

Static Authentication
Enhanced Basic
Attack Potential

Federal Office
for Information Security

# eIDAS Level of Assurance

- Enrollment
- Identification Means Management
  - Identification means characteristics & design
  - Issuance, delivery and activation
  - Suspension, revocation and reactivation
  - Renewal and replacement.
- ***Authentication***
- Management & Organization



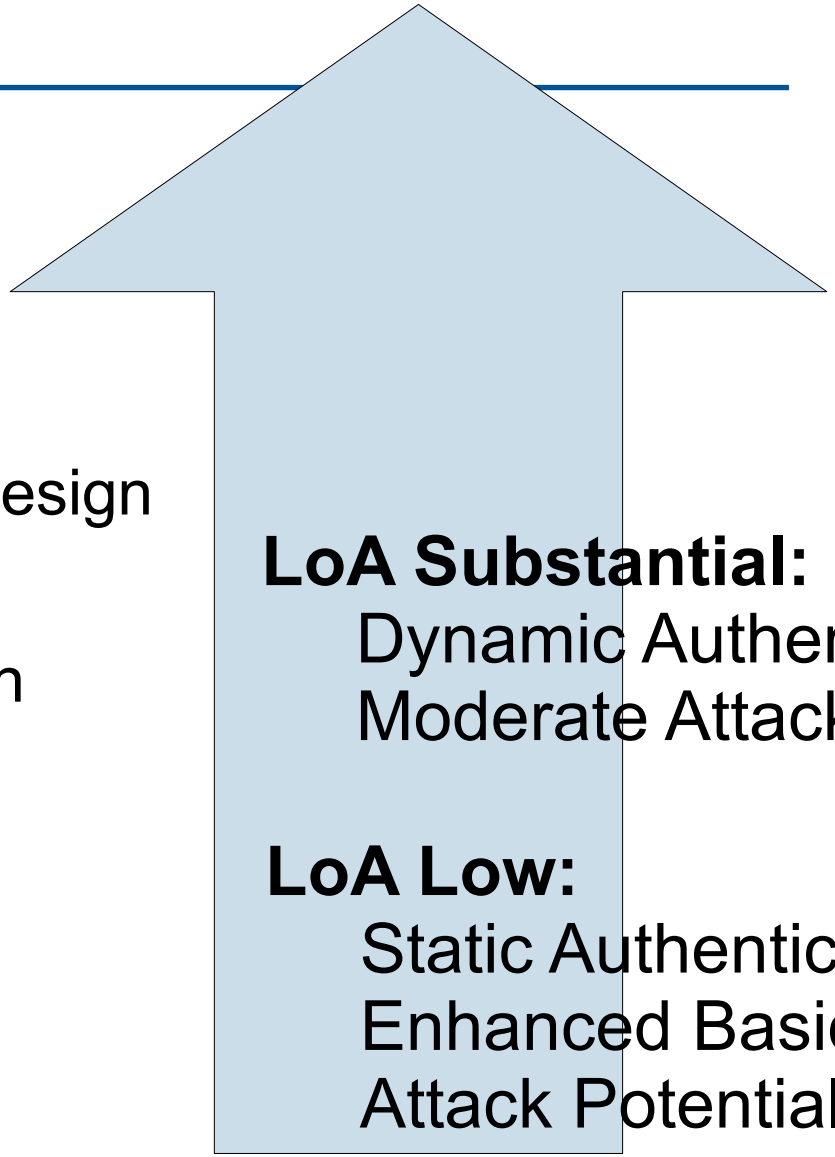
**LoA Substantial:**
Dynamic Authentication

**LoA Low:**
Static Authentication
Enhanced Basic
Attack Potential

Federal Office
for Information Security

# eIDAS Level of Assurance

- Enrollment
- Identification Means Management
  - Identification means characteristics & design
  - Issuance, delivery and activation
  - Suspension, revocation and reactivation
  - Renewal and replacement.
- ***Authentication***
- Management & Organization



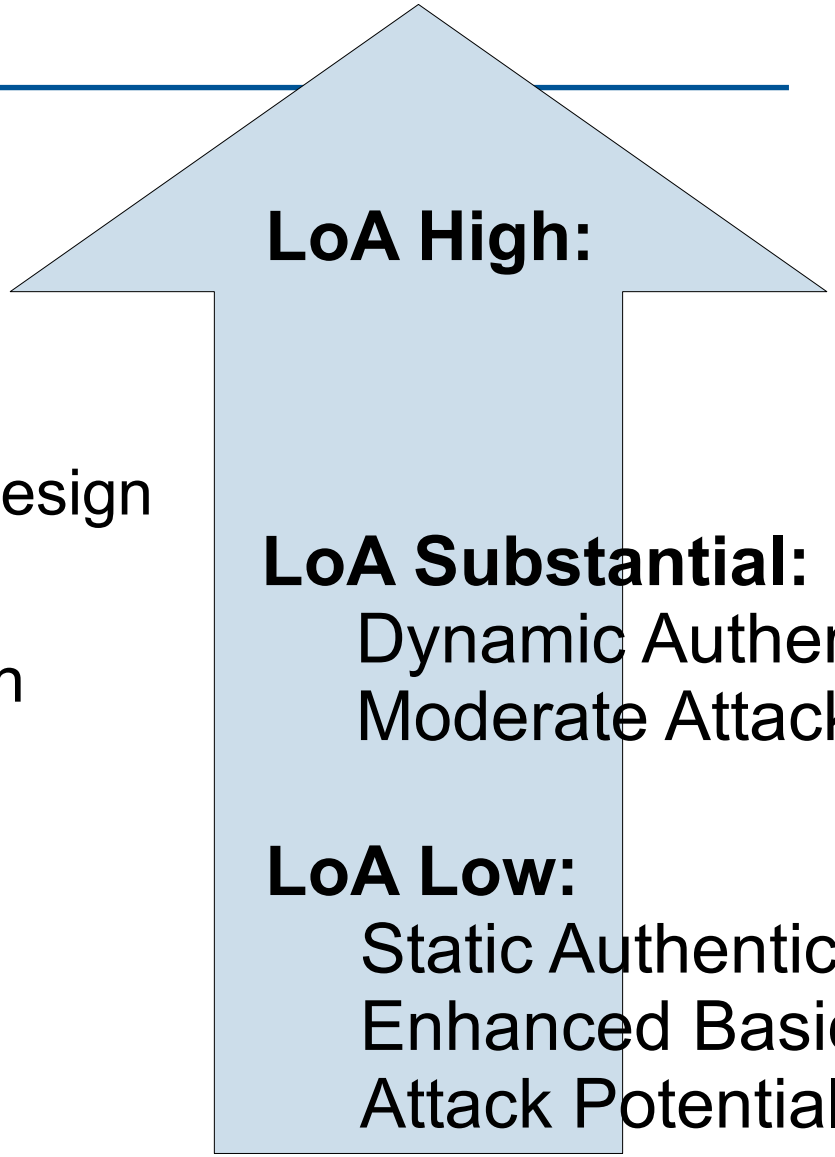
**LoA Substantial:**
Dynamic Authentication
Moderate Attack Potential

**LoA Low:**
Static Authentication
Enhanced Basic
Attack Potential

Federal Office
for Information Security

# eIDAS Level of Assurance

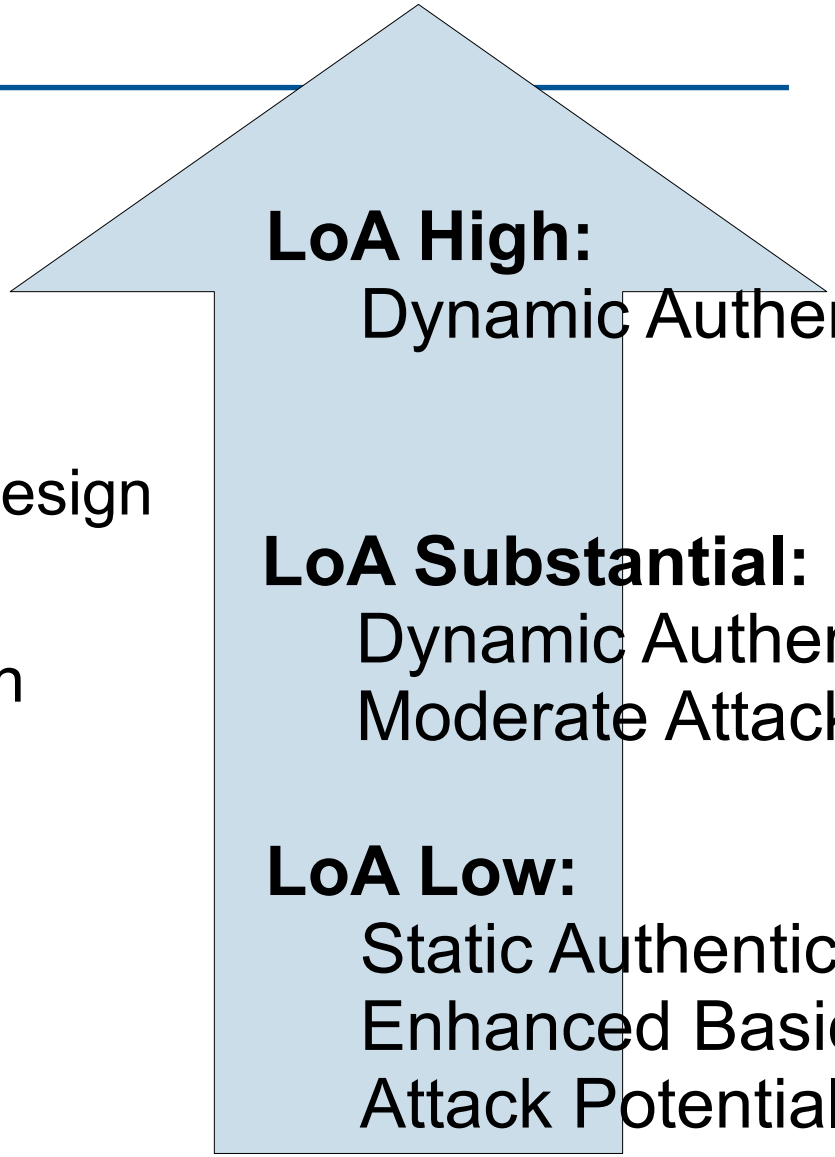
- Enrollment
- Identification Means Management
  - Identification means characteristics & design
  - Issuance, delivery and activation
  - Suspension, revocation and reactivation
  - Renewal and replacement.
- ***Authentication***
- Management & Organization



Federal Office
for Information Security

# eIDAS Level of Assurance

- Enrollment
- Identification Means Management
  - Identification means characteristics & design
  - Issuance, delivery and activation
  - Suspension, revocation and reactivation
  - Renewal and replacement.
- ***Authentication***
- Management & Organization



**LoA High:**
Dynamic Authentication

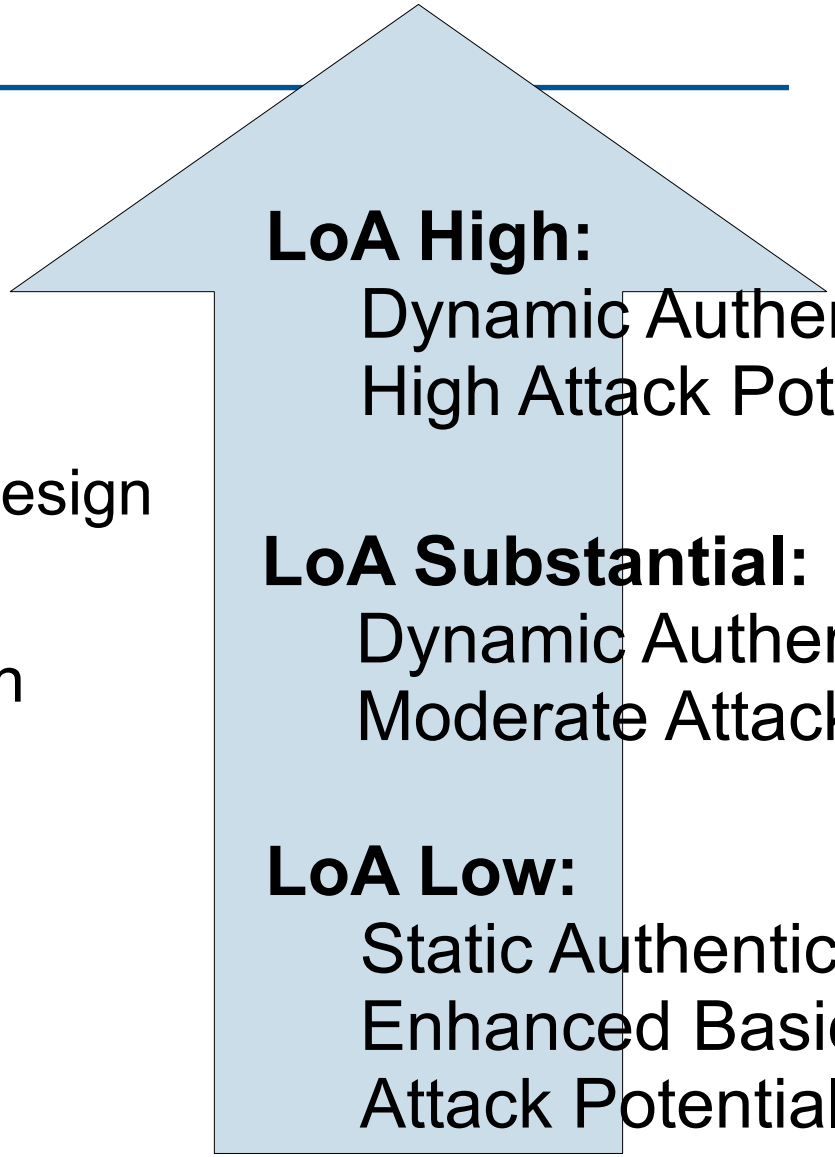
**LoA Substantial:**
Dynamic Authentication
Moderate Attack Potential

**LoA Low:**
Static Authentication
Enhanced Basic
Attack Potential

Federal Office
for Information Security

# eIDAS Level of Assurance

- Enrollment
- Identification Means Management
  - Identification means characteristics & design
  - Issuance, delivery and activation
  - Suspension, revocation and reactivation
  - Renewal and replacement.
- ***Authentication***
- Management & Organization



**LoA High:**
Dynamic Authentication
High Attack Potential

**LoA Substantial:**
Dynamic Authentication
Moderate Attack Potential

**LoA Low:**
Static Authentication
Enhanced Basic
Attack Potential

# COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502

eIDAS  Assurance levels of electronic identification schemes

- Low, **Substantial**, High

Authentication @ Substantial

- The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.

# COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502

eIDAS  Assurance levels of electronic identification schemes

- Low, **Substantial**, High

Authentication @ Substantial

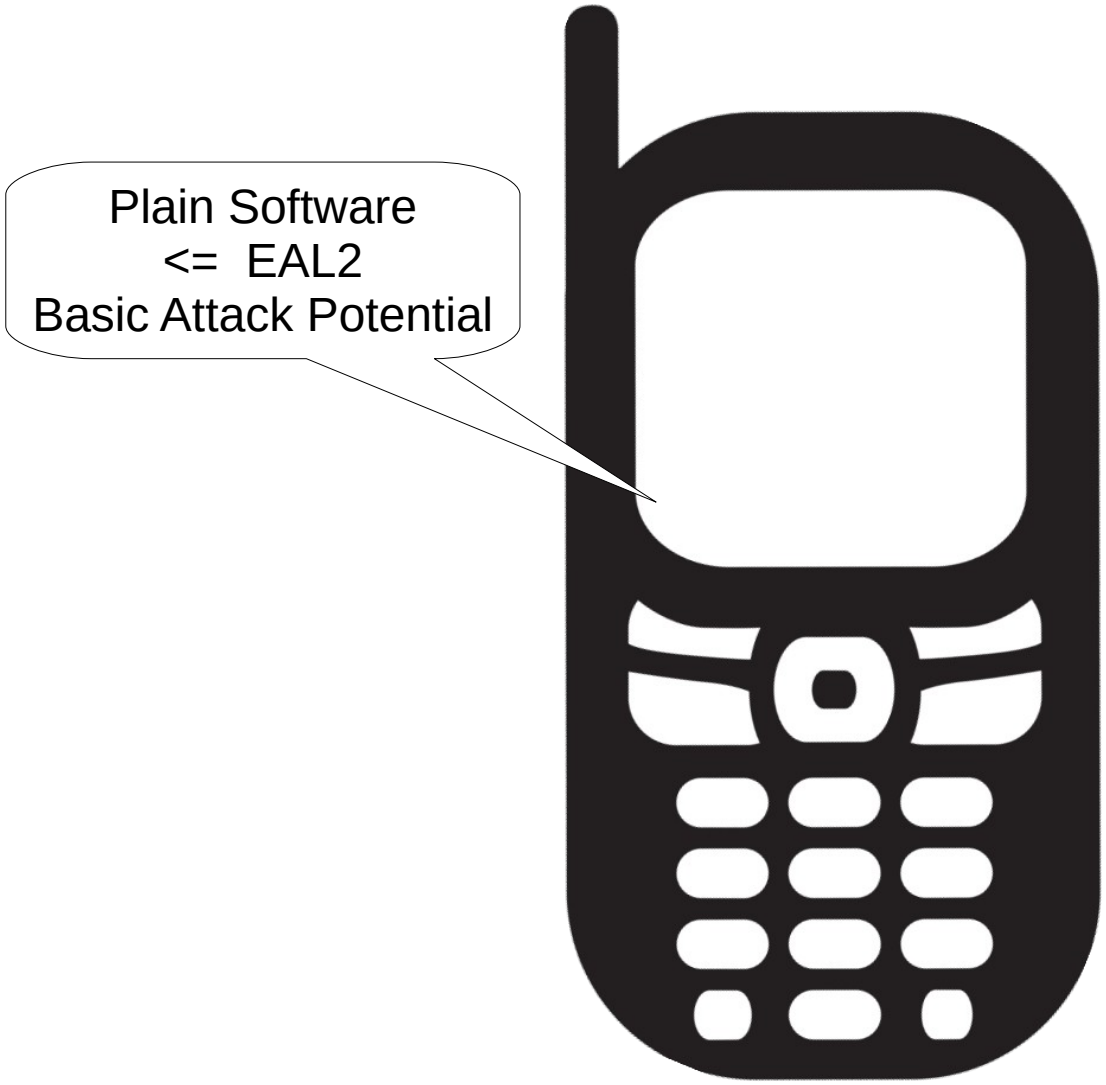
- The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.

Common Criteria
AVA_VAN.4

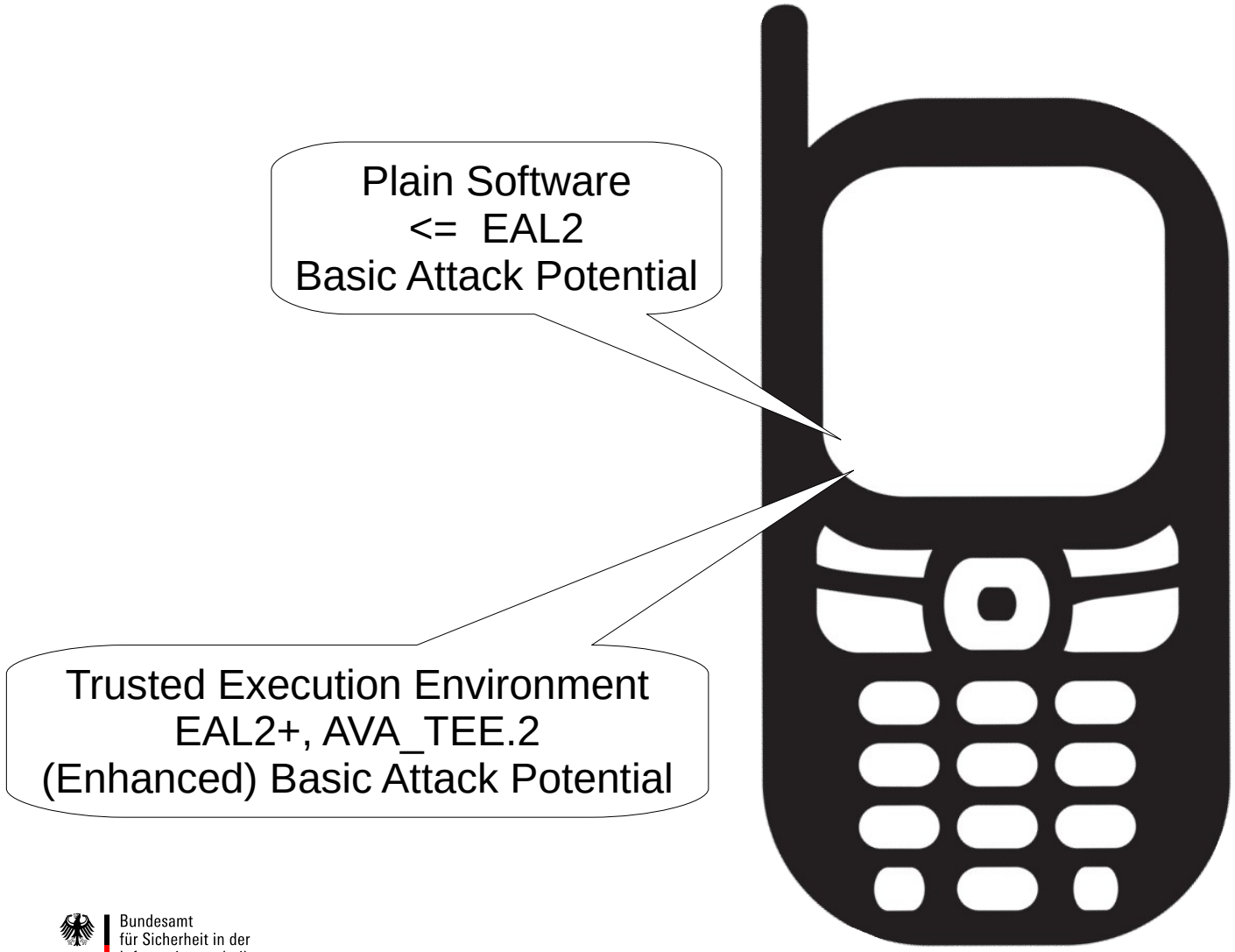
# Mobile eID resisting Moderate Attack Potential?

Bundesamt
für Sicherheit in der
Informationstechnik

# Mobile eID resisting Moderate Attack Potential?

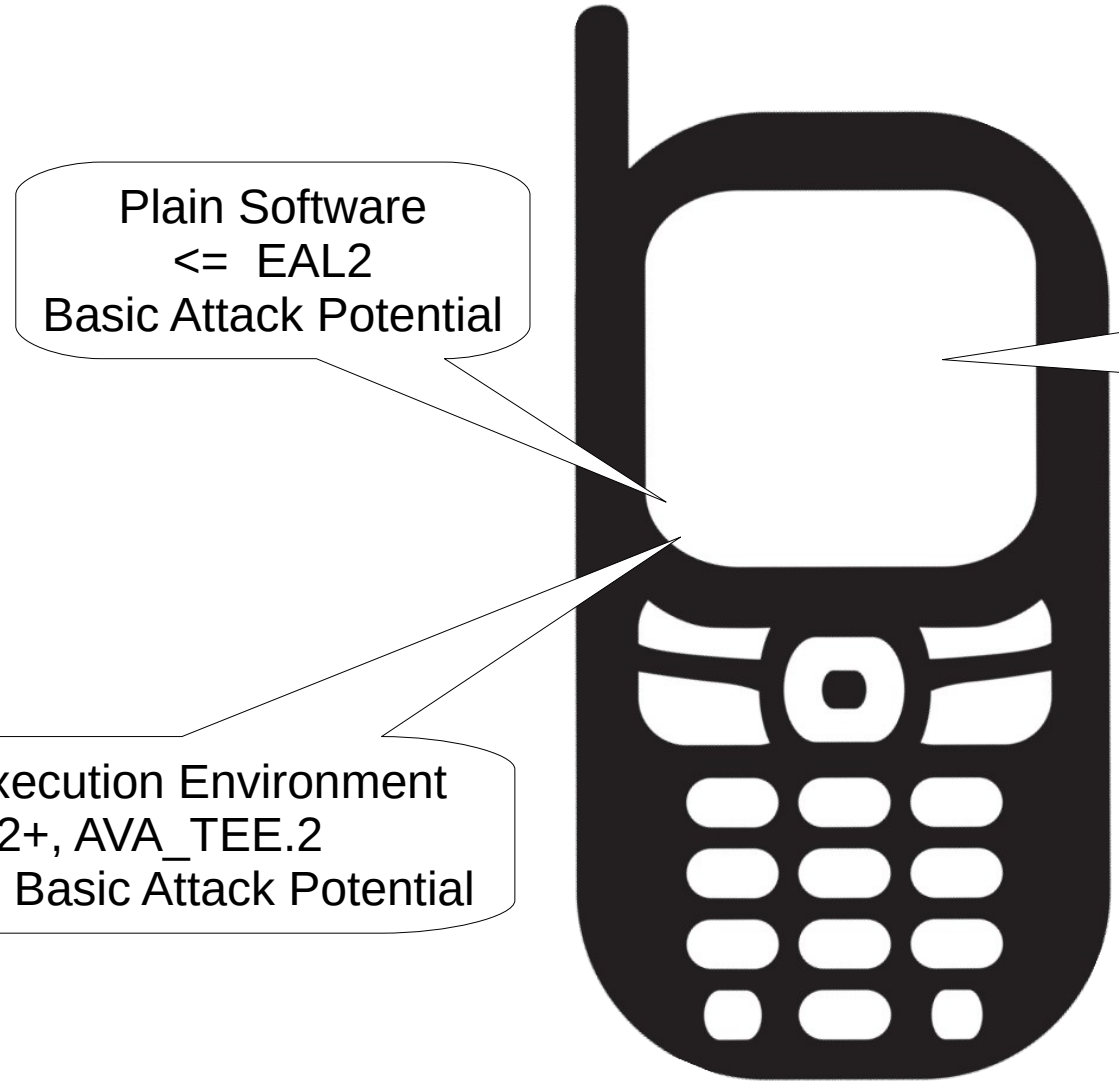


# Mobile eID resisting Moderate Attack Potential?




Bundesamt
für Sicherheit in der
Informationstechnik

# Mobile eID resisting Moderate Attack Potential?



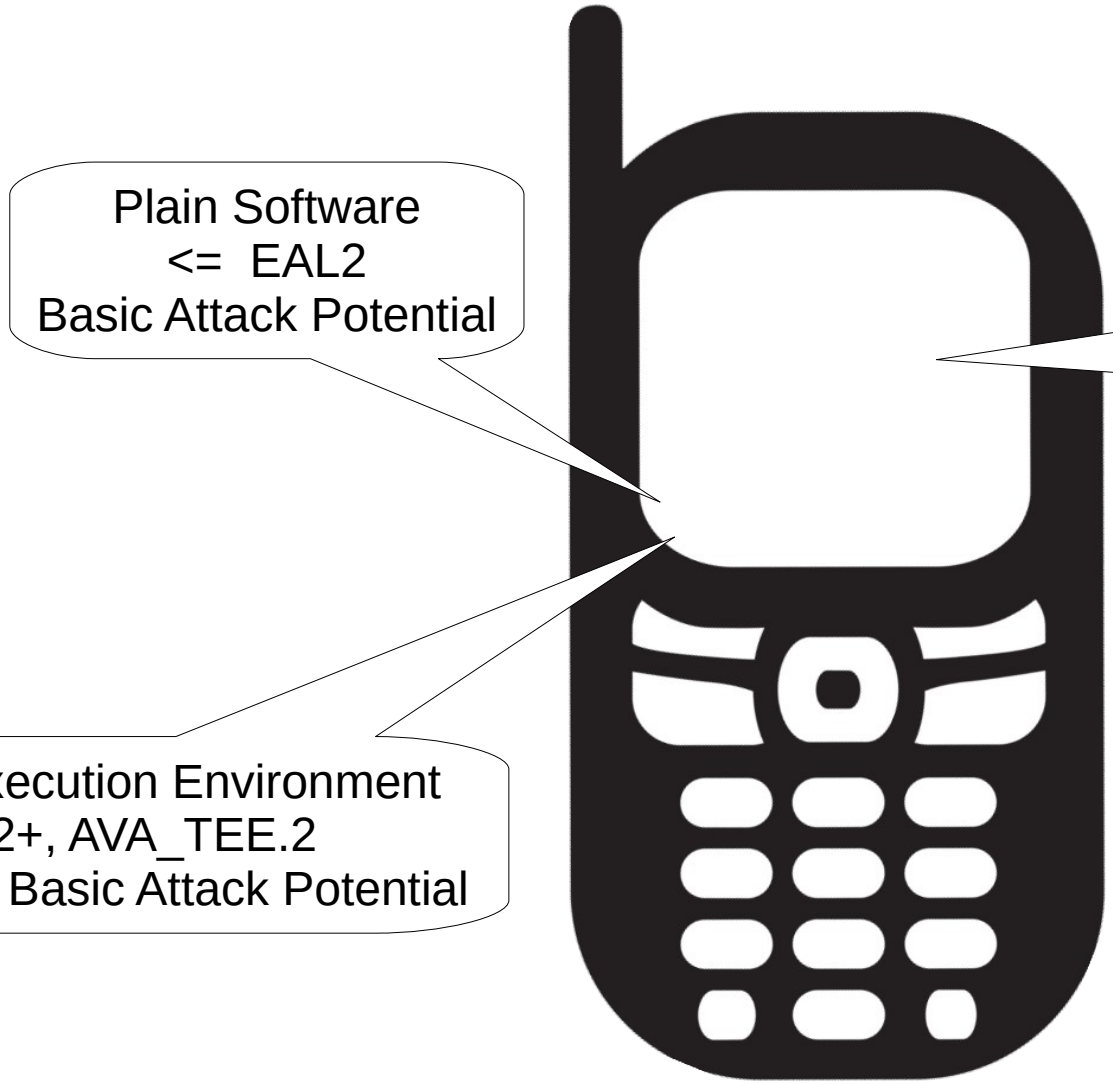
Plain Software
<= EAL2
Basic Attack Potential

Secure Element
EAL4+, AVA_VAN.5
High Attack Potential

Trusted Execution Environment
EAL2+, AVA_TEE.2
(Enhanced) Basic Attack Potential

Bundesamt
für Sicherheit in der
Informationstechnik

# Mobile eID resisting Moderate Attack Potential?



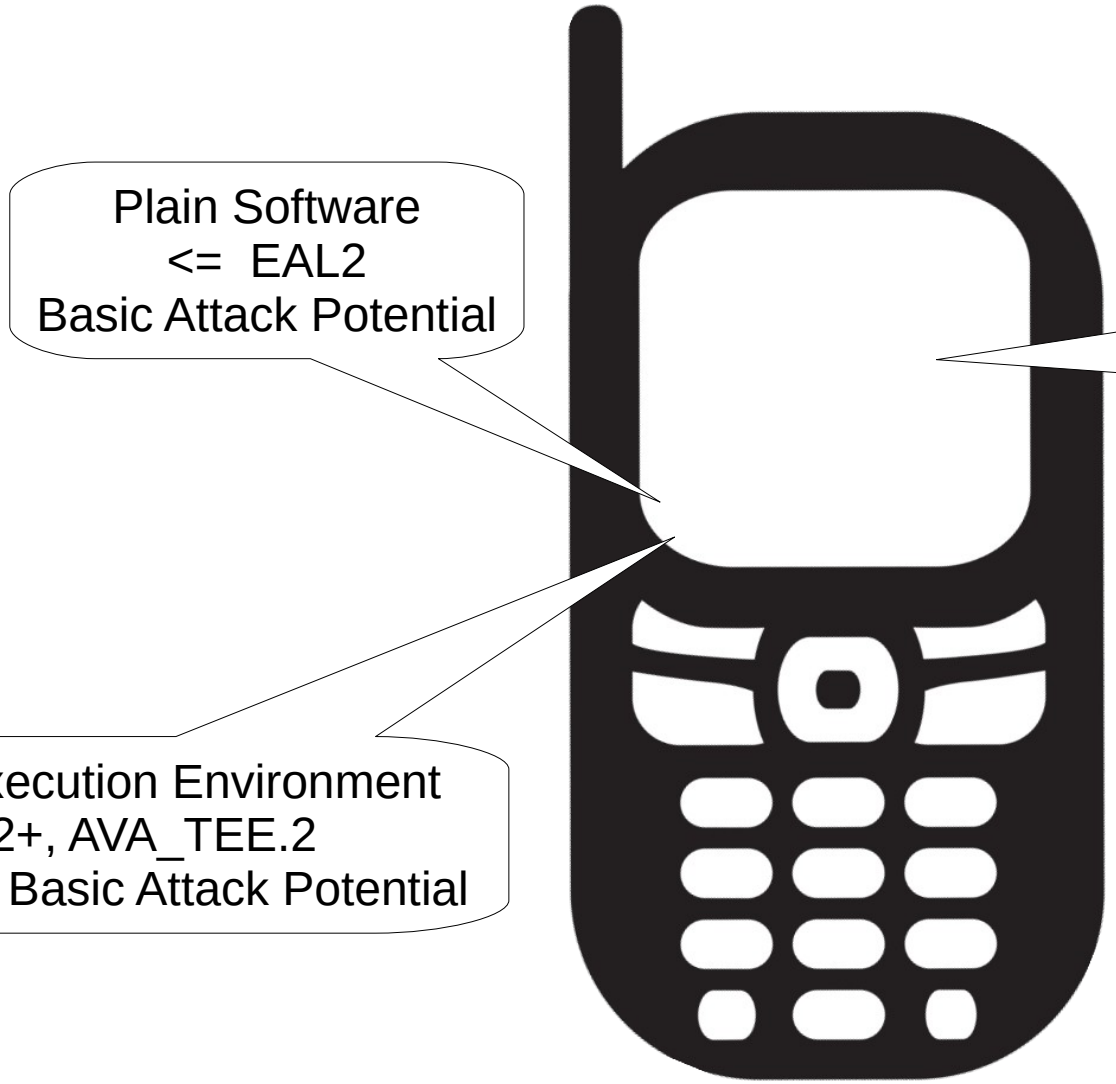
Plain Software
<= EAL2
Basic Attack Potential

Secure Element
EAL4+, AVA_VAN.5
High Attack Potential

**Requires Composite Certification**

Trusted Execution Environment
EAL2+, AVA_TEE.2
(Enhanced) Basic Attack Potential

# Mobile eID resisting Moderate Attack Potential?



Plain Software
<= EAL2
Basic Attack Potential

Secure Element
EAL4+, AVA_VAN.5
High Attack Potential

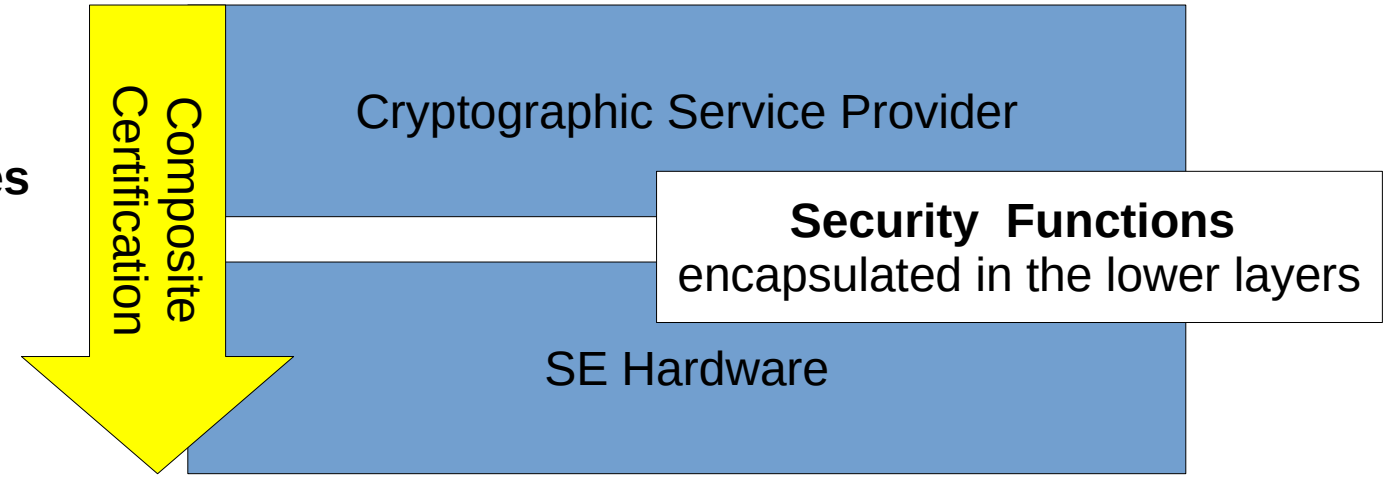
**Requires Composite Certification**
**… too much effort?**

Trusted Execution Environment
EAL2+, AVA_TEE.2
(Enhanced) Basic Attack Potential

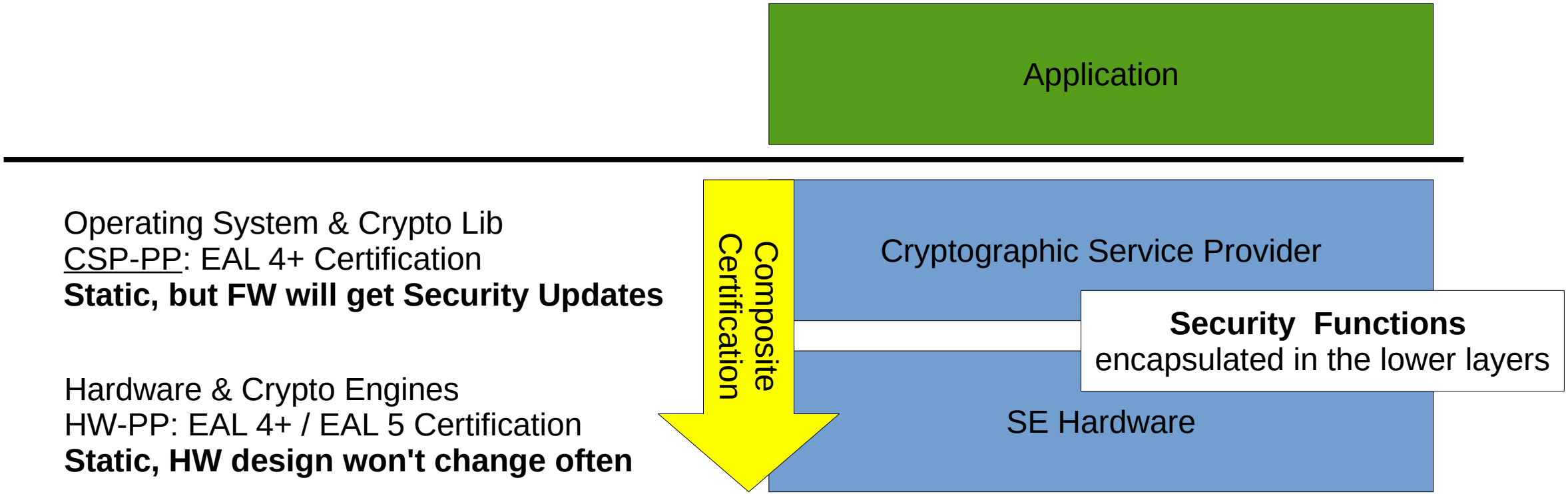
# Cryptographic Service Provider Architecture for Secure Elements

Operating System & Crypto Lib
CSP-PP: EAL 4+ Certification
**Static, but FW will get Security Updates**

Hardware & Crypto Engines
HW-PP: EAL 4+ / EAL 5 Certification
**Static, HW design won't change often**



# Cryptographic Service Provider Architecture for Secure Elements

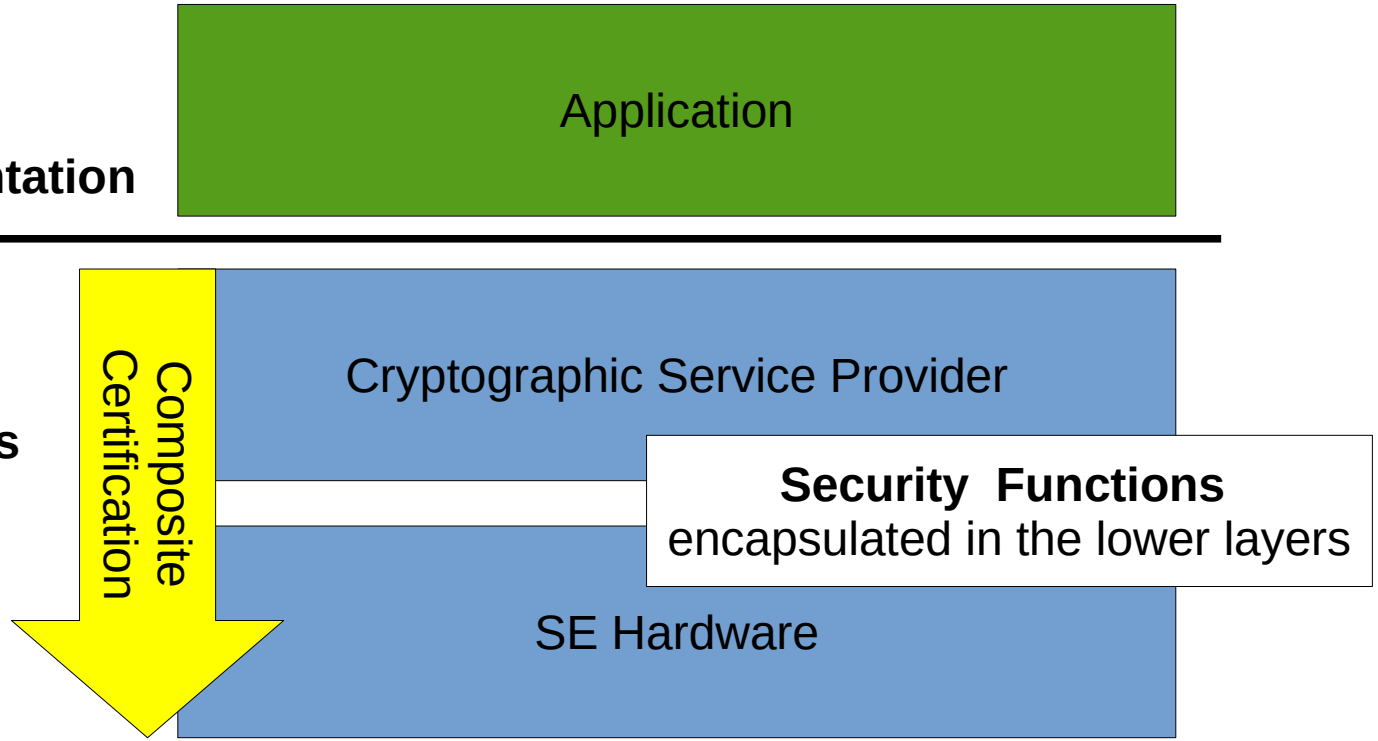


# Cryptographic Service Provider Architecture for Secure Elements

Application Logic
EAL 2 Certification or higher if desired
**Product/Application-specific implementation**

Operating System & Crypto Lib
CSP-PP: EAL 4+ Certification
**Static, but FW will get Security Updates**

Hardware & Crypto Engines
HW-PP: EAL 4+ / EAL 5 Certification
**Static, HW design won't change often**

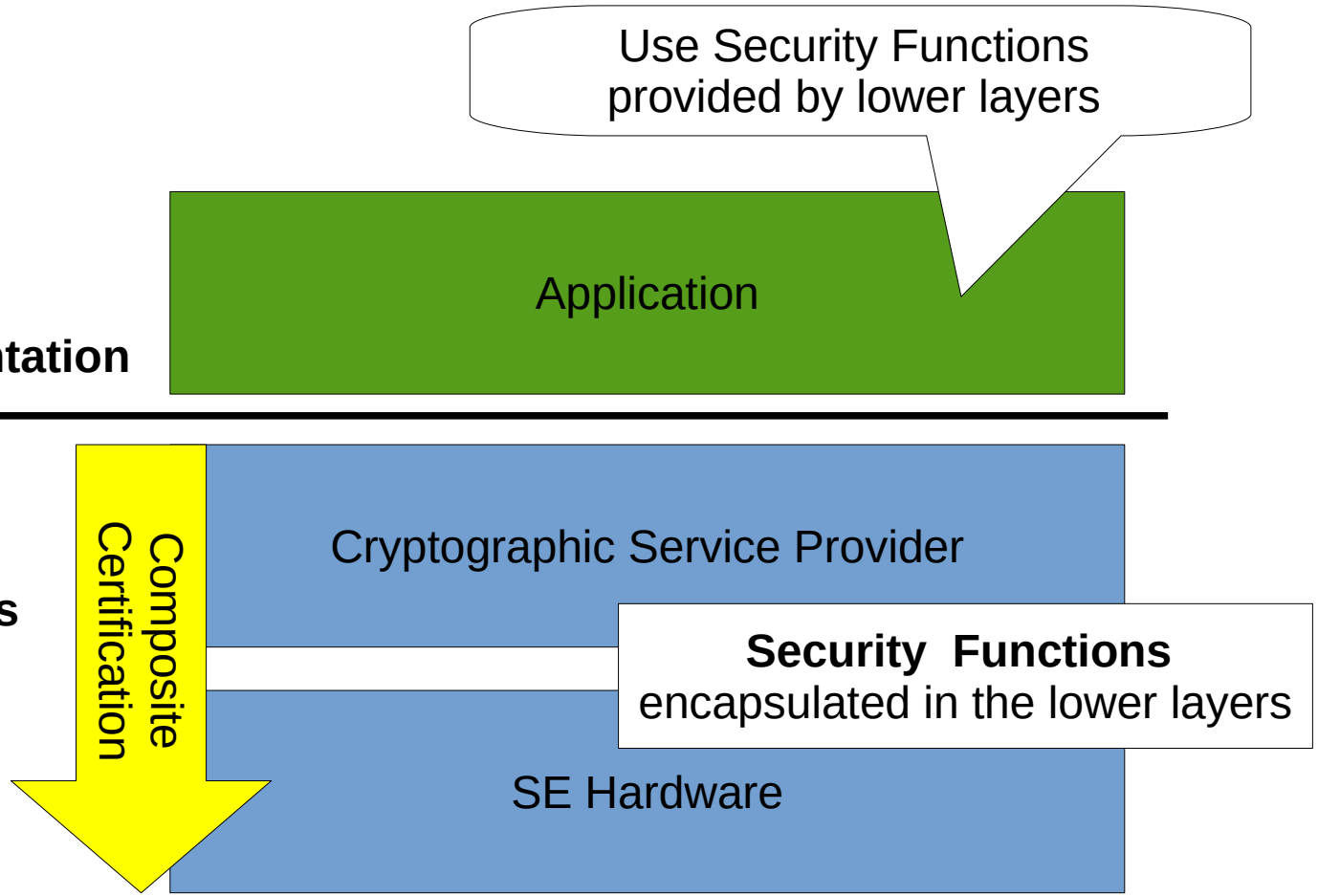


# Cryptographic Service Provider Architecture for Secure Elements

Application Logic
EAL 2 Certification or higher if desired
**Product/Application-specific implementation**

Operating System & Crypto Lib
CSP-PP: EAL 4+ Certification
**Static, but FW will get Security Updates**

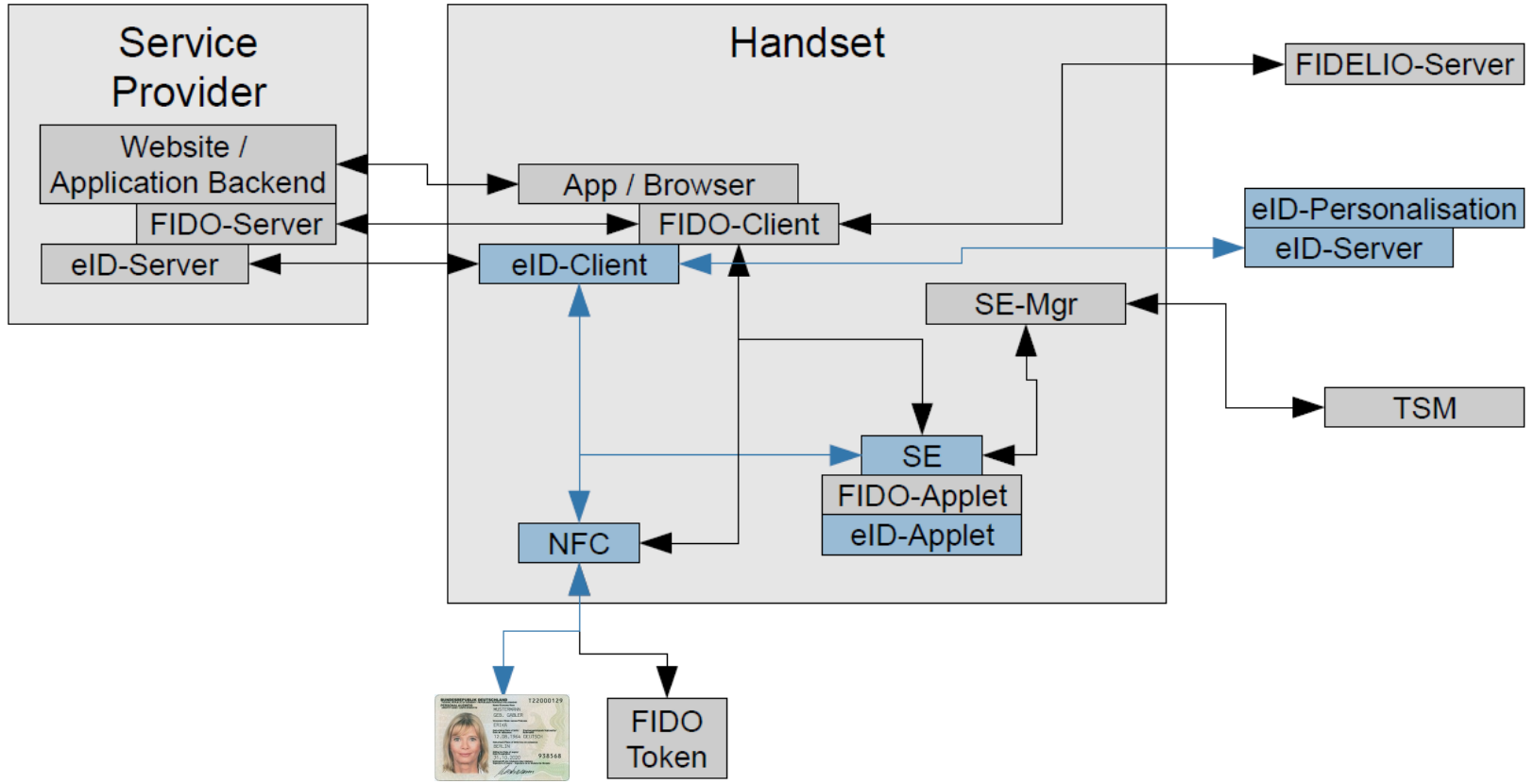
Hardware & Crypto Engines
HW-PP: EAL 4+ / EAL 5 Certification
**Static, HW design won't change often**



# BSI Technical Guideline TR-03159
# Mobile Identities

Part 1: *Security Requirements for eIDAS LoA "substantial"*
- Requirements from eIDAS Regulation (and GDPR)

Part 2: *EAC and FIDO based mobile identities*
- Requirements for the German eID System
- Secure Element with **CSP**
  - eID Appliet
  - FIDO Applet



Next Speaker

**Dr. Henry Lee**

Senior Vice President, Mobile Security Technologies,
Samsung Electronics Co., Ltd.

# Thank you
# for your attention!

## Contact

Dr. Dennis Kügler
Head of Center of Excellence “Chip Security“
dennis.kuegler@bsi.bund.de
Tel. +49 (0) 228 99 9582 5183
Fax +49 (0) 228 99 109582 5183

Federal Office for Information Security
Section TK11
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

Federal Office
for Information Security