



Mit freundlicher Unterstützung:



Informationstag

"Elektronische Signatur und Vertrauensdienste"

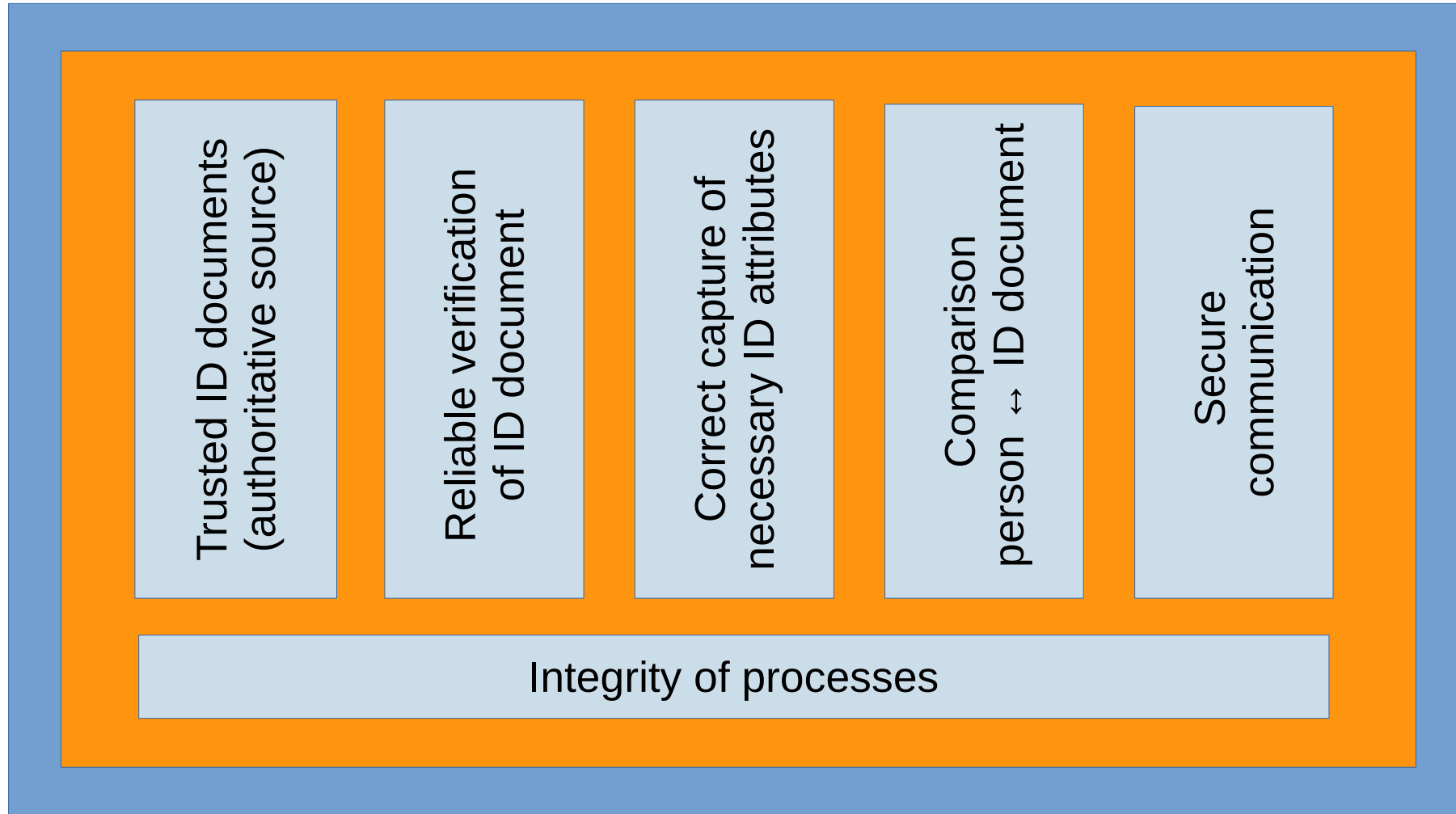
Gemeinsame Veranstaltung von TeleTrust und VOI

Berlin, 18.09.2018

Verifikation der Identität – Verwendung des nPA

Guido Frank, BSI

Bausteine verlässlicher Identitätsprüfung



Personalausweis

Staatlich verifizierte Identitätsdaten (Vertrauensanker)

Vorlage des physischen Dokuments

Fälschungssicheres physikalisches Dokument („Verlässliche Quelle“)

Elektronischer Identitätsnachweis

Elektronische Sicherheitsmerkmale

1-14 Multicoloured guilloches. Guilloches are security patterns that are made up of fine, interlaced lines. In reproductions, the line structures of the original are resolved into dotted screen structures. The central motif of the guilloche lines depicts the German eagle on the front and the Brandenburg Gate on the back of the card.

2-15 Microlettering. The positive and negative microtext "BUNDESREPUBLIK DEUTSCHLAND" is integrated into the security background printing.

3-16 UV overprint. The guilloche design luminesces in various colours under UV light. A UV overprint is additionally included on the front depicting the German eagle and endless text "BUNDESREPUBLIK DEUTSCHLAND".

4 Optically variable inks. When the card is tilted, the headline "BUNDESREPUBLIK DEUTSCHLAND" changes from green to blue depending on the viewing angle.

5 Holographic portrait. The portrait becomes visible as a holographic image on the right side of the conventional photograph when viewed at a flat angle. Four eagle designs are incorporated into the secondary portrait.

6 3D eagle. Depending on the angle at which the card is viewed, a 3D image of the German eagle appears in red on top of the six-digit card access number.

7 Kinematic structures. Kinematic structures are arranged above the conventional photograph and show a German eagle surrounded by twelve stars. When the card is tilted, the



motif changes from the eagle to a hexagonal structure and then to the letter "D". In addition, the hexagons move up and down while the stars change in size.

8 Macrolettering. On the left edge of the conventional photograph a curved band of macrolettering "BUNDESREPUBLIK DEUTSCHLAND" appears in the hologram. Several parallel lines of microlettering with the same text connect with the macrolettering.



9 Contrast reversal. When the card is tilted, the contrast of the kinematic eagle motif is reversed. The bright eagle then appears dark on a bright hexagon.

10 Machine-verifiable structure. The Identigram® features a structure that enables in addition to a visual inspection an automated authenticity check of the ID card. This structure does not contain any personal or document-related data.

11 Colour integration technology (InnoSec®FUSION). The colour photograph is securely integrated into the card material via the InnoSec®FUSION personalisation system. The same technology is also used for the alpha-numeric serial number (OCR-B font).



12-20 Laser engraving. All the personalisation data (except for the photograph and the serial number) is laser-engraved in high contrast into the inner card layers.

21 Tactile features. The expiry date and the six-digit card access number on the front of the ID card are laser-engraved and tactile.

17 Logo of the ID card. The logo is depicted on the back of the card. Beginning November 2010, this logo also identifies applications and reader devices which support the new ID card.

18 Fluorescent fibres. Transparent fluorescent fibres are integrated into the layers on the back of the card. They are randomly distributed and luminescent under UV light.

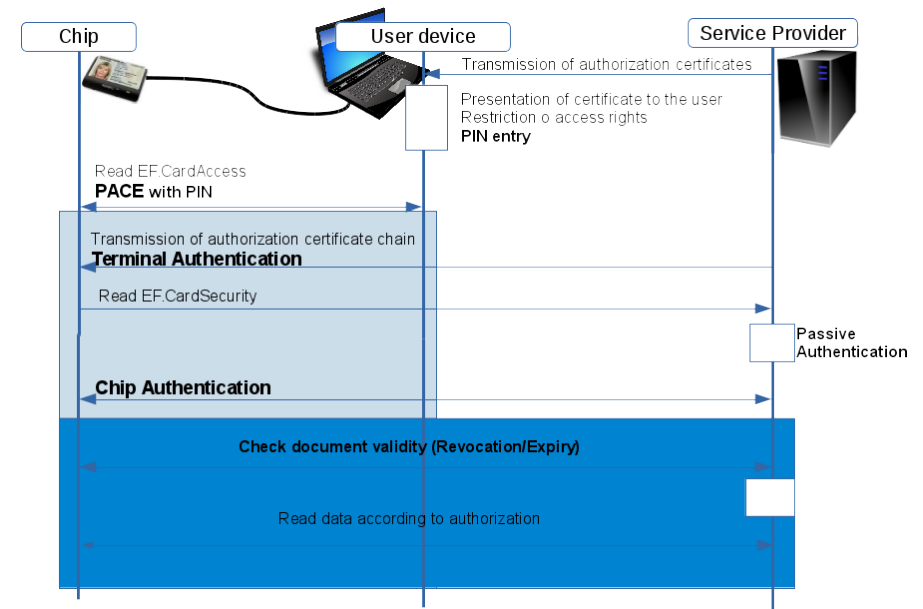
19 Surface embossing. Security-embossed microlettering and a map of Germany on the back of the card provide the document with a relief-type, tactile surface in the upper left-hand part of the card.

21 Changeable Laser Image. Depending on the viewing angle, the date of expiry or the portrait of the holder becomes visible in the Changeable Laser Image (CLI).

22 Machine-readable zone. The machine-readable zone on the back of the card includes the document type, issuing country, serial number, date of birth, expiry date, nationality along with the name and check digits in machine-readable format (OCR-B).

23 Personalised security thread. A horizontal, machine-verifiable security thread is embedded into the back of the card. This thread is personalised with the document number and the name of the ID card holder.

Later changes in address will be indicated on a label that can be protected by a transparent foil. The security paper used for the label is printed with a guilloche design in two colours and includes special fibres that are luminescent in various colours under UV light. In addition to the new address, the label will also contain the serial number of the ID card and the seal of the respective authority.



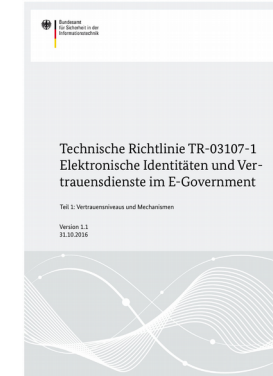
Bundesamt
für Sicherheit in der
Informationstechnik

Kategorisierung in Vertrauensniveaus

- „Normal“ / „Niedrig“
- „Substantiell“
- „Hoch“

VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES
vom 23. Juli 2014
über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im
Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

§§ CIR (EU) 2015/1502 §§



Enrolment	eID-Management	Authentifizierung	Management & Organisation
•Antragstellung •Registrierung •Identitätsprüfung	•Design des Identifizierungsmittels •Ausstellung •Aussetzung •Erneuerung und Ersatz	•Authentisierungsmechanismus	•Informationssicherheitsmanagement (ISM) •Aktenführung •Einrichtungen und Mitarbeiter •Kontrollen •Einhaltung und Überprüfung

Identifizierungsmittel

- **Ein-Faktor-Authentisierung**
- **Zwei-Faktor-Authentisierung**
- **Schutz gegen Duplizierung und Fälschung**

Authentisierung

- **Dynamische Authentisierung**
- **Schutz vor Handlungen wie Erraten, Abhören, Replay oder Manipulation der Kommunikation gemäß Angriffspotential**

Angriffspotential

- „enhanced-basic“
- „moderate“
- „high“



Notifizierung der eID-Funktion

Erste eIDAS-Notifizierung durch Deutschland

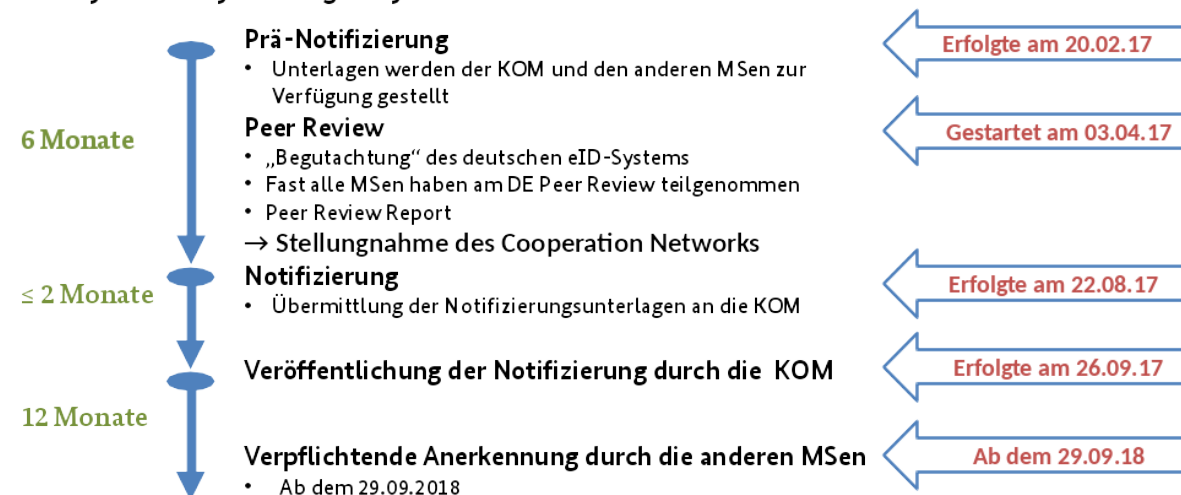


Notifizierung auf Vertrauensniveau ‚hoch‘

<https://www.bsi.bund.de/eIDAS-Notifizierung>

→ Ab dem 29.09.2018 müssen öffentliche Stellen anderer MS die Online-Ausweisfunktion in elektronischen Verwaltungsverfahren anerkennen. Auch Unternehmen können die eID-Funktion anerkennen.

Ablauf des Notifizierungsverfahrens



Gesetz zur Förderungen des elektronischen Identitätsnachweises

- **Förderung der eID-Funktion**
 - Einschaltung der eID-Funktion bei der Ausgabe
 - Vereinfachung des Prozesses zur Vergabe von Berechtigungszertifikaten
 - Entfall der dienstbezogenen, präventiven Erforderlichkeitsprüfung, aber weiterhin datenschutzrechtlicher Erforderlichkeitsgrundsatz
 - Organisationsbezogene Berechtigungen für Diensteanbieter
- **Erweiterung der Anwendungsmöglichkeiten**
 - Identifizierungsdiensteanbieter („Digitales Postident“)
 - Einzelfallbezogene Identifizierungsdienstleistungen
 - „Vor-Ort-Auslesen unter Anwesenden“
 - Ermöglicht medienbruchfreie Übernahme von Daten in Formulare
- **Anpassung an die Vorgaben der eIDAS-Verordnung**
 - Regelung der Berechtigung anderer MSen
- **Weitere Regelungen und Feintuning**

Mobile Nutzung

Mobile AusweisApp2

- Android-Version seit März 2017 im Play Store
- Kein externer Kartenleser
- NFC-fähiges Smartphone
 - NFC-Profil/Tests seit Mitte 2017 Bestandteil der Prüfspezifikationen für neue Smartphones
 - Liste kompatible Geräte auf AusweisApp-Portal
- Zertifiziert nach BSI TR-03124-2
- Winter 2018: iOS-Release
- Derzeit iOS-Feldtest

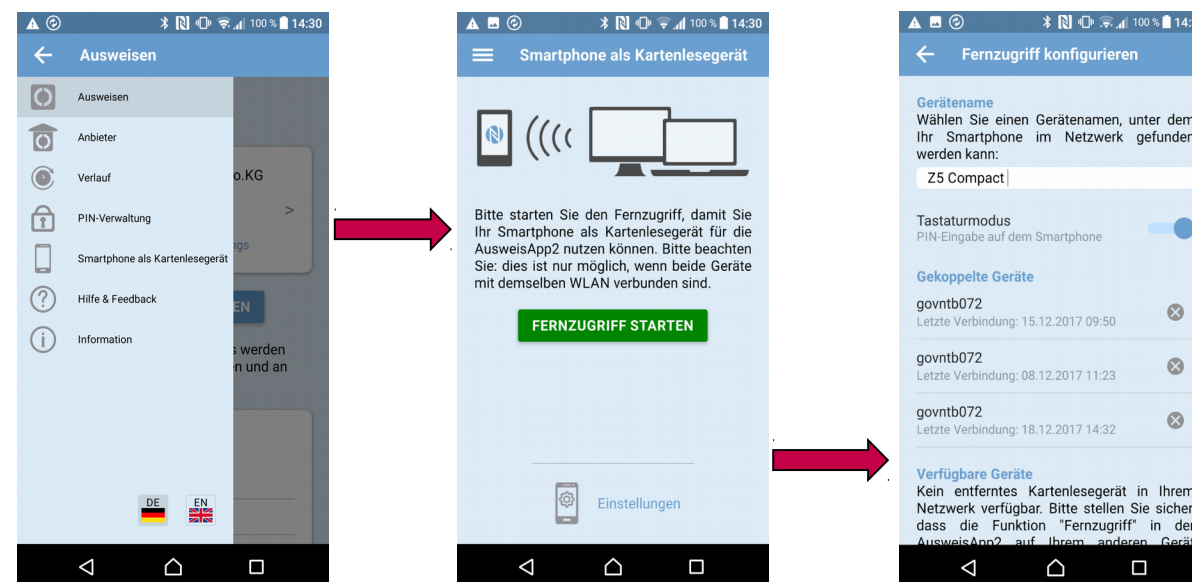
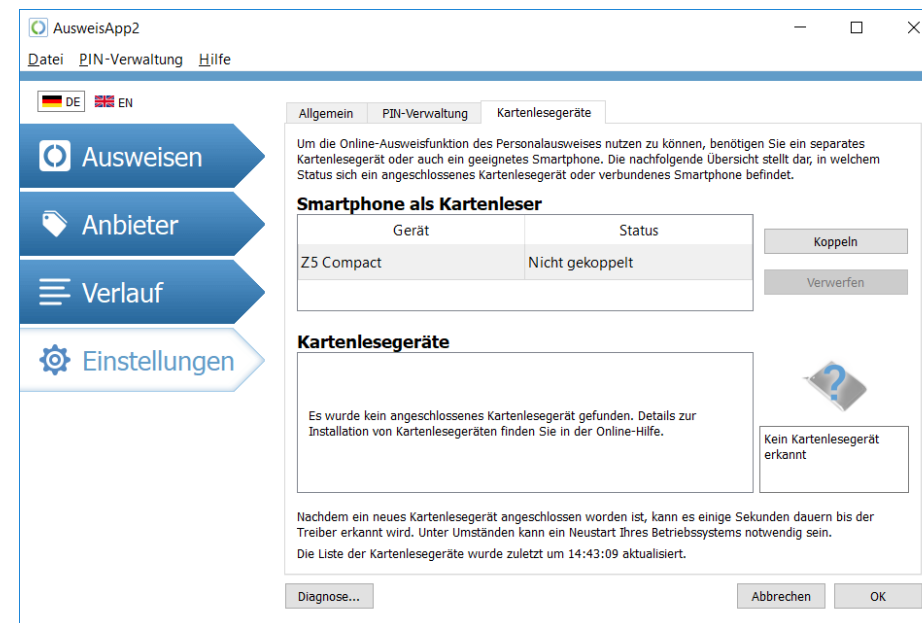
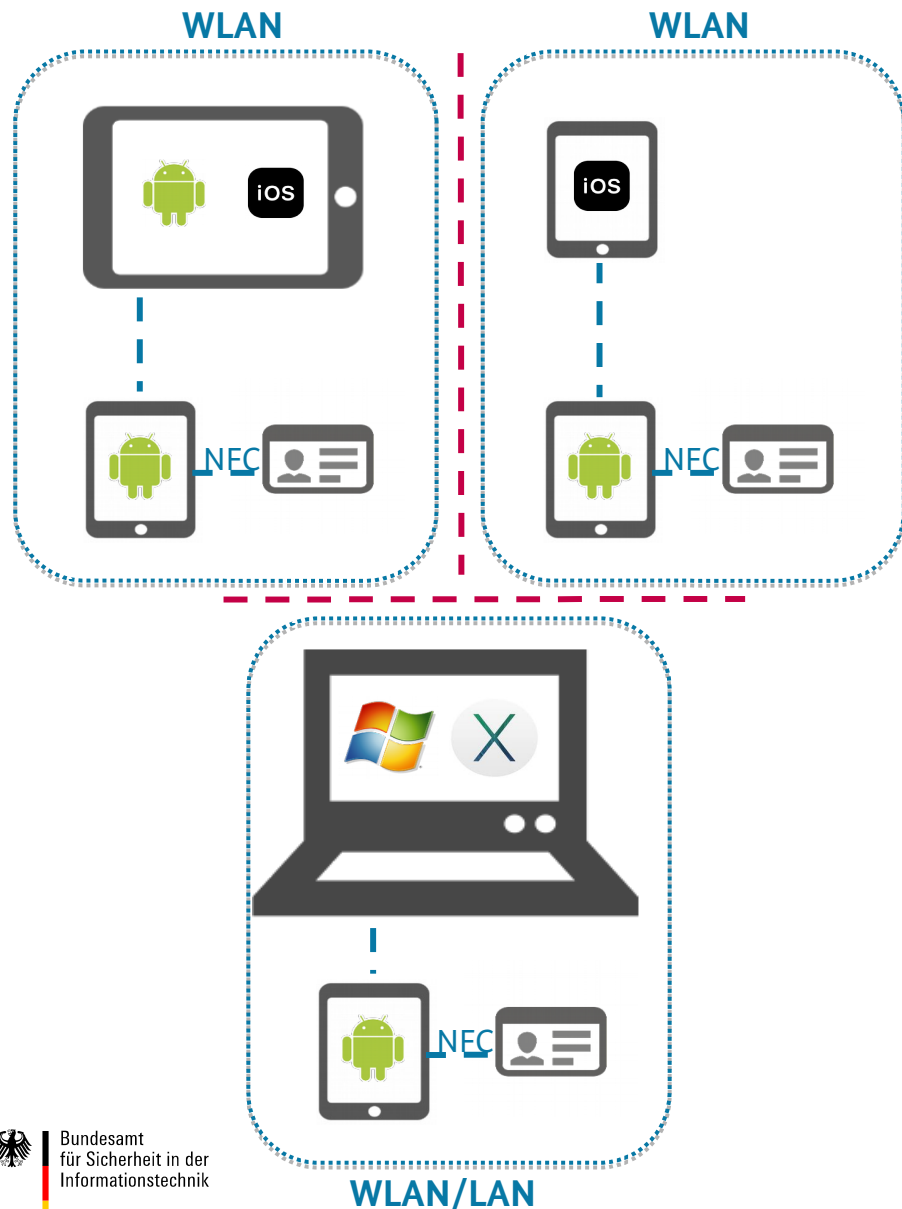


Personalausweis mit Ausweisapp2 und NFC-fähigem Android-Smartphone

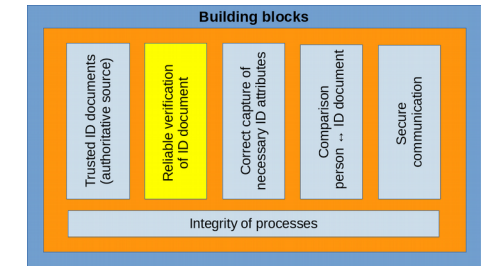
Flexible Integration in Anwendungen

- **Full eID-Client:** Stand-alone Anwendung (inkl. UI etc)
- **eID-Kernel/SDK:** (Voll-)Integration in eigene Apps
 - Mehrere zertifizierte eID-Clients und -Kernel verfügbar

Smartphone als Kartenleser



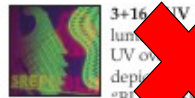
Sicherheitsmerkmale des Personalausweises im Videochat?



1+14 Multicoloured guilloches. Guilloches are security patterns that are made up of fine, interlaced lines. In reproductions, the line structures of the original are resolved into dotted screen structures. The central motif of the guilloche lines depicts the German eagle on the front and the Brandenburg Gate on the back of the card.



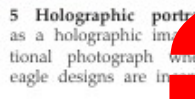
2+15 Microlettering. The positive and negative microtext "BUNDESREPUBLIK DEUTSCHLAND" is integrated into the security background printing.



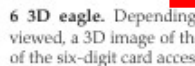
3+16 UV overprint. The guilloche design luminesces in various colours under UV light. A UV overprint is additionally included on the front depicting the German eagle and endless text "BUNDESREPUBLIK DEUTSCHLAND".



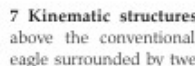
4 Optically variable inks. When the card is tilted, the background changes from green to blue depending on the viewing angle.



5 Holographic portrait. The portrait becomes visible as a holographic image on the right side of the conventional photograph when viewed at a flat angle. Four eagle designs are integrated into the secondary portrait.



6 3D eagle. Depending on the angle at which the card is viewed, a 3D image of the German eagle appears in red on top of the six-digit card access number.



7 Kinematic structures. Kinematic structures are arranged above the conventional photograph and show a German eagle surrounded by twelve stars. When the card is tilted, the

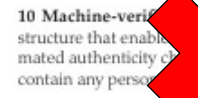


motif changes from the eagle to a hexagonal structure and then to the letter "D". In addition, the hexagons move up and down while the stars change in size.

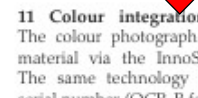
8 Macrolettering. The edge of the conventional photograph is covered by macrolettering "BUNDESREPUBLIK DEUTSCHLAND". This text appears in the hologram. Several parallel lines of lettering with the same text connect with the microlettering.



9 Contrast reversal. When the card is tilted, the contrast of the kinematic eagle motif is reversed. The bright eagle then appears dark on a bright hexagon.



10 Machine-verification. The Identigram® features a structure that enables only to a visual inspection an automated authenticity check of the ID card. This structure does not contain any personal or related data.



11 Colour integration technology (InnoSec®FUSION). The colour photograph is securely integrated into the card material via the InnoSec®FUSION personalisation system. The same technology is also used for the alpha-numeric serial number (OCR-B font).



12+20 Laser engraving. All the personalisation data (except the photograph and the serial number) is laser-engraved in high contrast into the inner card layers.

13+21 Tactile features. The expiry date and the six-digit card access number on the front of the ID card are laser-engraved and tactile.



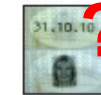
17 Logo of the ID card. The logo is depicted on the back of the card. Beginning November 2010, this logo also identifies applications and reader devices which support the new ID card.



18 Fluorescent fibres. Transparent fluorescent fibres are integrated into the layers on the back of the card. They are randomly distributed and luminescent under UV light.



19 Security embossing. Security-embossed printing and a map of Germany on the back of the card provide the document with a relief-like surface in the upper left-hand part of



21 Changeable Laser Image. Depending on the viewing angle, the date of expiry or the portrait of the holder becomes visible in the Changeable Laser Image (CLI).

22 Machine-readable zone. The machine-readable zone on the back of the card includes the document type, issuing country, serial number, date of birth, expiry date, nationality along with the name and check digits in machine-readable format (OCR-B).



23 Personalised security thread. A horizontal, verifiable security thread is embedded in the back of the card. This thread is personalised with the document number and the name of the card holder.

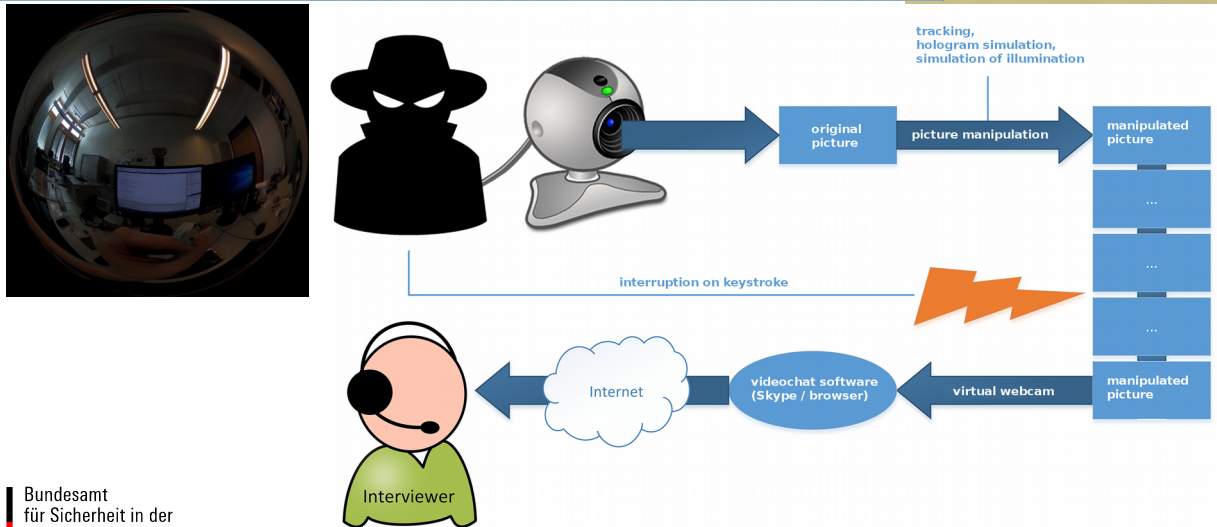
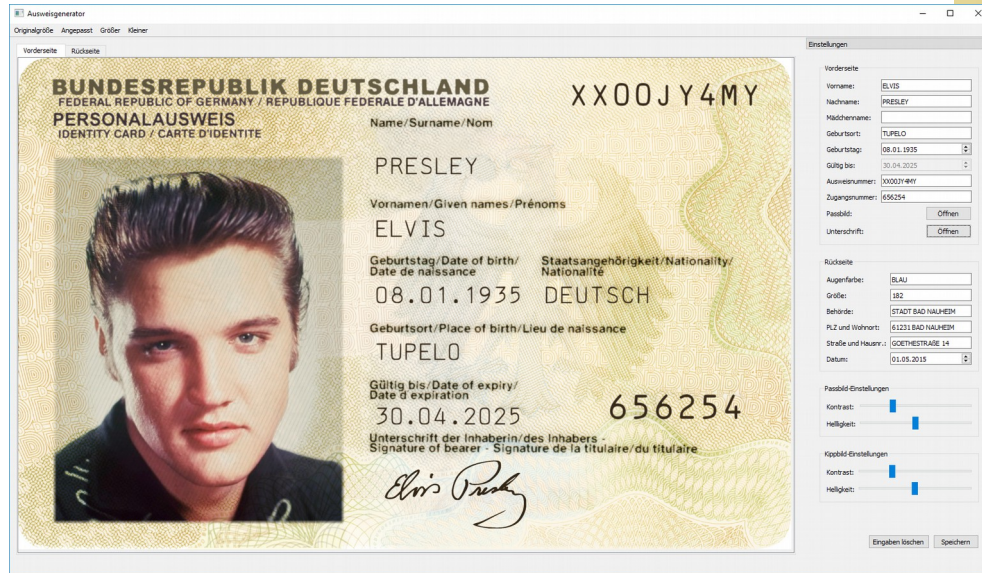
Later changes in address will be indicated on a label that can be protected by a transparent foil. The security paper used for the label is printed with a guilloche design in various colours and includes special fibres that are luminescent in various colours under UV light. In addition to the new address, the label will also contain the serial number of the ID card and the seal of the respective authority.



Only relevant for physical inspection
How to detect video manipulation?

Vor Ort prüfbar
mit Dokumentenleser

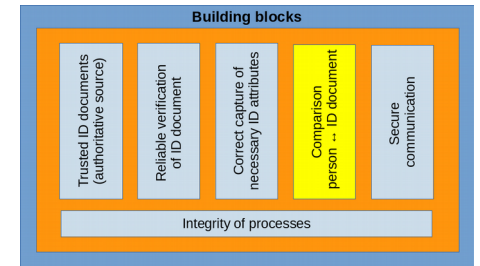
Manipulation/Simulation des Ausweisdokuments



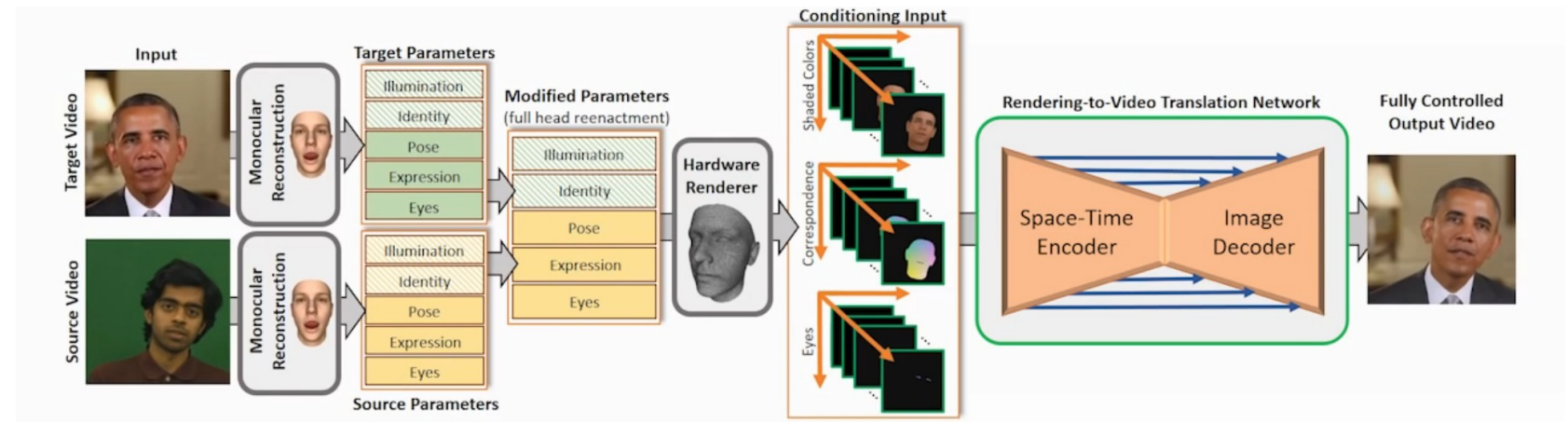
Ergebnisse / Demo Videos

Kontakt: fernident@bsi.bund.de

Biometrische Angriffe



Real-time reenactment



Quelle: <https://arxiv.org/pdf/1805.11714.pdf> (SIGGRAPH 2018)

Video: <https://www.youtube.com/watch?v=qc5P2bvfl44>

Fernidentifizierung per Video

- Optische Sicherheitsmerkmale können nicht sicher digitalisiert werden
 - Praktische Angriffe – Moderates Angriffspotential
- Presentation attacks
 - Enormer technischer Fortschritt (face reenactment, ...)
- Angriffe sind...
 - Skalierbar
 - Können weltweit ausgeführt werden
 - Nur schwer rückverfolgbar → Strafverfolgung schwierig

Elektronischer Identitätsnachweis

- Sicherheitsmechanismen für elektronische Prüfung konzipiert
- Höchstes Vertrauensniveau gemäß eIDAS

Wichtig:

- Festlegung des benötigten Vertrauensniveau für den konkreten Einsatzzweck
 - Einheitliche Kriterien zur Vergleichbarkeit von Identifizierungsverfahren
- eIDAS LoAs / BSI TR-03107 / BSI TR-03147

Fernidentifizierung per Video

- Optische Sicherheitsmerkmale können nicht sicher digitalisiert werden
 - Praktische Angriffe – Moderates Angriffspotential
- Presentation attacks
 - Enormer technischer Fortschritt (face reenactment, ...)
- Angriffe sind...
 - Skalierbar
 - Können weltweit ausgeführt werden
 - Nur schwer rückverfolgbar → Strafverfolgung schwierig

Elektronischer Identitätsnachweis

- Sicherheitsmechanismen für elektronische Prüfung konzipiert
- Höchstes Vertrauensniveau gemäß eIDAS

Wichtig:

- Festlegung des benötigten Vertrauensniveau für den konkreten Einsatzzweck
 - Einheitliche Kriterien zur Vergleichbarkeit von Identifizierungsverfahren
- eIDAS LoAs / BSI TR-03107 / BSI TR-03147

Blick in die IT-Fachpresse

„Ein schlechter Scherz!

Der Bund entwickelt mit dem nPA ein sicheres High-Tech-Produkt, und verwendet wird es durch Herumwedeln vor einer Webcam während eines Video-Chats.

Das wäre in etwa so, als ob man sich ein Elektroauto kauft und es dann von einem Ochsespann ziehen lässt, weil kein Ladekabel verfügbar ist.“

Quelle: c't Magazin, Ausgabe 18 / 2016, S.152

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Dr. Guido Frank
guido.frank@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik
Referat D12 – eID-Technologien und Chipkarten
<http://www.bsi.bund.de>

