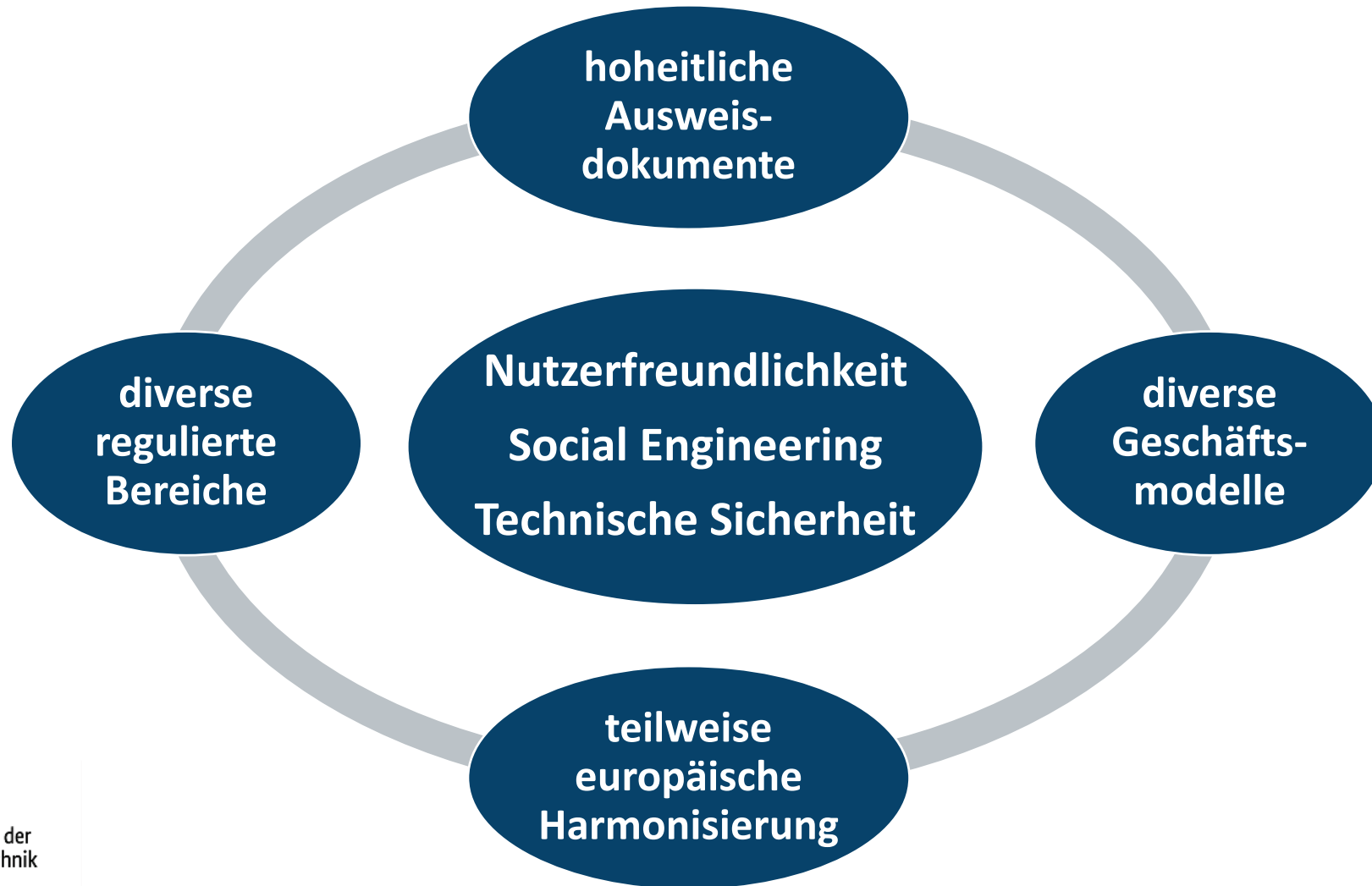




Fernidentifizierung – Sicherheit in der Digitalisierung und analoge Gefahren

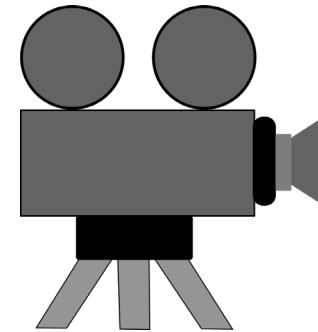
Thomas Schnattinger, BSI, 24 Mai 2023

Sicherheit im Kontext der Fernidentifizierung



Fernidentifizierung im Kontext der Digitalisierung

- „BSI gestaltet Informationssicherheit in der Digitalisierung“
 - Online-Ausweisfunktion
 - Wallets
 - Weitere Themen
- Videobasierte-Identifizierung
 - Mehrere analoge Komponenten
 - Digitale und analoge Bedrohungen



[https://openclipart.org/
image/800px/19654](https://openclipart.org/image/800px/19654)

Wie sicher sind unterschiedliche FernIdent-Verfahren?

- Darstellungen und Einschätzungen zu Risiken sind regelmäßig verzerrt
- Einheitliche Bewertungsmaßstäbe erforderlich

APPLIED COGNITIVE PSYCHOLOGY, VOL. 11, 495–506 (1997)

When a 12.86% Mortality is More Dangerous than 24.14%: Implications for Risk Communication

KIMIHIKO YAMAGISHI*

Shukutoku University, Saitama, Japan



Die Sicht des Angreifers – Technische Bewertungskriterien

Kriterium																										
Zeitaufwand	<table><tr><th>Factors</th><th>Identification</th><th>Exploitation</th></tr><tr><td>Elapsed time</td><td></td><td></td></tr><tr><td>< one hour</td><td>0</td><td>0</td></tr><tr><td>< one day</td><td>1</td><td>3</td></tr><tr><td>< one week</td><td>2</td><td>4</td></tr><tr><td>< one month</td><td>3</td><td>6</td></tr><tr><td>> one month</td><td>5</td><td>8</td></tr><tr><td>Not practical</td><td>*</td><td>*</td></tr></table>	Factors	Identification	Exploitation	Elapsed time			< one hour	0	0	< one day	1	3	< one week	2	4	< one month	3	6	> one month	5	8	Not practical	*	*	 Common Criteria
Factors	Identification	Exploitation																								
Elapsed time																										
< one hour	0	0																								
< one day	1	3																								
< one week	2	4																								
< one month	3	6																								
> one month	5	8																								
Not practical	*	*																								
Expertise	<table><tr><td>Expertise</td><td></td><td></td></tr><tr><td>Layman</td><td>0</td><td>0</td></tr><tr><td>Proficient</td><td>2</td><td>2</td></tr><tr><td>Expert</td><td>5</td><td>4</td></tr><tr><td>Multiple Expert</td><td>7</td><td>6</td></tr></table>	Expertise			Layman	0	0	Proficient	2	2	Expert	5	4	Multiple Expert	7	6										
Expertise																										
Layman	0	0																								
Proficient	2	2																								
Expert	5	4																								
Multiple Expert	7	6																								
Kenntnis des System	<table><tr><td>Knowledge of the TOE</td><td></td><td></td></tr><tr><td>Public</td><td>0</td><td>0</td></tr><tr><td>Restricted</td><td>2</td><td>2</td></tr><tr><td>Sensitive</td><td>4</td><td>3</td></tr><tr><td>Critical</td><td>6</td><td>5</td></tr><tr><td>Very critical hardware design</td><td>9</td><td>NA</td></tr></table>	Knowledge of the TOE			Public	0	0	Restricted	2	2	Sensitive	4	3	Critical	6	5	Very critical hardware design	9	NA							
Knowledge of the TOE																										
Public	0	0																								
Restricted	2	2																								
Sensitive	4	3																								
Critical	6	5																								
Very critical hardware design	9	NA																								
Zugriffsmöglichkeiten	<table><tr><td>Access to TOE</td><td></td><td></td></tr><tr><td>< 10 samples</td><td>0</td><td>0</td></tr><tr><td>< 30 samples</td><td>1</td><td>2</td></tr><tr><td>< 100 samples</td><td>2</td><td>4</td></tr><tr><td>> 100 samples</td><td>3</td><td>6</td></tr><tr><td>Not practical</td><td>*</td><td>*</td></tr></table>	Access to TOE			< 10 samples	0	0	< 30 samples	1	2	< 100 samples	2	4	> 100 samples	3	6	Not practical	*	*							
Access to TOE																										
< 10 samples	0	0																								
< 30 samples	1	2																								
< 100 samples	2	4																								
> 100 samples	3	6																								
Not practical	*	*																								
Ausrüstung	<table><tr><td>Equipment</td><td></td><td></td></tr><tr><td>None</td><td>0</td><td>0</td></tr><tr><td>Standard</td><td>1</td><td>2</td></tr><tr><td>Specialized (1)</td><td>3</td><td>4</td></tr><tr><td>Bespoke</td><td>5</td><td>6</td></tr><tr><td>Multiple Bespoke</td><td>7</td><td>8</td></tr></table>	Equipment			None	0	0	Standard	1	2	Specialized (1)	3	4	Bespoke	5	6	Multiple Bespoke	7	8							
Equipment																										
None	0	0																								
Standard	1	2																								
Specialized (1)	3	4																								
Bespoke	5	6																								
Multiple Bespoke	7	8																								
	<table><tr><td>Open samples (rated according to access to open samples)</td><td></td><td></td></tr><tr><td>Public</td><td>0</td><td>NA</td></tr><tr><td>Restricted</td><td>2</td><td>NA</td></tr><tr><td>Sensitive</td><td>4</td><td>NA</td></tr><tr><td>Critical</td><td>6</td><td>NA</td></tr></table>	Open samples (rated according to access to open samples)			Public	0	NA	Restricted	2	NA	Sensitive	4	NA	Critical	6	NA										
Open samples (rated according to access to open samples)																										
Public	0	NA																								
Restricted	2	NA																								
Sensitive	4	NA																								
Critical	6	NA																								

Range of values*	Resistance to attacker with attack potential of:
0-15	No rating
16-24	Low
25-30	Moderate
31 and above	High

Technische Richtlinien als Rahmen für einheitliche Bewertungen

BSI TR-03107 Elektronische
Identitäten und Vertrauensdienste im
E-Government

Vertrauensniveaus *normal*,
substantiell und *hoch*

Ziel dieser Technischen Richtlinie ist es, Verfahren zu elektronischen Identitäten und Vertrauensdiensten für verschiedene Prozesse des E-Government zu bewerten und Vertrauensniveaus zuzuordnen.

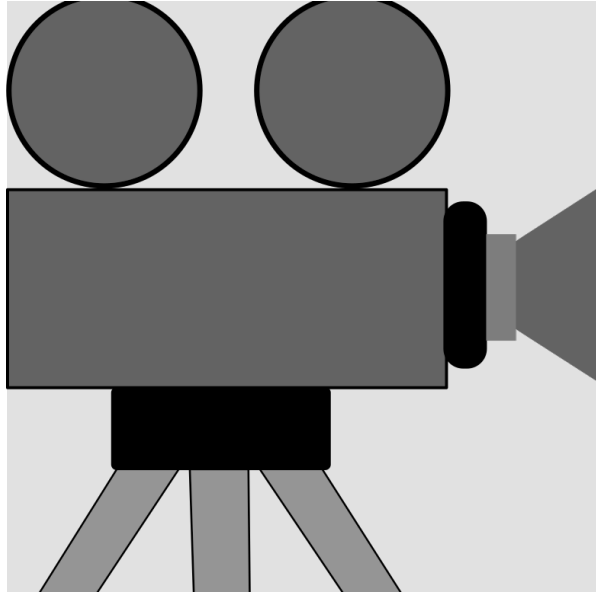
Im Laufe der Jahre wurden verschiedene technische Lösungen für unterschiedliche Anwendungsbereiche entwickelt und eingeführt. Diese Lösungen decken unterschiedliche Prozesse des Identitätsmanagements auf unterschiedlichen Sicherheitsniveaus ab.

BSI TR-03147
Vertrauensniveaubewertung von
Verfahren zur Identitätsprüfung
natürlicher Personen

www.bsi.bund.de/tr → TR-03147 →
Anforderungskatalog: Prüfung optischer
Merkmale mittels Videoübertragung

Eine sichere, zweifelsfreie Identifizierung von Personen ist in den verschiedensten
notwendig. Beispiele sind Grenzübertritte, Vertragsabschlüsse oder Verwaltungsprozesse und hierbei insbesondere
digitale E-Commerce und E-Government Prozesse.





<https://openclipart.org/image/800px/19654>

Videoident

Risiken durch gefälschte
Ausweisdokumente –
technische und finanzielle
Aspekte



Technische Bewertungskriterien – Lichtbedingungen

Beispiel Identigram®



Weiter entfernte, ausgedehnte Lichtquelle
(Schreibtischlampe, indirekt)



Geräte-eigene Lichtquelle
(Smartphone)

Technische Bewertungskriterien – Merkmalsprüfung nach BaFin RS

- **Beugungsoptisch wirksame Merkmale**
 - Hologramme
 - Identigram
 - Kinematische Strukturen
- **Personalisierungstechnik**
 - Laserkippbilder
 - Ausfüllschrift
- **Material**
 - Fenster (z.B. personalisiert)
 - Sicherheitsfaden (z.B. personalisiert)
- **Sicherheitsdruck**
 - Mikroschrift
 - Guillochenstruktur

Siehe auch www.bsi.bund.de/tr → TR-03147 → Anforderungskatalog:
Prüfung optischer Merkmale mittels Videoübertragung

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03147/TR-03147-1_Anforderungen.pdf

Die Sicht des Angreifers – Monetäre Bewertungskriterien

://www.safetymdetectives.com/blog/dark-web-the-average-cost-of-buying-a-new-identity/

um schnell darauf zuzugreifen. [Lesezeichen verwalten...](#)

 **SafetyDetectives** € ▾  ▾

BEST ANTIVIRUS **BEST PASSWORD MANAGERS** **BEST VPN** **BEST PARENTAL CONTROLS** **TOOLS** **DEALS & COUPONS** **BLOG** **NEWS** 

Home Blog **Dark Web: The Average Cost of Buying a New Identity in 2023**

Dark Web: The Average Cost of Buying a New Identity in 2023

 **SafetyDetectives Cybersecurity Team**

The people you see on a daily basis — the barista who makes your coffee, the bus driver who takes your kids to school, and the neighbor who waves to you each morning — **could all be using fake identities to hide an unsavory past.** Just a few years ago, such a scenario would have been a far-fetched plotline reserved for the Netflix series “You”. But recently, the dark web has made it extremely easy for anyone wanting to start a new life to **simply buy themselves a brand new identity.**



Region	Cost (USD)
USA	US\$850*
Canada	US\$745*
Europe	US\$750*
Australia	US\$745*



Die Sicht des Angreifers – Marktgespräche

**BDowner**  137 (TRADEVERBOT - OFFENER REPORT)
Replied: March 8, 2019 Report reply

Hey, es wurde bisher nie das OVI geprüft. Hauptaugenmerk solltest du eher auf das CLI legen, sofern die

 Quote , da dieses IMMER gefordert wird.

**BlackSkinhead**  74 (Fake IDs [01.06])
Replied: March 9, 2019 Report reply

Das CLI sollte ich
mfg
blackskinhead

Wenn das CLI einwandfrei funktioniert wird es eine 100% Quote geben



Die Sicht des Angreifers – Marktgespräche

**BlackSkinhead** 74 (Fake IDs [01.06])
Replied: April 20, 2019

Report reply

Videoident funktioniert grundsätzlich mit der AT ID. Manche Anbieter wollen allerdings Merkmale sehen, die die 250-Euro-Version nicht hat (CLI, OVI, Relief). In diesem Fall einfach vorher das Internet kappen und bei einem anderen Mitarbeiter erneut versuchen.

Dabei ist ein neues Merkmal derzeit in der Testphase.

Ja die ital. Pa **Videoident funktioniert grundsätzlich mit der AT ID.** abgeraten.

Nach Eingang von Daten und Zahlungsnachweis oder TH geht das innerhalb von 24-48h raus.

Manche Anbieter wollen allerdings Merkmale sehen, die die 250-Euro-Version nicht hat (CLI, OVI, Relief).

blackskinhead

In diesem Fall einfach vorher das Internet kappen und

bei einem anderen Mitarbeiter erneut versuchen



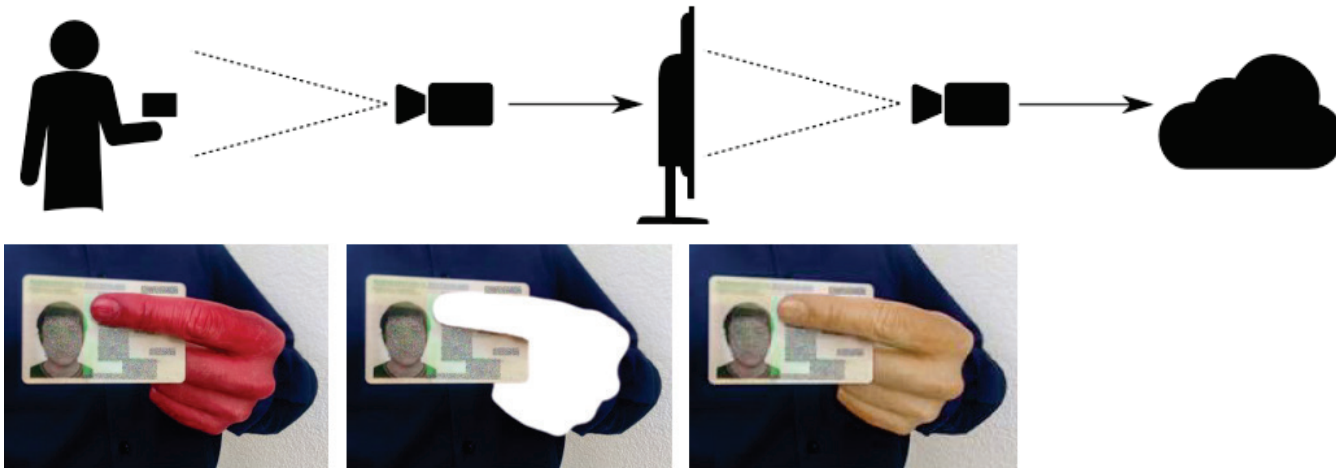
Die Sicht des Angreifers – Vorteile von Videoident

- Nachahmung vieler Merkmale nicht notwendig
→ Reduzierter Aufwand / Preis für Fälschungen
- Freie Wahl des Bildaufnahmeegeräts (Webcam, Smartphone)
→ niedrige oder hohe Auflösung etc.
- Gute Fokussierung ist nicht sichergestellt
- Evtl. eingeschränkte Bandbreite
- Ausgiebige Vorbereitung möglich
- Abbruch jederzeit möglich (Stecker ziehen)
- Mehrere Versuche möglich (anderer Prüfer, ggf. Anbieter)

**Reduziert
Entdeckungsrisiko
einer Fälschung**

Die Sicht des Angreifers – weitere Optionen bei Videoident

- BSI: Projektion des Identigrams auf eine Ausweiskopie (virtuelle Webcam)
- CCC: Abfilmen eines Fernsehers mit manipuliertem Bild. Passbild von einem Dokument in ein anderes projiziert.



Zusammenfassung: What you cannot measure, you cannot control

- **Technische Kriterien nach eIDAS, Common Criteria und Richtlinien des BSI**
 - Bewertung nach Vertrauensniveaus *normal, substantiell, hoch*
 - Teils aufwändig, für Biometrie oder Ausweisfälschungen nur teilweise etabliert
 - Identifizierte Schwachstellen bieten Potential für Verbesserungen
- **Goto where the money is**
 - Preise z.B. für Dokumentenfälschungen und Bankkonten als Marktindikator
 - Illegale Marktplätze
 - Gehandelte Produkte können verbreitetste Angriffe anzeigen

Kontakt

Thomas Schnattinger, thomas.schnattinger@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

<https://www.bsi.bund.de>

Danksagung

**In diesem Vortrag wurden Ergebnisse verwendet, die vom
Bundeskriminalamt (BKA) Referat KT54 – Urkunden,
Ausweissysteme erarbeitet und erstellt wurden.**