Bundesamt
für Sicherheit in der
Informationstechnik

Identifizierung und Authentifizierung für qualifizierte Vertrauensdienste nach eIDAS-Verordnung

Berlin, 22. Juni 2017

Inhalt

1. Vertrauensdienste in der eIDAS-Verordnung
2. Identifizierung bei Ausstellung qualifizierter Zertifikate
3. Authentifizierung bei Erstellung qualifizierter Signaturen und Siegel
4. Identifizierung und Authentifizierung bei Nutzung qualifizierter Zustelldienste
5. Vertrauensniveaus von Identifizierungsverfahren
6. Vertrauensniveaus von Authentifizierungsverfahren

1. Vertrauensdienste in der eIDAS-Verordnung

Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

Schaffung eines umfassenden europäischen Rechtsrahmens, um sichere und nahtlose elektronische Transaktionen zwischen Unternehmen, Bürgern und öffentlichen Verwaltungen zu ermöglichen

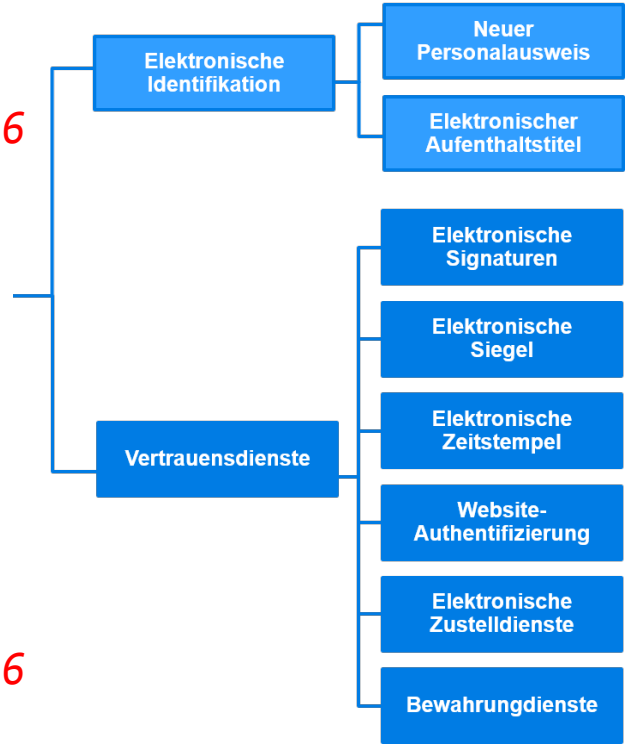
Elektronische Identifizierung *verpflichtende Anerkennung ab 09/2018*

- Personen und Unternehmen sollen mit ihren eigenen eIDs Dienste in anderen EU-Ländern nutzen können

Vertrauensdienste *seit 07/2016*

- Sollen grenzüberschreitend in ganz Europa funktionieren
- Sollen gleichen Rechtsstatus haben wie Papierverfahren
- Stärkung und Erweiterung der Vorschriften der SigRL
  - ✔ *Elektronische Signaturen, Siegel und Zeitstempel*
  - ✔ *Dienste für die Zustellung elektronischer Einschreiben*
  - ✔ *Zertifikate für die Website-Authentifizierung*
  - ✔ *Bewahrungsdienste*

Elektronische Dokumente *seit 07/2016*



Bundesamt für Sicherheit in der Informationstechnik

http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910&from=DE

Vertrauensniveaus elektronischer Identifizierungssysteme

Art. 8 Abs. (2) Die Sicherheitsniveaus „niedrig“, „substanziell“ bzw. „hoch“ erfüllen folgende Kriterien:

a/b/c) Das Sicherheitsniveau

„niedrig“/„substanziell“/„hoch“

bezieht sich auf ein elektronisches Identifizierungmittel im Rahmen eines elektronischen Identifizierungssystems, das ein

begrenztes/substanzielles/höheres

Maß an Vertrauen in die beanspruchte oder behauptete Identität einer Person

//als ein Identifizierungsmittel mit dem Sicherheitsniveau „substanziell“

vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich /entsprechender/ technischer Überprüfungen – deren Zweck in der Minderung der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung besteht – gekennzeichnet ist.

Vertrauensniveaus elektronischer Identifizierungssysteme (2)

Art. 8 Abs. (3) fordert eine Festlegung von ***Mindestanforderungen***, die *unter Bezugnahme auf die Zuverlässigkeit und Qualität folgender Elemente festgelegt [werden]:*
a) des ***Verfahrens zum Nachweis und zur Überprüfung der Identität*** *natürlicher oder juristischer Personen, die die Ausstellung elektronischer Identifizierungsmittel beantragen;*
b) des Verfahrens zur ***Ausstellung der beantragten elektronischen Identifizierungsmittel****;*
c) des ***Authentifizierungsmechanismus****, bei dem die natürliche oder juristische Person die elektronischen Identifizierungsmittel verwendet, um einem vertrauenden Beteiligten ihre Identität zu bestätigen;*
d) der ***Einrichtung, die die Identifizierungsmittel*** *ausstellt;*
e) jeder anderen ***Stelle, die mit dem Antrag für die Ausstellung elektronischer Identifizierungsmittel befasst ist****;*
f) ***technischer und sicherheitsbezogener Spezifikationen der ausgestellten elektronischen Identifizierungsmittel****.*

→ Durchführungsverordnung (EU) 2015/1502

http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32015R1502

Arten von Vertrauensdiensten

Art. 3 Nr. 16.: „Vertrauensdienst“ ist ein elektronischer Dienst,
*der **in der Regel gegen Entgelt** erbracht wird [...]*

*Erstellung, Überprüfung und Validierung von **elektronischen Signaturen, Siegeln und Zeitstempeln** sowie von diese Dienste betreffenden Zertifikaten*

- Ersetzung der Signatur-Richtlinie [...]
- neu: Fernsignaturen
- neu: elektronische Siegel als Herkunftsnachweis (Bezug zu juristischer Person)
- Bewahrungsdienste

Dienste für die Zustellung elektronischer Einschreiben

- Übermittlung von Daten zwischen Dritten mit elektronischen Mitteln
- Nachweis der Absendung und des Empfangs der Daten
- Schutz vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung

*Erstellung, Überprüfung und Validierung von **Zertifikaten für die Webseiten-Authentifizierung***

2. Identifizierung bei Ausstellung qualifizierter Zertifikate

Qualifizierte elektronische Zertifikate

Art. 3 Nr. 12.: „Qualifizierte elektronische Signatur“ ist eine fortgeschrittene elektronische Signatur, die von einer ***qualifizierten elektronischen Signaturerstellungseinheit*** *erstellt wurde und auf einem* ***qualifizierten Zertifikat*** *für elektronische Signaturen beruht.*

Art. 3 Nr. 14.: „Zertifikat für elektronische Signaturen“ ist eine elektronische Bescheinigung, die elektronische Signaturvalidierungsdaten mit einer natürlichen Person verknüpft und die mindestens den Namen oder das Pseudonym dieser Person bestätigt.

Art. 3 Nr. 15.: „Qualifiziertes Zertifikat für elektronische Signaturen“ ist ein von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat für elektronische Signaturen, das die Anforderungen des Anhangs I erfüllt.

Entspr. Art. 3 Nrn. 27., 29., 30. für qualifizierte elektronische Siegel

Art. 3 Nr. 39.: „Qualifiziertes Zertifikat für die Website-Authentifizierung“ ist ein von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat für Website-Authentifizierung, das die Anforderungen des Anhangs IV erfüllt.

Anforderungen an die Identifizierung (Art. 24 Abs. 1) [1/2]

Bei der Ausstellung eines qualifizierten Zertifikats *für einen Vertrauensdienst* ***überprüft der qualifizierte Vertrauensdiensteanbieter*** *anhand geeigneter Mittel und im Einklang mit dem jeweiligen nationalen Recht* ***die Identität*** *und gegebenenfalls die spezifischen Attribute* ***der natürlichen oder juristischen Person****, der das qualifizierte Zertifikat ausgestellt wird.*

Die Informationen nach Unterabsatz 1 werden vom qualifizierten Vertrauensdiensteanbieter im Einklang mit dem nationalen Recht entweder unmittelbar oder unter Rückgriff auf einen Dritten wie folgt überprüft:

Anforderungen an die Identifizierung (Art. 24 Abs. 1) [2/2]

*a) **durch persönliche Anwesenheit** der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person oder*
*b) aus der Ferne **mittels elektronischer Identifizierungsmittel**, für die vor der Ausstellung des qualifizierten Zertifikats eine **persönliche Anwesenheit** der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person gewährleistet war und die die Anforderungen gemäß Artikel 8 hinsichtlich der Sicherheitsniveaus **„substanziell“ oder „hoch“** erfüllen, oder*
*c) durch ein **Zertifikat** einer qualifizierten elektronischen Signatur oder eines qualifizierten elektronischen Siegels, das gemäß Buchstabe a oder b ausgestellt wurde, oder*
*d) durch **sonstige Identifizierungsmethoden**, die **auf nationaler Ebene anerkannt** sind und **gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit** bieten. Die gleichwertige Sicherheit muss von einer Konformitätsbewertungsstelle bestätigt werden.*

Nationale Anerkennung sonstiger Identifizierungsmaßnahmen

VDG-Entwurf § 11 Identitätsprüfung

(1) Die Bundesnetzagentur legt nach Anhörung der betroffenen Kreise und im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Verfügung im Amtsblatt fest, welche sonstigen Identifizierungsmethoden im Sinne des Artikels 24 Absatz 1 Unterabsatz 2 Buchstabe d Satz 1 der Verordnung (EU) Nr. 910/2014 anerkannt sind und welche Mindestanforderungen dafür jeweils gelten.

- regelmäßige Überprüfung
- vorläufige Anerkennung innovativer Identifizierungsmethoden
- Anerkennung nur sinnvoll, sofern Vertrauensniveau „hoch“ erreichbar (ansonsten keine Gleichwertigkeit möglich)

3. Authentifizierung bei Erstellung qualifizierter Signaturen und Siegel

Anforderungen an qualifizierte el. Signaturerstellungseinheiten (Anh. II)

Qualifizierte elektronische Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass
a) die ***Vertraulichkeit der*** *zum Erstellen der elektronischen Signatur verwendeten elektronischen* ***Signaturerstellungsdaten*** *angemessen* ***sichergestellt*** *ist,*
b) die zum Erstellen der elektronischen Signatur verwendeten elektronischen ***Signaturerstellungsdaten*** *praktisch* ***nur einmal vorkommen*** *können,*
c) die zum Erstellen der elektronischen Signatur verwendeten elektronischen ***Signaturerstellungsdaten*** *mit hinreichender Sicherheit* ***nicht abgeleitet werden können und die elektronische Signatur*** *bei Verwendung der jeweils verfügbaren Technik verlässlich* ***gegen Fälschung geschützt ist****,*
d) die zum Erstellen der elektronischen Signatur verwendeten elektronischen ***Signaturerstellungsdaten*** *vom rechtmäßigen Unterzeichner gegen eine Verwendung durch andere verlässlich* ***geschützt werden können****. […]*

Authentifizierung mit qualifizierten el. Signatur-/Siegelerstellungseinheiten

- Konformitätsnachweis durch Zertifizierung nach CC-Schutzprofil (gem. Art. 30, 39)
- verbindliche Normen gemäß Durchführungsrechtsakt 2016/650:
  - ISO/IEC 15408, 1-3; 18045:2008: Evaluationskriterien und Bewertungsmethoden
  - EN 419 211 — Schutzprofile für sichere Signaturerstellungseinheiten, Teile 1 bis 6

Es können keine Annahmen an die Umgebung gestellt werden; daher:

- Signaturschlüssel muss auch bei Verlust der SmartCard sicher bleiben
- Schutz gegen Extraktion aus dem Chip
- Schutz gegen Seitenkanalangriffe
- Schutz vor Manipulation der PIN-Authentifizierung

→ qualifizierte Signaturerstellungseinheiten werden bzgl. der Authentifizierung i. d. R. Vertrauensniveau **hoch** erreichen können

Anforderungen an die Authentifizierung für qualifizierte Fernsignaturen

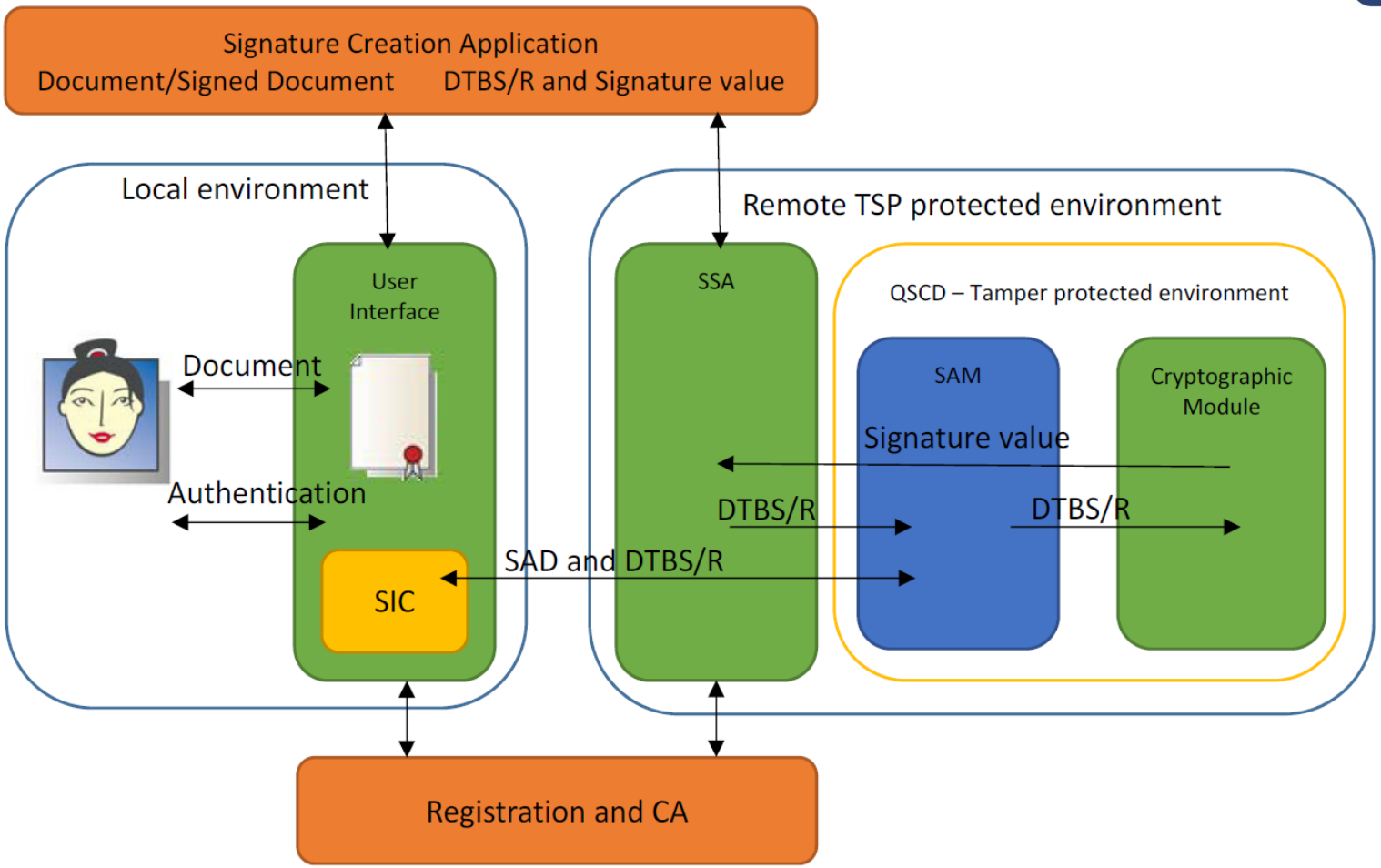
- Konformitätsnachweis durch Zertifizierung nach CC-Schutzprofil (gem. Art. 30, 39)
- verbindliche Normen noch in Arbeit, zunächst Zertifizierung nach Art. 30 Abs. 3 b)
  - Standardisierung des Verfahrens bei CEN durch EN 419 241-1 sowie die Schutzprofile PP EN 419 241-2 und PP EN 419 221-5

Vertrauensdiensteanbieter muss QSCD in gesichertem Rechenzentrum betreiben:

- Personal darf Sicherheitsmechanismen nicht manipulieren können
- Schutz gegen Extraktion aus Speicher des HSM
- Schutz vor Manipulation der Authentifizierungsmechanismen

- Identifizierung und Authentifizierung demnach mindestens auf Niveau **substanziell** nach Durchführungsrechtsakt (EU) 2015/1502
  → insbesondere **dynamische Zwei-Faktor**-Authentifizierung
  → für die Faktoren kann angenommen werden, dass diese **nur unter der Kontrolle** oder im Besitz der Person, der sie gehören, verwendet werden können

Qualifizierte Fernsignaturen – Umsetzung



4. Identifizierung und Authentifizierung bei Nutzung qualifizierter Zustelldienste

Identifizierung für qualifizierte Dienste für die Zustellung elektronischer Einschreiben

Art. 44. Abs. (1) Qualifizierte Dienste für die Zustellung elektronischer Einschreiben müssen folgende Anforderungen erfüllen: [...]
*b) Sie stellen die **Identifizierung des Absenders mit einem hohen Maß an Vertrauenswürdigkeit** sicher.*
*c) Sie stellen die **Identifizierung des Empfängers** vor der Zustellung der Daten sicher. [...]*

Identifizierung für qualifizierte Dienste für die Zustellung elektronischer Einschreiben

Art. 44. Abs. (1) Qualifizierte Dienste für die Zustellung elektronischer Einschreiben müssen folgende Anforderungen erfüllen: [...]

*b) Sie stellen die **Identifizierung des Absenders mit einem hohen Maß an Vertrauenswürdigkeit** sicher.*

hoch?

*c) Sie stellen die **Identifizierung des Empfängers** vor der Zustellung der Daten sicher. [...]*

substanziell?

Identifizierung für qualifizierte Dienste für die Zustellung elektronischer Einschreiben

Art. 44. Abs. (1) Qualifizierte Dienste für die Zustellung elektronischer Einschreiben müssen folgende Anforderungen erfüllen: [...]
*b) Sie stellen die **Identifizierung des Absenders mit einem hohen Maß an Vertrauenswürdigkeit** sicher.*
*c) Sie stellen die **Identifizierung des Empfängers** vor der Zustellung der Daten sicher. [...]*

Konsequenzen: Beweiswirkung qualifizierter Einschreiben (Art. 43 Abs. 2): *Vermutung der Unversehrtheit der Daten, der Absendung dieser Daten durch den identifizierten Absender und des Empfangs der Daten durch den identifizierten Empfänger [...]*

→ Wiederverwendung des Art. 24 Abs. 1 liegt nahe
→ Unterscheidung „*mit hohem Maß an Vertrauenswürdigkeit*“: eIDs auf Niveau **hoch**

Authentifizierung für qualifiz. Dienste für die Zustellung elektronischer Einschreiben

Art. 44. Abs. (1) Qualifizierte Dienste für die Zustellung elektronischer Einschreiben müssen folgende Anforderungen erfüllen: [...]
*b) Sie stellen die **Identifizierung des Absenders mit einem hohen Maß an Vertrauenswürdigkeit** sicher.*
*c) Sie stellen die **Identifizierung des Empfängers** vor der Zustellung der Daten sicher. [...]*

Authentifizierung?

Authentifizierung für qualifiz. Dienste für die Zustellung elektronischer Einschreiben

Art. 44. Abs. (1) Qualifizierte Dienste für die Zustellung elektronischer Einschreiben müssen folgende Anforderungen erfüllen: [...]
*b) Sie stellen die **Identifizierung des Absenders mit einem hohen Maß an Vertrauenswürdigkeit** sicher.*
*c) Sie stellen die **Identifizierung des Empfängers** vor der Zustellung der Daten sicher. [...]*

Identifizierung erfordert Sicherstellung, dass die handelnde Person auch diejenige ist, die auf entsprechendem Niveau identifiziert wurde

→ Identifizierung ergibt sich aus Erstregistrierung und Authentifizierung
→ Authentifizierung daher mindestens auch auf Vertrauensniveau **substanziell**
→ Unterscheidung „*mit hohem Maß an Vertrauenswürdigkeit*“: Authent. auf Niveau **hoch**

Guidelines for TSPs operating electronic registered delivery services

Non-Paper im Auftrag der Expert Group (AT, CZ, DE, FR, IT):

The identification of sender and addressee according to Art. 44.1 (b) and (c) has to meet the requirements according to Art. 24.1. For the identification of the sender, the eID means in case of Art. 24.1 (b) shall meet the requirements of level high according to Commission Implementing Regulation (EU) 2015/1502 to reach the high level of confidence required from Art. 44.1 (b).

In the case of a common understanding that the "sender" and "addressee" are persons acting in the process of sending and receiving a message (if applicable, through legitimate representation by a natural person), and that the required proofs of sending and receiving shall comprise the person involved in the sending process or empowered to receive a message, the following recommendation should be published:

The authentication of a previously identified sender or addressee according to Art. 44.1 (b), (c) shall meet the requirements w.r.t. authentication mechanisms for assurance level high or substantial, respectively, according to Commission Implementing Regulation (EU) 2015/1502.

Bundesamt für Sicherheit in der Informationstechnik

https://circabc.europa.eu/w/browse/b1a45a4e-7278-48ff-ab82-93694df5bfcc

5. Vertrauensniveaus von Identifizierungsverfahren

Anwendungsgebiete für Identifizierungsverfahren

Grundlage	Anwendung	gesetzl. Anforderung (gekürzt)
§§ 3, 4 GwG § 6 Abs. 2 GwG	z. B. Kontoeröffnung	Prüfung Originaldokument/ beglaubigte Kopie; eID; qeS; persönliche Anwesenheit
Art. 24 Abs. 1 eIDAS-VO	Ausstellung qualifizierter Zertifikate	eID*, qeS; *sonstige national anerkannte Verfahren mit gleichwertiger Sicherheit*
§ 111 Abs. 1 TKG	Freischaltung von Prepaid-Mobilfunkdiensten	*andere geeignete Verfahren*
§ 3 Abs. 3 De-Mail-G	Eröffnung eines De-Mail-Kontos	eID; qeS; *sonstige geeignete technische Verfahren mit gleichwertiger Sicherheit*
div. / keine	z. B. Altersverifikation, Online-Zugänge, ...	

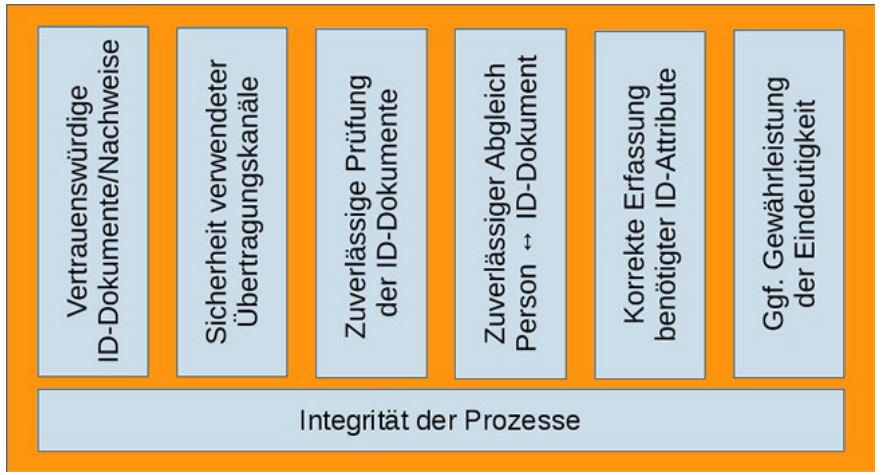
Ziele einer sicheren Identifizierung

Gewährleistung einer zuverlässigen Identifizierung:

- **Existenz:** Es gibt eine Person, auf die alle angegebenen Attribute zutreffen.
- **Legitimität:** Alle Attribute gehören zu der handelnden Person.
- **Eindeutigkeit:** Keine zwei Personen verfügen über identische Werte

Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen

- Neue Technische Richtlinie des BSI TR-03147
- Vergleichbarkeit von Identifizierungsverfahren
  durch Vertrauensniveaus angelehnt an eIDAS-Verordnung und ISO 29115
- Rechtssicherheit für Diensteanbieter
- Vermeidung anwendungsspezifischer Zusatzanforderungen
- Festlegung des Vertrauensniveau für den konkreten Einsatzzweck in Fachgesetzen / durch Aufsichtsstellen



https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03147/index_htm.html

Projekt Perso-Ident

- Einheitliche Vertrauensniveaubewertungen für personenbezogene Identitätsprüfungsverfahren
- Grundlage: BSI TR-03147
- Arbeitspakete (Auszug):
  - Erstellung einer Prüfberichtsvorlage
  - Auswahl von zwei konkret zu prüfenden Verfahren und Umsetzungen
  - Vertrauensniveaubewertung der zwei festgelegten Verfahren und Umsetzungen
  - ggf. Überarbeitung der Prüfberichtsvorlage
  - Veröffentlichung der Ergebnisse
- Laufzeit ca.: 10/2017 – 06/2018

6. Vertrauensniveaus von Authentifizierungsverfahren

Anwendungsgebiete für Authentifizierungsverfahren

Grundlage	Anwendung	gesetzl. Anforderung (gekürzt)
Art. 30 eIDAS-VO EN 419 211 EN 419 241-1	Implementierung qualifizierter elektronischer Signaturerstellungseinheiten	*substanziell oder höher*
§ 4 De-Mail-G	Anmeldung zu einem De-Mail-Konto	*zwei geeignete und voneinander unabhängige (einmalige, geheime) Sicherungsmittel*
Art. 97 PSD II	Zugriff auf Zahlungskonto Auslösung Zahlungsvorgang	*“starke Kundenauthentifiz.” (2FA)* *dynamische Authentifizierung*
	Zugang zu Servicekonten	
div. / keine	Online-Zugänge, …	

Vertrauensniveaus von Authentifizierungsverfahren

Vertrauensniveau	Anforderungen (IA 2015/1502)	Authentisierungsmittel (bsp.)
niedrig	+ zuverlässige Überprüfung + Schutz gegen Angreifer mit Angriffspotenzial *enhanced basic*	• Nutzername/Passwort • Softwarezertifikat
substanziell	+ dynamische Authentifizierung + Schutz gegen Angreifer mit Angriffspotenzial moderate	• Softwarezertifikat? • Hardware-Token
hoch	+ Schutz gegen Angreifer mit Angriffspotenzial high	• Hardware-Token • Online-Ausweisfunktion

Vertrauensniveaubewertung von Authentifizierungsverfahren

- Technische Richtlinie des BSI TR-03107 „Elektronische Identitäten und Vertrauensdienste im E-Government“
  Teil 1: Vertrauensniveaus und Mechanismen
- angepasst an eIDAS-Verordnung
- Lebenszyklus des Authentifizierungsverfahrens:
  - ✔ Ausgabe
  - ✔ Beteiligte Stellen
  - ✔ Authentisierungsmittel
  - ✔ Authentisierungsprotokoll
  - ✔ Absicherung
  - ✔ Sperren, Rückruf

https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03107/index_htm.html

Projekt Pro-eID

- Bewertung von der „Projektgruppe eID“ des IT-Planungsrats vorgeschlagener Identifizierungs- und Authentisierungsverfahren
- Grundlage: BSI TR-03107-1
- Arbeitspakete (Auszug):
  - Erstellung einer Prüfberichtsvorlage
  - Auswahl von drei konkret zu prüfenden Verfahren und Umsetzungen
  - Vertrauensniveaubewertung der drei festgelegten Verfahren und Umsetzungen
  - ggf. Überarbeitung der Prüfberichtsvorlage
  - Veröffentlichung der Ergebnisse
- Laufzeit ca.: 08/2017 – 04/2018

Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt

Dr. Ulf Löckmann
ulf.loeckmann@bsi.bund.de
Tel. +49 (0) 228 99 9582 5767
Fax +49 (0) 228 99 10 9582 5767

Bundesamt für Sicherheit in der Informationstechnik
Referat D 11 – eID-Anwendungen im E-Government
Godesberger Allee 185 -189
53175 Bonn
www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik