Bundesamt
für Sicherheit in der
Informationstechnik

Bewertung von eID-Verfahren

Onlinezugangsgesetz und Technische Richtlinien des BSI

Inhalt

1. Onlinezugangsgesetz und Vertrauensniveaus von eID-Verfahren
2. Vertrauensniveaus nach ISO/IEC 29115, eIDAS-VO und BSI TR-03107-1
3. eID-Verfahren für Nutzerkonten – Zulassungsverfahren

1. Onlinezugangsgesetz und Vertrauensniveaus von eID-Verfahren

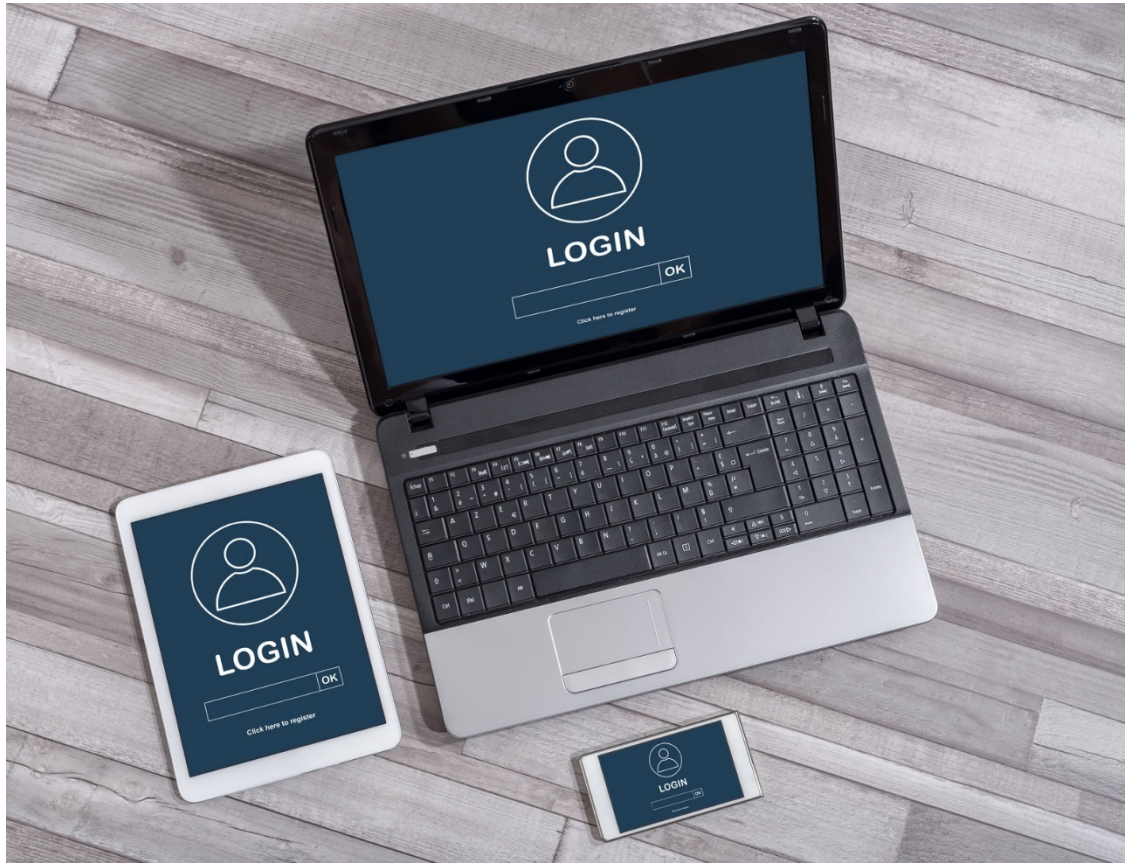
Onlinezugangsgesetz

Knapp 600 zu digitalisierende Verwaltungsleistungen

- Medienbruchfreie Nutzung
- Once Only
- Digital First

>60 Millionen potentielle Nutzer

- Portalverbund mit Nutzerkonten für Bürger und Unternehmen
- Welche eIDs für den Zugang?

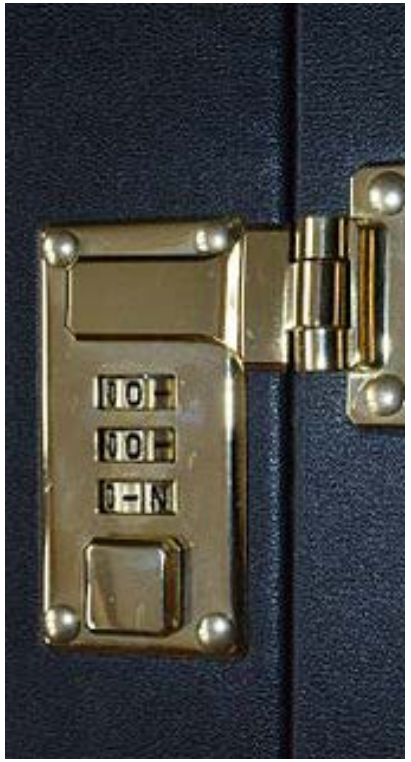


Benötigte Vertrauensniveaus für eID-Verfahren

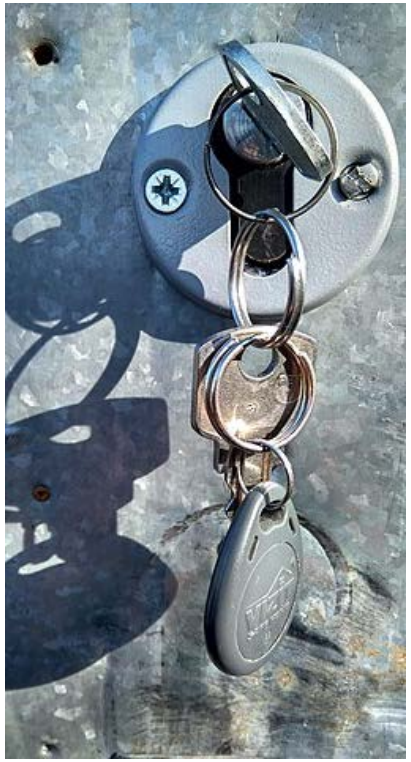
IT-Planungsrat

Für jede online angebotene Verwaltungsdienstleistung ist das erforderliche **Vertrauensniveau** für die Identifizierung und Authentisierung festzulegen:

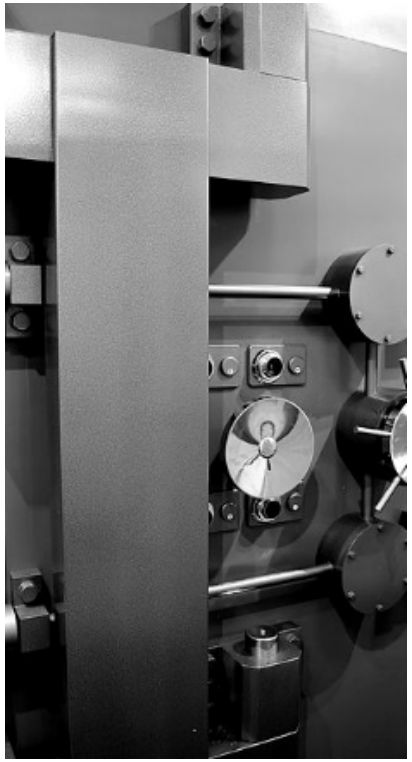
- **normal**
- **substantiell**
- **hoch**



https://commons.wikimedia.org/wiki/File:Combination-lock-254923_1920.jpg



https://commons.wikimedia.org/wiki/File:The_key_in_the_lock.jpg



https://commons.wikimedia.org/wiki/File:Vault_door_-_Reserve_Bank_Museum_-_Wellington,_New_Zealand.jpg

2. Vertrauensniveaus nach ISO/IEC 29115, eIDAS-VO und BSI TR-03107-1

Vertrauensniveaus für Identifizierung und Authentisierung

ISO/IEC 29115:2013
Entity authentication assurance framework

ISO/IEC TS 29003:2018
Identity proofing

eIDAS Verordnung 910/2014

eIDAS Durchführungsverordnung 2015/1502 – Mindestanforderungen elektronischer Identifizierungsmittel

IT-Planungsrat

Bundesamt für Sicherheit in der Informationstechnik

BSI TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government

BSI TR-03147 Vertrauensniveau-bewertung von Verfahren zur Identitätsprüfung natürlicher Personen

Vertrauensniveaus für Identifizierung und Authentisierung

Verschiedene Ordinalskalen, eingeschränkt vergleichbar

ISO/IEC 29115:2013	2 – Medium	3 – High	4 – Very High
eIDAS-VO	Niedrig	Substantiell	Hoch
BSI TR 03107-1	Normal	Substantiell	Hoch

Charakterisierung der Vertrauensniveaus – Beispiel eIDAS

Niedrig	Substantiell	Hoch
"**begrenztes Maß an Vertrauen** in die beanspruchte oder behauptete Identität"; "**Minderung** der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung"	"**substantielles Maß an Vertrauen** in die beanspruchte oder behauptete Identität"; "**substantielle Minderung** der Gefahr des Identitätsmissbrauchs oder der Identitätsveränderung"	"**höheres Maß an Vertrauen** in die beanspruchte oder behauptete Identität"; "**Verhinderung** des Identitätsmissbrauchs oder der Identitätsveränderung"

ISO/IEC 29115:2013 und ISO/IEC TS 29003:2018

Stärken	Schwächen
•Weltweite Bedeutung als ISO/IEC Dokumente	•Kleinster gemeinsamer Nenner, technisch wenig konkret •Langsame, formale Standardisierungsprozesse •ISO/IEC TS 29003:2018 nur Technical Specification (TS) •CommonCriteria ISO/IEC 15408 nicht berücksichtigt (!) •Keine Zertifizierungsprozesse
Chancen	**Risiken**
•Langfristig (>5 Jahre) weltweit anerkannte Standards, Methoden und Produkte	•Inhaltliche und zeitliche Weiterentwicklung aktuell unklar („Scope“ der Dokumente nicht stabil)

eIDAS-VO

Stärken	Schwächen
•Europaweit rechtsverbindlich •Verfügbare Erfahrungen aus bisherigen eID-Notifizierungen •Berücksichtigung der Common Criteria ISO/IEC 15408	•Technisch teilweise (zu) wenig konkrete Bewertungskriterien •Teilweise kleiner gemeinsamer Nenner bei den Kriterien
Chancen	**Risiken**
•Europaweit nutzbare eIDs mit definierten Vertrauensniveaus •Europaweite Verankerung umfassender technischer Bewertungskriterien („LoA Guidance“)	•Unterschiedliche Bewertungen der Mitgliedstaaten •Mangelnder Konsens bei der Fortentwicklung

Technische Richtlinien BSI TR-03107-1 und BSI TR-03147

Stärken	Schwächen
•Spezifische, detaillierte Kriterien •Kompatibilität zu eIDAS Vorgaben •Berücksichtigung der Common Criteria ISO/IEC 15408	•Praxiserprobung der TR-03147 noch nicht abgeschlossen •Unmittelbar keine internationale Anwendung
Chancen	**Risiken**
•Zunehmende Berücksichtigung bei der eIDAS Fortentwicklung	•Unzureichende internationale Harmonisierung

Angenommen vom IT-Planungsrat als technische Bewertungsgrundlage für Identifizierungs- und Authentisierungslösungen im Rahmen des OZG

Technische Richtlinien BSI TR-03107-1 und BSI TR-03147

- BSI TR 03107-1 „Elektronische Identitäten und Vertrauensdienste im E-Government“
  - Kriterien und Beispiele für Einstufung konkreter Authentisierungsmechanismen
  - Grundlage für die Vertrauensniveaubewertung von eID-Verfahren
- BSI TR 03147 „Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen“
  - Betrachtet Identifizierungsmittel (ID-Dokumente) und Prozesse
    - Übertragung relevanter Informationen, z. B. bei „Video-Ident“
    - Prüfprozess von ID-Dokumenten, z. B. maschinell oder manuell
    - Biometrischer Abgleich, z. B. Gesichtsbild
    - Korrekte Erfassung der ID-Attribute, Integrität der Prozesse

3. eID-Verfahren für Nutzerkonten – Zulassungsverfahren

Zulassungsverfahren für Nutzerkonten

Bundesministerium des Innern, für Bau und Heimat

Privatwirtschaftlicher Anbieter

Bundesamt für Sicherheit in der Informationstechnik

Siehe
https://www.**personalausweisportal**.de/DE/**Wirtschaft**/**Zulassungsverfahren**/zulassungsverfahren_node.html

Zusammenfassung

- Verfahrensanbieter elektronischer Verwaltungsdienstleistungen definieren das *benötigte* Vertrauensniveau
- Für eID-Verfahren wird das *erreichbare* Vertrauensniveau auf Grundlage der BSI TR-03107-1 bewertet
- Das BMI entscheidet über mögliche Verfahren und deren Zulassung; technische Bewertungen erfolgen durch das BSI

Kontakt

Bundesamt für Sicherheit in der Informationstechnik
Referat DI 14
Godesberger Allee 185 - 189
53175 Bonn

Ansprechpartner
Dr. Thomas Schnattinger
thomas.schnattinger@bsi.bund.de
www.bsi.bund.de
Tel. +49 228 9582 6132

Bundesamt
für Sicherheit in der
Informationstechnik