Identitätsglossar

Eine Übersicht über die relevanten Begriffe im Feld Digitale Identitäten.

Anonymisierung: Veränderung personenbezogener Daten, sodass diese Daten nicht mehr einer Person zugeordnet werden können. **[1]**

Angriffspotenzial: Das Angriffspotenzial eines möglichen Täters wird bestimmt durch Bewertung von:

- technischen und weiteren Fachkenntnissen
- verfügbaren Ressourcen (z.B. Spezialwerkzeug)
- den sich bietenden Gelegenheiten

Nach ISO 15408 wird zwischen erhöhtem, mäßigem und hohem Angriffspotenzial unterschieden. **[3]**

Authentifikation: Die Prüfung der Echtheit einer Behauptung (bspw. eine bestimmte Person zu sein). **[6]**

Authentisierung: Der Prozess, die Echtheit einer Information zu bestätigen lassen. *Der Benutzer authentisiert sich am Server und der Server authentifiziert ihn.* **[6]**

Authentifizierung: Der Prozess, der die Echtheit einer Information wie einer behaupteten Identität überprüft. **[6]**

Authentifizierungsmittel: Mittel, die zur Authentifizierung eingesetzt werden wie Ausweise, Passwörter etc. Während der Authentifizierung wird deren Echtheit oder Korrektheit bestätigt, womit die Authentifizierung des Mittels häufig die Authentifikation der Person ersetzt. **[Eigene Definition]**

Autorisierung: Abschließende Bestätigung der Authentifizierung. **[6]**

Diensteanbieter: Diensteanbieter werden auch Service Provider genannt. Sie bieten Dienstleistungen online für Nutzer*innen an. Diese Services können sowohl staatliche Leistungen wie ein Kindergeldantrag als auch privatwirtschaftliche Leistungen wie eine Onlinebestellung sein.

eID: Damit wird die elektronische Funktion des neuen deutschen Personalausweises bezeichnet. Mit der eID können sich Personen online gegenüber Dritten identifizieren. **[15]**

eIDAS: Der Name steht für "**e**lectronic **I**Dentification, **A**uthentication and trust **S**ervices" und bezeichnet die europäische Verordnung Nr. 910/2014. eIDAS harmonisiert Regeln und Standards für elektronische Identifikation, Authentifizierung und Vertrauensdienste im europäischen Binnenmarkt. **[12]**

Identity-on-the-fly: Identity-on-the-fly bezeichnet verschiedene Konzepte der unmittelbaren Identitätsfeststellung ohne weitere Authentifizierungsmittel (wie bspw. eine eID) zu nutzen. So könnte die Identität einer Person auch durch die Abfrage und Verknüpfung verschiedener Datenpunkte (zum Beispiel dem Wissen über die Steuernummer, letzten Wohnorte und andere Informationen) festgestellt werden. Solche Abfragen könnten in den Formularprozess oder einen Chatbot zur Identitätsprüfung integriert werden, sodass die Identitätsfeststellung von Nutzer*innen nicht als separater Teil der Dienstleistung wahrgenommen wird.
[Eigene Definition]

Identifikator: Ein mit einer bestimmten Identität verknüpftes Merkmal zur eindeutigen Identifizierung des tragenden Objekts. Eine Sozialversicherungsnummer könnte beispielsweise ein Identifikator sein. **[4] [7]**

Identifizierung: Verschiedene Bedeutungen: **[8]**

- bei Personen die amtliche *Identitätsfeststellung*
- in Datenbanken und Dokumentationssprachen die Vergabe eines Kennzeichens, siehe Identifikator
- das Wiedererkennen eines biologischen Exemplars, Identifizierung (Biologie)
- der Prozess, der eine Person eindeutig erkennen soll **[6]**

Identitätsfeststellung [auch Identprüfung]: Die Überprüfung, welche Personalien (Identität) einer natürlichen Person zuzuordnen sind. **[5] [6]**

Identity Broker: Ein Dienst, der als Intermediär mehrere Identitätsanbieter mit Dienstanbietern verknüpft. Dabei leitet ein Identity Broker die durch den Identitätsanbieter bestätigten Attribute an den Dienstanbieter weiter. **[16]**

Identitätsanbieter: Identitätsanbieter werden auch Identity Provider genannt. Es handelt sich dabei um Systeme, die für Nutzer Identitätsinformationen verwalten und diese gegenüber Dritten authentifizieren. Ein Identitätsanbieter bestätigt gegenüber einem Diensteanbieter dabei gewisse Attribute eines Nutzers. **[14]**

Privacy by Default: Standardeinstellungen von Privatsphäreoptionen sollten so datenschutzfreundlich wie möglich sein. Dadurch sollen sich Nutzer*Innen bewusst für weniger datenschutzfreundliche Einstellung entscheiden müssen. **[9]**

Privacy by Design: Durch technische oder organisatorische Maßnahmen soll dafür gesorgt werden, dass die Privatsphäre des Nutzers geschützt ist. Dies kann bspw. durch Pseudonymisierung von gespeicherten Daten geschehen. **[9]**

Pseudonymisierung: Identifikationsmerkmal wie bspw. der Name wird durch ein anderes Kennzeichen ersetzt. Dadurch soll ein Rückschluss auf die tatsächliche Person verhindert werden. **[2]**

Risikoanalyse: Verfahren zur Identifikation von Ursachen/Quellen für Risiken und der Abschätzung. Je nach Schadensauswirkung (tolerabel/geringfügig, beträchtlich oder katastrophal) gestaltet sich der Schutzbedarf (normal, hoch, oder sehr hoch). **[3]**

Sicherheitslevel/Sicherheisanforderungsstufe/Sicherheits-Integritätslevel: Vier Stufen, die aus der EN 61508 hervorgehen. Die Abstufung wird graduell höher, wobei Stufe 4 die höchste Sicherheitsanforderung aufweist. Die vier Stufen werden durch drei Faktoren bestimmt:

- PFD (probability of failure on demand)
- RRF (risk reduction factor)
- PFH (probability of failure per hour)

Für jedes der Level sind Grenzen für die Faktoren vorgegeben. **[11]**

Vertrauensniveau: Vertrauensniveau gibt den Grad an, mit dem einem Verfahren zur Identifizierung bzw. Authentifizierung vertraut werden kann. Unterschieden wird dabei zwischen drei Niveaus:

niedrig/normal, substanziell und hoch. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gliedert diese drei Kategorien nach den Schadensauswirkungen einer Fehlidentifikation wie folgt:

- Normal: Die Schadensauswirkungen sind begrenzt und überschaubar.
- Substanziell: Die Schadensauswirkungen sind substanziell.
- Hoch: Die Schadensauswirkungen sind beträchtlich. **[10]**

Vertrauensdienste: Dienste, die meist gegen Entgelt die Erstellung, Überprüfung und Validierung von elektronischen Signaturen, Siegeln und Zertifikaten erbringen. **[17]**

Verifikation: Bestätigung mittels eines Nachweises, dass eine Behauptung gewissen Anforderungen entspricht und der zu prüfende Sachverhalt damit der Wahrheit entspricht. **[13]**

Quellen

1) BDSG § 3 Abs. 6

2) BDSG § 3 Abs. 6a

3) Kersten, Heinrich; Reuter, Jürgen, Schröder, Klaus-Werner (2008): IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz: Der Weg zur Zertifizierung. Springer Verlag. S. 24 ff.
URL:https://books.google.de/books?id=Q8QhBAAAQBAJ&dq=einstufungen+von+angriffspotential&hl=de&source=gbs_navlinks_s

4) IT Administrator: Identifikator
URL: https://www.it-administrator.de/lexikon/identifikator.html
Abrufdatum: 26.08.2019

5) Juraforum: Identitätsfeststellung
URL: https://www.juraforum.de/lexikon/identitaetsfeststellung
Abrufdatum: 26.08.2019

6) Theißen, Sascha (2009): Risiken informations- und kommunikationstechnischer (IKT-) Implantate im Hinblick auf Datenschutz und Datensicherheit. KIT Scientific Publishing. S. 506-508.
URL:https://books.google.de/books?id=AL0IU4d5NAsC&dq=Identit%C3%A4tsfestellung+glossar&hl=de&source=gbs_navlinks_s

7) Smart PLM: Identifikator
URL: https://smart-plm.com/glossary/identifikator/
Abrufdatum: 26.08.2019

8) Wikipedia: Identifizierung
URL: https://de.wikipedia.org/wiki/Identifizierung
Abrufdatum: 26.08.2019

9) Europäische Kommision: What does data protection ‘by design’ and ‘by default’ mean?
URL:https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en
Abrufdatum: 23.09.2019

10) BSI: Technische Richtlinie TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government
URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf?__blob=publicationFile&v=4
Abrufdatum: 24.09.2019

11) EN 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

12) 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
URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910
Abrufdatum: 24.09.2019

13) DIN EN ISO 9000:2015-11: Qualitätsmanagementsysteme - Grundlagen und Begriffe. Abschnitt 3.8.4

14) MIT Knowledge Base. Identity Provider
URL: http://kb.mit.edu/confluence/display/glossary/IdP+(Identity+Provider)
Abrufdatum: 27.09.2019

15) Personalausweis
URL: https://www.oeffentliche-it.de/personalausweis
Abrufdatum: 28.09.2019

16) IDAPWiki
URL: https://ldapwiki.com/wiki/Identity%20Broker
Abrufdatum: 28.09.2019

17) Verordnung (EU) Nr. 910/2014 Art. 3 Nr. 16