Identität im digitalen Gesundheitswesen

Fachtagung Datenschutz im Gesundheitswesen

Christoph Isele

Cerner

11. Mai 2022

Christoph Isele

Cerner
IP Reg & Compliance

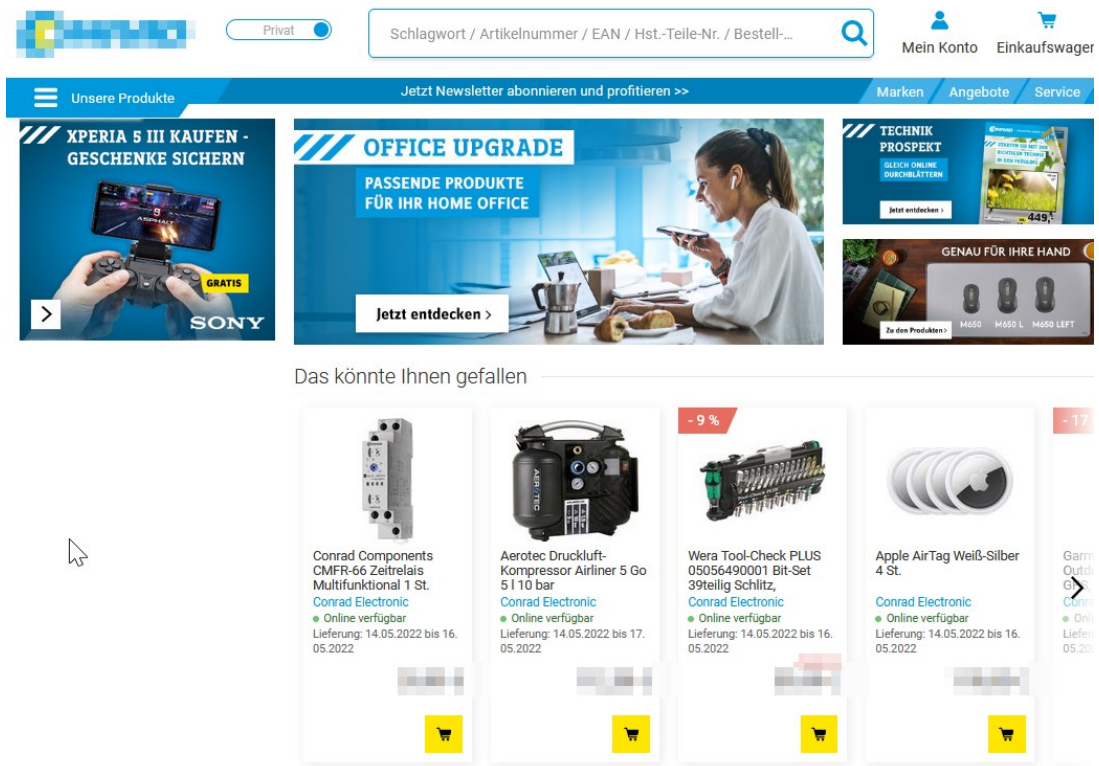
Lead Regulatory Affairs Strategist

Christoph.isele@cerner.com
+49 173 2385940

Digitalisierung im Gesundheitswesen (BMG)

- Die zunehmende Digitalisierung des Gesundheitswesens … bieten in den kommenden Jahren große Chancen.
- Nutzen der Daten um Abläufe einfacher, schneller oder sicherer zu machen
- Speicherung und Zugriff auf relevante Daten aus der Krankheitsgeschichte
- Organisatorisches Grüst im Hintergrund

Internet Service im Alltag



- Aufruf einer bekannten Seite
- Allgemein üblich sich mit Benutzer (meist email-Adresse) und Passwort anzumelden
- Diensteanbieter kann zusätzliche Funktionen anbieten, bei Finanzdienstleistern gerne eine Zusatzfrage
- Typischerweise Low Risk Anwendungen

Bsp. Online Shop

- Konto kann einfach angelegt werden
- Verwaltung des Accounts beim Diensteanbieter,
- rechtliche Grundlage Einwilligung
- Schutz: Nutzer/Passwort, selten 2-Faktor-Authetisierung
- Zusätzliche Sicherheit z.B. Benachrichtigung, wenn ein neuer Client verwendet wird.

- Risiko
  - Einblick in Interessen, Bestellliste,
  - mit hinterlegten Bezahlinformationen umfangreiche „fremde“ Bestellungen möglich
  - Hacken des Dienstes, entwenden der Kreditkarteninformationen und Verwendung an anderer Stelle

Bsp. Terminvergabe Portal

- Zugriff über Konto bietet die Möglichkeit vereinbarte Termine einzusehen, zu ändern, abzusagen
- Konto anlegen muss niederschwellig möglich sein
- Verwaltung der Identität beim Dienstanbieter,
- mehrere Registrierungen möglich, keine „öffentliche Regelung“ für Vertreter und Kinder
- Eingrenzung durch Mailadresse oder Telefonnummer

- Rechtliche Grundlage Einwilligung
- Schutz: Nutzer/Passwort, selten 2-Faktor-Authetisierung
- Verifizierung der Identität bei der Registrierung durch Mail oder Telefon

Bsp. Terminvergabe Portal (2)

- Der Schaden aus der Information, dass der Bürger einen Termin in einer bestimmten Praxis hat, ist in der Regel gering.

- Hochladen von Befunden und anamnestischen Fragebögen
- Bei manchen Anbietern Ende-zu-Ende verschlüsselt

Bsp. Videosprechstunde

- Konto kann einfach angelegt werden auch in Verbindung mit einem Terminreservierungsportal

- Verwaltung der Identität beim Dienstanbieter,
- Identität teilweise gesteuert durch die Arztpraxis

- Rechtliche Grundlage Einwilligung
- Schutz: Konto/Passwort, Meeting ID

- Kritische Gesundheitsdaten werden erst im Gespräch ausgetauscht.

Bsp. eFA oder medizinisches Netzwerk

- Der/ein Leistungserbringer setzt den organisatorischen Rahmen.

- Der Leistungserbringer sorgt für Zugang

  … oft auf zusammenarbeitende Leistungserbringer beschränkt
  … hält User / Identität für den Geschäftspartner bereit und
  … verwaltet gegebenenfalls die Informationen

- Sicherungsmechanismen wie 2FA, Virtual Desktop, authenticator app, …

- Vertragliche Absicherung
- Schulung

Kurzer Blick zu Social Media

Facebook (AGBs)

- Denselben Namen verwenden, den du auch im täglichen Leben verwendest.
- Genaue und korrekte Informationen über dich zur Verfügung stellen.
- Nur ein einziges Konto (dein eigenes) erstellen und deine Chronik für persönliche Zwecke verwenden

Facebook Login („Entwicklerhandbuch“)

- Wahre Identität, weniger Spam, …
- Facebook Login ergänzt dein bestehendes Kontosystem.
- Präzise Berechtigungen
- Mit Facebook Login können Nutzer genau festlegen, welche Informationen sie deiner App zur Verfügung stellen möchten.
- …

Neue Dienste
mehr klinische Daten,
mehr sensible Daten

Cerner

BMG: Digitalisierung im Gesundheitswesen

Beispiele

- Patientenportal Terminvereinbarung, digitale Anamnese,
- TI KIM (Hausarzt)
- TI ePA, Patienten geführte Akte, use case Patient gewährt dem LE Zugriff auf die Akte
- TI weitere Dienste …

- Vor allem Kommunikationsdienste
- TI hat das Verzeichnis der potentiellen Kommunikationsteilnehmer
- Weitere Anwendergruppen folgen …
- „Closed shop“

Vorteile für den Patienten

- Freiwillige Angebote
- Kassen gehen in die Vorleistung und kümmern sich um die „Benutzerverwaltung“ auf der Seite der Patienten

TI kontrollierte Umgebung

- ePA: Steuerung wer auf die Daten zugreifen kann
- Leistungserbringer stellt Daten in die ePA ein
- Hohe Sicherheit

- Gerne einfacherer Zugang; keine / wenig zusätzlich Hardware
- Aber auch Wellness, DIGA, …

Aus Sicht des Leistungserbringers

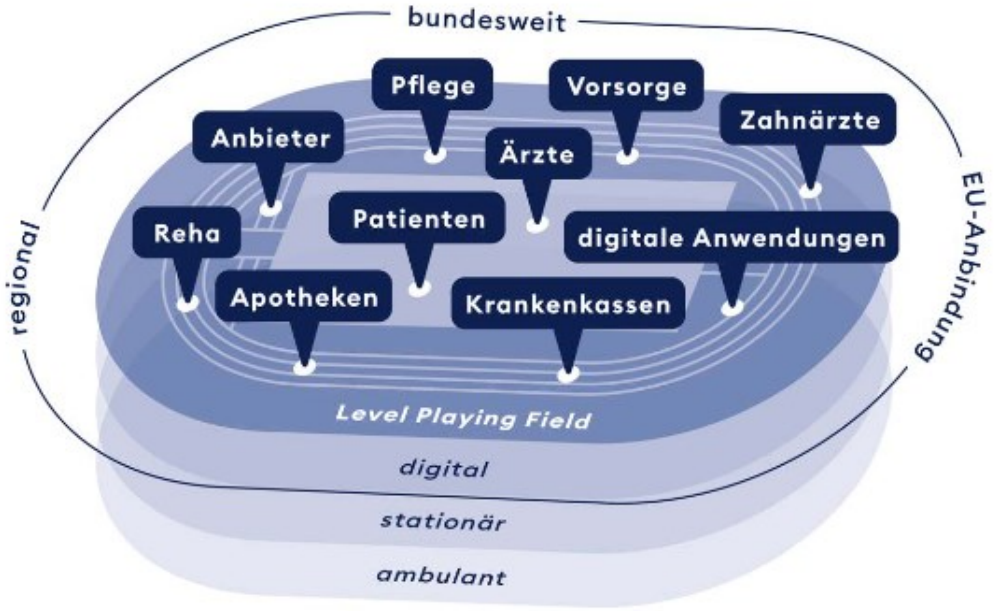
- Gesetzliche Vorgaben, muss sich selbst die Eintrittskarten besorgen

- Austausch von Daten zwischen Leistungserbringern
- Korrektheit der Daten, Metadaten zur Entstehung
- Frage: Vollständigkeit bzw. Angaben zur Vollständigkeit

- Geschäftsprozesse sollten verschiedene Organisationsformen unter stützen

- Neue gesetzliche Anforderungen müssen umgesetzt werden
- Möglichst wenig zusätzliche Kosten

Gematik / TI möchte sich öffnen: TI 2.0



1. Föderiertes Identitätsmanagement
2. universellen Erreichbarkeit der Dienste
3. modernen Sicherheitsarchitektur
4. verteilten Diensten
5. Interoperabilität und strukturierten Daten
6. automatisiert verarbeitbaren Regelwerk

Geht das auch verteilt?

Vertrauensniveau

Das BSI verwendet drei Vertrauensniveaus

- **normal:** Die Schadensauswirkungen bei einer Kompromittierung sind begrenzt und überschaubar. Dieses Vertrauensniveau entspricht in etwa dem Sicherheitsniveau normal gemäß IT-Grundschutz
  (Schäden haben Beeinträchtigungen der Institution zur Folge)
- **substantiell**: Die Schadensauswirkungen bei einer Kompromittierung sind substantiell. Dieses Vertrauensniveau liegt zwischen den Sicherheitsniveaus normal und hoch gemäß IT-Grundschutz
- **hoch**: Die Schadensauswirkungen bei einer Kompromittierung können beträchtlich sein. Dieses Vertrauensniveau entspricht in etwa dem Sicherheitsniveau hoch gemäß IT-Grundschutz
  (Im Schadensfall tritt Handlungsunfähigkeit zentraler Bereiche der Institution ein. Schäden haben erhebliche Beeinträchtigungen der Institution selbst oder betroffener Dritter zur Folge.)
-

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf?__blob=publicationFile&v=1

Potentieller Schaden bedingt Vertrauensniveau

	Normal
Verstoß gegen Gesetze/Vorschriften	Verstoß mit geringfügigen Konsequenzen
Unrichtige Identifizierung oder Zuordnung zu einer Identität	Geringfügige Konsequenzen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen beeinträchtigen können
Beeinträchtigung körperlicher/persönlicher Unversehrtheit	Beeinträchtigung erscheint nicht möglich
Beeinträchtigung der Aufgabenerfüllung	Beeinträchtigung wird von den Betroffenen als tolerabel eingeschätzt
Negative Innen- oder Außenwirkung	Geringe/nur interne Ansehens- oder Vertrauensbeeinträchtigung zu erwarten
Finanzielle Auswirkungen	Finanzieller Schaden tolerabel

Potentieller Schaden bedingt Vertrauensniveau

	Substantiell
Verstoß gegen Gesetze/Vorschriften	Verstoß mit substantiellen Konsequenzen
Unrichtige Identifizierung oder Zuordnung zu einer Identität	Substantielle Konsequenzen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen substantiell beeinträchtigen können.
Beeinträchtigung körperlicher/persönlicher Unversehrtheit	Beeinträchtigung kann nicht vollständig ausgeschlossen werden
Beeinträchtigung der Aufgabenerfüllung	Beeinträchtigung wird von einzelnen Betroffenen als tolerabel eingeschätzt
Negative Innen- oder Außenwirkung	Substantielle Ansehens- oder Vertrauensbeeinträchtigung zu erwarten
Finanzielle Auswirkungen	Substantieller finanzieller Schaden möglich

Potentieller Schaden bedingt Vertrauensniveau

	Hoch
Verstoß gegen Gesetze/Vorschriften	Verstoß mit erheblichen Konsequenzen
Unrichtige Identifizierung oder Zuordnung zu einer Identität	Erhebliche Konsequenzen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen können.
Beeinträchtigung körperlicher/persönlicher Unversehrtheit	Beeinträchtigung kann nicht ausgeschlossen werden
Beeinträchtigung der Aufgabenerfüllung	Beeinträchtigung wird als nicht tolerabel eingeschätzt
Negative Innen- oder Außenwirkung	Breite Ansehens- oder Vertrauensbeeinträchtigung zu erwarten
Finanzielle Auswirkungen	Beachtliche finanzielle Verluste, jedoch nicht existenzbedrohend

Registrierung

Organisation / Verantwortung

Dienstanbieter eines Dienstes der klinische Daten verarbeitet muss natürlich auch die Grundsätze des Datenschutzes einhalten u.a. der Zugang kontrollieren.

„relativ einfach“ im Krankenhaus, wenn der Dienstanbieter alle Berechtigten kennt bzw. diese aus der eigenen Organisation kommen.

Enrolment im „öffentlichen Raum“

Die **Registrierung eines Benutzers** in einem Authentisierungssystem (Identity Management System). Typischerweise wird als Teil des Enrolments eine Identitätsprüfung des Benutzers durchgeführt und anschließend ein Authentisierungsmittel (gegebenenfalls bestehend aus mehreren Faktoren) ausgegeben bzw. ein vorhandenes Authentisierungsmittel registriert.

Die **Identitätsprüfung** kann anhand physisch vorgelegter Dokumente oder elektronisch mittels eines eID-Systems auf geeignetem Vertrauensniveau erfolgen.

Authentisierungsmittel

- Besitz, Hardware
- Wissen
- Biometrie

Dienstleister

Oft werden Dienstleister eingesetzt, um die Identitätsfeststellung und die Ausgabe von Autorisierungsmitteln zu erbringen.
Die Mindestanforderungen an die Vertrauenswürdigkeit hängen wieder von dem Vertrauensniveau ab.

Bei Vertrauensniveau „normal“ reicht ein bekannte Stelle nach entsprechender Prüfung

Bei „substantiell“ oder „hoch“ sollte es schon eine vertrauenswürdige Stelle sein. Hier sollten regelmäßige Auditierungen und entsprechende Zertifikate vorliegen.

Verschiedene Identifizierung Verfahren

- Post Ident Verfahren
  - Unterlagen ausdrucken zur Post gehen, Beamter kontrolliert und schickt den Brief zum Anfragenden
  - Bekanntes Verfahren, aber aufwändig für der sich registrieren will und durch Aufgabe der Postfilialen in manchen Gegenden noch mühsamer

- Video Ident Verfahren
  - Video Session Mitarbeiter z.B. der Bank und Neukunde sind in einer Video Session
  - Unterlagen werden fotografiert
  - Mitarbeiter prüft Übereinstimmung
  - Garantierte Überprüfung von Sicherheitsmerkmalen durch technische Werkzeuge

  - (vollautomatische) Variante ohne menschliche Mitarbeiter wird von einzeln Firmen angeboten

Enrolment: Telematik Infrastruktur

- Das Sicherheitskonzept der gematik basiert auch darauf, dass die Teilnehmer bekannt sind und im „Schadensfall“ etwas zu verlieren haben.
- Teilnehmer an der Telematik Infrastruktur sind Institutionen wie Kassen und Leistungserbringer wie Ärzte, Pflegekräfte, Apotheker, deren Kammern bei dem Enrolment helfen
sowie begrenzt die Patienten

Enrolment: Telematik Infrastruktur

- Authentisierung Karten basiert

- Ausgabe entsprechender Karten wie eHBA durch die Kammern (z.B. Ärztekammer)
- Ausgabe von Institutskarten (SMC-B) über die DKTIG und Trusted Service Provider z.B. (d-trust, SHC, T-Systems, medisign)
- Ausgabe von Karten für die Patienten durch die Krankenkassen

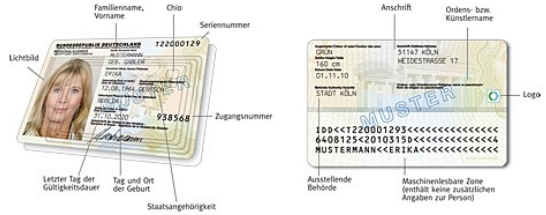
Enrolment: Telematik Infrastruktur

Bei Institutskarten (SMC-B) und Heilberufeausweis (eHBA):

- Zusammenspiel von Kammer und Trusted Service Provider
- Identitätsprüfung
  - Prüfung schriftlicher Unterlagen
  - Postidentverfahren
  - Vertrauensdienst Ident (eigene Mitarbeiter, Provider oder KH)
- „Ausgabe“ von Authentisierungs-mittel durch individuelle Post per Einschreiben

Authentisierungs-verfahren

Elektronischer Identitätsnachweis



- Personalausweis
- Aufenthaltstitel (Personen ohne die deutsche Staatsbürgerschaft)

- Der Elektronische Identitätsnachweis stellt die Identifikation einer Person auf dem Vertrauensniveau „hoch“ sicher. Als einziges Mittel auch für die Registrierung (Erstanmeldung)
- Der elektronische Identitätsnachweis erfüllt die Anforderung einer behördlichen Identitätsprüfung des Ausweisinhabers und ist damit geeignet, für die Identifizierung besondere Formvorschriften zu erfüllen.
- Der Personalausweis verfügt über eine qualifizierte Signaturfunktion

- … aber das Schutzniveau wird nicht überall gebraucht …

Kryptographische Token Hardware

- In Verbindung mit einer zwei Faktor Authentifizierung ist es möglich, auch Personen bei der Anmeldung mit dem Vertrauensniveau hoch zu identifizieren
- Beispiel elektronischer Mitarbeiterausweis, zusätzliche Dienste möglich

- Kosten, Zusatzanwendung

Kryptographische Token Software

- Für das Vertrauensniveau „substantiell“ wird eine zwei Faktor Authentifizierung benötigt. Am besten auch getrennte Hardware.

- Vertrauensniveau „hoch“ kann wegen der Anforderung der Resistenz gegen Duplizierung und Manipulation gegen hohes Angriffspotential durch Softwaretoken nicht erreicht werden.

- Einfacher zu verwalten, preiswerter

One Time Passwords / TAN

Beispiele für TAN Verfahren:

- Mobile TAN - über registrierte Telefonnummer
- push TAN - über die Internet-Verbindung des Mobilgerätes an eine vorher registrierte App übermittelt.
- TAN-Generatoren (auch chipTAN) nutzen eine separate Hardware, den TAN-Generator, zur Erzeugung von vorgangsspezifischen TANs

- Für eine Anmeldung mit dem Vertrauensniveau „substantiell“ muss die 2-Faktor-Authentifizierung richtig ausgestaltet werden.
  Sonst vor allem für das Vertrauensniveau „normal“.

Nutzername / Passwort

Für die Anmeldung einer Person nur Vertrauensniveau „normal“

Bekanntes Verfahren mit den bekannten Schwächen

Nicht-technische Angriffe

- Beobachtung während der Passworteingabe
- „Educated Guessing“ eines Passworts oder von Wiederherstellungsinformationen
- Missbrauch veröffentlichter Passworte
- Phishing

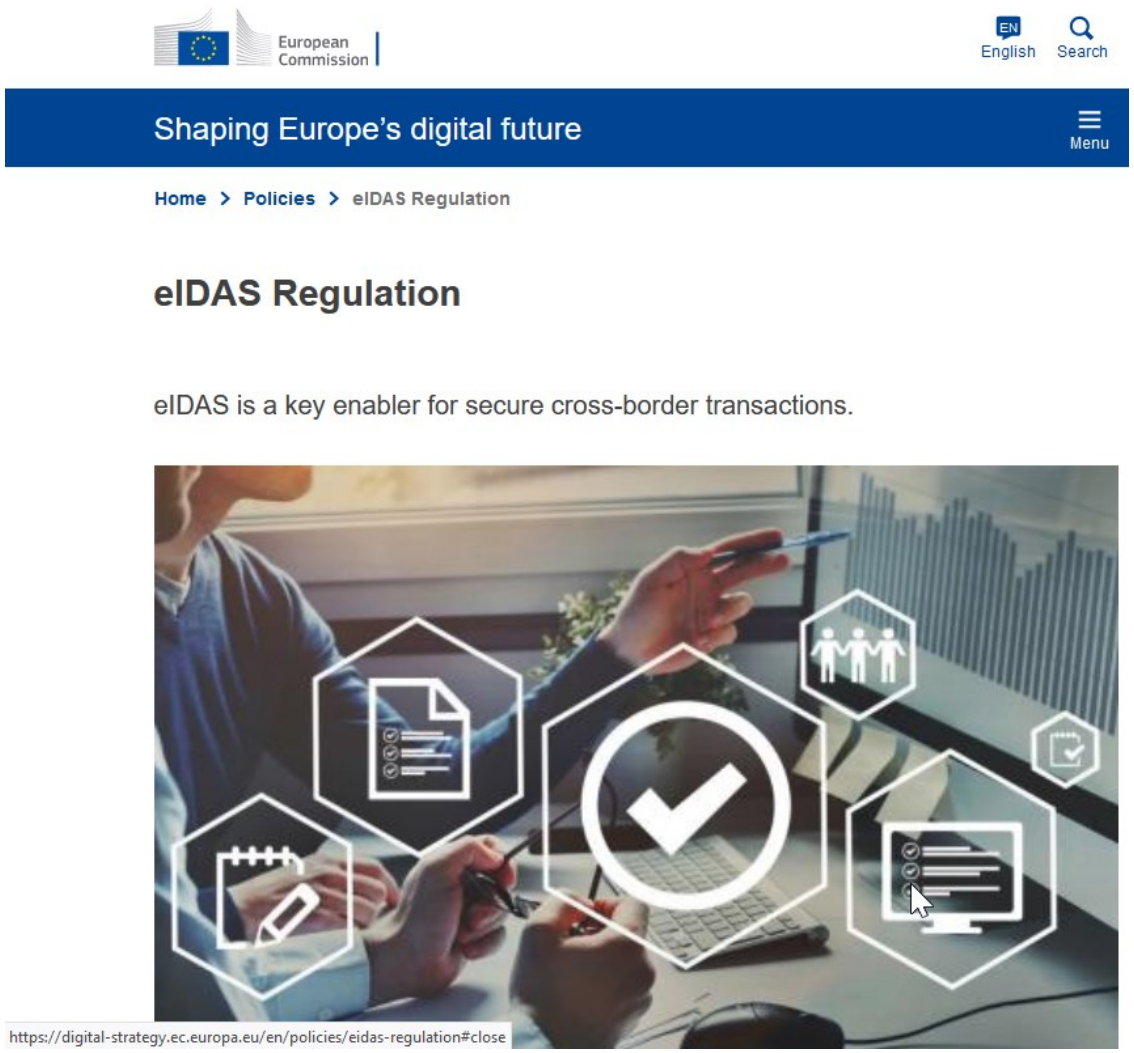
Technische Angriffe

- „Brute Force“ Angriffe
- Wörterbuchbasierte Angriffe
- Kompromittierung eines Systems (Key logging, Traffic Logging)
- Kompromittierung von Kommunikationskanälen („Man-in-the-Middle“)

Wie oft stehen Vertrauensniveau und Bequemlichkeit im Widerspruch

- Nicht immer wird das hohe Vertrauensniveau benötigt
- Möchte man dass die Bürger das Verfahren anwenden, sollte es „öfter“ im Alltag vorkommen, so dass die Mittel zur Hand sind und der Umgang gewohnt ist.
  - Bei einem Verfahren das max. einmal im Jahr angewandt wird, sind Karte und Anleitung irgendwo abgeheftet
  - Die Pin der Bezahlkarte wird auswendig gelernt und die Kreditkarte steckt im Portemonnaie

eIDAS soll den Rahmen schaffen für moderne Konzepte



eIDAS

Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

eIDAS 2.0

von der EU Kommission 2020 zum Review veröffentlicht

Überarbeitung im Gang, Veröffentlichung geplant Herbst 2022

ID Wallet - Idee

Basis Identität aus dem elektronischen Personalausweis

Gegenseitige Anerkennung von verschiedenen (nationalen) Identitäten

Im deutschen Pilotprojekt

- Ergänzung durch elektronischen Führerschein
- Ergänzungen durch weitere elektronischen Ids möglich

Sicherheit: Smartphone + PIN (Hardware + Wissen)

Sicherheit durch Hardware Komponenten

Sicher - aber teuer und unflexibel

Ein Ausweg föderierte Identitäten

- Zugelassener (vertrauenswürdiger) Identitätsprovider
- Aufwand für eine Hauptidentität
- Zusätzliche abgeleitete Identitäten beispielsweise im Mobilphone
  Das Projekt OPTIMOS 2.0 oft zitiert, aber die verwendeten Secure Elements nur begrenzt verfügbar (wenige Handy Serien)

Self Sovereign Identity

Nicht immer werden alle auf einer ID Karte gespeicherten Informationen benötigt.

- Verifiable Credentials (VC)
- Freigabe nur bestimmter Informationen
- Steuerung der Granularität (Beispiel Alterskontrolle)

- Herausforderung Steuerung und Kontrolle: Verteilte Rollen führen zu entsprechenden Prüfstrukturen und müssen auf einander abgestimmt sein. Ein Vorschlag für eine Basis Architektur findet sich bei enisa

Aus der Bitkom Kommentierung

- Geht in die richtige Richtung: Der Vorschlag zur Schaffung der EU ID und Wallet ist ein wichtiger Schritt.
- Im Detail lässt der Vorschlag noch Fragen offen und bedarf der Nachbesserung, insbesondere bezüglich folgender Punkte:
  - Die technischen Details des Designs der Wallet und die zugrunde gelegten Standards sind noch nicht abschließend geklärt und müssen gemeinsam mit der Industrie konsultiert und entwickelt werden. Außerdem ist Kohärenz im Regulierungsrahmen unbedingt sicherzustellen.
  - Für erfolgreichen Wettbewerb mit bestmöglichen Lösungen und einer erfolgreichen Durchsetzung der Wallets sollte sich die EU aus unserer Sicht dafür einsetzen, dass mehrere zertifizierte Wallets nebeneinander im Markt existieren können. Die Anforderungen an die Zertifizierung sollten einheitlich, realistisch und praxisnah von der EU vorgegeben werden.
  - Wir sind der Überzeugung, dass die EU die Mitgliedstaaten ermutigen sollte, digitale Lösungen anzubieten, die für Nutzer attraktiv und überzeugend genug sind, um sie anzunehmen. Eine pauschale, undifferenzierte Verpflichtung bürdet Unternehmen der Privatwirtschaft unnötige Anstrengungen, sowie hohe Verunsicherung und Kosten auf.

https://www.bitkom.org/Bitkom/Publikationen/eIDAS-Review-Digitale-Identitaeten

Andere Ansätze

- OpenID /oAuth2 von OpenID Foundation (OIDF)

- Horizon 2020 Initiatives - Projekte, Erfahrungen

Technische Aspekte

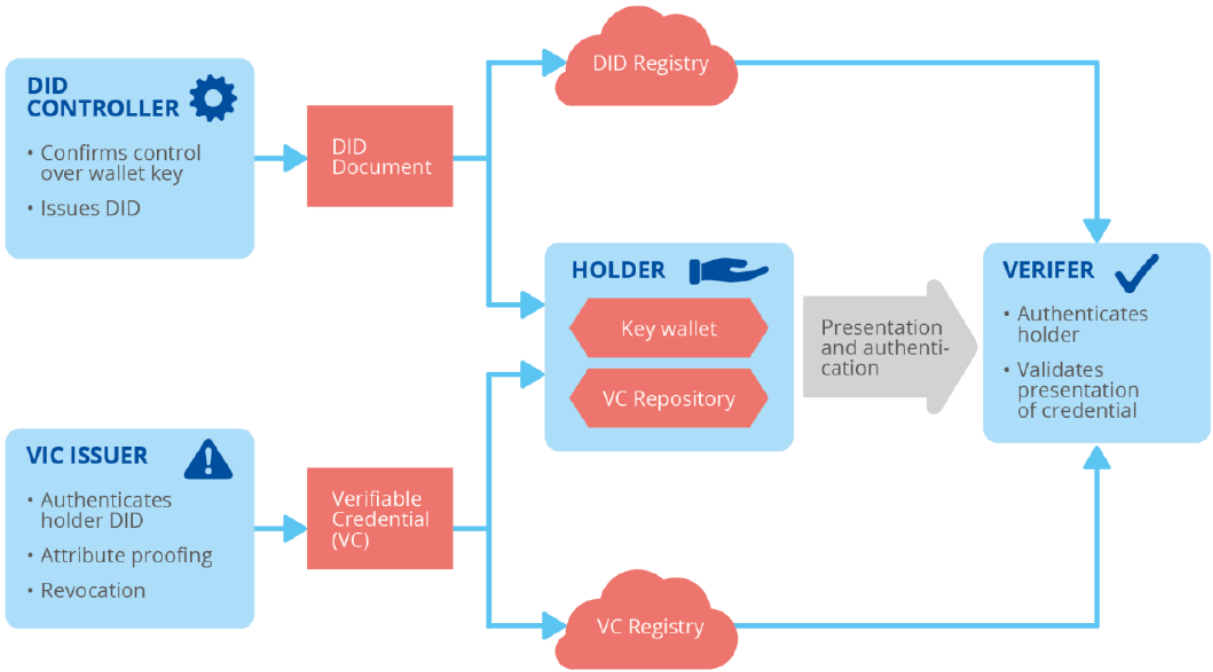
Für einen zentralen Erfolgsfaktor von Geschäftsbeziehungen im Internet gibt es noch keine verlässliche Herangehensweise:

- Aus Sicht eines Dienstanbieters:
  - Authentifizierung Ist diejenige wirklich die, die sie zu sein vorgibt? Besteht das Risiko von Identitätsdiebstahl?
  - Risikoabschätzung Mit welcher Wahrscheinlichkeit sind Identitätsattribute zutreffend? Wie verlässlich ist die Identitätsinformation?

- Aus Sicht eines Individuums:
  - Identitätsdiebstahlrisiko Wie vermeide ich, dass meine Identität missbräuchlich verwendet werden kann?
  - Datenschutz/Privatsphäre Wie behalte ich die Kontrolle über die Verwendung meiner Identitätsinformationen?

Föderierte Identität

- Setzt sich aus dem Zusammenspiel verschiedener Dienstleister zusammen u.a. Identitätsanbieter, Intermediär und Dienstanbieter.
- Die wechselseitigen Aufrufe müssen abgesichert werden



Graphik aus: enisa Digital Identity
ISBN: 978-92-9204-555-5 - DOI: 10.2824/8646 -
Catalogue Nr.: TP-09-22-024-EN-N

Identitätsdiebstahl

- Hauptquelle dürfte immer noch Phishing sein
- Hacken von Firmen bzw. Diensteanbieter bei denen tausende von Passwort Kombinationen und Bezahlinformationen gestohlen werden können
- Handel im Darknet

IT Sicherheit: User - Passwort

Für den Diensteanbieter vorteilhaft der User identifiziert sich über email-Adresse oder Telefonnummer

Für Hacker auch nicht schlecht, weil er „nur noch“ das passende Passwort braucht.

- Wörterbuch Attacken

Häufige Lücke:

- „MickeyMaus116117“ wird oft eine sehr hohe Sicherheit attestiert
- Gleiches Passwort bei mehreren Providern ist ein Problem, wenn einmal gehackt bzw. im Darknet bekannt

Passwort Empfehlungen

Passwort Listen im Browser sind angreifbar, weil der Ort bekannt ist

Passwort Listen in unverschlüsselten Dateien auf dem Desktop meiden

BSI Umgang mit Passwörtern

Passwort Manager

Passwort ändern bei Auffälligkeit wie Mitteilung über unbekannte Anmeldungen, wenn der Computer von Schadsoftware befallen ist/war, ...

IT Sicherheit: gestohlene Passwörter

Nachfragen, ob mein Passwort geleakt wurde …

- Identity Leak Checker Hasso Plattner Institut
- https://sec.hpi.de/ilc

- „Have I been pwned”
- https://haveibeenpwned.com/

2-Faktor-Authentisierung

- Aktivieren wenn möglich
- Abrufen der Push TAN aus einer Passwort oder Biometrie geschützten App
- Am besten TAN App auf einem anderen Gerät installiert.

- Herausforderung Bequemlichkeit

Fragen / Diskussion