E-Government Standards

Grosse Erwartungen

IAM in einem föderalen System: Was ist der Schlüssel zum Erfolg?

Gefahren, Abgrenzung zum BGEID und UIDG, Notwendigkeit von Standards, Möglichkeiten

Daniel Muster
8003 Zürich
daniel.muster@it-rm.ch
www.it-rm.ch

Ein IT-Projekt ist ein Erfolg u.a. dann, wenn es die Erwartungen erfüllt

Inhalt des Vortrags

- (Wecken von falschen) Erwartungen bei IAM im eGovernment
- Präsentation der IAM Komponenten
- Abgrenzung zum UIDG und E-ID-Gesetz
- Notwendigkeit von Standards
- Hinweise zur (IT-)Sicherheit (Gefahren)

Hinweis

Eine Liste von Referenzen ist am Ende dieser Präsentation aufgeführt.

Problematik bei Erwartungen

- Widersprüchliche Erwartungen. Z.B. ein Prozess soll anonym und gleichzeitig vertraulich sein.
- Priorisierung der Erwartungen wegen des Kostendrucks. Z.B. beim e-Voting zwischen Genauigkeit des Resultats des Urnengangs und Wahrung des Stimmgeheimnisses.
- Falsche Erwartungen wecken. Z.B. eine elektronische Signatur unter ein Dokument schützt dieses gegen Veränderung (Schutz der Unveränderbarkeit). Oder eine IT-Anwendung ist benutzerfreundlich (einfach und bequem), sicher, hat eine hohe Funktionalität und ist kostengünstig

Der Fokus des Vortrags liegt auf dem Wecken falscher Erwartungen.

IAM (Identity Access Management)

Komponenten

Access

Identity

Registrierung, Identifikation und Erfassen der Personen-daten, wie:
- Name
- Adresse
- Handy Nr
- E-Mail
- …….

Authentisierung

Festlegen mit welchen Mitteln, wie:
- UserID, Passwort
- mit SMS
- elektroni-sche Zertifikate
- ……

Autorisierung

Rechte definieren, zuteilen

Rechte gewähren

IT-Dienst

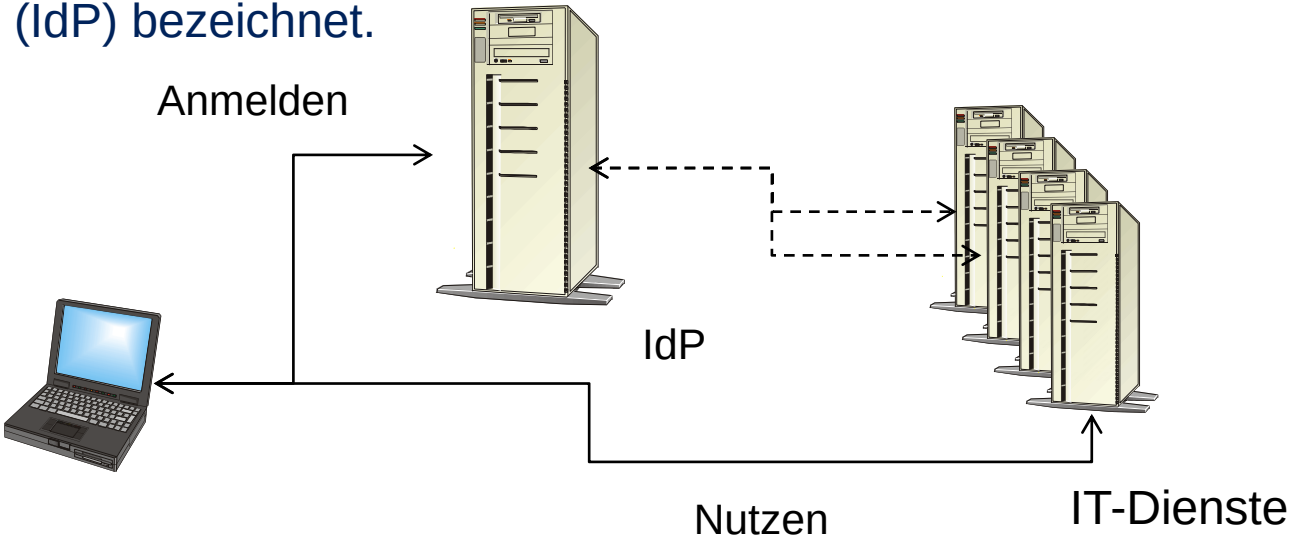
IT-Dienste wie
- Web-Mail
- Register
- Patienten-dossier
- ……

Delegation der Authentisierung an eine zentrale Stelle möglich

Begriffe

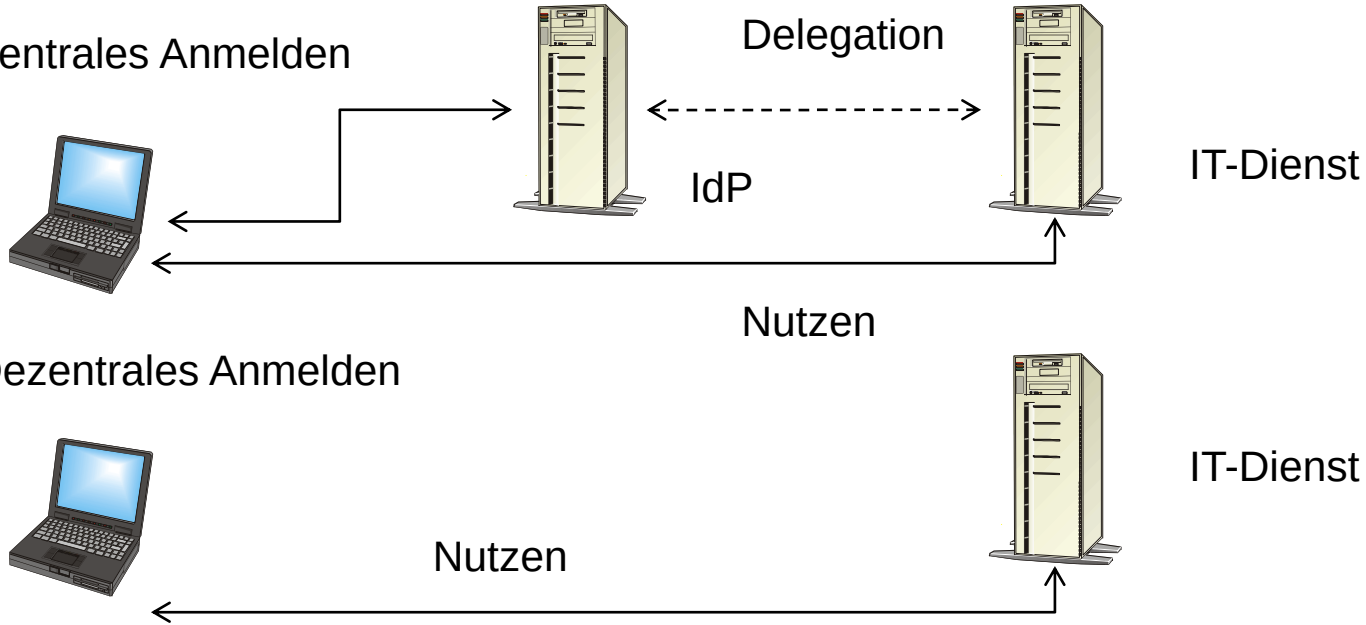
Wird die Authentisierung des Users für verschiedene IT-Diensten zentral an ein System delegiert, dann spricht man auch von Single Sign ON (SSO)

Das System, welches die Authentisierung vornimmt, wird u.a. als Identity Provider (IdP) bezeichnet.



Falsche Erwartungen I

Gleichsetzen der IT-Sicherheit bei zentralem Anmelden für viele Systeme (SSO) a) mit dezentralem Anmelden beim jeweiligen IT-Dienst (b). Letzteres (b) kann enorm viel sicherer ausgestaltet werden, siehe [1]



Wichtig

Das Authentisieren und Identifizieren sind strikte auseinander zu halten. U.a. weil:

- Die Mittel/Merkmale zum Authentisieren sind übertragbar (PIN, Smart Card, SecureID). Die Merkmale zum Identifizieren zum Glück (noch) nicht.
- Informationen zum Authentisieren, wie elektronische Zertifikate, können widerrufen werden, Informationen zum Identifizieren, wie biometrische Angaben, jedoch nicht. Sind biometrische Informationen einmal bekannt gegeben, können sie nicht zurückgerufen werden. Bsp. Indien [2]
- => Biometrische Informationen sollen beim Authentisieren nicht verwendet werden.

Falsche Erwartungen II

Das Authentisieren („Sich Ausweisen in der IT“) wird dem Identifizieren gleichgestellt. Z.B.

- In Bundesgesetzen (ZertES, BGEID, **Büpf**)
- => Wecken falscher Erwartungen/ falscher Assoziationen beim Sammeln von Randdaten (Büpf) => z.B. Justizvorfall in Dänemark [3]

Identifikator (Personen-Nr. E-ID-Nr.) dient dem Identifizieren

- Ein Identifikator ist lediglich ein Schlüsselattribut (Verwaltungsnummer) für Personendaten. Gleiches gilt für die AHV-Nr.
- Analogie dazu: Nummernschild beim Auto und Fahrzeughalter/Fahrer [5]

<u>Schlussfolgerung: Authentisieren (Das «sich Ausweisen» in der digitalen Welt) ist «lediglich» die Zuordnung der Verantwortlichkeit.</u>

Falsche Erwartungen II

Mehr Sicherheit mit der Verwendung eines Handy in Kombination mit SMS beim Authentisieren

- Die grössten Sicherheitsprobleme bestehen bei der Attacke auf bestehende Verbindungen (CSRF, CSS) oder bei der Verlinkung von Informationen. Betreffend Verlinkung bei XML s. eCH-0091.
- Die Sicherheitstechnologie und die Anwendung sind meist nicht aufeinander abgestimmt (miteinander «verschweisst»).
- Grundsätzlich nur Informationen zum Authentisieren verwenden, welche rasch widerrufen werden können. E-Mail-Adresse?, Handy-Nr?

Abgrenzung, Umfang UIDG, E-ID-Gesetz

Das **UIDG** (Bundesgesetz über die Unternehmens-Identifikationsnummer) regelt im Wesentlichen:

– das Erfassen der Daten betreffend eine juristische Person, die Speicherung dieser Daten und die Zuordnung einer Administrativ-Nr. (UID-Nr.).

Das E-ID-Gesetz (**BGEID**) regelt u.a. :

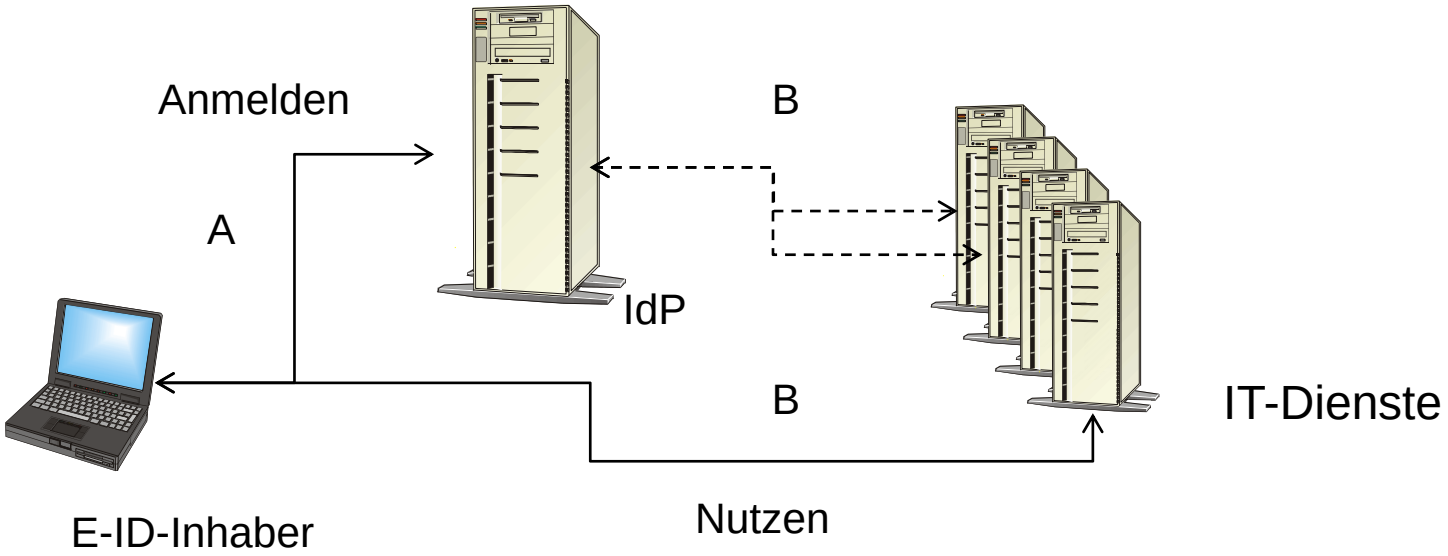
– das Erfassen der Daten natürlicher Personen

– Weitergabe der Personendaten an die IT-Dienstanbieter

Unklar ist, weil nicht im E-ID-Gesetz explizit beschrieben/definiert:

– Was eine E-ID ist, ob nur eine «UID» für natürliche Personen oder ob noch eine zentrale Authentisierung durch den IdP enthalten ist.

Falls eine zentrale Authentisierung enthalten ist, dann werden im BGEID in etwa noch die Komponenten/Schnittstellen A geregelt, nicht aber Komponenten/Schnittstellen B.



Die Komponenten B können nicht in einer Bundesvorschrift geregelt werden. Doch es bedarf einer Koordination, damit es reibungslos(er) funktionieren wird. => (eCH)-Standards werden benötigt.

eCH-Dokument [4] verfasst, was alles nicht durch eine Vorschrift betreffend E-ID-Gesetz geregelt werden kann/darf, aber doch genormt werden muss.

Besondere Konstellation im eGovernment

IT-Dienste, IdP und User können je in einer anderen «Gesellschaftsform» (juristische, natürliche Person, öffentlich-rechtliche Anstalt, Verwaltung) sein. Typischerweise:

- User (Privatperson, Vertreter einer juristischen Person)
- IdP (Privatunternehmen, Organisationseinheit einer Verwaltung)
- IT-Dienst (Organisation der Verwaltung)

Quellennachweis

[1] **Florian Forster, Daniel Muster**, Vergleich Authentisierung, http://www.it-rm.ch/files/Technologie_Vergleich_1_1.pdf

[2] **ARD Reportage**, Pässe für Kriminelle, https://www.youtube.com/watch?v=VhbMVtcB_mY

[3] **Echo der Zeit**, Falsche Daten könnten zu falschen Urteilen geführt haben, https://www.srf.ch/play/radio/echo-der-zeit/audio/falsche-daten-koennten-zu-falschen-urteilen-gefuehrt-haben?id=c7ea15ba-1bd2-4c75-a04b-979f32667cee&expandDescription=true

[4] **eCH,** Möglichkeit und Notwendigkeit von Standards im Umfeld des Bundesgesetzes über elektronische Identifizierungsdienste (BGEID)

[5] **Daniel Muster**, Irrtum - Identifizieren versus Authentisieren, Definition von Sicherheitsdiensten, http://www.it-rm.ch/dokumente.html