



Digitale Identität und Sicherheit

Referat anlässlich der Innovationstagung

16. Mai 2018 19:50 – 20:10

HSR Hochschule für Technik Rapperswil, Raum 4.101



- Ausgangslage / Probleme bei der «klassischen» Authentifizierung
- Multifaktor Authentifizierung
- Authentifizierung mittels Drittdienst
- Probleme und Gefahren bei Authentifizierungen
- Vor-/Nachteile der verschiedenen Lösungen
- Fazit / Fragen



Fakten Valentin Tanner / taNET:

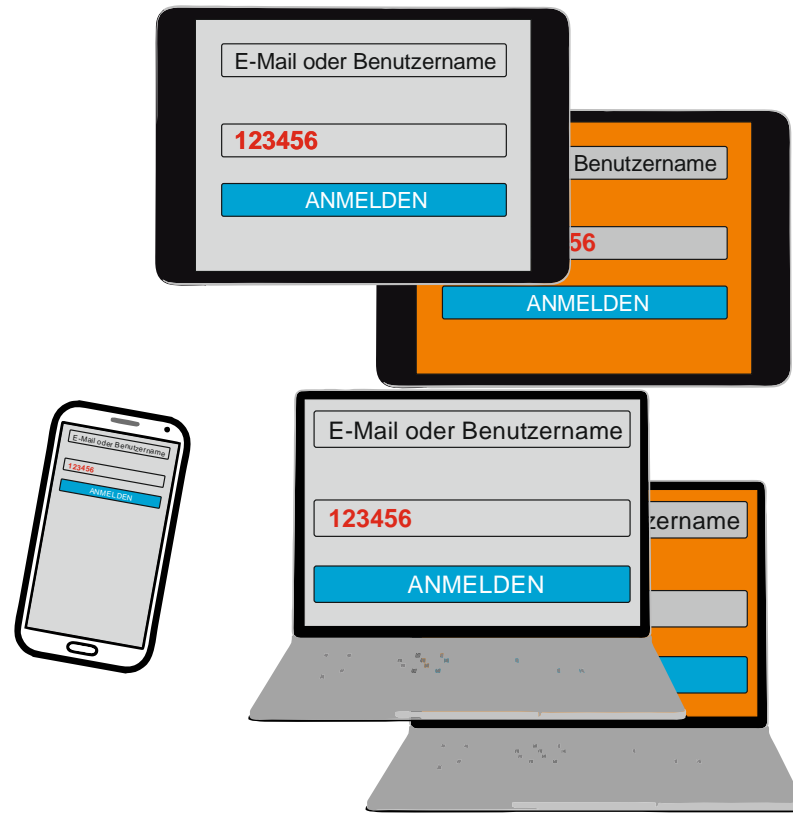
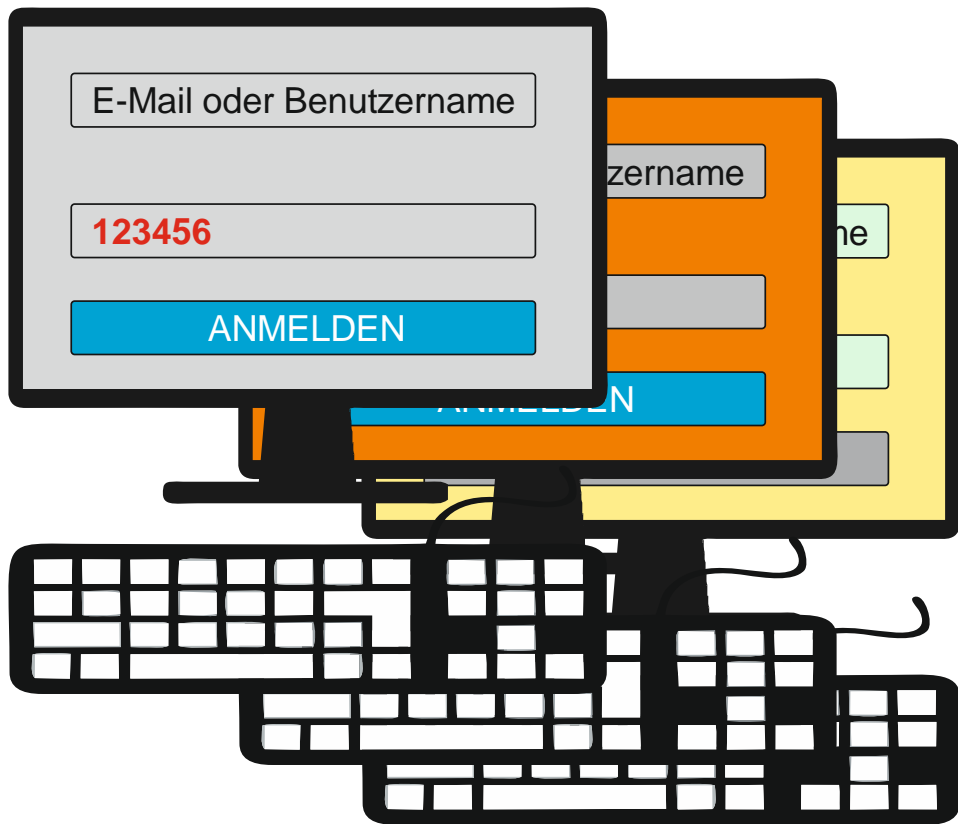
- Gründung der taNET GmbH nach meinem Informatikstudium im 2001
- Unabhängiges Ingenieurbüro mit den Schwerpunkten Netzwerkdesign und IT-Sicherheitsplanung sowie Überprüfung von IT-Systemen und Prozessen
- Firmengröße: 10 Mitarbeiter
- Eigene Softwareentwicklung
 - Benutzerverwaltung – Identity Management **ADPROFILER**
 - Authentifizierungslösung **LOGINity**
 - Kennwort-Verwaltung **Turtle**
 - Diverse Netzwerk- und Verwaltungstools





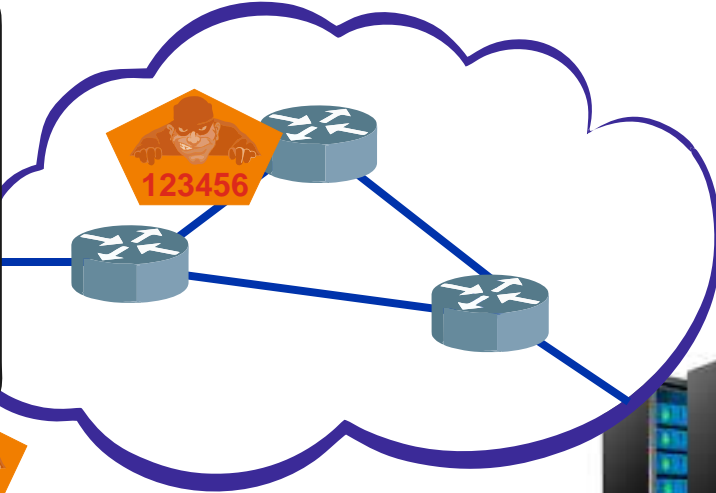
Digitale Identität und Sicherheit

Ausgangslage «klassische» Authentifizierung



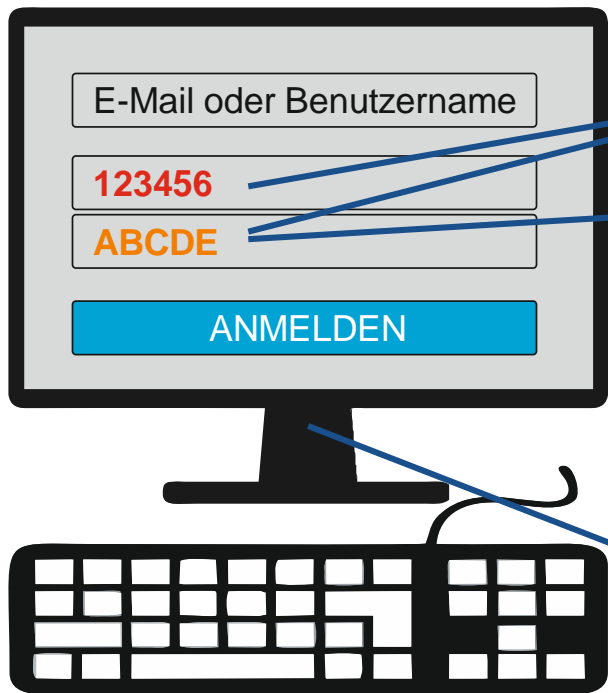
Digitale Identität und Sicherheit

Problem / Gefahren



Digitale Identität und Sicherheit

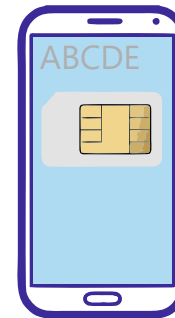
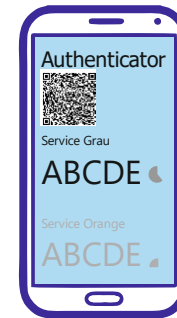
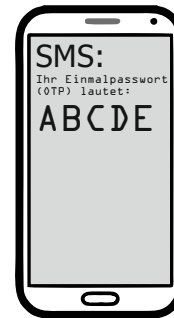
Multifaktor-Authentifizierung



Wissen – Kennwort



Besitz – Code

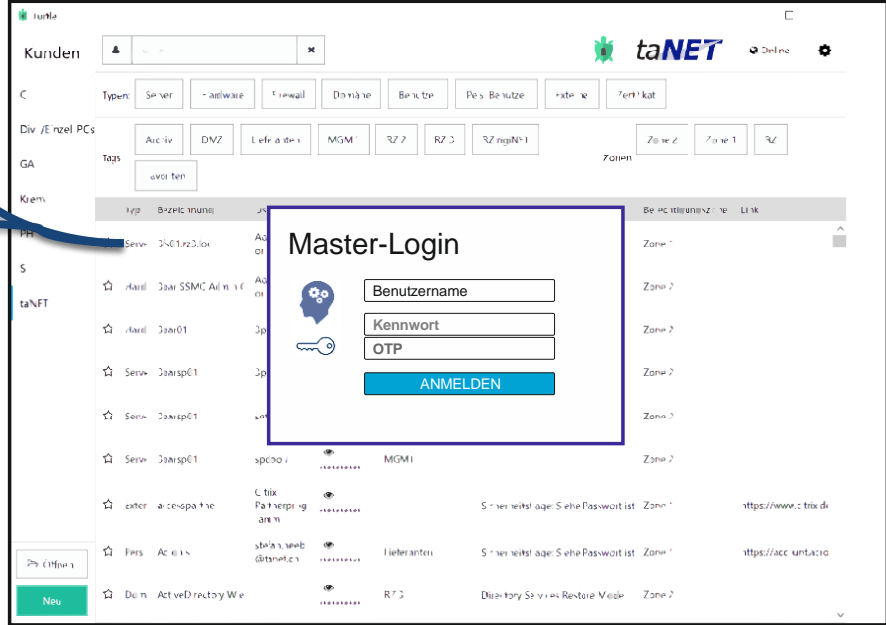
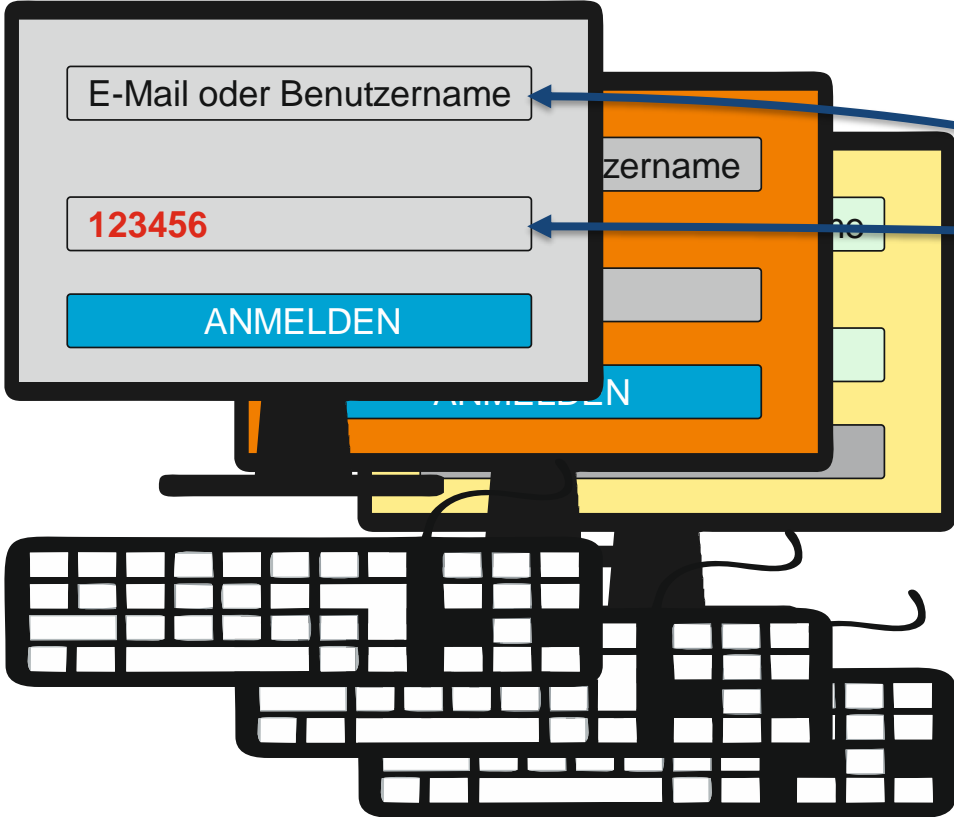


Merkmal – «DNA»

Fingerabdruck, Gesichts-, Stimm-, Iriserkennung,
Tippverhalten, Handgeometrie, Standort, Browser, IP, ...

Digitale Identität und Sicherheit

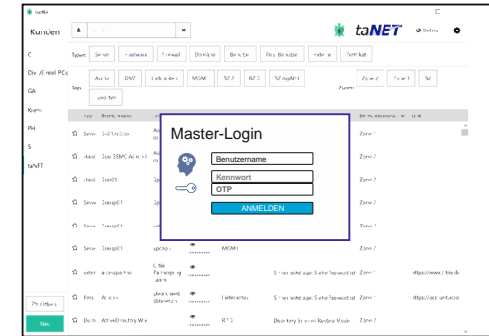
Kennwort Manager





Anforderungen an einen Passwort-Manager

- **Sicheres Speichern der Anmeldeinformationen**
Offene Implementierung von aktuellen und geprüften kryptographischen Algorithmen
- **Zwei-(Mehr) Faktor-Authentifizierung**
(Wissen, Besitz und/oder mehrere Merkmale)
- **Komplexe Kennwort-Generierung**
- **Übernahme/Übergabe der Anmeldeinformationen**
- **Sicheres Teilen von Passwörtern**



KeePass



dashlane



1Password



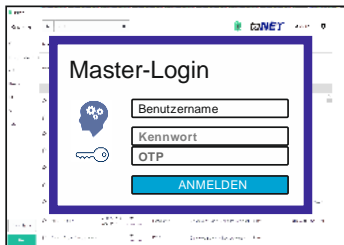
LastPass



Keepersecurity

Digitale Identität und Sicherheit

Beispiel einer Anmeldung im Online-Shop



Kontakt | Hilfe | Über uns | Standorte | Social Media | Stellenangebote | Deutsch | Inkl. MwSt.

GALAXUS Suche

ANMELDEN 0 0 0

GESAMTSORTIMENT

- HAUSHALT
 - Raumklima
 - Haushaltgrossgeräte
 - Kaffee + Tee
 - Küche
 - Gourmet + Genuss
 - Waschen + Bügeln
 - Handarbeit
 - Saugen + Reinigen

Top 10 Kategorien

Haushalt

Küchenmaschinen-Guide: Finde das passende Gerät für dein Budget

Produktpromotion

Produkte...
Stöber...
und las...

Kundenkonto X

Benutzername

Passwort

Hast du dein Passwort vergessen?

Angemeldet bleiben

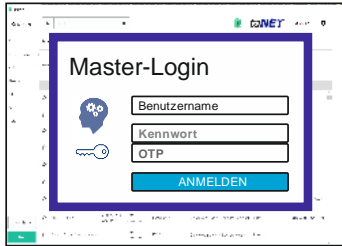
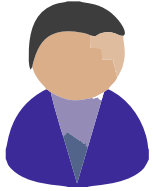
Anmelden

Mit externem Konto anmelden i

f G W

Digitale Identität und Sicherheit

Beispiel einer Anmeldung im e-Finance Portal



PostFinance+

Hilfe und Support ▾

Login

PostFinance ID Mobile ID

E-Finance-Nummer / Benutzername

Passwort

[Passwort vergessen / ändern >](#)

Falls vorhanden:

Benutzeridentifikation

Weiter

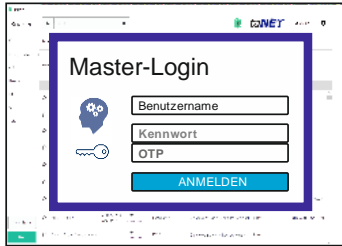
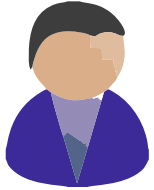
Hilfe zum Login

- 1 Login-Verfahren wählen:
 - Kartenlesegerät + PostFinance Card oder
 - Mobiltelefon + Mobile ID
- 2 E-Finance-Nummer oder Benutzername:
 - 9-stellige E-Finance-Nummer oder
 - selbstgewählter Benutzername
- 3 Benutzeridentifikation:
 - Nur eingeben, wenn dieselbe E-Finance-Nummer für mehrere Benutzer gilt (z.B. Partnerkonto, Geschäftskonten)

[Weitere Hilfe >](#)

Digitale Identität und Sicherheit

Beispiel einer Anmeldung bei ZHservices



ZHservices

Willkommen bei ZHservices

Anmelden

Benutzername

Passwort

Anmelden

Digitale Identität und Sicherheit

Beispiel einer Stimmabgabe bei E-Voting



Initialisierungscode



Prüfcodes



Bestätigungscode



Finalisierungscode



Hilfe DE

[Gesetzliche Bestimmungen](#) > Stimmabgabe starten

Stimmabgabe starten

Geben Sie Ihren Initialisierungscode und Ihr Geburtsjahr ein. Der Initialisierungscode befindet sich auf dem Stimmrechtsausweis, den Sie auf dem Postweg erhalten haben. Drücken Sie anschließend auf STARTEN und haben Sie bitte einen Moment Geduld. Bitte beachten Sie, dass während des Prozesses der Stimmabgabe die Webseite nicht neu geladen werden darf.



Initialisierungscode [Was ist das?](#)

Es spielt keine Rolle, ob Sie Gross- oder Kleinbuchstaben verwenden.

d e 9 f 9 j 9 g y z f 6 h e s a t 9 f p X

Geburtsjahr

1 9 7 0 |

STARTEN

Digitale Identität und Sicherheit

Authentifizierung beim Anbieter



Online-Shop

Zahlungsverkehr

Ausfüllen der Steuererklärung



Digitale Identität und Sicherheit

Authentifizierung mittels Drittdienst



Kontakt | Hilfe | Über uns | Standorte | Social Media | Stellenangebote | Deutsch | Inkl. MwSt.

GALAXUS

Suche

Anmelden

Kundenkonto

Benutzername

Passwort

Hast du dein Passwort vergessen?

Angemeldet bleiben

Anmelden

Mit externem Konto anmelden

f G Windows

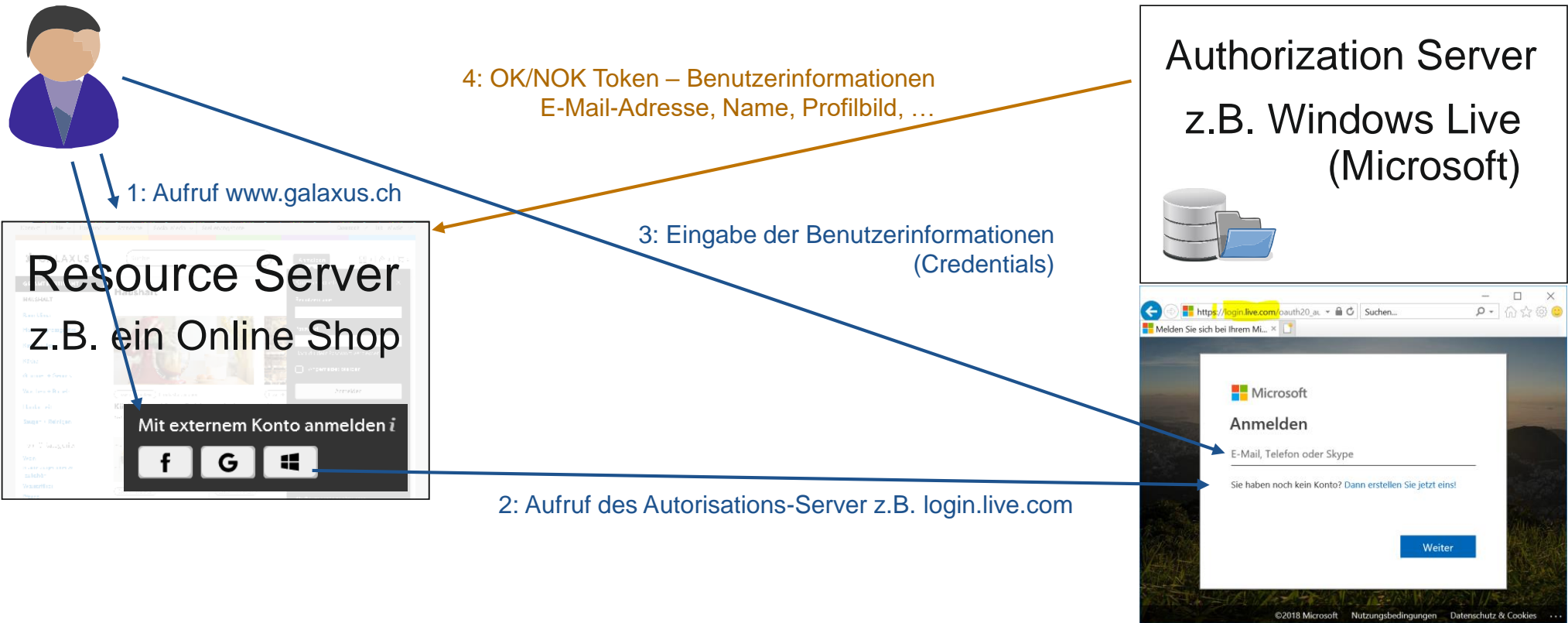
Haushalt

Küchenmaschinen-Guide: Finde das passende Gerät für dein Budget

- Facebook
- Google
- Twitter
- Yahoo
- Microsoft
- Apple-ID
- MobileID
- swissID
- SwissID
- Switchaai
- Switch edu-ID
- ...

Digitale Identität und Sicherheit

Ablauf einer Authentifizierung mittels Drittdienst





Digitale Identität und Sicherheit

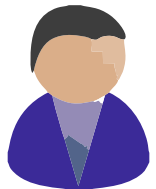
Authentifizierung mittels Drittdienst

- Komfortsteigerung für den Endbenutzer (Kennwort-Verwaltung, Datenübertragung)
- Bessere Datenqualität für den Betreiber des "Resource Server" (Online-Shop)
- Endbenutzer gibt Loginzeiten, Interesse und Kaufverhalten an den Betreiber des "Authorization Server" weiter (z.B. an Facebook, Google, Microsoft, ...)
- Anmeldung beim "Authorization Server" z.B. Facebook -> automatische Anmeldung beim "Resource Server" respektive Online-Shop
- Nur Authentifizierung / keine Autorisierung (Rechte)
- Bei richtiger Implementierung (OAuth 2.0) und bei richtiger Anwendung durch den Benutzer ist eine sichere Authentifizierung gewährleistet. Datenschutz?



Digitale Identität und Sicherheit

Authentifizierung mittels SwissID



Benutzer -
Identitätsbesitzer

Online Shop

Post

Bank

Verwaltung

Gesundheit

Versicherung

Transport

...

seit Oktober 2017

Modul 1:
Einloggen

Frühjahr 2018

Modul 2:
Freigeben

ab Sommer 2018

Modul 3:
Bestätigen

ab 2020

Modul 4:
Ausweisen

Übergabe von überprüften Identitätsdaten.
Foto/Video Identifikation mit Reisepass oder
Identitätskarte

Modul 5:
Unterschreiben

Rechtsgültige Signatur von Verträgen und anderen
Dokumenten.
Bundesgesetzes über die elektronische Signatur
(ZertES) und der EU-Richtlinie (eIDAS) sollen erfüllt
werden.

Authorization Server



SwissSign

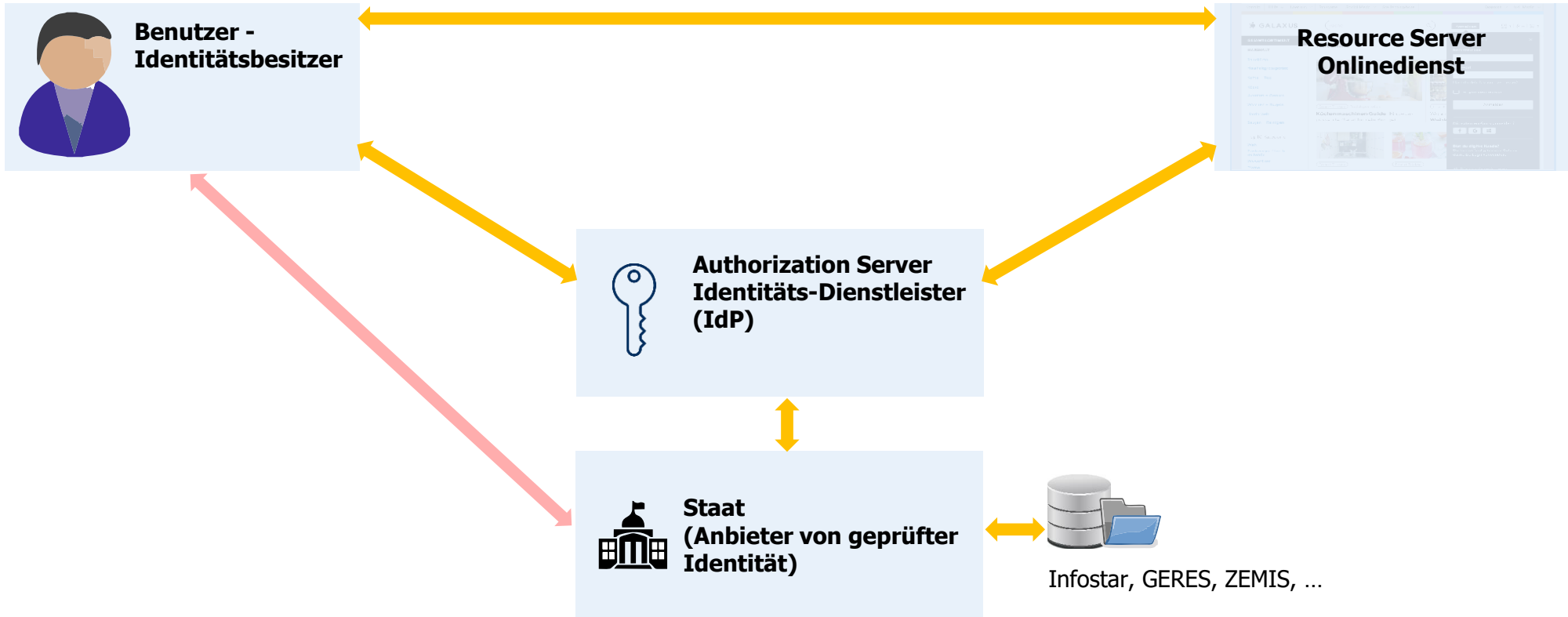
Joint Venture aus staatsnahen Betrieben,
Finanzunternehmen, Versicherungsgesell-
schaften und Krankenkassen.

SBB
Schweizerische Post
Swisscom
Credit Suisse
Entris Banking
Raiffeisen
Six Group
UBS
Zürcher Kantonalbank

Axa
Baloise
CSS
Helvetia
Mobiliar
SWICA
Swiss Life
Vaudoise
Zürich

Digitale Identität und Sicherheit

Authentifizierung - Interessenkonflikte





- Bei Anwendungen innerhalb eines Unternehmens reicht eine reine Authentifizierung nicht aus, es wird zusätzlich eine Autorisierung für die Vergabe der Zugriffsrechte benötigt.
- Sicherheit, Datenschutz und Benutzerkomfort stehen auch bei der Authentifizierung im Gegensatz zueinander.
- Technisch gibt es Möglichkeiten, die Sicherheit aktuell zu gewährleisten.
- Bei der Entwicklung von Systemen muss auch die Sicherheit im Fokus stehen.
- Eingesetzte Technologien, Verfahren und Integrationen (Designs) müssen periodisch überprüft und der «aktuellen Bedrohungslage» angepasst werden.
- Vertrauen ist gut – Kontrolle ist besser ;-)



Vielen Dank für Ihre Aufmerksamkeit



Valentin Tanner
Dipl. Informatik Ing. HTL
taNET GmbH
tanner network & security engineering
Parkstrasse 25, 6410 Goldau

Tel: 041 857 07 07 Direkt: 041 857 07 10
valentin.tanner@taNET.ch
<http://www.taNET.ch>