HSLU Hochschule Luzern

E-ID für die Schweiz +++

Der nächste Versuch mit Fokus SSI

CAS BLOCKCHAIN

Studienleiter:
Prof. Dr. Georges Grivas
Co-Studienleiter und Betreuer:
Marcel Harmann

MATHIASGENZ
MICHELLEDÜNNER-MELI
MIRCOPIETRINFERNO
PATRICKBROUWER

Einleitung

Ziele und Vorgehen

Ziele der Transferarbeit

- Identitätserfassung im digitalen Raum mit SSI ganzheitlich untersuchen
- Evaluation einer «Stossrichtung»
- Identifikation der Schlüsselfaktoren für eine erfolgreiche Adaption

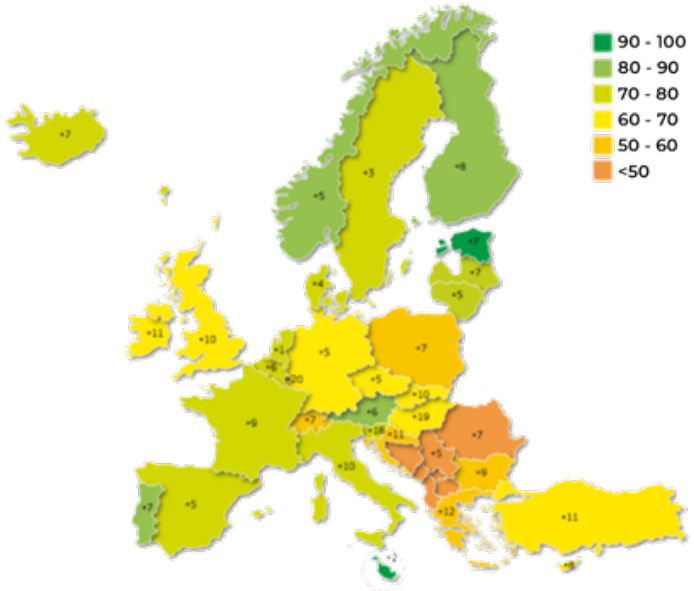
Einleitung

Einleitende Fragenstellungen

- Warum ist das Internet so erfolgreich?
- Weshalb sind Google/Facebook Login so erfolgreich?

Urgency

Die Schweiz hinkt bei eGovernment Europa hinterher



EU eGoverment Benchmark 2020[1]

- Die Schweiz hinkt im eGovernment europaweit stark hinterher
- Die E-ID ist essentiell für die digitale Verwaltung

Ohne E-ID sei effiziente Verwaltung kaum möglich

Doch die E-ID sei eine zentrale Voraussetzung, um die sichere und einfache Kommunikation zwischen der Bevölkerung und der Verwaltung möglich zu machen, glaubt Giarritta. Er will sich darum weiter für deren Einführung einsetzen: «Ohne E-ID wird die digitale Verwaltung langfristig nicht funktionieren, das zeigt auch die Entwicklung im Ausland.»

« Ohne E-ID wird die digitale Verwaltung langfristig nicht funktionieren. »

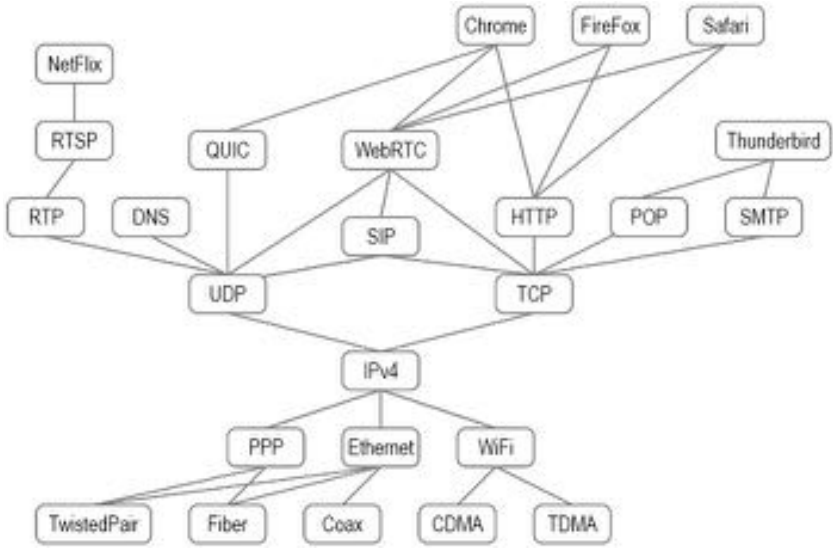
Peppino Giarritta
Leiter Digitale Verwaltung Schweiz

SRF 2021[2]

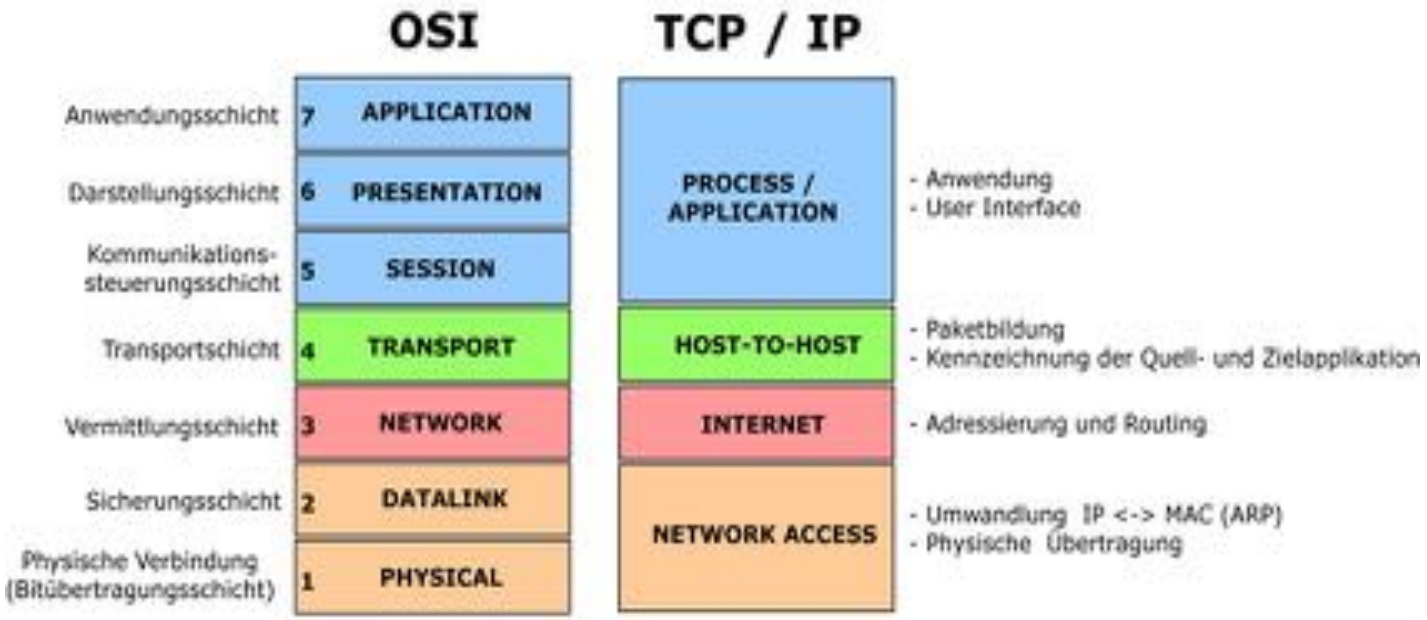
[1]Quelle: eGovernment Benchmark 2020: eGovernment that works for the people | Shaping Europe's digital future (europa.eu
[2]Quelle: https://www.srf.ch/news/schweiz/digitalisierung-der-verwaltung-der-leidensdruck-der-verwaltung-ist-oft-noch-zu-wenig-gross

Urgency

SSI kann das Problem des Internets der fehlenden Vertrauensschicht lösen



«Internet Protocoll as «The narrow waist»[1]



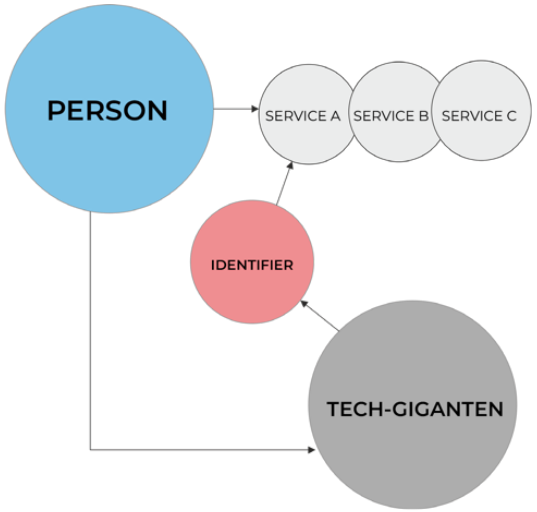
The OSI-Modell[2]

„The Internet was built without an identity layer“
Kim Cameron, Chief Architecture, Microsoft, May 2005

[1]Quelle: Papers/KERI_WP_Papers/KERI_WP_2.x.web.pdf at master · SmithSamuelM/Papers (github.com)2.x.web.pdf at master · SmithSamuelM/Papers (github.com)
[2]Quelle: https://kompendium.infotip.de/netzwerktechnologie2-referenzmodelle-und-protokolle.html

Urgency

Die Tech-Giganten besitzen unsere «Identität»



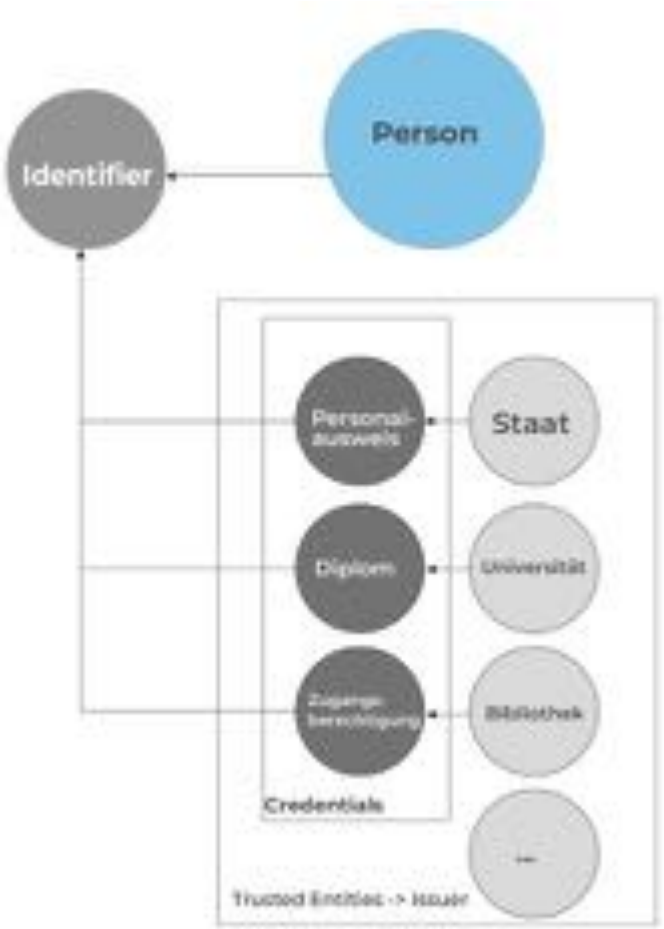
Wahlmanipulation – Cambridge Analytica Daten Skandal[1]

- Die Tech-Giganten besitzen unsere Identitäten
- Datenmissbrauch gefährdet die Souveränität des Einzelnen und die Demokratie

[1]Quelle: Facebook Cambridge Analytica Data Scandal Revealed - Fawad Khan | Facebook, Teknoloji, Ordu (pinterest.dk)

Schlüsselfaktoren

Der Identifier gehört den Menschen



- Der Identifier gehört den Personen
- Ist der Staat in der Hoheit des Identifiers, ist die Lösung nicht besser als heute
- Der Staat als Herausgeber stellt und kontrolliert nur die ISSUER-Infrastruktur und gibt darüber die Credentials für die Basis E-ID aus

Schlüsselfaktoren

Darum sind Facebook & Co. erfolgreicher

Die Kernanforderungen	Google/Facebook Login	SwissID
• Benutzerfreundlich	Ja	Ja
• Kompatibilität / Interoperabilität / Einf. Verbreitung	Ja	Nein
• Hoher Datenschutz	Niedrig	Mittel
• E-ID Durch den Staat	Nein	Nein
• Privacy by Design	Nein	Teilw.
• Datenhoheit bei Nutzer	Nein	Nein
• Datensparsamkeit	Nein	Ja
• Einfaches Onboarding	Ja	Ja
• Kostenlos für NutzerIn	Ja	Ja

Fazit

Die Kernvoraussetzung für eine erfolgreiche Adaption, ist aus der Erfahrung, die Kompatibilität, die Interoperabilität und die einfache Verbreitung der Lösung. Besonders für den Holder wie auch den Verifier.

Schlüsselfaktoren

Unsere Zukunft verschiebt sich in die digitale Welt

Metaverse

- Megatrend
- Web3.0 ermöglicht Besitz und Tausch
- Arbeitsplätze und mit ihnen die Menschen verlagern sich in das Metaverse
- Staat muss und will seine Bürger in dieser Welt identifizieren

DeFi

- DeFi erlebt massives Wachstum
- Regulatorik wird Identifikation voraussetzen

Fazit

Eine staatlich kontrollierte Lösung, wird mit der dynamischen Entwicklung nicht schritthalten können.

Schlüsselfaktoren

Der Anpassungsfähigere gewinnt!

Permissioned vs. Permissionless

- Um ein maximal offenes Ökosystem zu etablieren, müssen alle «mitmachen» dürfen - analog dem Internet.
- Permissioned Systeme werden zwangsläufig eingeschränkt. Die staatliche Governance wird das System schwerfällig machen. Top-down Evolution ist per se träge und hat wenig Dynamik.
- Die digitale Welt entwickelt sich Bottom-up in einer hohen Dynamik, analog dem Internet.
- Permissionless Blockchains sind so gebaut, dass sie kein Vertrauen brauchen, da mit der Kryptografie die Wahrheit erstellt wird. Jeder kann teilnehmen und maximale Offenheit ist von Grund auf gegeben.
- Permissioned Systeme setzen Vertrauen voraus. Vertrauen zu etablieren kostet Zeit und Geld.

Schlüsselfaktoren

Der Anpassungsfähigere gewinnt!

Permissioned vs. Permissionless

- Integrität: Höher bei Permissionless, da unveränderbar.
  (Bei Permissioned könnte Konsortium oder Berechtigter ändern)
- Verfügbarkeit: Höher bei Permissionless, da weltweit dezentral und verteilt.
  (Beispiel Ausfall Betreiber)
- Angriffsfläche: Bei Permissioned höher, da Nodes bekannt sind.
  (z.B. für DDoS Attacke)

Fazit

Permissionless Blockchains bieten die beste Voraussetzung, damit ein offenes Ökosystem florieren kann.

Top Risiken

- Heutige verfügbare Blockchains (Generation 3) haben noch keinen langen proof record. Ethereum (Generation 1) hat aktuell Skalierungsprobleme und setzt auf Energie ineffizienten Konsensus-Algorithmus.
- Verständnis und Akzeptanz bei der Bevölkerung.

Auflösung der Einstiegsfragen

Das Internet:

- hat bis heute, das am schnellsten gewachsene, weltweite Ökosystem hervorgebracht.
- ist erfolgreich, da es offen ist und jeder teilnehmen kann
- dynamisch ist mit einer dezentrale Entwicklung und Community Driven

Google/Facebook Login sind so erfolgreich weil es:

- für den Nutzer sehr einfach und bequem zu nutzen ist
- für den Nutzer kein Geld kostet
- für den Webseitenanbieter einfach einzubauen ist

Fazit

Permissionless Lösungen sind für die E-ID zu berücksichtigen!

Öffentliche, Permissionless Blockchains bieten dabei die besten Voraussetzungen um den Anforderungen gerecht zu werden:

- Entwickeln sich mit der Dynamik des Internets
- Maximale Offenheit
- Höhere Daten-Integrität
- Höhere Verfügbarkeit

Permissionless Lösungen sollten ernsthaft geprüft werden!

+ + +

THANK YOU

MATHIASGENZ
MICHELLEDÜNNER-MELI
MIRCOPIETRINFERNO
PATRICKBROUWER

HSLU Hochschule Luzern

CAS Blockchain Transferarbeit

CAS.BLOCKCHAIN