

Souveräne Digitale Identität (SDI) / Self-Sovereign Identity (SSI) & FreedomBox im Zeitraffer für Eilige

Das ist ein Versuch jenen, die nicht die Zeit aufbringen wollen oder können den ganzen Abend (insgesamt knapp über 2 Stunden) zu konsumieren, wesentliche Elemente in geraffter Form zu vermitteln. Die zeitlich weitaus überwiegende Diskussion ist nicht in ein paar Aussagen zusammenzufassen – die muß man nachhören. Dieser Text konzentriert sich auf das Kommentieren ausgewählter Folien welche die Diskussion begleitet haben.

Vor dem Weiterlesen bitte aus Teil1 der Videoaufzeichnung ab Minute 5:10 die 10 minütige Einführung anschauen.

=====

Willkommen zurück!

... es geht weiter mit der Präsentation „Souveräne_Digitale_Identität2018_MarkusSabadello.pdf“

Folie 5

Die Sovrin Foundation ist eine non profit Organisation welche

a) die von ihr entwickelte Distributed Ledger Technology (DLT), in Deutsch „verteiltes Kontobuch, dezentrales Transaktionsregister) einbringt
und

b) sich als unabhängige Registrierungsstelle und Kontrollorgan (ähnlich ICANN) für die Vergabe von Berechtigungen für die Erbringung von Leistungen in dem zu etablierenden Identitätsnetzwerk anbietet.

Folie 7

Decentralized Identifiers (DIDs) sind einer neuer Typ von Kennzeichen im Rahmen der Souveränen Digitalen Identität. Sie werden ausschließlich vom Eigentümer der Identität (dem Owner) also uns als Einzelperson verwaltet. DIDs kann man mit den URLs im WWW vergleichen. Sie identifizieren Teilelemente für eine vertrauenswürdige Beziehung und Verarbeitung.

Das World Wide Web Consortium (W3C) ist federführend in der DID Standardisierung. Die Nutzung des DID Formats in unterschiedlichen Blockchain Umgebungen (wie Sovrin, bitcoin, uport, usw.) ist das erklärte Ziel.

Folie 11

Als SDI Nutzer (Owner) verwaltet die Person alle persönlichen Daten selbst und gestattet Dritten (Verifier) den selektiven Zugriff auf die jeweils relevanten Elemente aus diesen Daten.

Die Zertifizierung dieser persönlichen & verifizierbaren Identitätsdaten (verifyable claims) erfolgt durch Dritte (Issuer). Das können - je nach „Qualitätsanforderung“ – andere Nutzer, offizielle Stellen, usw. sein. Die Wohnadresse z.B. über das Zentrale Melderegister, die Kontoinformation durch die Bank, private Daten durch Familie oder Freunde.

Folie 14

eID => IDA „Identity Austria“ - die staatliche Identität. Praktisch jeder Staat verwaltet für seine Bürger eine Identität (z.B. Bürgerkarte, Handysignatur) – historisch zum Zwecke der Besteuerung und für den Militärdienst eingeführt.

Welche Rolle eine Souveräne Digitale Identität dabei spielen könnte ist in einem Whitepaper des E-Government Innovationszentrum (egiz.gv.at) nachzulesen.

Folie 16

In den entwickelten Ländern sind wir überidentifiziert = es gibt zu viele, die zu viel über jeden Einzelnen von uns wissen. Weltweit gibt es jedoch einiges über 1 Mrd. Menschen die unteridentifiziert sind. D.h. sie haben nicht einmal staatliche Dokumente und sind damit von Ausbildung, Gesundheitsvorsorge, usw. ausgeschlossen. Internationale Organisationen (UNO, ...) arbeiten an Lösungen und Initiativen um hier Abhilfe zu schaffen.

Allgemein laufen derzeit weltweit, in entwickelten und weniger entwickelten Ländern & Regionen und meist als Konsortium organisierte, Machbarkeits/PoC-Projekte wo dieses Konzept eingesetzt wird. Die praktischen Erfahrungen aus diesen Feldversuchen werden die theoretischen Überlegungen und die zugrunde liegenden Technologien als richtungsweisend/praktikabel bestätigen oder nicht.

Folie 22

Die FreedomBox – streng genommen eigentlich nur ein Stück Software, das grundsätzlich auf allen Geräten die Debian Linux installiert haben läuft (alter PC, NAS Box, ...). Das immer noch gültige Ur-Konzept sieht die Nutzung einer möglichst günstigen und energieeffizienten Hardware vor. Es sieht auch vor, dass interessierte Nutzer die wenigen notwendigen Komponenten kaufen und selbst zusammenbauen. DanubeTech hat ein paar „plug&play“ Prototypen produziert. Die Produktion weiterer Komplettgeräte ist möglich und könnte z.B. durch einen Gemeinschafts Kauf angestossen werden.

Abschliessend ...

Die Blockchain Technologie ist schon eine Weile am Markt und wurde speziell durch den Bitcoin Hype bekannt und auch gleich wieder in Verruf gebracht (z.B. riesige Rechenleistungen, enormer Energieverbrauch). Richtig angewandt (z.B. Auswahl und Zertifizierung der Leistungserbringer / Serverzentren) können solche Auswüchse vermieden werden.

Die Souveräne Digitale Identität ist keine fertige Lösung. Alle Konzepte (inkl. Sovrin) sind im experimentellen Stadium und konzentrieren sich aktuell auf die technische Infrastruktur und nur am Rande auf Anwendungen/Applikationen.

Konzepte zur Realisierung einer Souveränen Digitalen Identität gibt es von einer Reihe von Anbietern. Viele mit Open Source Ansatz, manche auch mit proprietären Ideen.

Souveräne Digitale Identität ist kein Stück SW/HW dass man kauft und für sich einfach einsetzt. Souveräne Digitale Identität funktioniert grundsätzlich nur in einem Mehr/Vielparteien Eco-System und solche finden sich gerade in den schon angesprochenen Konsortien für laufende & geplante Machbarkeitsaktivitäten (PoCs) zusammen.



Ing. Gerhard Fischer
Management der Digitalks