myIDsafe

Selbst-Souveräne Identitäten auf der Blockchain

Günter Weinhandl
März 2019

bat groupware
besser gemeinsam

Innovative Software-Lösungen für die
Zusammenarbeit im professionellen Umfeld.

DAS INTERNET KENNT KEINE IDENTITÄTEN

myIDsafe

"On the Internet, nobody knows you're a dog."

myIDsafe - KURZÜBERBLICK

- „Digitale Identitäten“ sind Basis für digitale Transformation unserer Gesellschaft. Bestehende Lösungen decken die Bedürfnisse der Wirtschaft nicht ab und sind auch für Benutzer nicht zufriedenstellend.

- Mit myIDsafe schaffen wir ein „Ökosystem des Vertrauens“, an dem sich Unternehmen aus unterschiedlichen Branchen beteiligen, um Nutzungsfrequenz = Attraktivität zu schaffen.

- myIDsafe stellt gewohnte, dezentrale Bestätigungsmechanismen zur Verfügung. (z.B. Universitätsabschluss, Versicherungsbestätigung, Meldeadresse, etc.)

- myIDsafe gibt allen Benutzern die Möglichkeit, ihre sensiblen Daten sicher mit Unternehmen oder anderen Benutzern auszutauschen. Der Zugriff erfolgt dabei mittels mobiler App.

- myIDsafe nutzt Möglichkeiten der Blockchain-Technologie (dezentrales Register, das keinem einzelnen Unternehmen oder Staat gehört).

DAS PROBLEM

myIDsafe

OHNE DIGITALE IDENTITÄT
KEINE DIGITALE TRANSFORMATION
UND SOMIT KEINE DIGITALE WIRTSCHAFT

KUNDEN

- Viele Benutzernamen und Passwörter
- Im Internet verteilte persönliche Informationen
- Keine Kontrolle über Nutzung persönlicher Daten
- Hohes Missbrauchsrisiko

UNTERNEHMEN

- Hohe Kosten
  - KYC Prozess
  - Fraud
  - DSGVO Compliance
- Digitale Geschäftsmodelle schwierig
  - Online-Registrierung neuer Kunden
  - Mangelnde Datenqualität
  - Legale Monetarisierung von Daten

Bestehende Lösungen sind unbefriedigend !

WAS IST myIDsafe?

- myIDsafe ist ein Ökosystem der Wirtschaft für die Wirtschaft und unterstützt:
  - im KYC Prozess (Kostenreduktion, Fraudreduktion) und bei der Datenqualität
  - Unternehmen bei Neukunden-Registrierung und Online-Produktabschluss
  - Jede Form von digital ausgestellten Bestätigungen (z.B. Uni-Abschluss)
  - Und in Folge auch legale und DSGVO-konforme Datenmonetarisierung

- myIDsafe bringt somit Vertrauen - als wesentliche Basis jeder Geschäftsabwicklung – von der analogen in die digitale Welt.

- Neue Blockchain-Technologien schaffen auf technischer Ebene die Rahmenbedingungen zur Abbildung des Ökosystems myIDsafe.

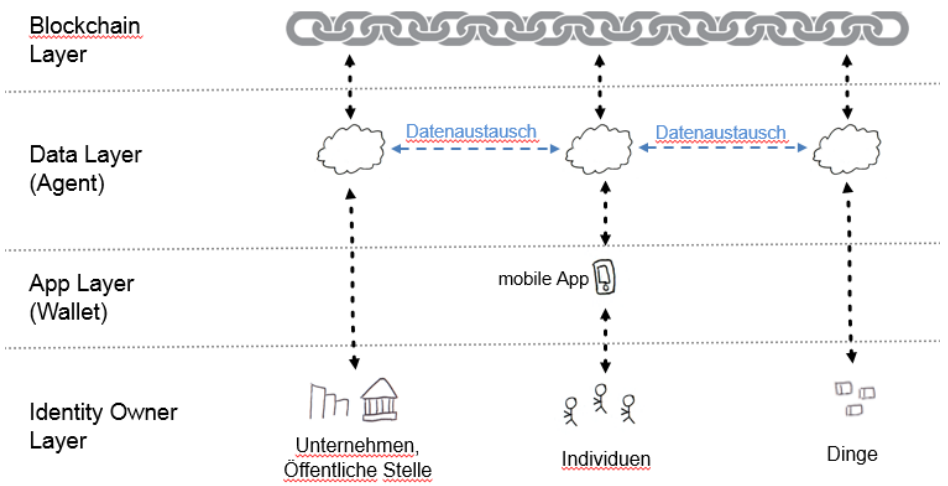
- Vor allem regt die Blockchain aber dazu an, über neue Zusammenarbeitsmodelle nachzudenken!

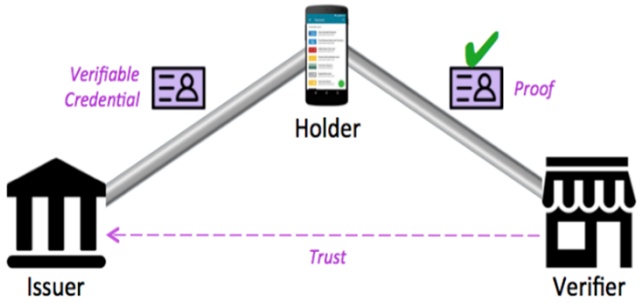
TECHNISCHER RAHMEN

myIDsafe

- Die Self-Sovereign Identity Architektur von myIDsafe besteht aus einer Blockchain (Register) und aus Agents, mit denen Individuen, Unternehmen, und Dinge Verbindungen aufbauen und Verifiable Claims (verifizierte Bestätigungen) sowie andere Daten austauschen können.

- Die Architektur basiert auf gängigen open source Komponenten, die aktuell in Standardisierung sind.





ARCHITEKTUR DER SELF SOVEREIGN IDENTITY

myIDsafe

- Die Blockchain dient als Register für verschiedene Meta-Informationen zu digitalen Identitäten, z.B. Kennnummern oder kryptografische Schlüssel (DIDs)
- Die Blockchain dient somit als Quelle für digitale Identitäten, die von zentralen Stellen unabhängig sind (Identity Backbone für das Internet)
- Es besteht für den User daher keine Abhängigkeit vom Aussteller (z.B. Bank)
- Identitäten können ohne Zustimmung des Individuums nicht manipuliert oder gelöscht werden (dezentrale, verteilte Speicherung)
- Bestimmte Vorgänge können unwiderruflich und transparent festgehalten werden (z.B. Einverständnis des Kunden zur Nutzung bestimmter Daten)
- Privatsphäre ist trotz Blockchain garantiert, da die persönlichen Identitäts-Daten “off-chain” in sogenannten Agents gespeichert werden.
- Datenportabilität ist sichergestellt (Agents können gewechselt werden, aber die Identität und alle zugeordneten Attribute bleiben unverändert)
- Die Verwendung der Identität ist nicht rückverfolgbar, bei gleichzeitiger Möglichkeit zur Überprüfung des Ausstellers

„VERIFIABLE CLAIMS“ ALS ELEMENTARER BAUSTEIN

myIDsafe

- Verifiable Claims sind persönliche Daten, die “attestiert” statt nur “selbst behauptet” sind (z.B. Adresse, Uniabschluss, etc.)
- Daten werden durch „Issuer“ bestätigt - das sind in der Regel Unternehmen oder öffentliche Einrichtungen, die über diese Daten verfügen
- Austausch dieser Daten zwischen Unternehmen ist nur unter Kontrolle und Zustimmung des Kunden möglich
- Die Daten können dann vom „Verifyer“ geprüft und verarbeitet werden.
  Es ist für das empfangende Unternehmen also ersichtlich, wer die Daten ursprünglich bestätig hat
- Die Verwendung der Daten ist allerdings für den Aussteller nicht ersichtlich, es besteht keine Möglichkeit zur Rückverfolgung.
- Dies erfolgt bei gleichzeitiger Sicherstellung der Privatsphäre durch Unterbindung der Korrelierbarkeit zwischen Unternehmen
- Verifiable Claims sind somit eine Grundlage für Vertrauen in der digitalen Geschäftsabwicklung.
- Verifiable Claims sind auch die Basis für neue, digitale Geschäftsmodelle
  (z.B. Datenmonetarisierung in Form von digitalen Bestätigungen, etc. = Premium Claims)

ROLLEN IM ECO-SYSTEM

VERIFIER

Nutzer digitaler Claims

- Konsument/Nutzer von verifiable Claims (akzeptiert Attribute zum IDOwner)
- entscheidet, welchen Issuern er vertraut

IDOWNER

Besitzer digitaler Claims

- Natürliche und Juristische Personen
- erfasst „self issued“ Claims
- bezieht Claims und gibt diese zur Nutzung frei
- hat Servicevertrag mit Agency

ISSUER

Aussteller/Bestätiger digitaler Claims

- stellt verifiable (überprüfbar, wer ausgestellt hat) Claims, die der IDOwner zur Nutzung freigeben kann, aus
- bestätigt die (Korrektheit der) ausgegebenen Daten mit seiner digitalen Signatur

STEWARD

Betreiber myIDsafe Knoten

- betreibt die BlockChain Basis Infrastruktur
- speichert DIDs (Identifikatoren für digitale Identitäten) und Transaktionen in der BlockChain
- sorgt für Sicherheit und Schutz vor Manipulation
- Compliance mit den Netzwerk-Vorgaben (Stewards werden nominiert)

AGENCY

IdentitätsServiceProvider

- hat Servicevertrag mit IDowner
- speichert Attribute zu digitalen Identitäten (z.B. Adresse, Bonität, …) in einem persönlichen Speicher (digitaler Agent)
- stellt Software (Apps, WebSite, API, …) und Funktionen (Verification, Austausch von Claims zwischen Unternehmen + Usern, …) im Wettbewerb zur Verfügung

TRUST ANCHOR

Registrierungsstelle

- Erstregistrierung (onboarding) digitaler Identitäten (DIDs)
- Eintrittspunkt (Gate) in das System
- Compliance mit den Netzwerk-Vorgaben (Trust Anchors werden nominiert)

ERFOLGREICHER PROOF OF CONCEPT (PHASE I)

myIDsafe

- Technische Machbarkeit im Rahmen eines PoC im ersten Halbjahr 2018 in einer Arbeitsgruppe mit mehreren österreichischen Unternehmen bewiesen
- Teilnehmer der Phase I haben die Notwendigkeit des Ökosystem-Gedankens erkannt, dieser Gedanke ist eine wesentliche Grundlage für die Phase 2
- Aufmerksamkeit und Interesse zur Mitgestaltung bei Unternehmen, im universitären und öffentlichen Bereich sowie bei Verbänden und Kammern erzeugt
- Erste rechtliche Einschätzung mit Schwerpunkt DSGVO erfolgt – DSGVO Compliance wird durch myIDsafe erleichtert
- Austausch mit internationaler SSI-Community und auf EU-Ebene

PROJEKTUMWELTEN

myIDsafe im Verhältnis zu aktuellen Entwicklungen im Bereich digitaler Identität:

DSGVO:

- ✓ Datenaustausch erfolgt immer mit expliziter Zustimmung des Individuums
- ✓ Zustimmung wird digital signiert und kann von allen Beteiligten eingesehen werden
- ✓ Zustimmung kann jederzeit mittels Agent widerrufen und an verbundene Unternehmen “signalisiert” werden
- ✓ Agents erlauben Datenportabilität
- ✓ Off-ledger DIDs ermöglichen es, Daten auf einem Distributed Ledger für Privatpersonen zu vermeiden

eIDAS:

- ✓ Qualifizierte eID Attribute können zu myIDsafe-kompatiblen Verifiable Claims ”abgeleitet” werden
- ✓ Vertrauen in staatlich gesicherte Identität würde dadurch in das dezentrale myIDsafe Ökosystem “importiert” werden
- ✓ Hätte Einfluss auf Trust Framework und Haftungsfragen
- ✓ Staatliche Identität könnte mit Wirtschaft, Zivilgesellschaft, usw. kombiniert werden
- ✓ Diskussion der Integration hat auf EU-Ebene begonnen

WARUM DIE PARTNER MITMACHEN?

myIDsafe

„Ich sehe die aktive Mitarbeit als Kickstarter für neue Geschäftsideen“

„Jetzt kann ich aktiv mitgestalten und meine eigene Position finden“

„Starkes Momentum für die Entwicklung eines dezentralen Ecosystems, um nicht als Unternehmen auch in Abhängigkeiten der Internetgiganten zu geraten“

„Wenn wir jetzt nicht mitmachen, dürfen wir uns in 2 Jahren nicht wundern, dass Google, Facebook & Co die Sache übernommen haben“

„Ich kann mir jetzt einen Startvorteil am Markt erarbeiten“

„Die Digitale Identität ist eine Basis für meine eigenen, künftigen, digitalen Geschäftsmodelle“

Digitale Identität als Basis für die digitale Transformation

myIDsafe

BRINGEN WIR GEMEINSAM VERTRAUEN
IN DIE DIGITALE WELT!