Matthias Fuhrland, Jürgen Anke (HTW Dresden), 2023

Der Aufbau des Trustnets

Die Umsetzung des Trustnets erfordert das Wachstum eines ID-Ökosystems mit Herausgebern, ID-Inhabern, Akzeptanzstellen, Modifizierern und ID-Diensten als Basis für eine Vielzahl von Anwendungsökosystemen. Dies ist ein langfristiger Prozess und eine globale, gesamtgesellschaftliche Aufgabe. Initial wird das Trustnet auf drei Pfeilern gebaut.

Trust Framework

Das **Trust Framework** soll als Strukturhilfe und Regelwerk mit Standards zum sicheren Interaktions-management digitaler Identitäten und digitaler Nachweise die Entstehung dieses ID-Ökosystems anregen, in dem verschiedene ID-Dienste koexistieren können. Das Trustnet wird die bestehende Welt der zentral verwalteten Basisidentitäten inkl. eID und die neue SSI-Welt miteinander verbinden. Der Gedanke dieses Brückenschlags ist bereits in die eIDAS-Novellierung eingeflossen. Das Trust Framework soll darüber hinausgehend die technische, semantische und organisatorische Interoperabilität sicherstellen, damit Credentials unabhängig von der Art der Wallet-App und von der jeweiligen in der Vertrauensdomäne verwendeten Basistechnologie oder Dateninfrastruktur überprüft werden können. Dieser Gedanke ist in bestehenden bzw. in Entwicklung befindlichen Trust Frameworks, wie dem kanadischen PCTF, dem USamerikanischen NIST 800-63 oder bei den entsprechenden EU-Aktivitäten (eIDAS-Novellierung) noch zu gering ausgeprägt. Deswegen wird zur Entwicklung des Trustnets ein auf diesen Arbeiten aufbauender Neuentwurf erforderlich.

Funktionale Mindestanforderungen an technische Lösungen der Akteure innerhalb des Trustnets sind:

1) Ausweisfunktion: Die sichere automatisierte Identifizierung eines Akteurs muss bei Bedarf möglich sein. Hierfür sollten Identifizierungsmittel auf allen Vertrauensniveaus für jede Art von Akteur verfügbar sein.
2) Nachweisfunktion: Die Herausgabe und automatisierte Prüfung einzelner gesicherter Attribute muss möglich sein, auch ohne dass eine eindeutige Identifizierung möglich ist.
3) Technische, semantische und organisatorische/rechtliche Interoperabilität
4) Vertretungsfähigkeit: Neben Wallets für Bereitstellung einfacher Aus- und Nachweise werden auch Wallets und Verifiable Credentials für die Abbildung von persönlichen und juristischen Beziehungen gebraucht.
5) Privacy-Werkzeuge zur Filterung und Binärisierung des Informationsgehaltes von Attributen bzw. zum Festlegen der Bedingungen für die Freigabe und Nutzung verifizierbarer Informationen.

Funktionale Mindestanforderungen an Anwendungsprozesse innerhalb des Trustnets sind:

6) sichere und eindeutige Identifizierung aller am Prozess beteiligten Akteure
7) Überprüfung aller innerhalb des Prozesses ausgetauschten Informationen
8) eindeutige Definition der Prozessabläufe, Rollen, Rechte, Kontrollorgane und Regularien inkl. der Sanktionierungsmechanismen innerhalb des Anwendungsökosystems
9) DSGVO-konforme Datenverarbeitung
10) optionale Redundanz, d.h. die Möglichkeit, bei Bedarf den Wahrheitsgehalt bzw. die Aktualität von Informationen zu prüfen

Die bisherige Diskussion in Fachwelt und Politik fokussierte stark auf die technischen Aspekte der Ausstellung hoheitlicher digitaler Identifizierungsmittel und anderer Credentials in eine Wallet. Es ist aber evident, dass die o.g. funktionalen und prozessseitigen Anforderungen weder allein durch die Verfügbarkeit der eID, noch allein durch das Ausstellen anderer Verifiable Credentials erfüllt werden können. Der Entwurf eines ID-Ökosystems erfordert einerseits eine *strukturierte ganzheitliche Betrachtung* und andererseits eine *detaillierte Betrachtung der digitalen Anwendungsprozesse* über den gesamten Lebenszyklus der dafür erforderlichen Credentials. Die Basis für die ganzheitliche Betrachtung bildet der bereits erwähnte und in Abb. 1 dargestellt Trustnet-Stack, der maßgeblich auf dem von der Trust Over IP Foundation entwickelten Trust over IP-Stack[1] beruht. Der Stack soll angesichts der Komplexität der Thematik als Orientierungshilfe zur Strukturierung der Diskussion dienen. Der technische Teil des ID-Ökosystems sind Ebene 1 und 2 und der organisatorische Teil des ID-Ökosystems sind die ID-Lösungen für sämtliche Akteure auf Ebene 3. Damit bildet das ID-Ökosystem die Basis für die Anwendungsökosysteme in Ebene 4.

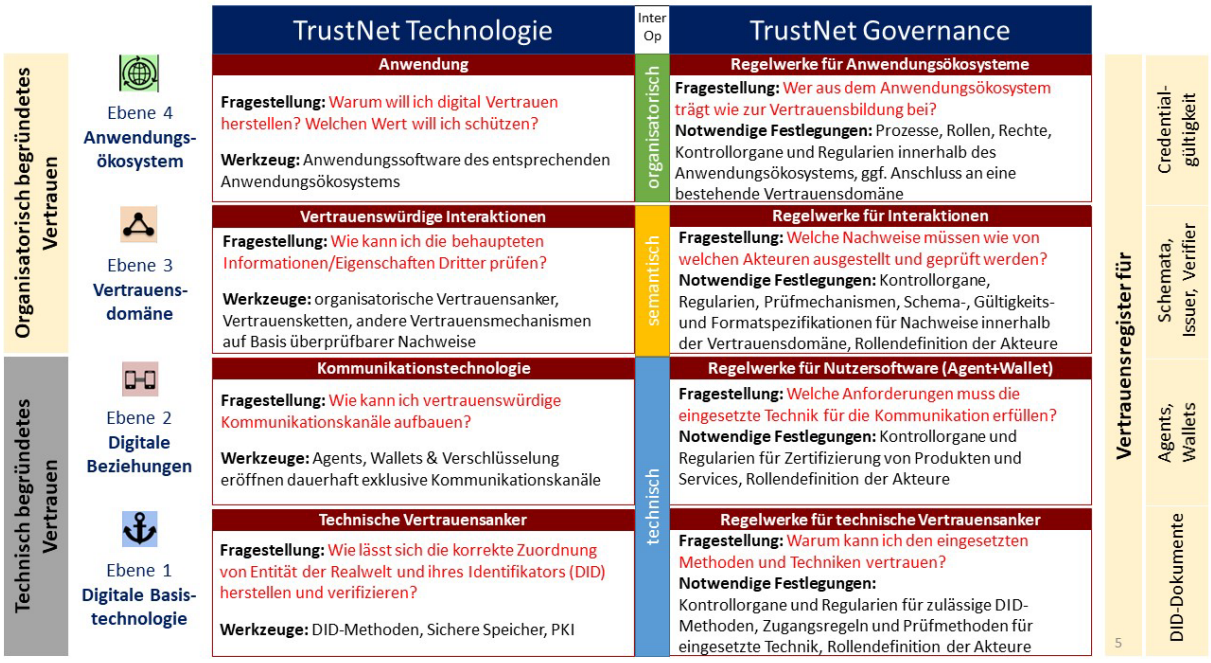

Abb. 1: Trustnet-Stack

Das Trust Framework soll auch die Digitalisierung der anwendungsspezifischen Governance (Regelwerke der bestehenden Vertrauensdomänen und Anwendungsökosysteme) anregen. Der

[1] https://trustoverip.org/wp-content/toip-model/

Trustnet-Stack verdeutlicht, dass bei jeder geplanten Anwendung nicht nur die einzusetzenden *technischen Komponenten* auf allen vier dargestellten Ebenen festgelegt werden müssen. Es muss auch die *Governance* auf allen vier Ebenen des Trustnet-Stacks geregelt und organisiert werden. Hinzu kommen die Definition, Umsetzung und Pflege erforderlicher Dateninfrastrukturen (Vertrauensregister) sowie die Organisation der Hoheit über das Trust Framework und dessen Weiterentwicklung. Hierfür müssen Kontrollorgane (*Governance Authorities)* definiert bzw. neu gegründet werden. Auf der Ebene der Vertrauensdomänen und auf der Ebene der Anwendungsökosysteme existieren bereits Governance Authorities, die in der Realwelt die entsprechenden Regeln machen und deren Durchsetzung überwachen. Diese Akteure sind auch die logische Wahl, wenn es um die jeweilige Digitalisierung geht. Auf Ebene der Vertrauensdomäne ist in Deutschland z.B. das Bundesinnenministerium die Governance Authority für den Personalausweis und damit logischerweise auch für die eID. Auf Ebene der Digitalen Basistechnologien und auf Ebene der digitalen Beziehungen existieren hingegen noch keine Governance Authorities, weil dieser Bereich noch sehr jung, hochdynamisch und unreguliert ist. Hier müssen neue Governance Authorities gegründet bzw. etabliert werden. Es existieren aber bereits internationale Arbeitsgruppen, wie Decentralized Identity Foundation (DIF), World Wide Web Consortium (W3C), OpenID-Foundation, Trust over IP Foundation oder Open Wallet Foundation, deren Vorarbeiten zu Standardisierung und Interoperabilität die Basis für Regulierungs- und Zertifizierungsarbeit der künftigen Governance Authorities werden können und sollten. Darüber hinaus braucht das ID-Ökosystem ebenso *Service-Strukturen*, d.h. es müssen sich vertrauenswürdige Akteure finden, die die erforderlichen Services (ID-Dienste, Vertrauensdienste, Zertifizierungen, Wissens- und Technologietransfer …) entsprechend dem gemeinsamen Regelwerk übernehmen. All diese Aufgaben erfordern die Organisation einer **Trustnet Community**, geleitet durch einen Kanon gemeinsamer Werte. Die Formierung dieser Community ist ein Gegenstand der Trustnet-Initiative. Die Mission der Trustnet Community als zentralem Pfeiler beinhaltet als mittelfristiges inhaltliches Ziel die Schaffung, Anwendung und Verbreitung des Trustnet Frameworks.

Digitalisierung der bestehenden Vertrauensbasis

Bei der konkreten und strukturierten Betrachtung von Anwendungen und zugehörigen Prozessen kommen weitere Aspekte ins Rampenlicht. Wie kann das Sozialamt der Stadt München einem vom Arbeitsamt der Stadt Berlin ausgestellten digitalen ALG II-Bescheid vertrauen? Warum sollte ein potentieller Arbeitgeber einem von der Hochschule für Technik und Wirtschaft Dresden digital ausgestellten Masterzeugnis vertrauen? Wie ist die Herausgeberschaft dieser Credentials zu verifizieren? Die Beantwortung dieser Fragen führt zwangsläufig zum erforderlichen dritten Pfeiler des Trustnets, der **Digitalisierung der in der Realwelt bestehenden Vertrauensbasis,** d.h. dem gezielten Aufbau einer digitalen Vertrauenskaskade (siehe Abb. 2). Das beinhaltet zunächst die möglichst einheitliche Festlegung digitaler Identitäten hoheitlicher Akteure, die als vertrauenswürdige Herausgeber (Trusted Issuers) fungieren, inkl. der dazu erforderlichen Dateninfrastruktur in Form von Vertrauensregistern. Gleiches gilt für die bestehende Vertrauensbasis im Bereich der juristischen Personen. Durch sichere ID-Lösungen nicht nur für natürliche Personen, sondern auch für hoheitliche Akteure, wie Behörden und Ämter, für Unternehmen und Organisationen sowie für smarte Objekte entsteht initiales Vertrauen im Trustnet basierend auf bestehenden Vertrauensmechanismen der Realwelt. Die SSI-Mechanismen und Verifiable Credentials verbinden anschließend diese vier Stufen

und formen digitale Vertrauensketten zwischen den Akteuren. Durch die Realisierung dieser digitalen Vertrauenskaskade anhand einer großen Anzahl von Use Cases / Business Cases kann in Summe ein initiales Trustnet entstehen, das über die Bandbreite der Anwendungsökosysteme und über Nationalisierung / Internationalisierung skaliert.

Abb. 2: Die digitale Vertrauenskaskade (Pfeiler 3)

Der zweite Teil dieser Digitalisierung betrifft die digitale Organisation bestehender Vertrauensdomänen der Realwelt. Z.B. muss sich ein bestehender Interessenverband ggf. mit der zugehörigen Aufsichtsbehörde dahingehend abstimmen, welche Nachweise künftig in welchem digitalen Format (VC-Schema) herausgegeben und akzeptiert werden sollen und wer innerhalb bzw. außerhalb der Vertrauensdomäne welche Service-Struktur übernimmt. Vertrauenswürdige Herausgeber und Akzeptanzstellen müssen entsprechend ihre Prozesse technisch anpassen, denn das ID-Ökosystem braucht *organisatorische Vertrauensanker* in Form der Autorität und sicheren Prozesse staatlicher Akteure zur Ausstellung von Identifizierungsmitteln (eIDs, Unternehmens-IDs, kommunale Datenkarten, …) und Nachweisen (Registerauszüge, Bescheide etc.) und ebenso ein Netz verschiedenster Vertrauensmechanismen zwischen den damit international identifizierbaren und authentifizierbaren Akteuren, die sich in vielen verschiedenen Arten sicherer Prozesse und verschiedenen technischen Implementierungen niederschlagen. Denn ohne eine Vielzahl an Akzeptanzstellen und die technische, organisatorische und juristische Einbindung der digitalen Ausweise und Nachweise in deren Prozesse nützt die Herausgabe von eIDs und VCs nichts. Die digitale Organisation bestehender Vertrauensdomänen erfordert aber ebenso *anwendungsspezifische, sichere Dateninfrastrukturen auf Ebene 3 und 4 des Trustnet-Stacks*, die den o.g. Anforderungen Rechnung tragen. Aufgrund der unterschiedlichen regulatorischen Rahmenbedingungen für Verwaltung und Wirtschaft einerseits und in unterschiedlichen Staaten andererseits ist klar, dass sowohl Public Key Infrastrukturen als auch DLT- und Blockchain-basierte Infrastrukturen im Trustnet ihre Berechtigung haben und unterschiedliche Vertrauensniveaus und/oder Vertrauensdomänen bedienen werden. Die große Herausforderung beim Aufbau des ID-Ökosystems besteht in der grenzübergreifenden technischen und regulatorischen Harmonisierung all dieser Aspekte.