Matthias Fuhrland, Jürgen Anke (HTW Dresden), 2023

Trustnet

Die Trustnet-Vision

Das Designziel für das World Wide Web war einfacher Informationsaustausch. Die generelle Überprüfbarkeit von Informationen war nicht Bestandteil der Konzeption. Im Nachhinein entstand zwar ein regelrechter Wildwuchs an Verfahren, um Akteure identifizierbar und Informationen überprüfbar zu machen, aber die daraus entstandene Vielzahl an Insellösungen kann das grundlegende Vertrauensproblem im digitalen Raum nicht lösen. Es ist Zeit, die DNA des World Wide Web zu verändern. Das Thema der hier adressierten Community ist das **Trustnet – die nächste Evolutionsstufe des Internets**. Das heutige Internet der Informationen (WWW), in dem die meisten von uns täglich unterwegs sind, grenzt sich hinsichtlich Auffindbarkeit/Sichtbarkeit von Informationen schon heute vom sogenannten Darknet ab. Akteure im Darknet verschaffen sich Anonymität, im WWW wird das Identifizieren von Akteuren durch Pseudonymität erschwert. Dem Bedarf der Nutzer nach Vertrauen im Internet wird hier bislang nicht hinreichend Rechnung getragen. Mit dem Trustnet soll deswegen durch Mechanismen für digitales Vertrauen ein rechtssicherer digitaler Raum entstehen, in dem

- Akteure aus Wirtschaft, Verwaltung und Gesellschaft im Zuge der Abwicklung von Geschäfts- und Verwaltungsprozessen eindeutig identifizierbar sind,
- Informationen verifizierbar und damit vertrauenswürdig sind und einen Wert besitzen,
- Transaktionen sicher und rechtskonform stattfinden und
- die Nutzer Hoheit über ihre eigenen Daten haben.

All dies erfordert eine Weiterentwicklung des Internets, an dem nicht nur der Staat, sondern alle Diensteanbieter, Nutzer und Stakeholder, die Vertrauen bei digitalen Interaktionen benötigen, aktiv mitwirken müssen. Wir nennen es Trustnet. Die Vision unserer Innovationscommunity ist die Erweiterung des bestehenden Internets der Informationen um dieses Internet der Werte und Originale (Trustnet) – einer der größten digitalen Herausforderungen der kommenden Jahrzehnte.

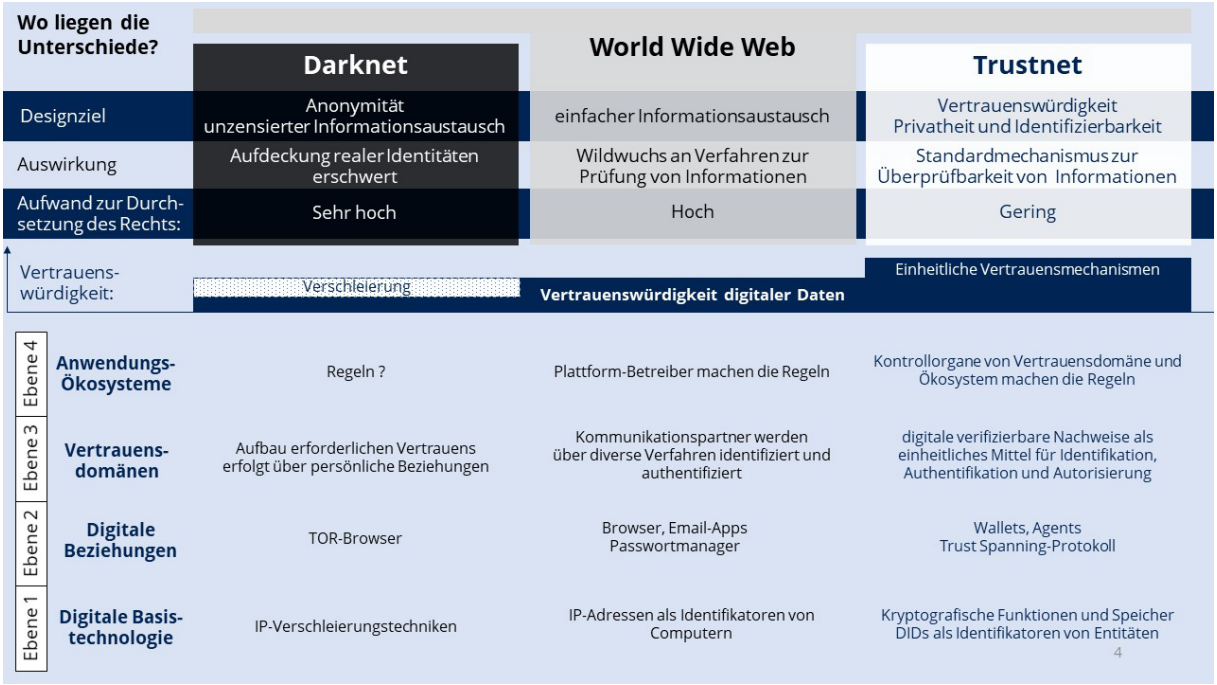

Abb. 1: künftige Erweiterung des Internets um das Trustnet

Sowohl Privatheit, als auch Identifizierbarkeit - gewichtet je nach Anwendungsfall - sind wichtige Forderungen im digitalen Raum und daher Designkriterien des Trustnets. Jeder digitale Akteur hat das Recht, nur so viele personenbezogene Informationen im Netz bereitzustellen, wie er will. Jemandem, der seine Identität verbirgt, kann man jedoch nur sehr begrenzt Vertrauen entgegenbringen, denn Pseudonymität und Anonymität erschweren die Durchsetzung geltenden Rechts. Für Vertrauen im Netz sind Transparenz und Überprüfbarkeit jeweils relevanter Identitätsmerkmale erforderlich. Der technologische Schlüssel dafür ist die Verbindung des Werkzeugs der überprüfbaren Nachweise (**Verifiable Credentials**) mit dem Prinzip der Selbstsouveränen Identitäten (SSI). Mit dem **SSI-Prinzip** lässt sich jede Art von überprüfbaren Nachweisen digital herausgeben, vorzeigen und verifizieren.[1] Der damit entstehende universelle Vertrauensmechanismus für Austausch und Überprüfung von Informationen ist der **Gamechanger** im Kontext des Trustnets, denn im Unterschied zu signierten PDF-Dokumenten sind Verifiable Credentials hinsichtlich der Authentizität von Herausgeber, Empfänger und Inhalt überprüfbar. Sie sind maschinenlesbar, auch in Bezug auf einzelne Attribute, und dank des Austauschprotokolls auch im Internet skalierbar. Jede Information, die nach dieser Methode digital zur Verfügung gestellt wird, kann unter verschiedenen Vertrauensfragen automatisiert überprüft werden. Was zur universellen Einsetzbarkeit im Internet bislang fehlt, sind

1.) sichere digitale Identitäten für hoheitliche Akteure, juristische Personen, natürliche Personen und (smarte) Objekte, die über das Abbilden der Basisidentitätsmerkmale (z.B. eID) hinaus auch weitere Identitätsmerkmale, Rechte und Beziehungen zu anderen natürlichen Personen, juristischen Personen und Objekten abbildbar und überprüfbar machen,
2.) ein digitales ID-Ökosystem mit Vertrauensdiensten, Zertifizierungsstellen, Beratungsstellen und Sanktionierungsmechanismen,
3.) der große organisatorische Rahmen mit Regelwerk, vertrauensbildender Dateninfrastruktur und Governance (Verwaltung) sowie Labels für Compliance,
4.) der rechtliche Rahmen, der nicht nur den Umgang mit hoheitlichen Identifizierungsmitteln regelt, sondern z.B. auch den Umgang mit digitalen Ausweisen und Nachweisen in sämtlichen Fachanwendungen rechtssicher macht.

Erst damit werden Nachweis-basierte Interaktionen digitalisierbar, die zugehörigen Prozesse automatisierbar und das Ganze breitenwirksam in der Praxis einsetzbar.

Definition: *Das Trustnet ist das universelle digitale Abbild von Beziehungen zwischen Personen, Organisationen und Objekten der Realwelt. Es ermöglicht vertrauenswürdige und rechtskonforme digitale Interaktionen und verhindert Fake und Betrug. Die Grundlage dafür ist ein einheitlicher, skalierbarer Vertrauensmechanismus für den Austausch und die Prüfung von digitalen Nachweisen zu beliebigen Sachverhalten. Damit wird die Organisation von und der Zugang zu offenen digitalen Ökosystemen radikal vereinfacht.*

Die Umsetzung dieser Vision erfordert die Festlegung von Rahmenbedingungen (Trust Framework) für **sichere digitale Identitäten von hoheitlichen Entitäten, Organisationen, natürlichen Personen und Objekten** und ein nutzerzentriertes ID-Ökosystem mit einer Vielzahl kompatibler ID-Dienste, die den spezifischen Bedürfnissen verschiedener Nutzergruppen gerecht werden.

[1] Anke, J., Richter, D. Digitale Identitäten. HMD 60, 261–282 (2023). https://doi.org/10.1365/s40702-023-00965-1