SocietyByte
BFH-Magazin für die Humane Digitale Transformation

Die Schweiz und die Globalisierung der digitalen Identitätsbrieftasche

Von Reinhard Riedl (BFH Wirtschaft) | 0 Kommentare

Gelingt eine globale digitale Kooperation bei der digitalen Vertrauensinfrastruktur? Ziehen Europa, USA, China und die Schweiz an einem Strang? Und wenn ja – stehen die Rechte der Menschen im Zentrum oder der Überwachungsdrang von Staaten und Unternehmen?

Ach, wie toll wäre es doch, eine globale digitale Vertrauensinfrastruktur zu haben. Eine Infrastruktur, die es Menschen und autonomen Maschinen ermöglicht, ihre Identität bei Online-Interaktionen nachzuweisen, samt vielen wichtigen persönlichen Attributen wie Ausbildung, Berufserfahrung, Wohnort, et cetera. Und das über Staatsgrenzen hinweg! Aber wird es jemals dazu kommen?

Der Kickoff für eine globale digitale Kollaboration [https://globaldigitalcollaboration.org/] zum Thema digitale Identitätsbrieftaschen in Genf (am 1. Und 2. Juli) löst Hoffnungen und Befürchtungen aus. Beides, weil so viele Akteure vertreten sind und es insbesondere um die Zusammenarbeit zwischen Europa, USA und China geht. Es stellen sich dabei folgende Fragen: Wollen sie wirklich an einem Strang ziehen? (wenn ja, wäre es eine Riesenchance!) Steht dabei wirklich die digitale Selbstbestimmung der Menschen im Zentrum? (wenn nein, ist dies ein NO GO!) Und die letzte Frage: sind wir geschützt davor, dass das Vorhaben nicht in ein paar Jahren der digitalen Totalüberwachung über alle Ländergrenzen hinweg endet? (Absichtserklärungen und Gesetze reichen dazu nicht aus.)

Dabei ist es faszinierend zu beobachten, wer als Feind der digitalen Selbstbestimmung gesehen wird. Allein schon unter den Digitalexpert*innen der Schweiz gehen die Ängste in alle Richtungen. Die einen glauben, dass die EU-Kommission einen Überwachungssuperstaat schaffen will – Tut mir leid, liebe Kolleginnen und Kollegen in Brüssel, das ist das, was ich von einigen Menschen mit viel IT-Expertise höre … – die anderen fürchten sich vor den USA oder China. Und selbst in diesen Ländern werden sehr unterschiedliche Akteure als gefährlich wahrgenommen. Natürlich fürchten sich nur ganz wenige vor allen. Die meisten sehen in einem ganz bestimmten Teil der Weltgesellschaft die Gefahr. Aber aufsummiert über alle Expert*innenängste kommt man zum Schluss, dass alle Akteure für uns eine Bedrohung darstellen.

Die globale digitale Kollaboration sollte dementsprechend drei Ziele verfolgen. Erstens sollte sie die Entstehung einer weltweiten digitalen Vertrauensinfrastruktur durch die globale Interoperabilität der digitalen Identitätsbrieftaschen fördern. Das ist ihre Mission und steht weitgehend ausser Streit. Zweitens sollte sie sicherstellen, dass es technisch ausgeschlossen ist, dass daraus eine Überwachungsmaschinerie entsteht. Und drittens sollte sie dazu beitragen, die öffentliche Diskussion zu versachlichen und den Menschen die diffusen Ängste zu nehmen. Ahnungen von Gefahren mögen in Krisengebieten nützlich sein, wo es auf schnelle Reaktionen ankommt, doch im Technologiediskurs bringt uns nur ein klares Benennen vorwärts. Ein diffuses Werweissen ist dagegen oft kontraproduktiv.

Was sind digitale Identitätsbrieftaschen eigentlich?

Die Idee ist bestechend: Jede Person erhält eine sichere digitale Identitätsbrieftasche, in der man vertrauenswürdige digitale Eigenschaftsnachweise in Form von überprüfbaren digitalen Eigenschaftszertifikaten speichern kann, um bei Bedarf eigene Eigenschaften in vertrauenswürdiger Weise gegenüber Online-Kommunikationspartnern nachzuweisen.

Die digitalen Eigenschaftszertifikate werden von Institutionen ausgestellt, deren Identität vertrauenswürdig überprüft werden kann. Sie existieren nur in der digitalen Identitätsbrieftasche und sind damit unter der Kontrolle durch deren Besitzer*innen. Für jenen, denen gegenüber sie zum Eigenschaftsnachweis benutzt werden, gibt es aber die Möglichkeit, ihre Authentizität und Gültigkeit zu überprüfen.

Solang das System als Ganzes gegen Manipulationen geschützt ist, hängt die Vertrauenswürdigkeit der Eigenschaftsnachweise von der Vertrauenswürdigkeit der Institutionen ab, welche sie ausstellen. Im wirklichen Leben mit seiner hohen Komplexität ist das die maximal erreichbare Vertrauenswürdigkeit in der digitalen Kommunikation.

Hier ein Beispiel: Wenn ich der Altersangabe einer Person nicht vertraue, kann ich einen Altersnachweis verlangen. Und ich entscheide dann, ob ich die Institution in Bezug auf das Zertifizieren des Alters von Personen für vertrauenswürdig halte. Gut möglich, dass ich im Fall der digital ausgestellten Geburtsurkunde eines mir fremden Landes nicht vertraue, dem digitalen Alterszertifikat basierend auf einem Eintrag im digitalen Personenregister eine mir gut bekannten Nachbarlands hingegen schon. Gut möglich auch, dass beide unterschiedliche Angaben enthalten, und faktisch die Institution, der ich mehr vertraue, falsche Daten hat. Aber es gibt keinen Deus Ex Machina, den ich im wirklichen Leben nach der Wahrheit fragen kann – und die Gefahr wäre gross, dass wenn es so etwas gäbe, ich die Antwort missverstehen würde. Die Mythen der Antiken illustrieren solche gefahren eindrücklich.

Damit die Idee von den digitalen Identitätsbrieftaschen umfassend überzeugt, sind weitere Eigenschaft notwendig. Neben Menschen besitzen auch autonom agierende Maschinen digitale Identitätsbrieftaschen. Die digitalen Eigenschaftszertifikate sind vertrauenswürdig und sicher. Sie ermöglichen es, dass einerseits sehr differenzierte Eigenschaften angegeben werden können («Die Sicherheitsüberprüfung Level N hat ergeben, dass …»), anderseits aber auch nur ausgewählte Eigenschaften gezeigt und nachgewiesen werden, respektive sogar nur Teilaspekte dieser Eigenschaften (solange das Verständnis der Aussagen damit nicht eingeschränkt wird)- beispielsweise, dass die Inhaberin des Zertifikats unter 14 Jahre alt ist. Insbesondere sollen anonyme Eigenschaftsnachweise möglich sein.

Es versteht sich von selbst, dass die ausstellende Institution in den Eigenschaftsnachweis nicht involviert ist und nichts davon erfährt. Und dass alles so gestaltet ist, dass anonyme Eigenschaftsnachweise nicht auf technische Weise miteinander in Beziehung gesetzt werden können.

Zwei kritische Fragen

So weit, so einfach. Es gibt zwei Fragen: Vertrauen wir solch einer digitalen Vertrauensinfrastruktur? Das heisst: Sind die digitalen Identitätsbrieftaschen und die Eigenschaftsnachweise vor Überwachung und Manipulation sicher? Und: Kommt diese digitale Vertrauensinfrastruktur zum Fliegen? Das heisst: Können wir das diesbezügliche Henne-Ei-Problem lösen? Gibt es genügend Nutzer*innen der digitalen Identitätsbrieftaschen und gibt es genügend Nutzungsmöglichkeiten?

Ob wir dieser digitalen Identitätsbrieftaschen samt ihnen Eigenschaftsnachweisen – inklusive der elektronischen Identität (eID), welche das digitale Analogon zum Pass darstellt – vertrauen, hängt von der Implementierung ab. Das heisst, es hängt unter anderem von der Architektur, den verwendeten Algorithmen, der eingesetzten Software und der genutzten Hardware ab. Darüber braucht es einen strukturierten, wissenschaftlichen und öffentlichen Diskurs.

Ob das Ganze zum Fliegen kommt, hängt zum einen von eben diesem Vertrauen der Menschen in die technische Implementierung ab und von den Kosten für die Menschen: Ist es kostenlos und einfach zu installieren und nutzen? Zum anderen hängt es aber auch davon, dass die Wirtschaft genügend Anwendungsmöglichkeiten bietet und die Menschen, den Nutzen für sie erkennen. Es braucht betriebswirtschaftliche Business Cases und Standard-Software für die Implementierung auf Unternehmensseite, aber auch eine erfolgreiche Kommunikation, welche den Nutzen für die Menschen sichtbar macht, wenn sie eine digitale Identitätsbrieftasche einsetzen.

Die Schweizer eID-Abstimmung als Vertrauenstest

In der Schweiz steht im September eine Volksabstimmung über das BGEID (Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise) an, welches auf die Schaffung einer digitalen Vertrauensinfrastruktur wie der gerade skizzierten abzielt. Derzeit sind viele Befürworter*innen sehr zuversichtlich, weil die Schweizer Lösung einerseits unter breiter Partizipation der Expert*innen entstand und auf einer Open Source Software basiert, anderseits viele Schweizer Firmen versprochen haben, Business Cases im Abstimmungskampf zu präsentieren.

Das Problem dabei: Dass die Schweizer Banken Kosten beim Onboarding von Neukund*innen sparen, trägt zwar dazu bei, dass die digitale Vertrauensinfrastruktur zum Fliegen kommt, hat aber nur beschränkte Überzeugungskraft für jene, die sich vor systematischer Überwachung fürchten. Voraussichtlich wird sich die Abstimmung primär um die Frage drehen, ob die langfristige Sicherheit der Vertrauensinfrastruktur garantiert ist. Wichtig ist es deshalb, über die technische Sicherheit und die Governance zu reden. Dabei empfiehlt sich eine Strukturierung des Diskurses durch die gewählte Architektur.

Der Kickoff für eine globale digitale Kollaboration [https://globaldigitalcollaboration.org/] zum Thema digitale Identitätsbrieftaschen in Genf (am 1. Und 2. Juli) stellt die Vertrauensfrage ins helle Scheinwerferlicht. Wenn die Schweiz die internationale Anschlussfähigkeit sucht, insbesondere jene an die digitale Identitätsbrieftasche der EU – wie sicher kann man da vor ausländischer Überwachung sein? Es zeigt aber auch die umgekehrte Frage: Wie realistisch ist es, dass die Schweizer Lösung in der EU akzeptiert wird? Denn die EU besteht auf einer Zertifizierung von Hardware und Software, wie sie so in der Schweiz nicht vorgesehen ist.

Dass die EU dabei noch ein kleines Problem hat – es gibt für die Zertifizierung noch keine Vorgaben (die ENISA arbeitet dran), weshalb in einer Übergangszeit die Mitgliedsländer selbst die eigenen Lösungen zertifizieren müssen – bedeutet nicht, dass sie langfristig auf die Durchsetzung ihrer Sicherheitsstandards verzichten wird. Allerdings wäre es auch falsch, so zu tun, als ob man aus dem Stand die richtigen Lösungen präsentieren könnte. Wenn wir eines in den letzten zwei Jahrzehnten zu digitalen Vertrauensinfrastrukturen gelernt haben, dann ist es, dass ein Erfolg einer eID das Durchlaufen von Lernkurven verlangt.

AUTHOR: REINHARD RIEDL

Prof. Dr. Reinhard Riedl ist Dozent am Institut Digital Technology Management der BFH Wirtschaft. Er engagiert sich in vielen Organisationen und ist Mitglied des Steuerungsausschuss von TA-Swiss. Zudem ist er u.a. Vorstandsmitglied von eJustice.ch, Praevenire - Verein zur Optimierung der solidarischen Gesundheitsversorgung (Österreich) und All-acad.com.

Posts from Reinhard Riedl

Create PDF

Ähnliche Beiträge

Es wurden leider keine ähnlichen Beiträge gefunden.

0

COMMENTS