Jörn von Lucke et al. (Hrsg.):
Auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2012 137

Elektronische Identitäten – Öffentliche und private Initiativen

Erich Schweighofer, Walter Hötzendorfer

Universität Wien
Arbeitsgruppe Rechtsinformatik
Schottenbastei 10-16/2/5, 1010 Wien
{vorname.nachname}@univie.ac.at

Abstract: In der virtuellen Welt bedarf es eines umfassenden Identitätsmanagements. Den hohen Anforderungen des öffentlichen Sektors hinsichtlich der Eindeutigkeit der Identität werden die praxisnäheren privaten Federation-Modelle mit einer hohen Flexibilität sowie Relativität und Vielschichtigkeit der Identität gegenübergestellt. Die – notwendige und realisierbare – Integration beider Ansätze wird behandelt und es werden offene Forschungsfragen im Zusammenhang mit privaten Federation-Modellen besprochen. Auf Initiative österreichischer Unternehmen arbeitet derzeit eine Gruppe an der Entwicklung und Umsetzung eines privatwirtschaftlich geprägten Federation-Modells sowie an der Integration bestehender öffentlicher und privater Lösungen.

1 Einleitung

Während in der realen Welt die Identität einer natürlichen Person auf dem Menschen an sich beruht und von staatlicher Seite nur Hilfsmittel in Form von Personalausweisen angeboten werden müssen, bedarf es in der virtuellen Welt eines umfassenden Identitätsmanagements. Identitätsmanagement umfasst die Sammlung, Authentifizierung und Nutzung von Identitäten und damit verbundenen Informationen [HSC08].

Elektronische oder digitale Identitäten können definiert werden als „Sammlungen von digitalen Informationen, die zu einem Individuum oder einer Organisation gehören." [HM06, S. 543] Sie sind digitale Repräsentationen eines Teils der gesamten Identität einer Person (Teilidentitäten). Die einzelnen gespeicherten Informationen über einen Nutzer, die zusammen eine solche elektronische Identität bilden, werden als Attribute bezeichnet [PH10]. Für die virtuelle Welt gilt, dass es ohne die elektronische Identität praktisch keine Handlungsmöglichkeit gibt. Eine Person kann mehrere elektronische Identitäten besitzen. Gerade im Internet gibt es eine große Vielfalt an Identitäten, die Möglichkeiten reichen von der österreichischen Bürgerkarte mit eindeutiger Identifikation und Authentifizierung mittels Smartcard oder Handy-Signatur bis zur kurzfristig zugeordneten dynamischen IP-Adresse.

Die große Zahl von Identitäten verursacht hohe Kosten in der Wartung und bringt Datenschutzprobleme und das Risiko von fehlerhaften und inkonsistenten Daten mit sich. Daher gibt es vielerlei Anstrengungen, elektronische Identitäten zu schaffen, die für mehrere und nicht nur ein einzelnes Service im Internet verwendet werden können. Wichtige Beispiele sind von öffentlicher Seite die österreichische Bürgerkarte und in Deutschland der neue Personalausweis; von privater Seite Microsoft Passport, OpenID, Liberty Alliance Project, Facebook, Google et cetera.

Ziel des Ansatzes der in Kapitel 3 erläuterten Identity Federation ist die Verwendbarkeit bestehender Identitäten über Organisationsgrenzen hinweg, in Zusammenarbeit von Identitätsprovidern, Serviceprovidern und Attributsprovidern. Für jeden Geschäftsfall wird nur die unbedingt nötige Identität offengelegt und jede Person kann auch unter Personentypen oder Pseudonymen auftreten. Diesem entscheidenden Mehrwert an Datenschutz steht aber kein Verlust an Rechtssicherheit gegenüber: Im Streitfall wird der „Schleier" des Personentypus oder des Pseudonyms gelüftet.

2 Öffentliches Identitätsmanagement am Beispiel Österreichs

Die Ausgabe von Identitätsdokumenten ist seit langem eine wichtige staatliche Aufgabe. Die technologischen Möglichkeiten der Einbeziehung eines direkten Links zur jeweiligen Person haben sich nunmehr wesentlich erweitert: Beschreibung, Bild, Fingerabdrücke, et cetera. Neuere Identitätsdokumente sind maschinenlesbar und verfügen oft über einen RFID-Chip.[26] Das öffentliche Identitätsmanagement ist dadurch gekennzeichnet, dass der Eindeutigkeit der Personenbindung ein großer Stellenwert eingeräumt wird. In Österreich besteht das System Bürgerkarte, das technisch als Smartcard oder als Handy-Signatur ausgestaltet ist. Für kooperative Anwendungen werden derzeit in diesem Zusammenhang das Unternehmensserviceportal sowie das Bürgerserviceportal aufgebaut.

2.1 Bürgerkarte

Die Bürgerkarte ist eine logische Einheit, die technologisch unabhängig die Personenbindung mit einer qualifizierten elektronischen Signatur verbindet [§ 2 Z. 10 öE-GovG] [Ku08]. Bei natürlichen Personen erfolgt die eindeutige Identifikation mit der an das Zentrale Melderegister geknüpften Stammzahl, bei juristischen beziehungsweise nicht gemeldeten Personen mit der Ordnungsnummer des Firmenbuchs, Vereinsregisters oder des Ergänzungsregisters. Der Vorteil dieser Verknüpfung liegt in der Eindeutigkeit im Vergleich zu den mehrfach verwendeten Personennamen, die auch in Kombination mit dem Geburtsdatum häufig nicht eindeutig sind. Die Bürgerkarte wird im Standardfall auf der e-card (Sozialversicherungskarte) gespeichert. Die Authentifizierung erfolgt über eine qualifizierte elektronische Signatur; vornehmlich nunmehr als Handy-Signatur.

[26] Beispiele dafür sind der neue Personalausweis in Deutschland [Bo10] und das biometrische Großprojekt UID in Indien [Ec11].

2.2 Handy-Signatur

Die wesentliche Neuerung der Handy-Signatur besteht in der der sicheren Signaturerstellungseinheit (SSEE), mit welcher die elektronische Unterschrift erfolgt. Diese befindet sich nicht mehr in Form der Smartcard beim Nutzer, sondern auf einem Hochsicherheitsserver und wird mit einem per SMS an das Handy zugesandten Einmalpasswort vom Signator ausgelöst [Sc10] [KR10].[27] Die Handy-Signatur entspricht damit zwei Trends der IT: mehr Benutzerfreundlichkeit und Cloud Computing.

Die SSEE muss gewährleisten, dass die Signaturschlüssel praktisch nur einmal auftreten können, mit hinreichender Sicherheit nicht abgeleitet werden können, ihre Geheimhaltung hinreichend gewährleistet ist und die Signatur vor Fälschungen bei Verwendung der jeweils verfügbaren Technologie geschützt ist. Vom rechtmäßigen Unterzeichner müssen SSEE vor der Verwendung durch andere verlässlich geschützt werden können [Anhang III SigRL].

Bei der Handy-Signatur besteht die Signaturerstellungseinheit aus einem Rechner (HSM-Server), in dem sich ein Hardware Security Modul (HSM) vom Typ nShield 500e F31 befindet. Zu diesem Rechner in einem Safe im Hochsicherheitsbereich des Rechenzentrums hat nur spezielles Sicherheitspersonal Zugriff. Der Signator muss sich beim Hochsicherheitsrechner durch seine Mobilfunknummer und ein Signaturpasswort identifizieren; die Signaturerstellungseinheit wird sodann entschlüsselt. Zum Auslösen einer qualifizierten elektronischen Signatur wird an die Mobilfunknummer eine SMS mit einem vom HSM generierten, zeitlich begrenzt gültigen Einmalpasswort gesendet. Das Einmalpasswort ist über eine Signatur des HSM mit dem Hashwert der zu signierenden Daten verknüpft.

Die bisher im Zusammenhang mit der Bürgerkarte propagierten Komponenten der Signaturerstellung benötigt der Nutzer nicht mehr. Es ist nur mehr ein Handy erforderlich; die anderen Komponenten befinden sich im HSM. Kartenleser, Signatursoftware und Chipkarte sind nicht mehr notwendig.[28] Am „biometric touch“ wird nichts geändert; nach wie vor ist Geheimhaltung bestimmten Wissens und Besitz bestimmter Komponenten der stärkste Link zu einer bestimmten Person. Ohne Entschlüsselung der Signaturerstellungseinheit durch den Signator ist diese nicht verwendbar.

Die Handy-Signatur entspricht noch einem weiteren Trend, jenem zum Mobiltelefon als Universalinstrument des Menschen. Das Handy ist in Verbindung mit strengen Datensicherheitsauflagen sowie bei Verwendung von mobilen Transaktionscodes geeignet, den erforderlichen Link mit dem Signator sicherzustellen, sodass mittels sicherer Signaturerstellungseinheiten auf einem Hochsicherheitsserver rechtsverbindlich signiert werden kann. Weitere Sicherheitsmaßnahmen sind aus öffentlicher Sicht nicht erforderlich,

[27] Anbieter der Handy-Signatur ist A-Trust (http://www.a-trust.at). Vgl. zu den Sicherheitsauflagen die entsprechende Belehrung (https://www.a-trust.at/docs/belehrung/a-sign-premium-mobile/a-sign-premium-mobile-Belehrung.pdf, Zugriff am 15.01.2012).

[28] Auch die Online-Aktivierung der Bürgerkartenfunktion in Form der Handy-Signatur (mit postalischer Rückantwort) ist nunmehr möglich, sodass dies auch von zuhause aus durchgeführt werden kann [Fu11].

können aber je nach Nutzer durch Vereinbarung mit dem Signaturprovider vorgesehen werden [Sc10].[29]

2.3 Unternehmensserviceportal

Als Schnittstelle zur Wirtschaft wird vonseiten des Bundes das Unternehmensserviceportal als elektronisches Portal der österreichischen Wirtschaft aufgebaut.[30] Mit diesem zentralen Internetserviceportal für Unternehmen soll der elektronische Austausch von Informationen (Transaktionen) sowie die Bereitstellung von Informationen unterstützt werden. Ein wesentliches Ziel ist die Verringerung von Verwaltungslasten aus Informationsverpflichtungen. Mit der einmaligen Registrierung soll eine Vielzahl von Anwendungen der Verwaltung genutzt werden können. Die Verwendung einer eigenen einheitlichen Registrierungsnummer ist vorgesehen. Derzeit läuft ein Pilotbetrieb mit ausgewählten Unternehmen und Anwendungen.

Durch die Vielzahl von Meldeverpflichtungen, die Einbindung von E-Government-Anwendungen sowie die einheitliche Registrierungsnummer wird eine im Vergleich zum Firmenbuch verbesserte Identifikation von Unternehmen geboten. Neben der verbesserten Datenqualität liegt ein wesentlicher Vorteil auch darin, dass – im Gegensatz zur Stammzahl privater Personen – die Registernummer, Firmenbuchnummer, et cetera öffentlich ist und daher einheitlich verwendet werden kann. Je nach Bedarf kann in Verbindung mit einer Handysignatur, einer fortgeschrittenen Signatur, aber auch einfachen Signaturen eine hohe Transaktionssicherheit erreicht werden.

2.4 Bürgerserviceportal

Die Bundesministerien müssen für das Bürgerserviceportal HELP.gv.at möglichst verständliche und aktuelle Informationen zu Rechtsvorschriften und deren Entwürfen bereitstellen, um Bürger bei der Erfüllung von Informationspflichten zu unterstützen.

Eine Registrierung von Bürgern sowie die Einbindung von E-Government-Anwendungen in das Bürgerserviceportal sind aus Datenschutzgründen derzeit nicht vorgesehen. Die Option MyHELP als **personalisierte Version** von HELP bietet nur eine personenbezogene Unterstützung bei Informationen, Formularen und Behörden. Hierfür sind Daten zur persönlichen Lebenssituation einzugeben.

Die eindeutige Identifikation kann in der jeweiligen Geschäftsbeziehung erfolgen. Das österreichische E-Government-Gesetz [öE-GovG] verbietet aus Datenschutzgründen die Speicherung der einheitlichen Stammzahl. Nur das einem von 26 öffentlichen Anwendungsbereichen zuzuordnende, aus der Stammzahl der betroffenen Person und der Bereichskennung abgeleitete, auf diese nicht rückführbare bereichsspezifische Personenkennzeichen (bPK) darf verwendet werden. Im privaten Bereich tritt anstelle der

[29] Bei Verwendung von Smartphones ist es erforderlich, dass ein entsprechender Datensicherheitsstandard gegeben ist oder jedenfalls für die Transaktion ein vom Smartphone unabhängiger Rechner verwendet wird.
[30] https://www.usp.gv.at/Portal.Node/usp/public (Zugriff am 15.01.2012).

Bereichskennung die Stammzahl des Auftraggebers des privaten Bereichs [§ 14 öE-GovG].

3 Private Federation-Modelle

Der Großteil der Identifikations- und Authentifizierungsvorgänge im Internet erfolgt – ohne Einbeziehung der eben beschriebenen öffentlichen Systeme – zwischen Privaten, in der Regel zwischen Serviceprovidern und deren Nutzern. Jeder Serviceprovider verwaltet dazu üblicherweise Daten über seine Nutzer in Form von Nutzerkonten, welche die Nutzer beim erstmaligen Kontakt durch Eingabe selbstbehaupteter Daten angelegt haben [OM07]. Die laufende Identifikation und Authentifizierung der Nutzer erfolgt mittels Benutzername und Passwort. Die meisten der existierenden elektronischen Identitäten werden somit – in Form dieser Nutzerkonten – von Privatunternehmen verwaltet.

3.1 Grundlagen der Identity Federation

Ziel von privatwirtschaftlich geprägten Federation-Modellen ist es, diesen Status quo zu nützen und zugleich weiterzuentwickeln, indem sie die organisationsübergreifende Verwendung dieser elektronischen Identitäten ermöglichen. „Identity federation can thus be defined as a set of agreements, standards and technologies that enable SPs to recognise user identities and entitlements from other SPs.“ [JZS07, S. 147] Grundprinzip der Identity Federation ist also, dass der Nutzer nicht bei allen neu zu nutzenden Serviceprovidern eine elektronische Identität (ein Nutzerkonto) anlegt. Vielmehr veranlasst er, dass ihn Organisation A, bei der er bereits eine elektronische Identität angelegt hat, gegenüber Organisation B, deren Service er nutzen möchte, identifiziert, und dass Organisation A an Organisation B die zur Service-Nutzung benötigten Attribute des Nutzers übermittelt [Hi11]. Organisation A kann beispielsweise ein Serviceprovider sein, dessen Service(s) der Nutzer bereits verwendet, oder aber ein eigenständiger Identitätsprovider, dessen Hauptzweck die Authentifizierung von Nutzern sowie die Abwicklung des eben geschilderten Procedere ist und der ein besonderes Vertrauen seitens der Nutzer und der übrigen Teilnehmer einer Federation genießt. Das Konzept der Identity Federation schließt somit auch jenes der einmaligen Authentifizierung (Single-sign-on, SSO) [OM07, S. 344f.] mit ein, geht aber aufgrund seines organisationsübergreifenden Charakters und des Austauschs von Attributen weit darüber hinaus.

Die Umsetzung des Konzepts der Identity Federation bedarf eines institutionellen Rahmens, eines gemeinsamen Regelwerks und vertraglicher Beziehungen zwischen den beteiligten Organisationen. Das solcherart gebildete Netzwerk von Organisationen kann als Identity Ecosystem oder kurz als Federation bezeichnet werden, die einzelnen Organisationen als deren Teilnehmer.

Der Terminus Identity Ecosystem entstammt der National Strategy for Trusted Identities in Cyberspace (NSTIC) des Weißen Hauses. Diese definiert ein Identity Ecosystem als „an online environment where individuals and organizations can trust each other because they follow agreed-upon standards and processes to identify and authenticate their

digital identities—and the digital identities of organizations and devices. Similar to ecosystems that exist in nature, it will require disparate organizations and individuals to function together and fulfill unique roles and responsibilities, with an overarching set of standards and rules. The Identity Ecosystem will offer, but will not mandate, stronger identification and authentication while protecting privacy by limiting the amount of information that individuals must disclose." [Ns11, S. 21]

Für ein eng verwandtes Konzept wurde von der Liberty Alliance, deren Bestrebungen zur Förderung der Identity Federation nunmehr von der Kantara Initiative fortgesetzt werden, der Begriff Circle of Trust geprägt [OM07]. In Anlehnung an die drei von der Liberty Alliance unterschiedenen Modelle von Circles of Trust [Sh07] können drei verschiedene Organisationskonzepte einer Federation definiert werden, das konsortiale, das zentralisierte und das kollaborative Modell. Im kollaborativen Modell erstellen die Gründer der Federation gemeinsam deren Regelwerk und schaffen eine eigenständige zentrale Organisationseinheit, welche für die Weiterentwicklung und Einhaltung der Regeln sowie für den laufenden Betrieb der Federation sorgt. Eine konsortiale Federation besteht demgegenüber aus einem kleineren, beständigeren Kreis von Teilnehmern, die miteinander einen multilateralen Vertrag schließen. Charakteristikum des zentralisierten Modells ist die Dominanz des einzigen Gründers der Federation. Diesem Modell ähneln die beschriebenen Ansätze des öffentlichen Identitätsmanagements. Im Vergleich sind kollaborative Federations am besten skalierbar, da weder ihre Organisationsstruktur die Größe limitiert, noch ihr universeller Anspruch durch die Dominanz eines Teilnehmers konterkariert wird.

Trotz hoher Skalierbarkeit des kollaborativen Ansatzes ist nicht zu erwarten, dass sich in Zukunft eine einzelne große Federation entwickelt, welche die Nutzung aller erdenklichen Services im Internet ermöglicht. Stattdessen ist davon auszugehen, dass nebeneinander – ausgehend von bestimmten, zunächst möglicherweise eng gefassten Anwendungsdomänen – zahlreiche Federations entstehen. Um deren Interoperabilität zu gewährleisten bedarf es gemeinsamer Standards sowie eines Metamodells, mit welchem die Gemeinsamkeiten und Unterschiede verschiedener Federation-Modelle formalisiert werden können.

3.2 Stärken privater Federation-Modelle

Obwohl das Themengebiet Identity Federation im Rahmen der genannten Initiativen und zahlreicher Forschungsprojekte[31] insbesondere aus technischer Sicht bereits ausführlich erforscht wurde, sind den Autoren existierende kollaborative Federations außerhalb sehr enger Nischen nicht bekannt. Die Einführung solcher Federations brächte allerdings im Vergleich zum Status quo, der am Beginn von Kapitel 3 beschrieben wurde, viele Vorteile und insbesondere ein erhöhtes Datenschutz- und Datensicherheitsniveau mit sich [Ns11]. Die Nutzer würden sich die zeitraubende Registrierung und Wartung ihrer Identität bei den verschiedenen Serviceprovidern ersparen. Die derzeit übliche redundante Datenspeicherung bei den einzelnen Serviceprovidern vervielfacht zu-

[31] Insbesondere sind die einschlägigen von der EU in FP6 und FP7 geförderten Projekte, wie etwa FIDIS, PRIME, PrimeLife und TAS3 zu nennen.

dem die Angriffsfläche für unautorisierten Datenzugriff und die Vielzahl an benötigten Zugangsdaten birgt die Gefahr des sorglosen Umgangs mit Passwörtern durch die Nutzer.

Identity Federation führt somit potenziell zu höherer Datensicherheit und bietet den Serviceprovidern ein vertrauenswürdiges Identifikations- und Authentifizierungssystem sowie konsistente und aktuelle Nutzerdaten. Federations könnten überdies neue Nutzungsmöglichkeiten des Internets schaffen, weil die Nutzer ein Attribut wie beispielsweise ihr Alter nicht nur wie bisher behaupten, sondern belegen können, indem sie die Übertragung des Attributs von einem Attributsprovider veranlassen.

Im Regelwerk einer Federation kann für die Richtigkeit einer übertragenen Information (Identität, Attribut) eine Haftung der übertragenden Organisation und allenfalls des als Mittler zwischen den beteiligten Organisationen stehenden Identitätsproviders definiert werden. Die Haftung kann für mehrere abgestufte Sicherheitsniveaus unterschiedlich hoch festgelegt werden, sodass der eine Information bereitstellende Teilnehmer einer Federation abhängig von deren Sicherheitsniveau in unterschiedlichem Ausmaß für deren Richtigkeit haftet. Jeder Serviceprovider kann in der Folge das angemessene Sicherheitsniveau wählen, welches er von einem Nutzer für eine bestimmte Information verlangt und jeder Identitätsprovider kann selbst festlegen, welche Mittel der Authentifizierung er von den Nutzern für die jeweiligen Sicherheitsniveaus fordert, von Benutzername und Passwort für das niedrigste Niveau, bis hin zur Bürgerkarte oder etwa einer vom Identitätsprovider selbst ausgegebenen Smartcard für das höchste Niveau.

Die derzeitigen Datenschutzprobleme im Internet ergeben sich hauptsächlich daraus, dass gegenwärtig bei jedem Serviceprovider, dessen Service(s) man nutzen möchte, eine elektronische Identität angelegt werden muss. Die Nutzer können nicht mehr überblicken, wer welche Daten über sie gespeichert hat. Zudem müssen häufig mehr Daten angegeben werden, als für die Service-Nutzung erforderlich sind. In einer Federation ist hingegen jedes Attribut im Idealfall nur bei einer einzigen Organisation gespeichert, die als Attributsprovider fungiert und das jeweilige Attribut bei Bedarf an andere Teilnehmer der Federation übermitteln kann. Die Attribute eines Nutzers sind somit insgesamt auf mehrere Teilnehmer verteilt und werden nur im Bedarfsfall auf Veranlassung des Nutzers zusammengeführt. Eine Federation ermöglicht somit mehr Datensparsamkeit und verschafft den Nutzern Kontrolle und Nachvollziehbarkeit der Verwendung ihrer personenbezogenen Daten.[32] Zudem kann eine Federation so ausgestaltet werden, dass anonyme Transaktionen möglich sind und die Quelle einer Information dem Empfänger nicht zwangsläufig bekannt werden muss, die Transaktion im Schadensfall aber nachvollzogen werden kann.

[32] Wie dies gestaltet werden könnte, wird in [SJ10] beschrieben.

Anonyme Transaktionen entsprechen dem gewohnten Geschäftsverkehr, denn abseits des Internets ist es häufig nicht erforderlich, seine Identität offenzulegen, etwa bei einem Barkauf. Diese „Lebensnähe“ sowie eine möglichst nutzerfreundliche und nachvollziehbare Gestaltung einer Federation und der angebotenen Authentifizierungsmöglichkeiten, könnte die – bisher zurückhaltende – Nutzung des Internets für sicherheitssensible Anwendungen einerseits, andererseits auch für Transaktionen, deren Durchführung im Internet den Nutzern bisher zu kompliziert erschien, revolutionieren.

4 Integration öffentlichen und privaten Identitätsmanagements

Die beiden beschriebenen Systeme des Identitätsmanagements schließen sich keinesfalls gegenseitig aus, sondern können einander ergänzen. Identitätsprovider innerhalb einer Federation benötigen Mechanismen der Identifikation und Authentifizierung ihrer Nutzer. Ein Identitätsprovider kann mehrere solcher Mechanismen unterstützen, die verschiedenen Sicherheitsniveaus entsprechen können. Diese Mechanismen werden vom Nutzer bestimmt (zum Beispiel Nutzername und Passwort, Mobiltelefon/M-TAN), vom Identitätsprovider selbst ausgegeben (zum Beispiel Smartcard), oder sind öffentlich-rechtlicher Natur (Bürgerkarte).

Letzteres bedeutet, dass sich der Nutzer innerhalb einer Federation im Sinne des SSO bei einem Identitätsprovider, der dies unterstützt, identifiziert und authentifiziert und mittels dieses Identitätsproviders seine Bürgerkarten-Identität in der gesamten Federation nutzen kann. Dies wird ermöglicht, da § 14 des österreichischen E-Government-Gesetzes [öE-GovG] die Verwendung der Bürgerkartenfunktion im privaten Bereich unterstützt. Zu diesem Zweck wird aus der Stammzahl des Identitätsproviders und jener des Nutzers ein bPK gebildet, welches den Nutzer im Verhältnis zum Identitätsprovider eindeutig identifiziert. Festzuhalten ist, dass der Identitätsprovider weder aus diesem bPK noch auf andere Art Verknüpfungen zur übrigen Verwendung der Bürgerkartenfunktion durch den jeweiligen Nutzer im öffentlichen oder privaten Bereich herstellen kann.

Die Nutzung der Bürgerkarte ist in Österreich bisher weit hinter den Erwartungen geblieben [Sc10].[33] Ein Grund dafür könnte im privaten Bereich der erhebliche Aufwand sein, den die Bereitstellung einer Bürgerkartenumgebung für Serviceprovider mit sich bringt. Setzen sich private Federations durch, könnte dies die Verbreitung und Nutzung der Bürgerkarte fördern, denn durch die beschriebene Möglichkeit der Verwendung der Bürgerkartenfunktion innerhalb einer Federation mittels eines Identitätsproviders wird dieses Problem gelöst: Nicht mehr die einzelnen Serviceprovider, sondern nur noch

[33] Ob die bereits erwähnte neue Möglichkeit der Online-Aktivierung der Bürgerkartenfunktion in Form der Handy-Signatur [Fu11] dies ändern wird, bleibt abzuwarten.

mindestens) ein Identitätsprovider muss die für die Verwendung der Bürgerkarte notwendige technische Umgebung bereitstellen.[34]

Die Integration öffentlichen und privaten Identitätsmanagements ist nicht auf die Nutzung vom Staat ausgegebener elektronischer Identitäten für privatwirtschaftliche Services beschränkt. Mahler beschreibt den umgekehrten Fall am Beispiel des norwegischen E-Government-Identitätsportals („ID-porten“) [Ma12]. Über das System dieses Portals erkennen staatliche Stellen elektronische Identitäten an, die von Identitätsprovidern des privaten Sektors ausgegeben wurden. Dies setzt einen Vertrag des betreffenden Identitätsproviders mit der norwegischen E-Government-Behörde voraus und beinhaltet die Einstufung jeder elektronischen Identität in einen von vier „Assurance Levels“.

5 Umsetzung in der Praxis

Der Boden für eine technische Realisierung privater Federation-Modelle wurde durch bisherige Projekte bereits weitgehend aufbereitet.[35] Die Etablierung einer privatwirtschaftlich geprägten, kollaborativen Federation bringt aber zahlreiche weitere Herausforderungen mit sich. So muss die Federation den rechtlichen Bestimmungen, insbesondere dem Datenschutzrecht entsprechen, und erfordert ein fundiertes internes Regelwerk, in welches organisatorische, wirtschaftliche und juristische Überlegungen einfließen.

Eine Federation kann sich überdies nur etablieren, wenn unter den gegebenen sozioökonomischen Bedingungen für alle (potenziellen) Teilnehmer und Nutzer ein ausreichend großer Anreiz besteht, sich daran zu beteiligen. Dazu muss die Federation so gestaltet sein, dass die – oben beschriebenen – Vorteile einer Federation für jeden einzelnen Teilnehmer die Kosten übersteigen, die ihre Realisierung mit sich bringt. Zudem müssen diese Vorteile potenziellen Nutzern auch bekannt gemacht werden.

Auf Initiative österreichischer Unternehmen hat sich unter dem Akronym EUSTIC eine Gruppe zusammengefunden, die an einem Federation-Modell inklusive technischen Prototypen sowie an Anwendungsfällen und Geschäftsmodellen einer Federation arbeitet.[36] In dieser Initiative haben die Autoren die Rolle inne, die technische Umsetzung mit den rechtlichen Vorschriften in Einklang zu bringen, am internen Regelwerk mitzuarbeiten und insbesondere auch den Datenschutz im Vergleich zu derzeitigen Anwen-

[34] Die Bürgerkarte dient in diesem Szenario als sicheres Mittel zur Identifikation und Authentifizierung, erfüllt aber in Bezug auf die Serviceprovider nicht mehr die Funktion einer eigenhändigen Unterschrift im Sinne des § 4 Abs. 1 des österreichischen Signaturgesetzes [öSigG]. Diese Funktion spielt allerdings im Geschäftsverkehr im Internet bisher ohnehin eine geringe Rolle.

[35] Siehe dazu die Ergebnisse der bereits angesprochenen von der EU in FP6 und FP7 geförderten Projekte sowie die Technologien, die bereits in den in Kapitel 2 beschriebenen staatlichen Lösungen eingesetzt werden, und Standards wie insbesondere die Security Assertion Markup Language (SAML). Zum Einsatz von SAML siehe [SJ10] sowie die dort zitierte Literatur.

[36] EUSTIC (Enterprise- and User-oriented Strategy for Trust and Identity in Cyberspace) ist ein Vorhaben von 21 europäischen Projektpartnern und weiteren 60 Partnern in der anwendungsorientierten EUSTIC Partner Alliance. Siehe http://eustic.eu beziehungsweise http://www.univie.ac.at/RI/EUSTIC.

dungen (Facebook, Google et cetera) wesentlich zu verbessern. Als nächster Schritt ist die sozioökonomische Erprobung unter wissenschaftlicher Beteiligung geplant.

In der Wirtschaftskammer Österreich wird derzeit an einem Wirtschaftsportalverbund (WPV) gearbeitet.[37] Es sollen Spezifikationen und Musterverträge für ein „Trust Framework" erstellt werden. Dies entspricht dem Konzept der Federation. Die Einbeziehung öffentlicher Ansätze wie des Unternehmensserviceportals wird als wichtiger Teil dieses Vertrauensnetzwerks angesehen.

6 Schlussfolgerungen und zukünftige Forschung

Während die Bürgerkarte Identifikation, Authentifizierung und Nichtabstreitbarkeit auf einem gesetzlich – sehr hoch – festgelegten Sicherheitsniveau bietet, allerdings bei geringer Flexibilität, strebt Identity Federation verschiedene, das heißt alle denkbaren Sicherheitsniveaus an und zielt – unabhängig von spezifischen Identifikations- und Authentifizierungsmethoden – auf den (nutzerbestimmten) Austausch von Attributen entsprechend dem jeweiligen Bedarf an Sicherheit und Vertrauen ab. Aufgrund der verschiedenen Sicherheitsniveaus und Authentifizierungsmechanismen kann jede Aktivität eines Nutzers innerhalb einer Federation mit dem für diese Aktivität angemessenen Sicherheitsniveau durchgeführt werden. Die Teilnehmer einer Federation können wiederum darauf vertrauen, dass die Identitäten und Attribute der Nutzer dem jeweils geforderten Sicherheitsniveau genügen und dies mit einer entsprechenden Haftung verbunden ist.

Im Konzept der Identity Federation sind Identitäten relativ und vielschichtig. Von der strikten Personenbindung des österreichischen E-Government-Modells kann hier vielfach abgesehen werden. Es wird auf die Verhältnismäßigkeit zwischen der Notwendigkeit von strikter Personenbindung und Authentifizierung und dem Zweck der jeweiligen geschäftlichen oder privaten Beziehung abgestellt. Dem einheitlichen Modell des öffentlichen Sektors wird ein vielschichtiges und hochgradig vernetztes Federation-Modell gegenübergestellt.

Private Federation-Modelle befinden sich derzeit im Konzeptions- und Entwicklungsstadium. Bis zu deren Marktreife sind noch zahlreiche Forschungsfragen zu lösen. Ökonomisch ist vor allem zu untersuchen, wie eine Federation insgesamt, sowie aus der Sicht jedes einzelnen Teilnehmers wirtschaftlich betrieben werden kann, und wie man die Phase des Aufbaus einer Federation gestaltet, sodass ausreichend Teilnehmer einen wirtschaftlichen Anreiz haben, sich an der Federation zu beteiligen.

Juristisch besteht die Herausforderung vor allem in der Vielzahl von Rechtsgebieten, die bei der Konzeption einer Federation zu beachten und somit im Detail zu untersuchen sind. Zentrale Fragen sind die datenschutzrechtskonforme Ausgestaltung der Datenflüsse in einer Federation, die Haftung einzelner Teilnehmer einer Federation gegenüber anderen Teilnehmern sowie gegenüber den Nutzern, und welche gewerberechtlichen,

[37] http://reloaded.wko.at/wk/format_detail.wk?angid=1&stid=573341&dstid=1637 (Zugriff am 15.01.2012).

wettbewerbsrechtlichen und weiteren Bestimmungen Teilnehmer einer Federation zu beachten haben. Im europäischen Binnenmarkt müssen mehrere Rechtsordnungen berücksichtigt als die Fragen des grenzüberschreitenden Charakters, wie insbes. nach dem anwendbaren Recht, der Streitschlichtung sowie der Äquivalenz der jeweiligen elektronischen Identitäten geklärt werden.

Auch ein geeigneter Organisationsrahmen einer Federation, etwa in Form einer eigenen Trägerorganisation, muss gefunden werden, sodass ein detailliertes internes Regelwerk einer Federation definiert und dessen Einhaltung kontrolliert werden kann. Ein System ausschließlich bilateraler Verträge zwischen den einzelnen Teilnehmern ist dazu aus der Sicht der Autoren keine hinreichende Lösung, da nur eine zentrale Organisationseinheit basierend auf klar definierten Rechtsregeln, Politiken und Standards effizient für Compliance und Streitschlichtung sorgen kann. Diese Standards und das damit zusammenhängende, oben angesprochene Thema der Interoperabilität von Federations sind schließlich weitere Forschungsfelder, die hier zu nennen sind.

Mehrere Initiativen beschäftigen sich derzeit intensiv mit Lösungsansätzen zu den genannten Fragen, um das Thema Identity Federation voranzutreiben. Eine weitere Hürde ist die Etablierung einer Federation in der Praxis, denn diese erfordert, dass zahlreiche – zum Teil konkurrierende – Stakeholder an einem Strang ziehen. Den Autoren sind allerdings zahlreiche Unternehmen mit sehr konkreten Anwendungsfällen bekannt, die sich an Federations beteiligen möchten und auf ein einsatzfähiges Federation-Konzept warten, beziehungsweise sich an der Entwicklung eines solchen Konzepts beteiligen. Der Umgang mit elektronischen Identitäten im Internet könnte sich also schon bald nachhaltig verändern.

Literaturverzeichnis

[Bo10] Borges, G.: Der neue Personalausweis und der elektronische Identitätsnachweis. In: Neue Juristische Wochenschrift (NJW) 2010; S. 3334-3339.

[Ec11] The Economist: Reform by numbers: Opposition to the world's biggest biometric identity scheme is growing. In: The Economist, 14.01.2012; S. 39-40.

[Fu11] Futurezone.at: Handy-Signatur jetzt mit Online-Anmeldung. Futurezone.at, 2011. http://futurezone.at/digitallife/5135-handy-signatur-jetzt-mit-online-anmeldung.php (Zugriff am 15.01.2012).

[Hi11] Hitachi ID Systems: Identity Management Terminology. Hitachi ID Systems, Inc., 2011. http://hitachi-id.com/access-certifier/docs/identity-management-terminology.html (Zugriff am 15.01.2012).

[HM06] Hansen, M.; Meints, M.: Digitale Identitäten – Überblick und aktuelle Trends. In: Datenschutz und Datensicherheit 30, 2006; S. 543-547.

[HSC08] Hansen, M.; Schwartz, A.; Cooper, A.: Privacy and Identity Management. In: IEEE Security & Privacy 6 (2), 2008; S. 38-45.

[JZS07] Jøsang, A.; Zomai, M.; Suriadi S.: Usability and privacy in identity management architectures. In (Brankovic, L.; Coddington, P.; Roddick, J.F.; Steketee, C.; Warren, J.R.; Wendelborn, A. Hrsg.): ACSW '07 Proceedings of the fifth Australasian symposium on ACSW frontiers - Volume 68, Australian Computer Society, Inc., Darlinghurst, 2007; S. 143-152.

[KR10] Kustor, P.; Rössler, Th.: Mobile qualifizierte elektronische Signatur: technisches Konzept und rechtliche Bewertung. In (Schweighofer, E.; Geist, A.; Staufer, I. Hrsg.): Globale Sicherheit und proaktiver Staat – Die Rolle der Rechtsinformatik, Tagungsband des 13. Internationalen Rechtsinformatik Symposions IRIS 2010, gewidmet Roland Traunmüller. books@ocg.at, Österreichische Computer Gesellschaft, Wien, 2. Auflage 2010; S. 295-306.

[Ku08] Kustor, P.: Novellierungen im Signatur- und E-Government-Recht 2007. In (Schweighofer, E. et al. Hrsg.): Komplexitätsgrenzen der Rechtsinformatik, Tagungsband des 11. Internationalen Rechtsinformatik Symposions IRIS 2008. Boorberg Verlag, Stuttgart, 2008; S. 42-48.

[Ma12] Mahler, T.: Governance Models for Interoperable Electronic Identities. In: Journal of International Commercial Law and Technology (JICTL), Forthcoming; University of Oslo Faculty of Law Research Paper No. 2011-37.

[Ns11] NSTIC: NSTIC Strategy Document. The White House, 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (Zugriff am 15.01.2012).

[öE-GovG] Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz - E-GovG), BGBl. I Nr. 10/2004, in der geltenden Fassung, zuletzt geändert: BGBl. I Nr. 111/2010. Elektronisch verfügbar: http://www.ris.bka.gv.at.

[OM07] Olsen, T.; Mahler T.: Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part I + II. In: Computer Law & Security Report 23, 2007; S. 342-351, 415-426.

[öSigG] Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG), BGBl. I Nr. 190/1999, in der geltenden Fassung, zuletzt geändert: BGBl. I Nr. 75/2010. Elektronisch verfügbar: http://www.ris.bka.gv.at.

[PH10] Pfitzmann, A.; Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management Version v0.34. Technische Universität Dresden, Dresden, 2010. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml (Zugriff am 15.01.2012).

[Sc10] Schweighofer, E.: Sind Handysignaturen qualifizierte elektronische Signaturen? In (Wimmer, M. et al. Hrsg.): Fachtagung Verwaltungsinformatik FTVI Fachtagung Rechtsinformatik FTRI 2010, Arbeitsberichte. Universität Koblenz-Landau, Koblenz, 2010; S. 78-81.

[Sh07] Sheckler, V. (Hrsg.): Liberty Alliance Contractual Framework Outline for Circles of Trust. Liberty Alliance Project, 2007, http://www.projectliberty.org/liberty/content/download/2962/19808/file/Liberty%20Legal%20Frameworks.pdf (Zugriff am 15.01.2012).

[SigRL] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (Signaturrichtlinie), ABl L 013, 12 vom 19.01.2000. Elektronisch verfügbar: http://eur-lex.europa.eu.

[SJ10] Scudder, J.; Jøsang, A.: Personal Federation Control with the Identity Dashboard. In (de Leeuw, E.; Fischer-Hübner, S.; Fritsch, L. Hrsg.): Policies and Research in Identity Management. Springer, Berlin, Heidelberg und New York, 2010; S. 85-99.