Design- und Implementierungsaspekte mobiler abgeleiteter Identitäten

Daniel Träder · Alexander Zeier · Andreas Heinemann

Hochschule Darmstadt
Fachbereich Informatik
{daniel.traeder | alexander.zeier | andreas.heinemann}@h-da.de

Zusammenfassung

Durch die immer weiter voranschreitende Digitalisierung können mehr und mehr unserer alltäglichen Aufgaben online erledigt werden. Dies schließt auch eGovernment-Dienste ein, welche definierte Anforderungen an die Sicherheit stellen. Um diese Anforderungen zu erfüllen, müssen digitale Identitäten an die Bürger ausgestellt werden. Zusätzlich ist eine 2-Faktor-Authentifizierung (2FA) essentiell, um ein ausreichendes Vertrauensniveau zu erreichen. Durch die hohe Verbreitung von Smartphones wird die mobile Nutzung von Online-Diensten immer beliebter. Diese unterstützen die 2FA auf natürliche Weise. Der Begriff *mobile abgeleitete Identität* bezeichnet eine Identität, die a) auf einem mobilen Gerät verwendet werden kann und b) von einem physikalischen oder digitalen Identitätsnachweis abgeleitet wurde. Diese Arbeit untersucht 21 Systeme, welche mobile abgeleitete Identitäten zur Authentifizierung der Nutzer verwendet. Dabei werden sowohl Systeme betrachtet, die sich bereits im Einsatz befinden (im öffentlichen sowie privaten Sektor) als auch wissenschaftliche Arbeiten. Dabei konnten wir erkennen, dass die bereits genutzten Systeme in der Regel eine Speicherung der Identitäten in der Cloud bevorzugen, während die Forschung eine lokale Speicherung bevorzugt. 2FA wird von beiden gleichermaßen unterstützt, wobei biometrische Verfahren die Ausnahme sind.

1 Einführung und Motivation

Viele Online-Dienste erfordern eine zweifelsfreie Identifizierung und Authentifizierung eines Nutzers durch den jeweiligen Anbieter. Um das Risiko von Identitätsdiebstahl und Missbrauch zu reduzieren, wird vermehrt auf 2-Faktor-Authentifizierung (2FA) gesetzt. Vor dem Hintergrund der Omnipräsenz von Smartphones, vgl. [Bund16, Pous16], wird hier vor allem auf Lösungen gesetzt, die das Smartphone als zweiten Faktor (Besitz) einbeziehen, z.B. unter Nutzung der im Smartphone verbauten SIM-Karte oder durch eine spezielle, personalisierte Applikation [TeVZ16].

Einen Sonderfall stellen Online-Dienste des eGovernments dar. So werden in der eIDAS-Verordnung [EU14] und den dazugehörigen technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI-TR-03107 [BSI16], BSI-TR-03127 [BSI15]) konkrete Vorgaben zur technischen Umsetzung von Verfahren zur Online-Authentifizierung gemacht, um definierte Sicherheitsniveaus zu erreichen. Auf Anbieterseite werden Dienste diesen Sicherheitsniveaus zugeordnet. Somit kann sichergestellt werden, dass gewisse sicherheits- bzw. datenschutzsensible Vorgänge nur dann online angestoßen werden können, sofern die Authentifizierung des Nutzers und der Dienst sich auf einem gleichen Vertrauensniveau befinden.

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 70-80.

Ein wichtiger Teilaspekt ist hier die Ausgestaltung der Registrierung einer digitalen Identität, d.h. einer initialen, zweifelsfreien Zuordnung von Identitätsdaten zu einer natürlichen Person. Bringt ein Nutzer hier eine bereits durch Dritte überprüfte digitale oder physikalische Identität ein, so spricht man von einer *abgeleiteten digitalen Identität*[1]. Sofern diese abgeleitete Identität beim mobilen Zugriff auf Online-Dienste nutzbar ist, sprechen wir von einer *mobilen abgeleiteten digitalen Identität*.

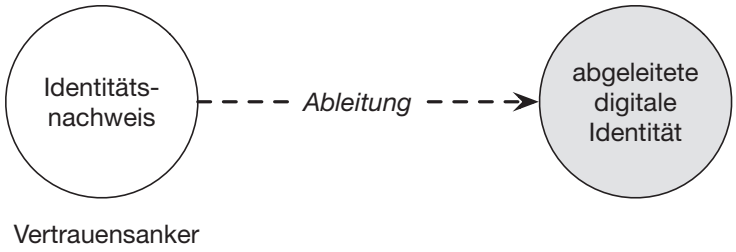

Abb. 1: Abgeleitete digitale Identität

Abgeleitete digitale Identitäten zeichnen sich also dadurch aus, dass sie mit dem Identitätsnachweis verbunden sind, von dem sie abgeleitet wurden. Die Ausgangsidentität stellt also einen Vertrauensanker dar. Abbildung 1 verdeutlicht diesen Zusammenhang.

Abgeleitete digitale Identitäten bringen hinsichtlich des Designs und der Implementierung eine Reihe von interessanten Fragestellungen mit sich:

- Wie wird die initiale Ableitung der abgeleiteten Identität von einer Ausgangsidentität umgesetzt?
- Wo wird die abgeleitete Identität[2] gespeichert und wie wird der Zugriff abgesichert?
- Wie oft kann eine abgeleitete Identität erzeugt werden, d.h. wie oft kann von einer Ausgangsidentität abgeleitet werden?

Im Rahmen dieser Arbeit werden insgesamt 21 Vorschläge aus Forschungsarbeiten zu mobilen abgeleiteten Identitäten sowie bereits in der Praxis im Einsatz befindliche Systeme untersucht und die wesentlichen Design- und Implementierungsaspekte herausgearbeitet. Die vorliegende Arbeit gibt hierzu einen Überblick.

Nachfolgend ist diese Arbeit wie folgt strukturiert: Zunächst wird kurz auf verwandte Arbeiten eingegangen (Abschnitt 2). Abschnitt 3 nennt wesentlichen Aspekte bezüglich Design und Implementierung mobiler abgeleiteter Identitäten. Anhand dieser Aspekte werden in Abschnitt 3 die konkret analysierten Arbeiten und Praxissysteme tabellarisch vorgestellt, bevor Abschnitt 4 diese Arbeit zusammenfasst.

2 Verwandte Arbeiten

Kubach et al. [KLRS+15] untersuchen den staatlichen und privaten Stand mobiler Identitäten in Europa und geben hierbei tieferen technischen Einblick in ausgewählte Lösungen. Gemalto [Gema14] gibt einen Überblick über staatliche mobile eID Lösungen. Das *Dutch Institute*

[1] *A credential issued based on proof of possession and control of a token associated with a previously issued credential, so as not to duplicate the identity proofing proces*; siehe hierzu [BDNP+11].

[2] Im weiteren Text als Kurzform für abgeleitete *digitale* Identität.

for Public Administration [Dut15] betrachtet europäische eID Lösungen mit Fokus auf die Finanzierung und geht hierbei nur vereinzelt auf mobilen Identitäten ein. Alle drei Arbeiten unterscheiden nicht zwischen mobilen und mobilen *abgeleiteten* Identitäten.

Nach unserer Kenntnis ist dies die erste Arbeit, die die Design- und Implementierungsaspekte *mobiler abgeleiteter* Identitäten in Europa sowie Forschungsarbeiten im Detail untersucht und zusammenfasst.

3 Design- und Implementierungsaspekte

Als Ausgangspunkt für die Realisierung mobiler abgeleiteter Identitäten sind a) eine bereits vorhandene digitale oder physikalische Identität und b) ein mobiles Endgerät wesentlich. Als typischer Vertreter eines mobilen Endgeräts ist das Smartphone anzusehen. Es sind aber auch andere *wearables* [Mann98] wie Smartwatches, Fitnesstracker etc. denkbar, sofern sie die Möglichkeit haben, direkt oder indirekt eine Verbindung zu einem Online-Dienst aufzubauen.

Speicherort: Zunächst stellt sich die Frage nach dem Speicherort der mobilen abgeleiteten Identität. Hier hat man zwei Optionen: Lokal auf dem mobilen Gerät oder entfernt in der *Cloud*. Sofern die abgeleitete Identität lokal gespeichert werden soll, müssen hier besondere Vorkehrungen getroffen werden, diese Daten nicht einfach unberechtigt auslesen zu können. Sichere Speicher (Secure Elements) oder SmartCards sind hier anerkannte Optionen. Analog erfordert eine Speicherung der abgeleiteten Identität in der Cloud eine kryptographische Absicherung dieser; Zugriff kann nur mittels Zutun des Eigentümers der abgeleiteten Identität erfolgen. Typischerweise wird ein privater Schlüssel eines asymmetrischen Krypto-Verfahrens eingesetzt, der besonders geschützt wird, um Identitätsdiebstahl zu vermeiden.

Aus der Entscheidung zum Speicherort ergeben sich nachgelagert weitere Aspekte, z.B. wie kann eine abgeleitete Identität bei Verlust oder Zerstörung des mobilen Endgerätes wiederhergestellt werden?

Registrierung: Bei der initialen Erzeugung einer abgeleiteten Identität und deren Registrierung in einem Identity Management System kann man zwischen einem Prozess in der realen Welt und einem Online-Prozess unterscheiden. Für beide Prozesse muss ein Nutzer seine digitale Ausgangsidentität bereithalten. Ein Prozess der realen Welt wäre bspw. der Besuch bei einer Behörde, die dort nochmal die Authentizität der Ausgangsidentität überprüft, die abgeleitete Identität erzeugt und auf das mobile Endgerät ablegt. Für einen Online-Prozess wird in der Regel weitere Hardware (bspw. Kartenleser, NFC-Leser, Kamera) benötigt, um die Echtheit der Ausgangsidentität zu überprüfen.

Anzahl der Ableitungen: Als weiterer Teilaspekt bei der initialen Erzeugung einer abgeleiteten Identität ist die Anzahl möglicher existierender abgeleiteter Identitäten zu nennen, d.h. ist es möglich, von einer Ausgangsidentität mehrmals eine Identität abzuleiten (um diese auf unterschiedliche mobile Endgeräte abzulegen) oder nicht? Sollen hier mehrere abgeleitete Identitäten unterstützt werden, so ist zu spezifizieren, ob diese abgeleiteten Identitäten unterscheidbar sind oder nicht und ob sie bei Verlust/Diebstahl einzeln oder als Gesamtheit revoziert werden müssen. Ebenso müssen die technischen Anforderungen an das oder die mobile(n) Endgerät(e) genau spezifiziert werden, um den Zugriff auf die abgeleiteten Identitäten auf allen Geräten auf die gleiche Art und Weise abzusichern. Konkret: Eine abgeleitete Identität muss auf einer Smartwatch genauso sicher abgelegt werden können wie auf einem Smartphone mit SIM-Karte.

Authentifizierung: Die gegebene Verfügbarkeit eines mobilen Endgerätes führt im Kontext von abgeleiteten Identitäten meist zu einer 2-Faktor-Authentifizierung gegenüber einem Online-Dienst. Neben dem Besitz des und damit exklusiven Zugriff auf das Smartphone (als 1. Faktor) kann der 2. Faktor je nach Fähigkeiten des Endgerätes ausgestaltet werden. Denkbar wären das Wissen um ein Geheimnis wie z.B. eine PIN oder ein Passwort oder biometrische Merkmale (bspw. Fingerabdruck, Stimme, Iris), die jedoch entsprechende Sensoren im Endgerät voraussetzen.

Die im Rahmen dieser Arbeit untersuchten Vorschläge und Systeme der Praxis sind anhand der in Abschnitt 3 diskutierten Aspekte in den Tabellen 1-3 zusammengefasst.

Es ist zu erkennen, dass viele der sich in der Praxis befindlichen Systeme in Europa die abgeleitete Identität in der Cloud speichern, während die wissenschaftlichen Arbeiten eher auf eine lokale Speicherung setzen. Ebenfalls wird die gleichzeitige physikalische und Online-Registrierung überwiegend unterstützt. Die 2-Faktor-Authentifizierung erfolgt fast durchweg mittels Wissen und Besitz. Biometrische Merkmale werden selten und wenn, dann nur optional unterstützt. Ebenso ist die Erzeugung mehrerer abgeleiteter Identitäten eher die Ausnahme.

3.1 Speicherort und Nutzung der abgeleiteten Identitäten

Ein großer Teil der Cloud Lösungen (Gemalto Mobile ID [Gema17], Mobile ID (Estland) [Mob], Audkenni (Island) [Aud], Finish Mobile ID [Murp13] (Finnland), MeID (Moldawien) [CEG15], MobilImza (Türkei) [GSM12]) nutzt die SIM Karte des Nutzers als Speicherort für den privaten Schlüssel eines asymmetrischen Verschlüsselungsverfahrens. Die Identität selbst wird jedoch auf einem Server gespeichert. Will sich der Nutzer nun gegenüber einem Diensteanbieter authentifizieren, so wird eine entsprechende Anfrage über den Mobilfunkanbieter an das Handy oder Smartphone des Nutzers gesendet. Diese Anfrage muss daraufhin vom Nutzer genehmigt werden. In diesem Fall wird die Anfrage im Hintergrund mit dem privaten Schlüssel signiert und zurück an den Diensteanbieter gesendet, welcher die Gültigkeit der Signatur überprüft. Kann diese bestätigt werden, so ist der Nutzer nun beim Dienst angemeldet.

Andere Cloud Lösungen (eHerkenning (Niederlande) [eHe], Chave Móvel Digital (Portugal) [Cha17], SPID (Italien) [SPI], NemID (Dänemark) [Nem], Handy-Signatur (Österreich) [Han], Gemalto Mobile ID, Idensys (Niederlande) [Ide], GOV.UK Verify (Großbritannien) [GOV17]) nutzen ebenfalls die SIM Karte des Nutzers, speichern jedoch keine zusätzlichen Informationen auf dieser oder auf dem Gerät. Stattdessen wird ein TAN Code per SMS gesendet, welche vom Nutzer in ein Eingabefeld auf der Webseite des Diensteanbieters eingetragen werden muss, bei dem er sich anmelden will. Andere Lösungen (Smart-ID (Estland, Lettland, Litauen) [Sma], GOV.UK Verify) nutzen eine Smartphone-Applikation zum Empfang der TAN, wiederum andere (Chave Móvel Digital (Portugal)) versenden die TAN per E-Mail. Bei Idensys, Gemalto Mobile ID und MIA (Österreich) [TeVZ16] können außerdem biometrische Merkmale zur Authentifizierung genutzt werden, sofern die dazu benötigte Applikation vom Nutzer installiert wurde.

Wird die Identität lokal auf dem Gerät gespeichert ([OtOM17], [BrHJ16], [ScMo13], [ScRa12], SkIDentity [HHWB+15], ShoCard [Sho17]), so wird sie verschlüsselt auf diesem abgelegt und der Schlüssel wird im Secure Element gespeichert. Um auf die Identität zuzugreifen (z.B. zur Authentifizierung), muss in den meisten Fällen eine PIN vom Nutzer eingegeben werden. Optional kann bei ShoCard Gesichtserkennung oder ein Fingerabdruck genutzt werden, um den Zugriff auf die Identität zu schützen. ShoCard ist die einzige Lösung, die eine Blockchain be-

Tab. 1: Realisierungen mobiler abgeleiteter Identitäten

Name (Projekt, Produkt, Titel)	Referenz	Typ	Speicher		Registrierung		Authentifizierung mit			# abg. IDs
			Lokal	Cloud	Physikalisch	Online	Wissen	Besitz	Biometrie	
Mobile Authentication with German eID	[OtOM17]	Forschung	✓		Brief mit QR Code	Foto vom Ausweis	PIN	Smartphone		nicht behandelt
Securely derived identity credentials on smart phones via self-enrolment	[BrHJ16]	Forschung	✓			Biometrie (z.B. Video) Ausweis (Kartenleser oder NFC)	nicht behandelt	Smartphone	nicht behandelt	nicht behandelt
eID mit abgeleiteten Identitäten	[ScMo13]	Forschung	✓			Ausweis (Kartenleser) + Computer	PIN	Smartphone		nicht behandelt
Vertrauenswürdige Identitäten mit dem neuen Personalausweis	[ScRa12]	Forschung	✓			Ausweis (Kartenleser oder NFC)	nicht behandelt	Smartphone	nicht behandelt	nicht behandelt
SkIDentity	[HHWB+15]	privater Sektor	✓			Ausweis (Kartenleser oder NFC)	PIN	Smartphone	Möglich, wird jedoch nicht in zertifizierter Applikation benutzt	≥1 (abhängig von Policy)
ShoCard	[Sho17], [SITA16]	privater Sektor	✓		Vor Ort*	Foto vom Ausweis + Daten der Machine Readable Zone	PIN	Smartphone	Optional: Gesichts-erkennung, Fingerabdruck	keine Informationen
MIA (Österreich)	[TeVZ16]	Forschung		✓	Vor Ort		PIN	Smartphone	Offline: Profilbild vergleichen, Online: FIDO	1

* optional für höheres Sicherheitslevel

** Konto erforderlich

*** Ein Nutzer kann sich im Prinzip bei mehreren Identitätsprovidern registieren, was aus unserer Sicht faktisch zu mehreren abgeleiteten Identitäten führt

Tab. 2: Realisierungen mobiler abgeleiteter Identitäten (fortgesetzt)

Name (Projekt, Produkt, Titel)	Referenz	Typ	Speicher		Registrierung		Authentifizierung mit			# abg. IDs
			Lokal	Cloud	Physikalisch	Online	Wissen	Besitz	Biometrie	
gemalto Mobile ID	[Gema17]	privater Sektor		✔		Abhängig von Umsetzung	PIN	SIM Karte		1
								Smartphone	Fingerabdruck	
Mobile-ID (Estland)	[Mob], [Mart10]	öffentlicher Sektor		✔		Ausweis (Kartenleser)	PIN	SIM Karte		1
Smart-ID (Estland, Lettland, Litauen)	[Sma], [Sma17]	öffentlicher Sektor		✔		Ausweis (Kartenleser)	PIN	Smartphone (App)		≥1
						Online-Banking				
						Mobile-ID (Estland)				
					Vor Ort (in Planung)					
Audkenni (Island)	[Aud]	öffentlicher Sektor		✔	Vor Ort		PIN	SIM Karte	keine Informationen	1
						Ausweis (Kartenleser)				
Chavel Móvel Digital (Portugal)	[Cha17]	öffentlicher Sektor		✔	Vor Ort		Passwort	Handy (SMS oder E-Mail)		1
						Ausweis				
SPID (Italien)	[SPI]	öffentlicher Sektor		✔	Vor Ort		Nutzername + Passwort	SIM Karte (SMS)*		≥1***
						Webcam				
						Ausweis (Kartenleser)				
						Zertifikat		Zertifikat (SmartCard)		
NemID (Dänemark)	[Nem]	öffentlicher Sektor		✔	Brief	Ausweis	PIN oder Passwort + OTP Liste (Beide Faktoren sind "Wissen")			1
					Vor Ort					
						Online Banking				

* optional für höheres Sicherheitslevel

** Konto erforderlich

*** Ein Nutzer kann sich im Prinzip bei mehreren Identitätsprovidern registieren, was aus unserer Sicht faktisch zu mehreren abgeleiteten Identitäten führt

Tab. 3: Realisierungen mobiler abgeleiteter Identitäten (fortgesetzt)

Name (Projekt, Produkt, Titel)	Referenz	Typ	Speicher		Registrierung		Authentifizierung mit			# abg. IDs
			Lokal	Cloud	Physikalisch	Online	Wissen	Besitz	Biometrie	
Handy-Signatur (Österreich)	[Han]	öffentlicher Sektor		✓	Brief	Online**	PIN	SIM Karte (SMS)		1
					Vor Ort	Ausweis (Kartenleser)				
						Online Banking				
Finish mobile ID (Finnland)	[Murp13]	öffentlicher Sektor		✓	Vor Ort	Ausweis (Kartenleser)	PIN	SIM Karte		1
						Online Banking				
MeID (Moldawien)	[CEG15]	öffentlicher Sektor		✓	Vor Ort		PIN	SIM Karte		1
Mobillmza (Türkei)	[GSM12]	öffentlicher Sektor		✓	Vor Ort + Telefonanruf		PIN	SIM Karte		1
GOV.UK Verify (Großbritannien)	[GOV17]	öffentlicher Sektor		✓	Öffentliche Dokumente + Online Banking		Nutzername + Passwort	SIM Karte (SMS)		≥1***
								Smartphone (App)		
eHerkenning (Niederlande)	[eHe]	öffentlicher Sektor		✓	Brief, Vor Ort*	Online	Nutzername + Passwort	SIM Karte (SMS)*		≥1***
					Vor Ort			OTP Responder (Hardware)		
						Bank Transaktion				
			(✓, Details unbekannt)			Zertifikat		Zertifikat (SmartCard)		
Idensys (Niederlande)	[Ide]	öffentlicher Sektor		✓		Ausweis (Kartenleser)	Nutzername + Passwort	SIM Karte (SMS)		≥1***
						Foto vom Ausweis		Smartphone (App)	Gesichts-erkennung	

* optional für höheres Sicherheitslevel

** Konto erforderlich

*** Ein Nutzer kann sich im Prinzip bei mehreren Identitätsprovidern registieren, was aus unserer Sicht faktisch zu mehreren abgeleiteten Identitäten führt

nutzt, um einen signierten Hash der Identität zu speichern [SITA16]. Auf diese Weise kann die Gültigkeit der Identität überprüft werden, indem diese mit dem in der Blockchain gespeicherten Hash verglichen wird. Die Identität selbst wird jedoch auch hier lokal auf dem Gerät des Nutzers gespeichert.

3.2 Registrierung

Die meisten Systeme der Praxis bieten eine Offline-Registrierung an, d.h. der Nutzer kann sich vor Ort bei einer Behörde, einer Bank oder beim Mobilfunkanbieter registrieren. Eine solche Registrierung ermöglichen ShoCard [Sho17], MIA (Österreich), Audkenni (Island), Chave Móvel Digital (Portugal), SPID (Italien), NemID (Dänemark), Handy-Signatur (Österreich), Finish Mobile ID (Finnland), MeID (Moldawien), MobilImza (Türkei) and eHerkenning (Niederlande). Smart-ID (Estland, Lettland, Litauen) will dies ebenfalls noch einführen.

Für die Online-Registrierung ist meistens ein Ausweis mit Online-Funktion erforderlich. Zur Kommunikation zwischen System und Ausweis wird ein Kartenlesegerät benötigt. Eine Online-Registrierung wird von Idensys (Niederlande), Handy-Signatur (Österreich), Finish Mobile ID (Finnland), SPID (Italien), Mobile-ID (Estland), Smart-ID (Estland, Lettland, Litauen), Audkenni (Island), SkIDentity [HHWB+15], [BrHJ16], [ScMo13] und [ScRa12] angeboten.

Einige der Lösungen benötigen zwar ebenfalls einen Ausweis, kommen jedoch ohne ein Kartenlesegerät aus. Chave Móvel Digital (Portugal) und ShoCard nutzen die *Machine Readable Zone* (MRZ) des Ausweises, um die benötigten Daten mit der Kamera auszulesen. Diese Daten werden dann benutzt, um die abgeleitete Identität zu erzeugen.

GOV.UK Verify (Großbritannien), eHerkenning (Niederlande), Finish Mobile ID (Finnland), Handy-Signatur (Österreich), NemID (Dänemark) und Smart-ID (Estland, Lettland, Litauen) kooperieren mit verschiedenen Banken und führen die Registrierung mithilfe der bereits bei der Bank durchgeführten Registrierung durch. Dabei gibt es grundsätzlich zwei Möglichkeiten: Ein kleiner Geldbetrag wird vom Konto des Nutzers, der den Identitätsnachweis erbringen will, auf das der Bank überwiesen. Alternativ kann der Nutzer Fragen zu seinen vergangenen Transaktionen beantworten, z.B. über den Zeitpunkt oder Betrag einer empfangenen oder geleisteten Überweisung. Hier wird der Identitätsnachweis durch das Wissen über die vergangenen Transaktionen erbracht.

SPID (Italien) bietet eine Identifikation über einen Video Chat an, wobei ein Mitarbeiter der Registrierungsstelle die Identifikation vornimmt. Dies wird ebenfalls von [BrHJ16] als Identifizierungsmethode vorgeschlagen.

Manche Systeme kombinieren auch Online- und Offline-Verfahren miteinander. Dies betrifft die Systeme, bei denen nur ein Foto des Ausweises oder dessen MRZ gemacht wird ([OtOM17] und ShoCard) oder eine Identifikationsnummer von einem Ausweisdokument in ein Online-Formular eingetragen werden muss (eHerkenning (Niederlande), NemID (Dänemark) und Handy-Signatur (Österreich)). In allen Systemen wird zusätzlich ein Brief an die registrierte Adresse des Nutzers gesendet. Dieser Brief enthält private Informationen, um den Registrierungsvorgang abzuschließen.

4 Zusammenfassung und Ausblick

Vorliegender Beitrag hat anhand einer Studie von insgesamt 21 Forschungsbeiträgen und Systemen der Praxis wesentliche Design- und Implementierungsaspekte mobiler abgeleiteter Iden-

titäten herausgearbeitet. Als zentrales Designkriterium haben wir den Speicherort (lokal/Cloud) der abgeleiteten Identität identifiziert. Dabei konnte gesehen werden, dass die meisten Lösungen im öffentlichen Sektor einer Speicherung der Identität in der Cloud nutzen, während alle Forschungsarbeiten (mit Ausnahme von [TeVZ16]) eine lokale Speicherung auf einem privaten Gerät bevorzugen.

Die meisten Systeme im öffentlichen Sektor bieten eine Vor-Ort-Registrierung an. Eine 2-Faktor-Authentifizierung ist bei allen Systemen gegeben, wobei die Verwendung von biometrischen Merkmalen als 2. Faktor eher die Ausnahme ist.

Weiter ist festzuhalten, dass im Kontext von eGovernment rechtliche Vorgaben berücksichtigt werden müssen, vgl. [EU14], die sich auf Designentscheidungen auswirken.

Die Identifizierung eines Nutzers wirft auch inhärent Fragen zur Privatsphäre auf – ein Tracking eines Nutzers über Systemgrenzen bzw. Anbieter hinweg sollte technisch unterbunden oder zumindest erschwert werden, vergleichbar mit den *Attribute-based Credentials for Trust*-Ansätzen [RaCS14, CaLN12, IBM17, Micr12].

Als nächstes wollen wir daher untersuchen, in welchem Umfang der Schutz der Privatsphäre im Sinne des *Privacy by Designs* [Scha10] bei den untersuchten Systemen zu abgeleiteten Identitäten berücksichtigt wurde und wie die Benutzbarkeit der einzelnen Lösungen zu bewerten ist. Zusätzlich wollen wir uns näher anschauen, ob die abgeleitete Identität bei den einzelnen Lösungen dasselbe Vertrauensniveau aufweist wie der digitale Identitätsnachweis, von dem abgeleitet wurde, sowie die Möglichkeiten des Nutzers mit Verlust oder Beschädigung des mobilen Gerätes umzugehen.

Danksagung

Diese Arbeit wurde vom Hessischen Ministerium für Inneres und Sport (HMdIS) im Rahmen der Förderung “Runder Tisch Cybersecurity@Hessen”gefördert.

Literatur

[Aud] Audkenni. https://www.audkenni.is/adstod/skilriki-i-farsima/, Stand 28.03.2017

[BDNP+11] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, S. Gupta, E. A. Nabbus: SP 800-63-1. Electronic Authentication Guideline. Tech. Rep., Gaithersburg, MD, United States (2011).

[BrHJ16] F. van den Broek, B. Hampiholi, B. Jacobs: Securely Derived Identity Credentials on Smart Phones via Self-enrolment. *In: G. Barthe, E. Markatos, P. Samarati (Hrsg.), Security and Trust Management: 12th International Workshop, STM 2016, Heraklion, Crete, Greece, September 26-27, 2016, Proceedings*, Springer International Publishing, Cham (2016), 106–121.

[BSI15] BSI: Architektur Elektronischer Personalausweis und elektronischer Aufenthaltstitel, Version 1.16. Tech. Rep., Bundesamt für Sicherheit in der Informationstechnik, Bonn, DE (2015).

[BSI16] BSI: Elektronische Identitäten und Vertrauensdienste im E-Government, Version 1.1. Tech. Rep., Bundesamt für Sicherheit in der Informationstechnik, Bonn, DE (2016).

[Bund16] Statistisches Bundesamt: 81 % der Internetnutzer gehen per Handy oder Smartphone ins Internet.

[CaLN12] J. Camenisch, A. Lehmann, G. Neven: Electronic Identities Need Private Credentials. In: *IEEE Security Privacy*, 10, 1 (2012).

[CEG15] Center of Electronic Government: Moldova Mobile e-ID Solution. http://egov.md/en/node/2846, Stand: 28.03.2017 (2015).

[Cha17] Chave Móvel Digital. https://cmd.autenticacao.gov.pt/Ama.Authentication.Frontend/, Stand 28.03.2017 (2017).

[Dut15] Dutch Institute for Public Administration (PBLQ): International Comparison eID Means. Tech. Rep. (2015).

[EGAM09] J. Eichholz, H. Grobbel, H. Aschauer, G. Meister: Verfahren und System zum Erzeugen einer abgeleiteten elektronischen Identität aus einer elektronischen Hauptidentität (2009).

[eHe] eHerkenning. https://www.eherkenning.nl/english/, Stand 28.03.2017 (o.J).

[EU14] EU: Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (2014).

[Gema14] Gemalto: National Mobile ID Schemes: Learning from Today's Best Practices. http://www.securitydocumentworld.com/creo_files/upload/article-files/wp_mobileid_overview_en.pdf (2014).

[Gema17] Gemalto: Mobile ID: Digital Identity Services by MNOs. http://www.gemalto.com/mobile/id-security/mobile-id, Stand 28.03.2017 (2017).

[GOV17] GOV.UK Verify. https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify, Stand 28.03.2017 (2017).

[GSM12] GSMA Mobile Identity Team and Turkcell: Mobile Signature in Turkey: A Case Study of Turkcell: MobilImza (2012).

[Han] Handy-Signatur. https://www.buergerkarte.at/, Stand 28.03.2017.

[HHWB+15] D. Hühnlein, T. Hühnlein, T. Wich, B. Biallowons, M. Tuengerthal, H.-M. Haase, D. Nemmert, S. Baszanowski, C. Bergmann: SkIDentity – Mobile eID as a Service. *In: D-A-CH Security 2015*, St. Augustin (2015).

[IBM17] IBM Research: Identity Mixer – A cryptographic algorithm to protect your privacy. http://www.research.ibm.com/labs/zurich/idemix/, Stand 28.03.2017 (2012-2017).

[Ide] Idensys. https://www.idensys.nl/, Stand 28.03.2017 (o.J.).

[KLRS+15] M. Kubach, H. Leitold, H. Roßnagel, C. H. Schunck, M. Talamo: SSEDIC. 2020 on Mobile eID. *In: GI-Edition : lecture notes in informatics - proceedings 251* (2015), 29–41.

[Mann98] S. Mann: WEARABLE COMPUTING as means for PERSONAL EMPOWERMENT. http://wearcam.org/icwckeynote.html, Stand: 28.03.2017 (1998).

[Mart10] T. Martens: Electronic identity management in Estonia between market and state governance. In: *Identity in the Information Society*, 3, 1 (2010), 213–233, http://link.springer.com/10.1007/s12394-010-0044-0.

[Micr12] Microsoft: U-Prove. https://www.microsoft.com/en-us/research/project/u-prove/, Stand 28.03.2017 (2012).

[Mob] Mobiil-ID. http://id.ee/?lang=en&id=36881, Stand 28.03.2017 (o.J.).

[Murp13] A. Murphy: Finnish Mobile ID: A Lesson in Interoperability. http://www.gsma.com/personaldata/wp-content/uploads/2013/03/GSMA_Mobile-Identity_Finnish_Case_Study.pdf (2013).

[Nem] NemID. https://www.nemid.nu/dk-en/, Stand 28.03.2017 (o.J.).

[Neve12] G. Neven: D32.2 Requirements Report for eID Service of FutureID Client. Tech. Rep. (2012).

[OtOM17] F. Otterbein, T. Ohlendorf, M. Margraf: Mobile Authentication with German eID. In: *11th International IFIP Summer School on Privacy and Identity Management* (2017).

[Pous16] J. Poushter: Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies. http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/, Stand 13.03.2017. (2016).

[RaCS14] K. Rannenberg, J. Camenisch, A. Sabouri: Attribute-based Credentials for Trust: Identity in the Information Society. Springer (2014).

[Scha10] P. Schaar: Privacy by Design. In: *Identity in the Information Society*, 3, 2 (2010), 267–274.

[ScMo13] M. Schröder, F. Morgner: eID mit abgeleiteten Identitäten. In: *Datenschutz und Datensicherheit-DuD*, 37, 8 (2013), 530–534, http://link.springer.com/article/10.1007/s11623-013-0213-z.

[ScRa12] M. Schmidt, M. Ramilli: Vertrauenswürdige Identitäten mit dem neuen Personalausweis. Dissertation, Diplomarbeit am Institut für Informatik der Freien Universität Berlin (2012).

[Sho17] ShoCard. https://shocard.com/, Stand 27.03.2017 (2017).

[SITA16] SITA: Travel Identity of the Future. https://shocard.com/wp-content/uploads/2016/11/travel-identity-of-the-future.pdf (2016).

[Sma] Smart-ID. https://www.smart-id.com/, Stand 11.05.2017 (o.J.).

[Sma17] Smart-ID Technical Overview (2017), https://www.smart-id.com/wordpress/wp-content/uploads/2017/01/smart-id-technical-overview-v0.6.html, Stand 11.05.2017.

[SPI] SPID – Sistema Pubblico di Identità Digitale. https://spid.gov.it/, Stand 28.03.2017 (o.J.).

[TeVZ16] O. Terbu, S. Vogl, S. Zehetbauer: One mobile ID to secure physical and digital Identity. *In: Open Identity Summit*, GI, Bonn (2016), 43–54.