Design and Implementation Aspects of Mobile Derived Identities[1]

Daniel Träder[2] Alexander Zeier[2] Andreas Heinemann[2]

Abstract: With the ongoing digitalisation of our everyday tasks, more and more eGovernment services make it possible for citizens to take care of their administrative obligations online. This type of services requires a certain assurance level for user authentication. To meet these requirements, a digital identity issued to the citizen is essential. Nowadays, due to the widespread use of smartphones, mobile user authentication is often favoured. This naturally supports two-factor authentication schemes (2FA). We use the term *mobile derived identity* to stress two aspects: a) the identity is enabled for mobile usage and b) the identity is somehow derived from a physical or digital proof of identity. This work reviews 21 systems that support mobile derived identities. One subset of the considered systems is already in place (public or private sector in Europe), another subset is subject to research. Our goal is to identify prevalent design and implementation aspects for these systems in order to gain a better understanding on best practises and common views on mobile derived identities. We found, that research prefers storing identity data on the mobile device itself whereas real world systems usually rely on cloud storage. 2FA is common in both worlds, however biometrics as second factor is the exception.

Keywords: Derived identities, design aspects, eGovernment, assurance levels

1 Introduction

Many online services require the unambiguous identification and authentication of users by the respective service providers. To reduce the risk of identity theft, two-factor authentication (2FA) schemes are more and more in place. The omnipresence of smartphones [rB16] make these devices a natural choice for the second factor (possession), e.g. by using the embedded SmartCard or a personalised app, cf. [TVZ16].

Online services provided by governments require special attention. For example, the European eIDAS regulation [EU14] and the ISO-15408 [IS09] define requirements for the technical realisation of eGovernment online authentication processes to fulfil predefined assurance levels. On the provider side, services are assigned to these assurance levels. This way, it can be ensured, that certain security and data sensitive processes can only be proceeded online if the authentication of a user and the corresponding online service operate on the same assurance level.

[1] Extended Version of Daniel Träder, Alexander Zeier, and Andreas Heinemann, "Design and Implementation Aspects of Mobile Derived Identities", in Open Identity Summit 2017

[2] University of Applied Science Darmstadt, Fachbereich Informatik, Haardtring 100, 64295 Darmstadt {daniel.traeder|alexander.zeier|andreas.heinemann}@h-da.de. This work was funded by the Hessian Ministry of the Interior and Sports (HMdIS) within the "Round Table Cybersecurity@Hessen".

One important aspect is how the enrolment of a user's digital identity takes place, meaning the initial secure association of the identity data with a real person. If a proof of identity (digital or physical), that was already verified by a trusted third party, is at hand, we call this new identity *digital derived identity*. Provided that this digital derived identity can be used for mobile authentication, we call this a *mobile derived digital identity*.

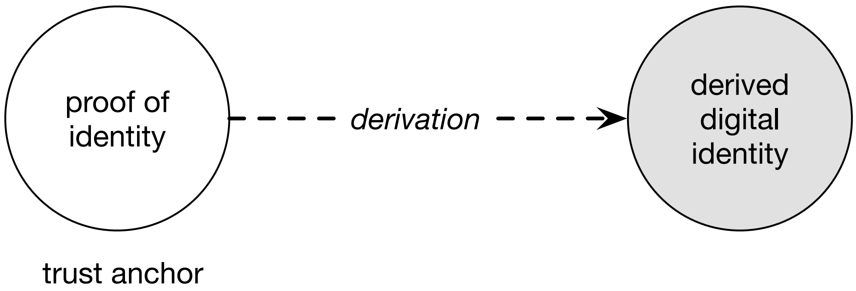

Fig. 1: Derived digital identity

Derived digital identities are characterised by the fact that they are linked to the proof of identity from which they were derived. This proof of identity is acting as a trust anchor, which is illustrated in Figure 1.

The concept of digital derived identities leads to a number of interesting questions in terms of design and implementation:

- How does the derivation process from the initial identity takes place?
- Where is the derived identity[3] stored and how is the access secured?
- How often can a derived identity be generated?

During the course of this work, 21 publications from research on mobile derived identities as well as systems already in place were analysed and essential design and implementation aspects were gathered. This paper provides an overview of our findings.

The remainder of this paper is structured as follows: First, we give an overview of related work (Section 2). Next, Section 3 covers important aspects that we identified regarding the design and implementation of mobile derived identities. Based on these aspects more details on implementations are presented in Section 4 before we summarise and conclude this work (Section 5).

2 Related Work

Kubach et al. [Ku15] investigate mobile identity solutions in Europe, both in the public and private sector. Their work provides a deeper technical insight into some of the solutions

[3] Further used as a short form for *digital* derived identity.

for mobile identities. Gemalto [Ge14] provides an overview of public sector mobile eID solutions. The *Dutch Institute for Public Administration* [Du15] looks at European eID solutions with a focus on financial aspects and is limited to few mobile solutions.

To our knowledge, this is the first work that systematically investigates design and implementation aspects of *mobile derived* digital identities within European countries as well as relevant research contributions in this field.

3 Design and Implementation Aspects

The realisation of mobile derived identities requires a proof of identity (a previous issued digital identity or a physical ID card/document) as well as a mobile device. The smartphone is a canonical representative of a mobile device. However, other *wearables* [Ma98] such as smart watches, fitness trackers etc. are also conceivable, as long as they have the possibility to connect directly or indirectly to an online service.

In the remainder of this section we elaborate more on the important design and implementation aspects we identified.

Storage: The foremost aspect addresses the storage location of the mobile derived identity. There are two options: local on the mobile device itself or remote in the *cloud*. If the derived identity is stored locally, special precautions must be taken to prevent unauthorised access. Secure storage (e.g. a Secure Element [Gl17]) or SmartCards are typical options here). Storing the derived identity in the cloud requires a cryptographic protection of the identity. Access must be granted only by means of the owner of the derived identity. Typically, a private key of an asymmetric cryptographic scheme is used in this context.

Registration and Enrolment: For the initial generation of a derived identity and its registration with an identity management system, a process in the real world and an online process can be distinguihed. In both cases, the user has to provide his own identity proof and his own mobile device. A real world registration process would be a visit to an authority which once again checks the authenticity of the identity proof and then generates the derived identity and places it on the mobile device.

For an online process further hardware (e.g. a card reader, a NFC reader, a camera) is often needed to verify the authenticity of the identity proof.

Authentication: The availability of a mobile device usually leads to the usage of a two-factor authentication scheme when accessing an online service. In addition to the possession and exclusive access to the device (as a first factor), the second factor varies depending on the capabilities of the device. Two possibilities are the knowledge of a secret (e.g. PIN) or the use of biometric features (e.g. fingerprint, voice, iris etc.) which require biometric sensors on the device.

Derivation: A last aspect of the initial generation of a derived identity is the number of possible derived identities in existence, i.e. is it possible to use the initial identity proof multiple times to derive an identity (e.g. to place it on different mobile devices)? If several derived identities are supported, one needs to specify whether these derived identities are distinguishable from each other and whether they have to be revoked individually or as a whole in case of loss or theft. Similarly, the technical requirements of the mobile devices have to be specified accurately to secure access to the derived identities on all devices in the same manner. For example, a derived identity must be stored equally secure on a smart watch as on a smartphone with a SIM card.

4 Current Implementations of Mobile Derived Identities

The proposals and systems investigated in this paper are summarised in table 1 based on the aspects discussed in section 3.

We notice, that many of the systems in use in European countries store the derived identity in the cloud, while scientific papers prefer local storage.

Both, offline/real world and online registration are supported in most cases. The two-factor authentication is present almost everywhere through knowledge and possession. Biometric readouts are rarely supported and even then only optional. Likewise, the generation of several derived identities is the exception.

We provide further details on individual systems below. The *Registration and Enrolment* and *Storage Location and Usage of Derived Identities* aspects are considered, since their implementations show remarkable differences.

4.1 Storage Location and Usage of Derived Identities

The majority of cloud storage solutions (gemalto Mobile ID [Ge17], Mobile ID (Estonia) [Mob], Audkenni (Iceland) [Aud], Finish mobile ID [Mu13], MeID (Moldova) [CEG15], MobilImza (Turkey) [GS12]) use the SIM card of a user's phone to store a private key as a credential while the identity itself is stored on a server. In this case, if a user wants to authenticate against an online service, a signing request is sent to the user via the mobile operator. The user gets prompted with a message asking him if he wants to accept the execution of the initiated action. If he does so, the message gets signed in the background and sent back to the service provider, which then checks the validity of the signature. If successful, the user is authenticated.

Other cloud storage solutions (eHerkenning (Netherlands) [eHe], Chavel Móvel Digital (Portugal) [Cha17], SPID (Italy) [SPI], NemID (Denmark) [Nem], Handy-Signatur (Austria) [Han], gemalto Mobile ID, Idensys (Netherlands) [Ide], GOV.UK Verify (Great Britian) [GOV17]) store no additional data on the mobile device and make use of the user's phone, or more specifically their SIM card, as a second factor by sending a SMS with a TAN code to the user which he then types into an input field in the browser, where the authentication process was initiated. With some solutions, the TAN can also be received by a smartphone application(Smart-ID (Estonia, Lithuania, Latvian) [Sma], GOV.UK Verify)

Name (Project, Product)	Reference	Type	Storage		Registration/Enrollment		Authentication with			# derived Ids
			Local	Cloud	Physical	Online	Knowledge	Posession	Biometrics	
Mobile Authentication with German eID	[OOM17]	research	✔		letter with QR code	Photo of ID card	PIN	smartphone		not discussed
Securely derived identity credentials on smart phones via self-enrolment	[vdBHJ16]	research	✔			Biometrics (e.g. video) ID card (card reader or NFC)	not discussed	smartphone	not discussed	not discussed
eID mit abgeleiteten Identitäten	[SM13]	research	✔			ID card (card reader) + computer	PIN	smartphone		not discussed
Vertrauenswürdige Identitäten mit dem neuen Personalausweis	[SR12]	research	✔			ID card (card reader or NFC)	not discussed	smartphone	not discussed	not discussed
SkIDentity	[Hu15]	private sector	✔			ID card (card reader or NFC)	PIN	smartphone	possible, but not used in certified application	≥1 (depending on policy)
ShoCard	[Sho17], [SI16]	private sector	✔		on-site*	Photo of ID card + data from machine readable zone	PIN	smartphone	optional: face recognition, fingerprint	no information
MIA (Austria)	[TVZ16]	research		✔	on-site		PIN	smartphone	offline: comparing profile picture, online: FIDO	1

* optional for higher assurance level

** account needed

*** A user can, in principle, register with multiple identity providers, which leads in our view to several derived identitites

Tab. 1: Realisation of mobile derived identities

Name (Project, Product)	Reference	Type	Storage		Registration/Enrollment		Authentication with			# derived Ids
			Local	Cloud	Physical	Online	Knowledge	Posession	Biometrics	
gemalto Mobile ID	[Ge17]	private sector		✔		depending on realisation	PIN	SIM card		1
								smartphone	fingerprint	
Mobile-ID (Estonia)	[Mob], [Ma10]	public sector		✔		ID card (card reader)	PIN	SIM card		1
Smart-ID (Estonia, Lithuania, Latvian)	[Sma], [Sma17]	public sector		✔		ID card (card reader)	PIN	smartphone (app)		≥1
						online banking				
						Mobile-ID (Estonia)				
					on-site (planned for the future)					
Audkenni (Iceland)	[Aud]	public sector		✔	on-site		PIN	SIM card	no information	1
						ID card (card reader)				
Chavel Móvel Digital (Portugal)	[Cha17]	public sector		✔	on-site		password	mobile phone (SMS or e-mail)		1
						ID card				
SPID (Italy)	[SPI]	public sector		✔	on-site		user name + password	SIM card (SMS)*		≥1***
						webcam				
						ID card (card reader)				
						certificate		certificate (smart card)		
NemID (Denmark)	[Nem]	public sector		✔	letter	ID card	PIN or password + OTP list (both factors are "knowledge")			1
					on-site					
						online banking				

* optional for higher assurance level

** account needed

*** A user can, in principle, register with multiple identity providers, which leads in our view to several derived identitites

Tab. 2: Realisation of mobile derived identities (continued)

Name (Project, Product)	Reference	Type	Storage		Registration/Enrollment		Authentication with			# derived Ids
			Local	Cloud	Physical	Online	Knowledge	Posession	Biometrics	
Handy-Signatur (Austria)	[Han]	public sector		✔	letter	online**	PIN	SIM card (SMS)		1
					on-site					
						ID card (card reader)				
						online banking				
Finish mobile ID (Finland)	[Mu13]	public sector		✔	on-site		PIN	SIM card		1
						ID card (card reader)				
						online banking				
MeID (Moldova)	[CEG15]	public sector		✔	on-site		PIN	SIM card		1
MobilImza (Turkey)	[GS12]	public sector		✔	on-site + phone call		PIN	SIM card		1
GOV.UK Verify (Great Britain)	[GOV17]	public sector		✔		official documents + online banking (optional)	user name + password	SIM card (SMS)		≥1***
								smartphone (app)		
eHerkenning (Netherlands)	[eHe]	public sector		✔	letter, on-site*	online	user name + password	SIM card (SMS)*		≥1***
					on-site			OTP responder (hardware)		
						bank transaction				
			(✔, details not clear)			certificate		certificate (smart card)		
Idensys (Netherlands)	[Ide]	public sector		✔		ID card (card reader)	user name + password	SIM card (SMS)		≥1***
						photo of id card		smartphone (app)	face recognition	

* optional for higher assurance level

** account needed

*** A user can, in principle, register with multiple identity providers, which leads in our view to several derived identitites

Tab. 3: Realisation of mobile derived identities (continued) or e-mail[4] (Chavel Móvel Digital (Portugal)). In case of Idensys, gemalto Mobile ID and MIA (Austria) biometric features (face, fingerprint) can be used if a user has installed a specific application on his device.

Locally stored derived identities are encrypted and saved on the device and the corresponding key is stored in its secure element. In order to access the identity (e.g. during authentication) the user has to provide a PIN code in most cases. In addition, ShoCard gives the option to use face recognition or fingerprint analysis to access the identity. ShoCard is also the only solution that makes use of a blockchain to store a signed hash of the user's identity. This way a 3rd party can check the validity of the identity by comparing it to the stored hash in the blockchain. However, the identity itself is stored locally.

4.2 Registration and Enrolment

Most systems in use offer offline/real world registration. This on-site enrolment offers the possibility to enrol locally either at an authority office, a bank branch, or at an office of a mobile operator. This kind of enrolment is possible with ShoCard [Sho17], MIA (Austria) [TVZ16], Audkenni (Iceland), Chavel Móvel Digital (Portugal), SPID (Italy), NemID (Denmark), Handy-Signatur (Austria), Finish mobile ID (Finland), MeID (Moldova), MobilImza (Turkey) and eHerkenning (Netherlands) [eHe]. Smart-ID (Estonia, Lithuania, Latvian) [Sma] plans to introduce on-site enrolment.

The online enrolment is mostly performed with the help of an ID card with online capabilities. For the communication between the infrastructure provided by the government and the ID card, a card reader is indispensable. This is provided by many solutions: Idensys (Netherlands), Handy-Signatur (Austria), Finish mobile ID (Finland), SPID (Italy), Mobile-ID (Estonia) [Mob], Smart-ID (Estonia, Lithuania, Latvian), Audkenni (Iceland), SkIDentity [Hu15], [vdBHJ16], [SM13] and [SR12].

Other solutions provide an enrolment without the need of a card reader but only the ID card. Chavel Móvel Digital (Portugal) and ShoCard make use of the machine readable zone (MRZ) printed on every card. The MRZ is read out with a camera. Next, the data is used as input for the generation of the derived identity.

GOV.UK Verify (Great Britain), eHerkenning (Netherlands), Finish mobile ID (Finland), Handy-Signatur (Austria), NemID (Denmark) and Smart-ID (Estonia, Lithuania, Latvian) cooperate with financial institutions for the registration based on previous online-banking enrolment. In general there are two methods to register based on online-banking: A small amount of money is transferred to the bank account of the registration provider. The proof of identity is given to the person who commissioned the transaction. To enrol with the second method, the customer of a bank has to answer questions about past bank transactions. The questions are about the transferred and received money on the customer account, e.g. the amount and time of a specific transaction. In this solution, the knowledge about past transactions proofs the identity of the account owner. SPID (Italy) offers a video

[4] Here, any other device able to access the user's e-mail is sufficient.

identification. During a video chat an employee of the registration provider performs the identification. Video identification is suggested by [vdBHJ16] as well.

In addition, a combination of offline and online actions that need to be carried out by a user already exist. [OOM17] and ShoCard make use of a photo taken from the physical ID card or just from the machine readable zone on the card. Whereas eHerkenning (Netherlands), NemID (Denmark) and Handy-Signatur (Austria) make uses of the serial number which has to be entered by the user in an online form. In all cases, a letter will be sent to the registered address of the card holder. This letter holds private information to complete the enrolment process.

5 Conclusion and Outlook

We have investigated prevalent design and implementation aspects of mobile derived identities. We studied 21 research contributions and systems used in practice. The most prominent design criterion is the storage location (local or cloud) of a mobile derived identity. It can be seen that most of the public sector solutions in European countries make use of a cloud storage, while all (except [TVZ16]) scientific works considered prefer a local storage on a personal device for the identity.

Most of the public sector solutions offer an on-site registration and enrolment. Two-factor authentication is implemented in all considered systems. For NemID both factors are knowledge. The use of biometric features as a second factor is the exception.

For the sake of completeness, we note, that in the context of eGovernment online services legal requirements must be taken into account, see [EU14] for example, affecting the design decisions.

As a next step, we will take a closer look at the different assurance levels and review whether a derived identity shows the same assurance level as the identity from which it was derived (this applies only for digital identities as an identity proof). In addition, we want to look closer into usability issues of the various realisations, and how a citizen must deal with loss or damage of their mobile device.

References

[Aud] Audkenni, `https://www.audkenni.is/adstod/skilriki-i-farsima/`, accessed: 28.03.2017, n.d.

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

[Cha17] Chave Móvel Digital, `https://cmd.autenticacao.gov.pt/Ama.Authentication.Frontend/`, accessed: 28.03.2017.

[Du15] Dutch Institute for Public Administration (PBLQ): International Comparison eID Means. Technical report, April 2015.

[eHe] eHerkenning, https://www.eherkenning.nl/english/, accessed: 28.03.2017, n.d.

[Ei09] Eichholz, Jan; Grobbel, Hubertus; Aschauer, Hans; Meister, Gisela: Verfahren und System zum Erzeugen einer abgeleiteten elektronischen Identität aus einer elektronischen Hauptidentität. 2009.

[EU14] EU: Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. July 2014.

[Ge14] Gemalto: National Mobile ID Schemes: Learning from Today's Best Practices. 2014. http://www.securitydocumentworld.com/creo_files/upload/article-files/wp_mobileid_overview_en.pdf.

[Ge17] Mobile ID: Digital Identity Services by MNOs, http://www.gemalto.com/mobile/id-security/mobile-id, accessed: 28.03.2017.

[Gl17] GlobalPlatform made simple guide: Secure Element, https://www.globalplatform.org/mediaguideSE.asp, accessed: 28.03.2017.

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

[GS12] GSMA Mobile Identity Team and Turkcell: Mobile Signature in Turkey: A Case Study of Turkcell: MobilImza. September 2012.

[Han] Handy-Signatur, https://www.buergerkarte.at/, accessed: 28.03.2017, n.d.

[Hu15] Huehnlein, Detlef; Huehnlein, Tina; Wich, Tobias; Biallowons, Benedikt; Tuengerthal, Max; Haase, Hans-Martin; Nemmert, Daniel; Baszanowski, Stefan; Bergmann, Christian: SkIDentity – Mobile eID as a Service. In: D-A-CH Security 2015. St. Augustin, 2015.

[Ide] Idensys, https://www.idensys.nl/, accessed: 28.03.2017, n.d.

[IS09] ISO: Information technology – Security techniques – Evaluation criteria for IT security. Standard, International Organization for Standardization, Geneva, CH, 2009.

[Ku15] Kubach, Michael; Leitold, Herbert; Roßnagel, Heiko; Schunck, Christian H.; Talamo, Maurizio: SSEDIC. 2020 on Mobile eID. In: GI-Edition : lecture notes in informatics - proceedings 251. pp. 29–41, 2015.

[Ma98] WEARABLE COMPUTING as means for PERSONAL EMPOWERMENT, http://wearcam.org/icwckeynote.html, accessed: 28.03.2017.

[Ma10] Martens, Tarvi: Electronic identity management in Estonia between market and state governance. Identity in the Information Society, 3(1):213–233, July 2010.

[Mob] Mobiil-ID, http://id.ee/?lang=en&id=36881, accessed 28.03.2017, n.d.

[Mu13] Murphy, Alix: Finnish Mobile ID: A Lesson in Interoperability. 2013. http://www.gsma.com/personaldata/wp-content/uploads/2013/03/GSMA_Mobile-Identity_Finnish_Case_Study.pdf.

[Ne12] Neven, Gregory: D32.2 Requirements Report for eID Service of FutureID Client. Technical report, February 2012.

[Nem] NemID, https://www.nemid.nu/dk-en/, accessed: 28.03.2017, n.d.

[OOM17] Otterbein, Florian; Ohlendorf, Tim; Margraf, Marian: Mobile Authentication with German eID. 11th Intl IFIP Summer School on Privacy and Identity Management, 2017.

[rB16] 81 % of Internet users access the Internet by mobile phone or smartphone, https://www.destatis.de/DE/PresseService/Presse/Pressemitteilungen/2016/12/PD16_430_63931.html, accessed: 13.03.2017.

[Ro12] Roßnagel, Heiko; Camenisch, Jan; Fritsch, Lothar; Gross, Thomas; Houdeau, Detlef; Hühnlein, Detlef; Lehmann, Anja; Shamah, Jon: FutureID - Shaping the Future of Electronic Identity. Datenschutz und Datensicherheit, 36(3):189–194, 2012.

[Sho17] ShoCard. https://shocard.com/, accessed: 27.03.2017.

[SI16] SITA: Travel Identity of the Future. 2016. https://shocard.com/wp-content/uploads/2016/11/travel-identity-of-the-future.pdf.

[SM13] Schröder, Martin; Morgner, Frank: eID mit abgeleiteten Identitäten. Datenschutz und Datensicherheit-DuD, 37(8):530–534, 2013.

[Sma] Smart-ID, https://www.smart-id.com/, accessed: 11.05.2017, n.d.

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

[SPI] SPID - Sistema Pubblico di Identità Digitale, https://spid.gov.it/, accessed: 28.03.2017, n.d.

[SR12] Schmidt, Maximilian; Ramilli, M: Vertrauenswürdige Identitäten mit dem neuen Personalausweis. PhD thesis, Diplomarbeit am Institut für Informatik der Freien Universität Berlin, 2012.

[TVZ16] Terbu, Oliver; Vogl, Stefan; Zehetbauer, Sebastian: One mobile ID to secure physical and digital Identity. In: Lecture Notes in Informatics. GI, Bonn, pp. 43–54, 2016.

[vdBHJ16] van den Broek, Fabian; Hampiholi, Brinda; Jacobs, Bart: Securely Derived Identity Credentials on Smart Phones via Self-enrolment. In: Security and Trust Management: 12th International Workshop, STM 2016, Heraklion, Crete, Greece, September 26-27, 2016, Proceedings, pp. 106–121. Springer International Publishing, Cham, 2016.