SSEDIC.2020 on Mobile eID

Michael Kubach[1] Herbert Leitold[2] Heiko Roßnagel[1] Christian H. Schunck[3]
Maurizio Talamo[3]

Abstract: Mobile electronic identity (eID) management solutions are on the rise worldwide and see a rapid take-up by stakeholders. In this paper experts from the SSEDIC.2020 network study and review the status of mobile eID deployment and use in e-government as well as industry with a focus on Europe. The findings demonstrate that mobile eID solutions have the potential to become a major means for digital identification but significant efforts still must be made to drive broad adoption across European member states, to guide secure integration of mobile solutions in the industry and to arrive at dedicated standards.

Keywords: mobile eID, eSignature, eIDAS, secure authentication, identity management, survey

1 Introduction

With the rapidly increasing world-wide use of mobile devices such as smartphones, mobile electronic identity (eID) and mobile signature applications are spreading quickly and are gaining significant traction in the markets where they are deployed. A number of developments further increase the potential of mobile eIDs:

In the EU the eIDAS regulation opens up new application possibilities for mobile eID and signature solutions as notifiable credentials for e-government applications and thus has the potential to drive EU wide adoption of mobile eID solutions [Eu15]. In the US the FIDO Alliance brings forward new technical specifications for online authentication, which are very mobile-friendly and have gained significant traction with the industry [Fi15]. The National Institute for Standards and Technology which hosts the national program office for implementing the National Strategy for Trusted Identities in Cyberspace (NSTIC) [Na15] joined the FIDO Alliance as well and thus connects it closely with the Identity Ecosystem Steering Group (IDESG) [Id15].

However, the opportunities and challenges associated with mobile eID use have not yet been sufficiently addressed within the public and private sectors, as well as regulation and standardization. For this reason SSEDIC.2020 [Ss15a], a large network of experts on digital identity that emerged from the SSEDIC ("Scoping the Single European Digital Identity Community") [Ss15b] thematic network, has decided to expand on the existing SSEDIC theme of mobile eID. The goal is to develop a truly global vision for mobile

[1] Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, firstname.lastname@iao.fraunhofer.de
[2] A-SIT, Inffeldgasse 16a. 8010 Graz, herbert.leitold@a-sit.at
[3] Fondazione Inuit, University of Rome Tor Vergata, Via dell'Archiginnasio snc, 00133 Rome, Italy, firstname.lastname@inuitroma2.it

identity, to point out existing challenges, to encourage best practice sharing and to promote global standardization and interoperability for mobile identity.

This paper is a first step towards developing strategic action plans to encourage adoption in a secure and trusted ecosystem both in the public and private sector and to drive harmonization of mobile authentication mechanisms suitable for eID use. We first look at current deployments of mobile eID in Europe and discuss two exemplary implementations in more detail in section 2, In section 3 we examine the integration of mobile eID solutions in European Commission and government funded research projects. We also analyze the usage of mobile eID in the European industry by example of the automotive sector in section 4 and briefly observe the status of mobile eID in standardization and regulation in section 5, before we summarize our results.

2 Mobile eID in e-government solutions

Mobile identity management solutions have been implemented in more than 35 countries worldwide [Fo15]. In the European Union specific mobile eID solutions have been deployed in four countries: Austria, Estonia, Finland and Lithuania (which adopted the Estonian solution) as well as in the associated country of Iceland [Ge14] and the candidate country Turkey [Gs15]. Compared to the very satisfactory take-up in the countries where these solutions have been released, the number of European countries that have deployed dedicated mobile eID solutions is still small. In the following we will take a closer look at two exemplary cases for these mobile eID initiatives by governments. Austria and Estonia both complemented the traditional smartcard eID with mobile eID. These two mobile eID systems are different both in their technology basis and in organisational aspects.

2.1 Case Study Mobile eID and eSignature in Estonia

In Estonia ID cards and eID are mandatory. All citizens have an active eID card and it is widely used: Since its introduction in 2002, more than 220 million electronic signatures were created and more than 350 million online authentications took place[4]. While the eID card is mandatory, "Mobiil-ID" is optional and was introduced in 2007 [Ma10, Mo15]. Mobile eID needs a special SIM card and the service is charged (1€/month for unlimited transactions). Although there are about ten times less active mobile e-ID users than ID-card/Digi-ID users in Estonia, the mobile e-ID users generate almost one quarter of the total monthly transactions (2.5 million out of 10.5 million transactions[5]). These numbers could in part be attributed to the fact that only those users who are particularly

[4] Figures taken 19 June 2015 at http://www.id.ee: Digital signatures 224 051 414; Active cards: 1 247 479; Electronic authentications: 356 230 150

[5] The data was kindly provided by the Estonian Certification Center Sertifitseerimiskeskus (www.sk.ee) on June 24 2015.

motivated to use their eID credentials very frequently are willing to sign up for a mobile eID at a cost. However, after obtaining the mobile e-ID most people abandon the use of their other Estonian eID credentials almost completely[5]. This strongly suggests that the mobile eID credentials are judged by their users as being the significantly more convenient option. Convenience and user friendliness can in turn be expected to contribute to the observed significantly higher usage rates of mobile eIDs as well.

2.2 Case Study Mobile eID and eSignature in Austria

In Austria eID is voluntary since its introduction in 2003. While there is full penetration of health insurance cards since 2005, its activation (or the activation of other tokens) as eID is a citizen's choice. Mobile eID was first introduced in 2005 by a mobile operator as a charged service, but was ceased in 2008. A similar service got contracted by the government end of 2009. The mobile eID does not need replacement of the SIM and works with any Austrian mobile operator. Both smartcard eID (on the health insurance card) and mobile eID are free of charge for the citizen and include qualified signatures.

The Austrian system is an interesting example for the card eID – mobile eID comparison, as it has similar basic conditions for the citizens for both card eID and mobile eID:

- Practically all citizens possess both tokens (a mobile phone and a health insurance card, probably also other smartcards like student service cards)
- Activation as eID and issuing a qualified signature certificate on it is free of charge for both the health insurance card and the mobile phone
- The activation procedures are comparable (can be done at the same registration offices like tax offices, service centers, etc.; online through the same portals)
- Basically the same eGovernment and private sector services can be used. More than 200 services that can be accessed using either a smartcard eID or the mobile eID are listed at the citizen card portal

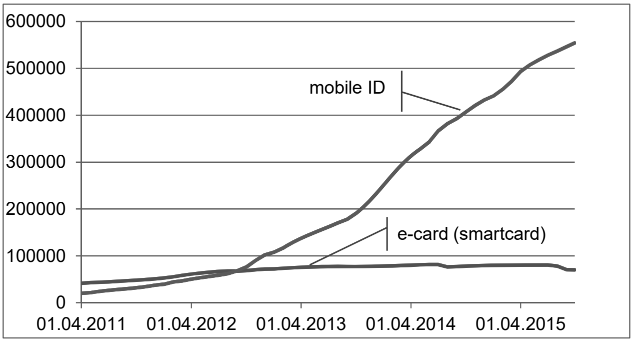

Fig. 1: Active e-cards and mobile eIDs in Austria

A first interesting question when comparing card eID and mobile eID is its take-up by the citizens. The figure above shows the active health smartcard eID (in blue) vs. active mobile eID (in red). As can be seen, mobile eID outperforms smartcard eID by far. This is also the case if considering that other smartcard eIDs exist in Austria that are not shown in the figure (like profession cards of notaries, lawyers, etc.).

Apart from one empirical study on electronic signatures [RH07], which shows that customer segments exist that prefer mobile signatures, no further scientific studies are known to the authors that give a reasoning for these trends. Still it is reasonable to assume that the mobile eID is chosen, as:

- No specific hardware (card-reader) is needed
- No specific software (card-drivers) is needed, just the browser
- Many today's devices like tablets can no longer be used with smartcards
- Mobile eID reflects current lifestyle and Internet access practices like with tablets
- Most citizens carry their mobile phone all the time (most have the health insurance card in their pocket also, though)

3 Mobile eID in selected EU and government funded R&D projects

3.1 SSEDIC Recommendations

SSEDIC.2020 emerged from the thematic network SSEDIC. After an intensive 3-year consultation period together with over 200 European and international digital identity management experts and many stakeholder organizations SSEDIC released a set of recommendations covering four key areas judged as central for the future development of digital identity: mobile identity, attribute usage, authentication and liability [Ta14]. With that SSEDIC recognized mobile identity as key enabler for the adoption of digital identity management solutions. The SSEDIC mobile eID recommendations include suggestions to encourage the acceptance of mobile eIDs as a notifiable credential for eGov use, to review Mobile eSignature/Wireless PKI standards relating to eIDs and to enable access to eGov services via mobile devices regardless of the contractual relationship with mobile providers (similar to emergency calls). The full recommendations are presented in detail in [Ta14].

3.2 FutureID

Practical insights supporting the rising importance of Mobile eIDs come from research in a European identity management-focussed project, where use cases play a major role. In this EU-funded project titled "FutureID - Shaping the Future of Electronic Identity" 19 partners from 9 EU states plus Switzerland and Norway cooperate to build a comprehensive, flexible, privacy-friendly and ubiquitously available identity management infrastructure for Europe to support the EU internal market for online services [Fu15]. The project integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims. The FutureID infrastructure provides benefits to all stakeholders involved in the eID value chain. Users benefit from the availability of a ubiquitously usable open source eID client that is capable of running on arbitrary desktop PCs but also on mobile android-based devices. FutureID allows service providers to easily integrate their existing services with the FutureID infrastructure, providing them with the benefits from the strong security offered by eIDs without requiring them to make substantial investments. To demonstrate the applicability of the developed technologies and the feasibility of the overall approach FutureID has developed two pilot applications as well as a technology demonstrator and is open for additional application services who want to use its technology. Moreover, substantial work on market analysis has been performed in the project. Together with various stakeholders a number of use and business cases have been constructed and evaluated. To this end, qualitative as well as quantitative surveys have been conducted and technology pilots and demonstrators are running. Mobile access is part of some of these use cases. From this look into the practical world of identity management it became even clearer that mobile electronic identity management is vital for secure and trustworthy digital services [Fu14, Fu13a]. This insight is further supported through the findings from the work on Mobile eID and eSignature in Austria [ZTL11].

However, the project does not try to re-invent the wheel. Rather, it builds on already existing elements. Therefore, for example, the Austrian Mobile eID has been integrated into FutureID so that it can be used with the FutureID infrastructure. The Android client is using the Open Mobile API to get access to security modules [Fu13b].

Although a variety of existing and newly developed elements are combined in the FutureID infrastructure, it was determined that it is reasonable to maintain a common user interface on different platforms to minimise confusion. Therefore, a flexible design of the FutureID client enables a similar user experience on different devices that reflect the users' expectations from existing services and functionalities. Therefore, the client has a lightweight GUI that enables platform independence. This is realized through a UI that is based on HTML5 technologies, enabling a responsive design [Fu13c].

3.3 SkIDentity

Another research project that is also working on mobile eIDs is funded by the German Federal Ministry for Economic Affairs and Energy (BMWi) in the "Trusted Cloud" program [Tr15]. The project "SkIDentity – Trusted Identities for the Cloud" is building a stable bridge between electronic identity cards and the existing and emerging cloud computing infrastructures [Sk15]. It aims at providing trusted identities for the cloud and secure complete business processes and value chains. For this purpose the existing components, services and trust infrastructures are integrated into a comprehensive, legally valid and economically viable identity infrastructure for the cloud and tested in pilot projects. Special attention is given to the demands of small and medium enterprises and public authorities. For example the SkIDentity infrastructure contains an eID-Broker, which will bundle the necessary eID-Services in a form which is accessible even for very small companies and municipal authorities. The project has won several international and German awards like the "European ID and Cloud Award 2015", "EuroCloud Germany Award 2015" and "Land der Ideen" 2014 and 2015 [Sk15].

Using the SkIDentity-Infrastructure, various electronic identity cards like the German eID ("neuer Personalausweis"), the Austrian social insurance card (e-card), the Estonian eID as well as several signature and banking cards from D-Trust, DATEV, S-Trust and GAD can easily be used in cloud and web applications. Moreover, cryptographically secured "Cloud Identities" can be created for pseudonymous authentication or self-determined identity proofing. These "Cloud Identities" can not only be autonomously managed by the user, they can also be transferred securely to almost any smartphone, thereby "mobilising" these eIDs for the use in mobile applications. Service providers that have registered themselves and their online services at the SkIDentity service can allow users to securely identify using their smartphone with the derived mobile eID [Hü15].

3.4 eSENS

The EU Large Scale Pilot (LSPs) eSENS is carried out by twenty EU/EEA member states and candidate countries. The purpose is to consolidate building blocks delivered by sibling LSPs and to pilot these in production environments. Such building blocks are inter alia eID, eSignatures, eDelivery, or eDocuments. eSENS piloting domains are eProcurement, eHealth, business lifecycle, eJustice, and citizen services [Es15]. For the basic building blocks eID and eSignatures eSENS recognises that the success of mobile devices asks for particular attention. One obvious reason is that many mobile devices no longer have the interfaces needed for traditional eID and eSignature means like smartcards. A further reason is a clear preference by users that use mobile devices as their preferred Internet access device.

eSENS addresses the mobile challenge in two dimensions: On the one hand, seamless integration of emerging mobile Id and mobile signature solutions in existing services is needed. On the other hand, states that do not yet have a large scale eID programme may deploy mobile solutions swifter, if they base these on the existing high penetration of mobile devices. The same holds for states that have eID and eSignature solutions but want to augment these as a next generation. The Austrian mobile eID and eSignature solution (cf. section 2.1) can be seen as a showcase: It has been developed in the LSP STORK, design, development, deployment and production integration in services could be achieved in about half a year.

eSENS does not develop mobile eID and eSignature solutions on their own, as little merit is seen if states develop solutions in an area as dynamic as mobile markets. What is developed is reference models on how emerging mobile solutions can be integrated into the states' infrastructure. This included interfaces to the identity basis (like population registers) and the registration infrastructure (like city halls).

4 Mobile eID in Industry and B2B - Automotive sector survey

To shed light on the current market situation for identity management in a business to business context we can present the first results from a quantitative survey in the European automotive industry. The survey in the form of an online questionnaire was conducted in Summer/Fall 2014 and focused on several aspects of electronic identity management in this specific professional context. As the target population was the European automotive industry, we used the customer database of an organization that governs the most important secure communications network of this industry. Respondents were contacted via e-mail and provided with a link to the survey. Follow-up e-mails were used to increase the response rate. Through this approach we received a total of 73 usable questionnaires. A total number of 1122 persons were effectively contacted (subtracting bounced e-mails). Thus, we achieved a response rate of roughly 7 percent. The data were analysed using SPSS. The profile of the respondents and the sample companies is shown in Figure 2 and Figure 3.

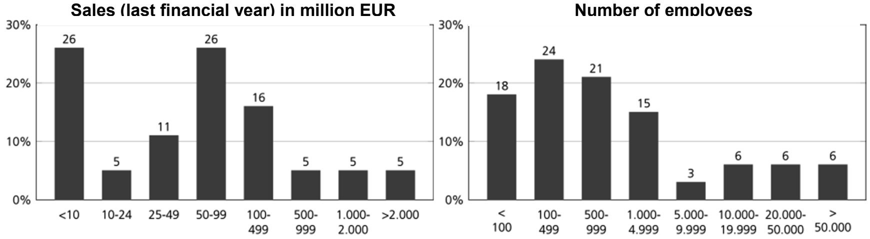

Fig. 2: Size statistics of the sample companies

As can be seen in Fig. 2, our sample covers a wide range of companies, from small to larger ones. Moreover, Fig. 3 shows that companies from different positions in the value chain are represented as well. The main market region of the sample is Europe, with Asia and Northern America being of less importance. This is certainly due to the basic population being customers of the European communication network organization. As SSEDIC 2020 is a project with a European focus this seems appropriate.

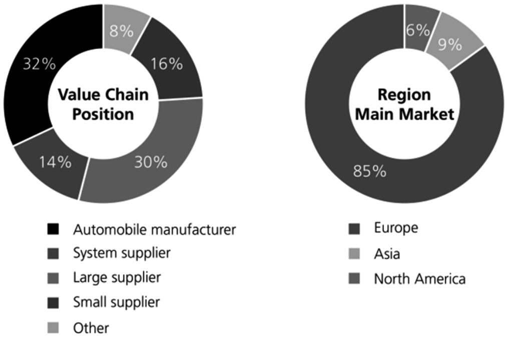

Fig. 3: Value chain position and main market regions of sample companies

The characteristics of the respondents show that most of them work in the IT-department (78 percent), another 13 percent works in the development department (9 percent "other"). IT-security and identity management are very important topics for the development departments due to the sensibility of the development data that is often exchanged with partner companies and the threat of industrial espionage. The respondents on average have 19.6 years of professional experience and work in their company for 14.1 years. Looking at the hierarchical position of the respondents we get a pretty balanced picture and see that 13 percent of the respondents are CEOs/Owners of the companies, 47 percent are on a management level and another 34 percent are employees (6 percent "other"). These data permits us to see the respondents as key informants with sufficient expertise and insight into the topics in question. The key informant approach is a well-established method for conducting survey-research [Ho12]. We can conclude that for a preliminary study the sample is relatively balanced and suitable to give us first insights into the topic.

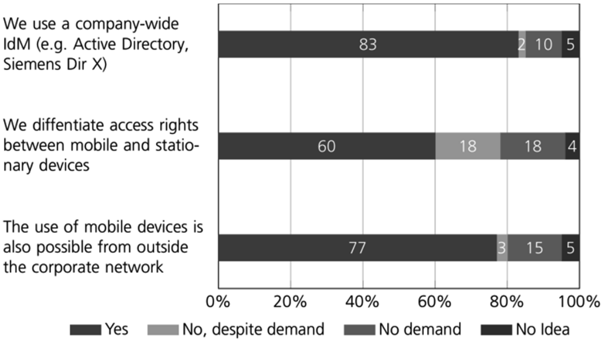

Fig. 4: Use of identity management (IdM) and with mobile devices

In this paper we focus on the parts of the study focusing on mobile aspects in the context of identity management. Fig. 4 first shows that generally, company-wide identity management is very well-established in the companies included in our sample. More than four-fifths of the companies use such a system. However, it is certainly interesting to note that only 60 percent of the sample companies differentiate in the access rights between mobile and stationary devices. 18 percent of the companies do not differentiate, even though the respondents see a demand for that – a demand that from a security perspective seems to be justified.

In Fig. 5 we show which kind of authentication method the companies in our sample currently used or plan to introduce in the near future (specified as the next two years). Obviously, despite its well-known shortcomings, username and password is still the dominant method for authentication. Three-quarters of the sample companies don't plan to abolish it while only 13 percent plan to do so or already have. As this paper focuses on the mobile aspects we omit a detailed discussion of the various other methods and discuss the use of the mobile telephone as an authentication method. This method, i.e. through SMS-TAN or special software is currently available in 10 percent of the companies. Another 5 percent plan to introduce it in the near future or are in the course of doing so. Thereby, the use of a mobile phone for authentication purposes is less important than all other alternatives to username and password except for national electronic identity cards (that are not yet rolled out in all countries of the European Union and other countries relevant to globally active companies). Public-Key-Infrastructures, One Time Password Generators and Biometric means for authentication are much more common. This means that currently, the relevance of mobile telephones for authentication purposes, despite their ubiquity, is very limited.

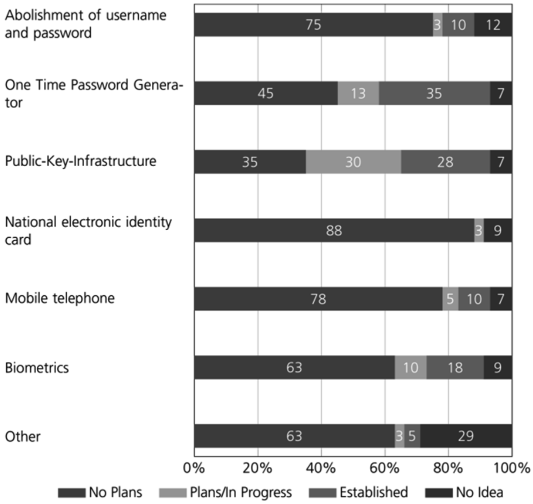

Fig. 5: Authentication method in use, plans to introduce other methods in the near future (approx.

next 2 years)

Summing up the first results from our empirical study we can note that sharing of data, services and application is commonplace in the European automotive industry. However, the development of adequate measures securing this interconnectedness, especially from an identity management perspective, seems to be lagging behind. This becomes especially visible in the mobile sphere. Today, mobile phones are a well-established means for work and are widely used to access (sensitive) data but are rarely integrated into adequate systems for identity management. Hence, mobile electronic identity management is apparently underdeveloped in the European automotive industry which leaves this key industry vulnerable to IT-security threats.

5 Mobile eID in Regulation and Standardization

In regulation and standardization mobile eID and signature solutions are rarely explicitly considered, but are implicitly seen as part of an ecosystem of digital identity management solutions. The eIDAS regulation mentions mobile solutions only once in the context of “innovative solutions and services (such as mobile signing, cloud signing, etc.)”. The NSTIC (as a strategy document) mentions cell phones in the context of “existing technology components in wide spread use today” and “identity media”. It also states: “mobile phone providers have specific technical needs. Carriers may thus join a trust framework to enable individuals to authenticate using their cell phones as a credential.” Overall it appears that the very promising take-up by end-users and industry of mobile eID technologies compared to other approaches is not reflected in the weight given in these documents to mobile eID solutions. This can of course be understood at least in part by efforts to keep such documents as technologically neutral as possible.

Also in standardization domain, specifics of mobile eID solutions are rarely considered in detail. ETSI GS INS 003 “Identity and access management for Networks and Services; Distributed User Profile Management; Using Network Operator as Identity Broker” [Et10] considers mobile carriers and networks as one architecture among others. ISO/IEC 29003 “Information technology - Security techniques - identity proofing” [In12] mentions mobile phones as one of many potential non person entities (NPEs) “or endpoint devices (e.g., mobile phones, PDAs, set-top boxes, laptops)”. ITU-T X.1251 “A framework for user control of digital identity” [In13] considers mobile devices together with personal computers as devices into which a user can “plug his/her identity information” in.

However, mobile devices enable a variety of new approaches to identity management that deserve specific attention by standardization bodies. Innovative solutions such as the provision of dynamic attributes through a large variety of sensors [Ta14], efficient means to integrate various biometrics into the authentication process and the integration of dedicated secure elements [Na08] are expected to offer unique and novel opportunities for example to implement efficient step-up authentication. Further, the interaction of mobile devices with networked services and their support through remote system accessed by mobile devices deserves detailed attention. The latter is currently addressed in the context of mobile signatures by ETSI [Et14].

6 Summary

In summary we have presented strong evidence that mobile devices have a unique potential to drive a large scale take-up of secure digital identity management solutions beyond username/password and smartcard based approaches. The Estonian and Austrian case studies demonstrate that mobile eIDs experience an extraordinarily high acceptance by end users. In both cases the successful take-up is supported by the integration of mobile eIDs in an ecosystem that offers a high number of appealing and convenient use cases.

In sharp contrast to this success stands the small number of European member states that have implemented mobile eIDs. However, the eIDAS regulation is expected to facilitate the roll-out of both mobile eID and e-signature solutions for e-government applications which should drive take-up and support further adoption.

Many national and EU projects actively consider mobile eIDs and have successfully integrated mobile eID solutions. However, mobile eIDs are usually not at the centre of attention. This is surprising as a detailed understanding of the mechanisms that drive the successful take up of mobile eIDs is incomplete. Further mobile devices offer the possibility to integrate a number of novel authentication options including step-up authentication that deserve further and more detailed research and development efforts.

The industry study in this work shows high demand for mobile eID solutions in a key industry sector but also presents evidence that the effective integration of these technologies is currently still underdeveloped. Assuming that these findings also apply to other key European industries a significant industry exposure to IT-security vulnerabilities caused by the non adequate integration of mobile eIDs is highly likely and must be addressed.

Finally, increased efforts dedicated to interoperable mobile eID standards that take advantage of the full range of authentication possibilities offered by networked mobile devices are required.

Acknowledgements

The authors would like to thank all members of the SSEDIC.2020 community and in particular Roger Dean, David Goodman, Hugo Kershot, Tarvi Martens, Daniela Merella, and Jon Shamah for engaging discussions and their ongoing support.

References

[Eu15] EU, „Regulation (EU) 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,“ 2014. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG. [Access 19 06 2015].

[Fi15] FIDO Alliance, Inc., „FIDO Alliance,“ 2015. [Online]. Available: https://fidoalliance.org/. [Access 19 06 2015].

[Na15] National Institute of Standards and Technology, „National Strategy for Trusted Identities in Cyberspace (NSTIC),“ 2011. [Online]. Available: http://www.nstic.gov. [Access 19 06 2015].

[Id15] Identity Ecosystem Steering Group, Inc., „Identity Ecosystem Steering Group,“ 2015. [Online]. Available: https://www.idecosystem.org/. [Access 19 06 2015].

[Ss15a] SSEDIC, „SSEDIC.2020,“ 2015. [Online]. Available: http://www.ssedic2020.eu/. [Access 19 06 2015].

[Ss15b] SSEDIC, „SSEDIC,“ 2015. [Online]. Available: www.ssedic.eu. [Access 19 06 2015].

[Fo15] N. Foggin, „Exploring the Role of Mobile in Digital Identity Assurance,“ 2014. [Online]. Available: http://oixuk.org/wp-content/uploads/2014/05/Mobile-White-Paper-final.pdf . [Access 19 06 2015].

[Ge14] Gemalto, National Mobile ID Schemes: Learning from Today's Best Practices, 2014.

[Gs15] GSMA Mobile Identity Team and Turkcell, „Mobile Signature in Turkey: A Case Study of Turkcell,“ 09 2012. [Online]. Available: http://www.gsma.com/personaldata/wp-content/uploads/2012/09/MI_TurkcellReport_print_FINAL.pdf. [Access 19 06 2015].

[Ma10] T. Martens, „Electronic Identity Management in Estonia Between Market and State Governance,“ in *Identity in the Information Society*, 2010.

[RH07] H. Roßnagel and O. Hinz, „Zahlungsbereitschaft für elektronische Signaturen,“ in *Wirtschaftsinformatik 2007 - eOrganisation: Service-, Prozess-, Market-Engineering*, A. Oberweis, C. Weinhardt, H. Gimpel, A. Koschmider, V. Pankratius and B. Schnizler, Hrsg., Karlsruhe, 2007, pp. 163-180.

[Ta14] M. Talamo, S. Ramachandran, M.-L. Barchiesi, D. Merella and C. Schunck, „Towards a Seamless Digital Europe: The SSEDIC Recommendations on Digital Identity Management,“ in *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI), P-237*, 2014, pp. 62-72.

[Fu15] FutureID Project, „FutureID Project,“ 2015. [Online]. Available: htttp://www.futureid.eu.

[Fu14] FutureID Project, „Deliverable D21.05,“ 2014. [Online]. Available: http://futureid.eu/data/deliverables/year1/Public/FutureID_D21.05_WP21_v1.0_Business_and_Use_Case_Analysis.pdf.

[Fu13a] FutureID Project, „Deliverable D21.03,“ 2013. [Online]. Available: http://futureid.eu/data/deliverables/year1/Public/FutureID_D21.03_WP21_v1.0_Vision.pdf.

[ZTL11] T. Zefferer, P. Teufl and H. Leitold, „Mobile qualifizierte Signaturen in Europa,“ *Datenschutz und Datensicherheit,* Bd. 35, Nr. 11, pp. 786-773, 2011.

[Fu13b] FutureID Project, „Deliverable D31.02," 2013. [Online]. Available: http://futureid.eu/data/deliverables/year1/Public/FutureID_D31.02%20_WP31_v1.0_Interface%20and%20module%20specification%20and%20documentation.pdf.

[Fu13c] FutureID Project, „Deliverable D34.02," 2013. [Online]. Available: http://futureid.eu/data/deliverables/year1/Public/FutureID_D34.02_WP34_v1.0_DesignMockups.pdf.

[Tr15] Trusted Cloud, „Trusted Cloud," 2015. [Online]. Available: http://trusted-cloud.de/.

[Sk15] SkIDentity Project, „SkIDentity Project," 2015. [Online]. Available: https://www.skidentity.de/.

[Hü15] T. Hühnlein, D. Hühnlein, T. Wich, B. Biallowons, M. Tuengerthal, H.-M. Haase, D. Nemmert, S. Baszanowski and C. Bergmann, „SkIDentity - Mobile eID as a Service," in *D-A-C-H Security 2015, 8./9.9.2015*, St. Augustin, 2015.

[Es15] eSens Pilot, „eSens Pilot Website," 2015. [Online]. Available: http://www.esens.eu/. [Access 01 07 2015].

[Ho12] C. Homburg, M. Klarmann, M. Reimann and O. Schilke, „What Drives Key Informant Accuracy?," *Journal of Marketing Research,* Bd. 49, Nr. 4, pp. 594-608, 2012.

[Et10] ETSI, Identity and access management for Networks and Services; Distributed User Profile Management; Using Network Operator as Identity Broker, 2010.

[In12] International Organization for Standardization, *International Standard Standard ISO/IEC WD1 29003:2012 (E), Information technology - Security Techniques - Identity Proofing,* 2012.

[In13] International Telecommunication Union, „Framework for Discovery of Identity Management Information, Recommendation ITU-T X.1255," 2013.

[Ta14] M. Talamo, M. L. Barchiesi, D. Merella and C. H. Schunck, „Global Convergence in Digital and Attribute Management: Emerging Needs for Standardization," in *Proceedings of the 2014 ITU Kaleidoscope Academic Conference: Living in a Converged World - Impossible Without Standards?*, St. Petersburg, 2014, pp. 15-21.

[Na08] I. Naumann et.al., „Security Issues in the Context of Authentication Using Mobile Devices (Mobile eID), ENISA Position Paper 2008-12-1," European Network and Information Security Agency (ENISA), 2008.

[Et14] ETSI, „Rationalised Framework of Standards for Advanced Electronic Signatures in Mobile Environment, ETSI Technical Report SR 019 020 v0.0.5f," 2014.

[Mo15] Mobile-ID, „Mobile-ID," [Online]. Available: http://mobile.id.ee/ . [Access 19 06 2015].