One mobile ID to secure physical and digital Identity

Oliver Terbu[1], Stefan Vogl[1] and Sebastian Zehetbauer[1]

Abstract: In this paper a mobile ID solution called My Identity App (MIA) is shown that combines traditional printed ID documents and electronic identities (eID) into a platform independent smartphone app embedded in an ID ecosystem. MIA aims for transparent identification and authentication in the physical and digital world while security, privacy, data protection, usability and user trust are at equilibrium. Security is built upon secure processes rather than hardware like secure elements, thus providing the fundament for broad adoption including technically challenged people. Scaleable architecture, standard future-proven technologies like OpenID Connect and FIDO authentication build the framework for secure, failsafe and large deployments.

Keywords: mobile ID, mobile eID, mobile verification, mobile identification, mobile documents, privacy-by-design, eIDAS

1 Introduction

Physical identification on documents and electronic IDs are widely used but there is no coherent solution available for integrating both identification modalities within one system. Governmental and private sector processes would heavily benefit from an electronic identity solution that offers easy access to ID documents and electronic IDs.

In 2014, the EU passed the new eIDAS regulation to allow interoperable and harmonized cross-border exchange of electronic identities between EU member states [Eu14]. From a technial point of view and according to the architectural specification electronic identities are conveyed using identity federation between „eIDAS-Nodes“. In this manner, an „eIDAS-Service“ providing cross-border authentication is either implemented as „eIDAS-Proxy-Service“ or „eIDAS-Middleware-Service“. [eI16]

The future General Data Protection Regulation (GDPR) of the European Union will facilitate the right of protection of personal data [Ag16]. As a consequence, privacy-by-design (PbD) will gain more and more attention and become an inherent and mandatory pillar in software engineering. In essence, PbD implies addressing privacy and data protection during the entire software development life cycle [Co16]. For this reason it is crucial in the course of implementing an eIDAS-compliant identity provider respectively „eIDAS-Service“ to follow a suitable software development process. [Te16] demonstrated an approach to facilitate both, security- and privacy-by-design by means of

[1] Österreichische Staatsdruckerei, e-government innovations, Tenschertstraße 7, 1239 Vienna, Austria, <lastname>@staatsdruckerei.at

the SCRUM framework.

Every new smartphone supports internet connectivity over mobile data networks. On the other hand, in Europe access to mobile networks is possible in almost every area, especially in urban regions where physical identification is needed. Smartphones typically obstruct Secure Elements (SE) or smart cards in various form factors like pluggable SIM cards provided by Mobile Network Operators (MNO) or built in Nearfield Communication (NFC) with a distinct SE [SE16]. Similarly, a Trusted Execution Environment (TEE) constitutes a secure runtime environment executed in protected areas on the chip hosting only dedicated privileged and trusted applications [TR16]. However, read and write access to SE and TEE is commonly forbidden or restricted to a certain domain. Consequently, a hardware-based only approach is not suitable to implement a broadly available mobile ID on smartphones.

In this paper a mobile ID solution that can be used with any internet-enabled smartphone is described which provides identities for physical and electronic identification in governmental and private sectors while ensuring compatibility with future-proof technologies and accordance to statutory regulations.

2 Related Work

2.1 Biometrics Authentication on mobile Devices

A market analysis on smart devices carried out by Acuity (a well-established market intelligence company) [Ac16] claims that by 2020, 100% of all mobile devices will have embedded biometrics. In 2016, this statement already applies to every fourth device in the field [Th15]. Finger print-, face-, hand geometry-, iris-, voice-, signature- and keystroke recognition are already utilized on smart devices for authentication [Da14]. Because there are many different ways of proving biometrics, a standard way of integrating authentication into a system is needed. Fast Identity Online (FIDO) is doing this by specifying the Universal Authentication Factor (UAF), an online client/server system that abstracts an authenticator relying on a challenge/response protocol [FI16]. Systems only have to integrate the abstract authenticator rather than implementing every authentication mechanism individually which dramatically reduces development effort and fosters compatibility.

2.2 Identity Federation

Identity federation protocols define a flow of proving a user’s identity at an identity provider on behalf of a service provider (i.e. relying party) and convey identities (i.e. attributes) between these trusted parties. It is up to the identity provider how the actual authentication is performed. Interoperatibility is key in order to receive broad adoption of mobile ID solutions. For this reason, it is important to leverage existing standard well-established identity federation protocols like OASIS Security Markup Language (SAML) [As16], WS-Federation [Un16] and OpenID Connect (OIDC) [Op16] which was built on top of OAuth [Th16]. However, eIDAS which incorporates the architecture [ST16a] of Secure idenTity acrOss boRders linKed (STORK) 2.0 [ST16b], relies on SAML 2.0 to exchange cross-border identities [Le14].

In the course of the ABC4Trust project [AB16] revealing more attributes than strictly needed was identified as one of the major privacy issues with current identity providers [Ra15]. In 2015, the Kantara Initiative finished the first specification of the User-managed Access (UMA) protocol [Ha15]. It was designed to address privacy issues by giving the user a fine-grained and unified control point to manage access to their data requested by service providers no matter where data is living on the internet. UMA is based on OAuth and is an authorization procotol complementary to OIDC. [Ho16]

2.3 Mobile ID Solutions

The demand of governmental institutions and bussiness for mobile ID solutions providing reliable identities comes along the increasing digitalization of the physical world (e.g., e-participation, online shopping, e-banking) and rising distribution of smart devices (e.g., smartphones, watches) with a wide variety of capabilities (e.g., biometrics, connectivity). We can doubtlessly assume, that this demand will also raise in the future.

In Europe, especially in Austria and Estonia, user conversion rates of governenmental mobile ID solutions are on the rise if citizens have access to a dedicated ecosystem as a study on mobile ID solutions shows in [Ku15]. According to [Ku15] only a small number of European member states have implemented mobile eIDs so far and there is a need for secure, interoperable solutions that make use of the full range of authentication possibilities provided by networked mobile devices.

The Austrian („Handy-Signatur“ [Ha16]) as well as the Estonian mobile eID („Mobiil-ID“ [Wh16]) can already be used for online authentication for electronic services (e.g., e-government, e-banking). While the Austrian model does not require any additional hardware and can be used on any mobile phone, the Estonian mobile eID relies on a special SIM card [EM16]. United Kingdom follows a different approach by introducing GOV.UK Verify [Gu16], a framework for IDs on how to certify companies of the private sector and use their IDs for governmental services.

Nevertheless, current proven implementations do not offer a comprehensive solution for the physical and digital world which are limited to eID and/or eSignature (e.g., no representation of printed ID documents) or requiring special hardware (e.g., Estonia).

In recent days, many blockchain-based ID solutions appeared like WorldCitizenship [Wo16], OneName [On16], and most promising ShoCard which aims to be used as a travelling ID [Tr16]. They all use a decentralized approach by managing IDs on a hash chain. A downside is that if the smart phone gets lost, there is no way for recovering one person's identity. Furthermore, potentially unqualified persons can create entries on the blockchain which leads to less trust in provided identities. On the other hand, no central node is needed to perform authentication between two parties.

Other interesting ID solutions exist, running on mobile phones like a prototype of the future British driver's license [Ne16], ID solutions presented by T-Systems [Mo16], and HID [HI16]. [Ne16] claims that the British driver's license is based on Apple Wallet. T-Systems solution is a cloud-based system for applications in the digital (e.g., access to applications) and physical world (e.g., parcel shops). HID's solution main intend seems similar but with a focus on governmental IDs (e.g., driver's license).

3 My Identity App – A smartphone-based mobile ID

My Identity App (MIA) refers to an entire physical and digital identity ecosystem and was built for countries with a need for a highly secure and efficient governmental ID as well as for business (e.g., banking, insurances, gaming industry) demanding easy to use identification (during registration), authentication (during system logon) and authorization of transactions. In contrast to traditional mobile ID or more generally eID solutions, MIA also provides a digital representation of ID documents (e.g., driver's license) in person-to-person scenarios (e.g., police roadside check). MIA follows a centralized approach, i.e. identities and credentials are retrieved from a central node. This decision was made to foster user acceptance. Decentralized approaches lack of user self-service or recovery in case the user lost his mobile phone or credentials.

During the implementation of MIA, a modified version of the SCRUM approach described in [Te16] was followed. Privacy and security representatives and corresponding teams accompanied the project from the beginning. Additionally, to facilitate user acceptance usability engineers helped by consulting and performing usability tests (e.g., thinking-aloud tests) in order to maximize usability.

The ecosystem consists of the following high-level components:

- ID.platform: Web service acting as a proxy for the MIA.backend to access already available data sources with personal data.
- MIA.backend: Collection of web services and applications retrieving and providing information to MIA.app and service providers (i.e. relying parties).
- MIA.app: Collection of standalone smartphone apps or standard development kits (SDK) to be integrated into existing apps, used to claim or prove identities, documents or commit transactions.

3.1 Security and Privacy by Process

MIA relies on security and privacy by process rather than by hardware while preserving high security, thus enabling high adoption rates by technically challenged people, creating a widely accepted and frequently used ID system. Nevertheless, hardware security is used whenever possible but is not necessarily required in order to ensure privacy and data protection (e.g., access to keychain, FIDO).

The following steps apply to application scenarios described in section 3.2 and explain in detail how identification, authentication and authorization is designed using MIA. First, a verifier wants to prove personally identifiable information of a person (claimant). The verifier might be either a physical person also using MIA.app or a service provider (e.g., online banking web application).

Second, the claimant starts MIA.app and requests a time-limited one-time token from MIA.backend. This token represents the claimant's identity valid for a small time frame (e.g., 30 seconds) and can only be used once. MIA.app displays the token as a QR or barcode and as a short string (e.g., length of six characters).

Then, the token is conveyed to the verifier. In the case of MIA.app, the token could be either scanned via the camera using the verifier's MIA.app, automatically transmitted by available transmission technologies (e.g., NFC), or manually entered by typing the string representation inside the verifier's MIA.app. If the verifier is a service provider, the claimant has to enter the string representation in either case, for instance in a dedicated web form.

After receiving the token, the verifier's MIA.app or the service provider sends a request to the MIA.backend asking for requested claims. Claims include entire ID documents (e.g., vehicle registration), single (e.g., lastname) attributes or sets of attributes (e.g., profile), assertions (e.g., age over 18) or transactions (e.g., details of a bank transfer). Requests made by verifiers using MIA.app always include the picture of the claimant because in person-to-person scenarios, the final verification of the claimant is carried out by comparing the picture with the actual appearance of the claimant. At this point, the claimant did not hand out any identity related data nor had to care about what data is actually requested in order to facilitate acceptance and simplicity.

MIA.backend receives the request and verfies the verifier and the verifier's permissions to file the requested claims. Verifiers can have different privileges (e.g., banks, governmental authories). If the request is legitimate, MIA.backend forwards the request to the claimant's MIA.app in order to approve it. All necessary information about the request is shown to the claimant (verifier's identity, requested attributes or information about the transaction) to make a precise decision. Service providers cannot perform a final picture verification. For this purpose, biometrics (e.g., fingerprint) is used as an extra anchor to confirm the authenticity of the claimant in an additional next step. On devices without native FIDO support, FIDO could be deactivated and a password is used instead. If the claimant denies the request, no personal data will be transmitted to the verifier. Otherwise, MIA.backend queries the ID.platform to answer the original request and delivers the requested data. No further steps are needed in the case of service providers because no final identity verification is needed.

After all the results of the request are shown in the verifiers's MIA.app for final picture verification. The data was transmitted from the MIA.backend and no data was transfered between the two devices. Additional technology can be used as an extra privacy enhancing measure in order to reduce misuse of the claimants's picture by unauthorized persons.

From the perspective of the claimant, the entire process is perceived as three simple steps. First, starting MIA.app, then linking his identity to another person or system by transmitting a one-time token. Finally, approving or denying the data request after verifying verifier and requested claims. Fig. 1: General person-to-person workflow visualizes the described steps.

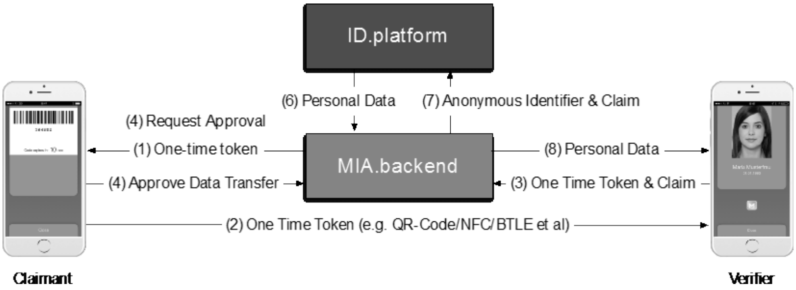
ID.platform
(6) Personal Data
(7) Anonymous Identifier & Claim
(4) Request Approval
(1) One-time token
MIA.backend
(8) Personal Data
(4) Approve Data Transfer
(3) One Time Token & Claim
(2) One Time Token (e.g. QR-Code/NFC/BTLE et al)
Claimant
Verifier

Fig. 1: General person-to-person workflow

3.2 Major Application Scenarios

Initially, users have to apply for MIA at public authorities that verify the user's personally identifiable information and receive a QR-code containing a one-time registration code. In the future, a video identification approach could be utilized additionally. The user starts MIA.app, scans the code to complete the registration process. In this course, ID.platform creates an identifier coupled with the user's identity. The identifier is known by MIA.backend and used to query encrypted personal data from ID.platform.

Governmental organisations and business would benefit from MIA in numerous use cases. In the course of person-to-person identification both parties have eye contact and can perform the final picture verification.

Under certain conditions, it is necessary to prove the identity between private persons. For example, in the event of buying a car in order to eliminate legal risks. This is a standard use case that MIA replicates. Both parties, seller and buyer have to run

MIA.app and execute the general person-to-person workflow.

In many countries, it is obligatory to bring the vehicle registration when driving a car. If a car was shared on a regular basis even for a limited period of time, an additional document would be necessary but often it is not desired to share the car permanently. MIA can circumvent this issue by providing means of sharing documents with other identities and revoking the shared document when it is no longer needed. Document sharing is similar to the general steps described in section 3.1. An additional claim is used to model the document sharing. A user can always ignore the sharing functionality for privacy reasons.

The police roadside check was identified as one of the major cases. For this purpose, a dedicated MIA.app (i.e. Mobile Police Workplace app) was implemented that is exclusively used by the police. The app establishes a particular level of trust with MIA.backend based on client certificates in order to gain access to exclusive interfaces. In contrast to Fig. 1: General person-to-person workflow, the police exchanges the one-time with personal data without explicit approval by the claimant. However, who received the information, when and what purpose the transaction had can always be checked through the timeline feature (i.e. history) in MIA.app. In rare situations, when no internet connection is available, MIA.app implicitly transmits a dedicated offline token. However, the user will have to perform the normal steps and will not notice any difference to the online scenario. Offline tokens can be used several times, have a different length than online tokens countering brute-force attacks and are updated on a regular basis when connectivity of MIA.app is restored. In regards to privacy, the user can always refuse to handout a one-time token as in scenarios not using any mobile ID. Depending on the present legislation, MIA can be configured to allow user consent also for this use case.

Privacy is faciliated by exposing a fine-grained set of claims or assertions rather than an entire document. For example, depending on the youth protection regulations of a country, buying alcohol in a supermarket or entering a club demands a minimum age. MIA.SDK can be integrated into the supermarket checkout terminal system, or a dedicated age verification app for security companies respectivley bouncers in order to check if a person is above a certain age (e.g., 18) rather than disclosing the true age or all attributes inside a printed document.

MIA provides a dedicated identity verification website to allow business or local authorities to prove someone's identity without necessarly using MIA.app themselves (e.g., at the reception of a hotel proving identities of hotel guests). This is useful in cases where the verifier has not enrolled MIA. The claimant enters the one-time token displayed in his MIA.app in the designated text field on the website, continues with the already familiar steps and then, the verifier verifies the picture displayed on the website.

Sometimes it is required to prove the identity against a service provider. In this case, no final picture verification would be possible as the verifier is a remote IT system. MIA speeds up the online registration, login and transaction processes at a service provider (e.g., opening a bank account, online banking login and bank transfers) dramatically. Especially service providers relying on vital and authentic information about the user (e.g., bank, insurance company) will benefit from MIA. Initial identification requires access to a certain set of attributes, whereas authentication during login only requires a unique anonymous and service provider specific identifier representing the claimant. MIA implements all three processes in a unified way by following the same steps.

3.3 Architectural Considerations and Integration Aspects

Technically, the entire system is based on REST micro services targeting large-scale, failsafe and secure deployments. All network traffic is secured by Transport Layer Security (TLS). Additionally certain privileged endpoints (e.g., exchanging offline tokens for personal data) are only reachable by providing a suitable client certificate.

Fig. 2: Simplified architectural overview gives an high-level overview of how components are interacting in the MIA ecosystem. A relying party can be any application (e.g., service provider) that is able to securely store a secret and implements the authorization code grant type of OpenID Connect respectively OAuth. After registration and receiving a client API key, third-party applications may integrate the MIA.SDK to utilize the public JSON based REST API, or provide their own implementation to call the API. MIA also acts as an „eIDAS-Proxy-Service" by exposing endpoints implementing the eIDAS SAML profile to allow communication between „eIDAS-Connectors" and MIA. MIA.backend acts as a trust anchor for verifier and claimant.

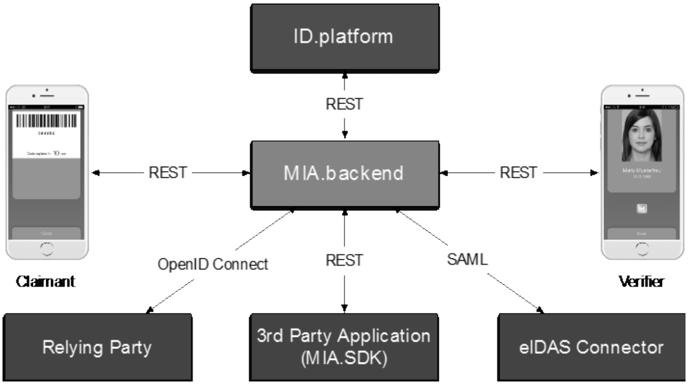

Fig. 2: Simplified architectural overview

Currently, OpenID Connect does not provide means of signing transactions. For this purpose, MIA introduces a lightweight profile of the OpenID Connect specification. The profile enables service providers to retrieve the public key of the claimant and convey the encrypted transaction text which can be decrypted and signed with the claimant's MIA.app.

eIDAS specifies three assurance levels on the identity of a person. However, MIA assumes that every user ran through the same registration process. Depending on the enclosing framework, all MIA identities will receive the same level of assurance (LOA). This approach fosters user acceptance by counteracting frustration caused by refusing a service unless elevating authentication to a higher LOA.

Before MIA can be rolled out to serve as a comprehensive ID solution, a set of well-defined ID.platform interfaces need to be implemented. In the case of a country operating central user repositories (e.g., identity register), the implementation will query these repositories and transform the data to the required format. End-to-end encryption between ID.platform and the claimant optionally guarantees privacy of personal data, hence inhibiting misuse of sensitive data. No personal data is stored in the MIA.backend. Furthermore, no personal data is exchanged between MIA.app instances or MIA.app and service providers. Instead verifiers always retrieve personal data through MIA.backend. Consequently, due to the logical and possibly organizational separation between ID.platform and MIA.backend privacy issues regarding traditional identity providers are addressed.

3.4 Differentiation from other ID Solutions

Compared to traditional printed ID documents (e.g., driver's license) and mobile ID solutions, an ID solution including an online smartphone app offers a broader spectrum of potential features. MIA implements or supports the following functionality in addition:

- Instant availability of changed data sets by retrieving current information from ID.platform every time the user has to prove his identity.
- Software updates are made easy by downloading the most recent version of MIA.app from app stores (e.g., when adding new attributes to existing documents).
- Revocation of ID documents in the case of loss or theft via user self-service through a user portal respectively web application.
- Enrolling multiple devices representing the same ID and documents per user.
- Sharing of ID documents with other users for a selectable period of time.
- Verification can be done on entire ID documents, specific attributes, sets of attributes, assertions or transactions which is more accurate and privacy-friendly as personal data exposure is reduced to a minimum.
- All relevant information is presented to the claimant before authorizing a transaction (e.g., in the case of an online bank transfer).
- Exhaustive usability testing resulted in an easy and intuitive user interface.

- No specific hardware requirements like NFC or a smartcard reader are required due to rely on security by process and offering multiple communication channels to transmit the one-time token (e.g., QR codes, Bluetooth, NFC, manually typing via the smartphone's virtual keyboard).
- No PIN code or password is required in all scenarios by leveraging biometrics through FIDO.
- Document related data is only transmitted to the verifier after showing the claimant's identity and explicit approval by the claimant. Hence, the claimant has full control of released data.
- A timeline (i.e. history) stores user interactions in all scenarios enabling traceability.
- The verifier can export requested data to XML or JSON as long as data remains visible in MIA.app. Regarding privacy, this can be compared to create a copy of a traditional ID document.

Due to a lack of comprehensive public information, a comparison with other ID solutions mentioned in section 2.3 was not conducted.

4 Summary and Conclusion

MIA is fully functional and can be introduced in any country. Requiring a standard smartphone with no special hardware (e.g., NFC) also makes the system broadly adoptable. A dedicated process guarantees the trustworthiness of the identity rather than relying on security (e.g., SE, TEE) established by hardware which is the anchor of traditional mobile ID solutions.

MIA was presented at the CeBIT 2016 and received very promising feedback by the MAPPING (Managing Alternatives for Privacy, Property and Internet Governance) award jury and made the second place in the category „Privacy via IT Security App“ [Wi16]. Furthermore, MIA was developed using a user-centric, privacy- and security-by-design approach to ensure usability and acceptance while upholding a very high degree of security. Hence, we are confident that MIA can serve as an ideal mobile ID respectively identification and verification solution for various countries. MIA is also eIDAS ready.

As a further step, we will investigate how UMA can be integrated and if mutual authentication between claimant and verifier by comparing security codes can additionally increase privacy while preserving user acceptance.

Acknowledgements

The authors would like to thank Österreichische Staatsdruckerei (GmbH) for promoting innovations in the field of e-government and thank the development, security and privacy teams for all efforts being made in the course of MIA.

References

[Eu14] European Union: 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. Official Journal of the European Union/L 257, Pg. 73-114, 2014.

[Ag16] Agreement on Commission's EU data protection reform will boost Digital Single Market, http://bit.ly/1J9ZUdt, Stand: 17.08.2016.

[eI16] eIDAS – Interoperability Architecture, http://bit.ly/2by1IFd, Stand: 17.08.2016.

[Co16] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe, http://bit.ly/2bxtmkS, Stand: 17.08.2016.

[Te16] Terbu, O. et. al.: Privacy and security by Design im agilen Softwareprozess. In (Schweighofer, E. et. al.): Proceedings of the 19th International Legal Informatics Symposium IRIS 2016, Österreichische Computergesellschaft (OCG), Pg. XXX, 2016.

[SE16] SECURE ELEMENTS AM BEISPIEL GOOGLE WALLET, http://bit.ly/2aYb7r6, Stand: 04.08.2016.

[TR16] TRUSTED EXECUTION ENVIRONMENT, MILLIONS OF USERS HAVE ONE, DO YOU HAVE YOURS?, http://bit.ly/2aK6fmm, Stand: 16.04.2016.

[Da14] Darwaisha, S. F. et. al.: Biometric identification on android smartphones. In (Jędrzejowicz, P. et. al.): Proceedings of Knowledge-Based and Intelligent Information & Engineering Systems 18th Annual Conference. Pages 832-841, 2014.

[As16] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, http://bit.ly/1N3pLZs, Stand: 17.08.2016.

[Un16] Understanding WS-Federation, http://bit.ly/2b0JImn, Stand: 16.04.2016.

[Op16] OpenID Connect Core 1.0 incorporating errata set 1, http://bit.ly/2b48WzP, Stand: 16.08.2016.

[Th16] The OAuth 2.0 Authorization Framework, Internet Engineering Task Force (IETF), 2012.

[ST16a] STORK as a foundation for the eIDAS e-ID architecture, http://bit.ly/2b86Cr7, Stand: 16.04.2016.

[ST16b] STORK 2.0, https://www.eid-stork2.eu, Stand: 16.04.2016.

[Le14] Leitold, H.; Lioy, A.; Ribeiro, C.: STORK 2.0: Breaking New Grounds on eID and Mandates. In (Mesago Messe Frankfurt GmbH): Proceedings of ID World International Congress. Pages 1-8, 2014.

[AB16] ABC4Trust, https://abc4trust.eu, Stand: 16.04.2016.

[Ra15] Rannenberg K.; Camenisch J.; Sabouri A.: Attribute-based Credentials for Trust. Identity in the Information Society, Springer, 2015.

[Ha15] Hardjono, T. et. al.: User-Managed Access (UMA) Profile of OAuth 2.0, Internet Engineering Task Force (IETF), 2015.

[Ho16] Home - WG - User Managed Access - Kantara Initiative, http://bit.ly/1h8beqZ, Stand: 16.04.2016.

[Ku15] Kubach M. et. al.: SSEDIC.2020 on Mobile eID. In Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, 2015.

[Gu16] Guidance GOV.UK Verify, http://bit.ly/1ASQBil, Stand: 03.08.2016.

[Ha16] Handy-Signatur - Your digital Identity, http://bit.ly/2aNPmJ3, Stand: 16.04.2016.

[Wh16] What is Mobiil-ID?, http://bit.ly/2aNPPuz, Stand: 16.04.2016.

[EM16] EMT, Elion Stores Issue New Mobile ID SIM Cards, http://bit.ly/2areFhd, Stand: 16.04.2016.

[Ne16] Never lose your ID again: DVLA reveals plans for iPhone driving licence, http://bit.ly/1YrtFPa, Stand: 03.08.2016.

[Mo16] Mobile Identity & Access Services, http://bit.ly/2b0KZK7, Stand: 03.08.2016.

[Wo16] World Citizenship Passports with Bitcoin-like Blockchain, http://bit.ly/2aK8JB6, Stand: 04.08.2016.

[On16] Onename, https://onename.com, Stand: 03.08.2016.

[Tr16] Travel Identity of the Future, http://bit.ly/2b884Kl, Stand: 03.08.2016.

[HI16] HID goID™ Mobile ID Solution, http://bit.ly/2aYKTG5, Stand: 16.04.2016.

[Ac16] Acuity Market Intelligence: The Definitive Source for Biometric Market Intelligence, http://www.acuity-mi.com, Stand: 16.04.2016.

[Th15] The Global Biometrics Mobility Report: The Convergence of Commerce and Privacy, Acuity Market Intelligence, 2015.

[FI16] FIDO UAF Protocol Specification v1.0, http://bit.ly/2aZ3egA, Stand: 17.08.2016.

[Wi16] Winners of the Privacy via IT Security App Competition, http://bit.ly/2aNRnol, Stand: 03.08.2016.