Towards a Decentralized Identity Management Ecosystem for Europe and Beyond

Bud P. Bruegger[1], Heiko Roßnagel[1]

Abstract:. The objective of the FutureID project was to build an identity management infrastructure for Europe in support of a single market of online services. This requires the availability and large-scale use of trusted and secure identities that replace current password credentials. In the FutureID concept the number and topology of intermediary components is not fixed and static. FutureID rather adopts an ecosystem-approach by creating a free market for identity intermediation services. This provides for the flexibility to: scale according to need, adapt to market needs, support special needs of market sectors including niche markets, adapt to established contractual relationships, and easily adapt to various possible business models that render the infrastructure sustainable. This paper summarizes the results from the 3 year EU-funded project.

Keywords: identity management, decentralized ecosystem, eID, intermediaries.

1 Introduction

Reliable authentication is one of the basic requirements of e-commerce and other transaction services on the web [SCH06]. So far, passwords have been the predominant authentication method. Passwords are easy to use and do not require expensive hardware or software on the client side [MAN07]. On the other hand, the use of passwords leads to several problems, such as inconvenient password management issues [REC06], password reuse [IVE04], and other security problems [NEU94]. Therefore, alternative forms of authentication are needed.

This requires the availability and large-scale use of trusted and secure identities that replace current password credentials, however. As usual in multi-sided markets the key success factor is to reach a critical mass of both, users and available services, solving the 'chicken and egg problem' [Cai03]: Users are only interested in taking up a credential, if it provides access to a critical mass of services; service providers are only willing to invest in a credential if they bring a large enough base of potential users to justify the investment.

The objective of the FutureID project was to build an identity management infrastructure for Europe in support of a single market of online services. This requires the availability

[1] Fraunhofer IAO, Identity Management, Nobelstr. 12, 70569 Stuttgart, {bud.bruegger, heiko.rossnagel}@iao.fraunhofer.de

and large-scale use of trusted and secure identities that replace current password credentials.

Today's landscape of secure credentials in Europe shows a very high diversity. Also, credentials that combine both security and convenience of use are possibly yet to come (for example, from the FIDO initiative [FID16]). In this situation, it is highly unlikely that a single credential or identity management technology reaches the required critical mass by itself. FutureID therefore attempts to find a solution that renders it easier to reach the required critical mass by providing interoperability between credentials and services.

The rest of this paper is structured as follows. Section 2 will give an overview of related work. Section 3 will outline the FutureID methodological approach and Section 4 will present the results of the project. Section 5 will give an outlook on future work, before we summarize our findings.

2 Related Work

Other projects have focused on the challenge of very large-scale identity management. In Europe, most notably, this includes the STORK project [STO16] that was funded in two phases by the European Commission (EC) as a large scale pilot project for a total of six years. STORK1 predated FutureID and was much larger, both, in terms of funding and size of the consortium. It focuses primarily on public sector services and the interoperable authentication with officially "notified" government eIDs. STORK is often seen as a partial implementation of the European eIDAS regulation [eIDAS] (see section 4).

There are several important differences between STORK and FutureID. FutureID has a considerably wider focus: beyond government eIDs, it is extensible to support all possible current and future credentials, including non-notified eIDs in sectors such as health care, justice and law enforcement, existing private sector credentials (like BankIDs and corporate IDs) with a considerable installed base, evolving mobile credentials e.g. from FIDO, and privacy-enhanced "Attribute Based Credential" (ABC) such as those from ABC4Trust [ABC16] or IRMA [IRM16]. The project demonstrated the ease of supporting different ID technologies with a representative subset of the mentioned cards [Fut15], including both mentioned ABCs. Another major difference lies in the conception of the identity management infrastructure. STORK is implemented by a government-operated node (a so called "Pan European Proxy Service") in each Member State. The resulting static topology only needs modification when new member states join or leave the union. The STORK identity management infrastructure supports a single perception of trust that is shared among all participating services. In contrast, FutureID avoids any central components including the need for central registration or approval. Its infrastructure is completely decentralized and supports a variable topology that auto-configures itself when new nodes join or leave the infrastructure (see section

4.1). This can support an open market place for identity and intermediation services that cater to the needs of the private sector (see section 4.3).

In the United States, much of the work on very large-scale identity management was related to the National Strategy for Trusted Identities in Cyberspace [NSTIC16]. A major difference in the focus compared to FutureID is the lack of existing eIDs in the United States. NSTIC therefore puts emphasis on the creation of electronic identities by private sector players. The universal use of these identities at larger scales was experimented typically with architectures that foresee a single hub. The scale of the identity management infrastructures that were experimented in various pilots was typically restricted to a limited number of credentials and a single business branch. In contrast STORK and FutureID address authentication of all European citizens toward any potential online service,

3 Approach

FutureID ran for three years and was partially funded as a large scale integrating project with a total budget of 14,517,219 under the EC's Seventh Framework Programme (FP7). The FutureID Consortium consisted of 19 partners from 11 countries. It combined the multi-disciplinary and complementary competence of large industry, small and medium enterprises, top research organizations and universities, a data protection agency, and a non-profit association. FutureID has implemented an ambitious methodology of collecting inter-disciplinary requirements and evaluate them in multiple feedback loops following the approach of design science [Sel15]. FutureID has collected a very large number of partly conflicting requirements in seven disciplines: Privacy, Usability, Security, Technical, Socio-Economic, Accessibility, and Legal. Extensive work has gone into defining priorities for requirements, defining the project artifacts that they affect, the detection, discussion and possible resolution of requirements from different disciplines that conflict with each other [Sel15]. An additional requirements overview deliverable that was not foreseen in the initial project plan was created to document this extensive analytical work [Sel15]. A specific instance of a MediaWiki was set up to manage the requirements beyond just a text in a deliverable and to efficiently support the multiple phases of evaluation.

Three major artefacts have been evaluated in FutureID: the reference architecture, the implementation, and the pilot applications. Wherever possible, feedback loops were created where the evaluation identified certain shortcomings that were fixed in an improved version of the artefact that was then again evaluated. In the case of the reference architecture, several rounds of the evolutionary loops were necessary to yield the present architecture that satisfies all major requirements. This work also underlines the interdisciplinary and participatory character of such an evaluation and improvement loop—no single person/expert can cover all the disciplines necessary to successfully design such a complex artefact. The separate evaluation of architecture, implementation,

and pilots also illustrates how different aspects of a project are verified with different artefacts. For example, an architecture must enable a wide range of possible uses, deployment scenarios, and configurations of which only a small part can be actually implemented and demonstrated within the limits of a project. Pilot applications are very concrete on the other hand. Here, it is clear, for example, which stakeholders with which legal characteristics actually operate given software components. Only now, certain legal requirements can be evaluated. Thanks to this approach, FutureID managed to satisfy all major requirements from all disciplines and there were very strong reasons (e.g., a tradeoff between conflicting requirements from different disciplines) for the few cases where a requirement was not satisfied.

4 Results

4.1 The FutureID Architecture

A main result of FutureID is its architecture of intermediation between existing credentials on one side and existing services on the other [Fut16]. Intermediation, within the constraints of trust, matches any credential to any service. With intermediation, each user credential can thus access a much larger number of services than without intermediation; and a service can reach out to a very large base of potential users through a single interface. This addresses the key success factor of reaching a critical mass.

This is illustrated in Figure 1. An infrastructure consisting of a multitude of intermediation services that operate in a free market provides interoperability, potentially privacy enhancement, and a common user experience between a multitude of credential technologies on the left side and arbitrary services on the right. The interoperability addresses both, credential technologies and federation technologies. An example for privacy enhancement are intermediaries who can derive the attribute “off age” from a date of birth contained in the user’s credential. Handling the selection of the credential by a specific (local or server-based) user component instead of each service offering provides users with a consistent look and feel. This includes ways of providing user consent or to be informed about the personal information that is disclosed.

Intermediation is designed to be completely decentralized with an arbitrary number of intermediation services, either existing Identity Providers or FutureID Brokers, making up the potentially global intermediation infrastructure. Intermediation services can join or leave the infrastructure without need for central registration or approval. Instead, the infrastructure auto-configures itself: The specifically designed FutureID authentication request that is issued by service providers directly or indirectly specifies all trusted intermediaries (and credential issuers) using their network address. This can be seen as a decentralized discovery mechanism. As soon as an intermediary is trusted by a single service provider, it can take part of the infrastructure.

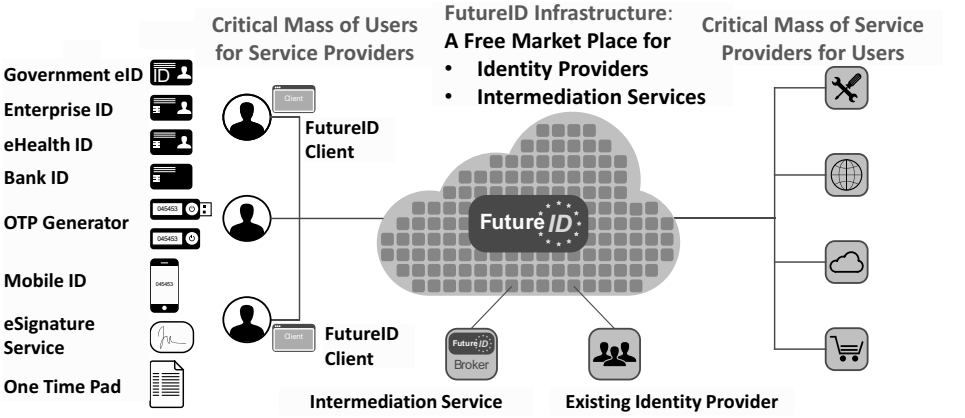

Figure 1: Intermediation to reach a critical mass of both users and services.

In most practical cases, there are multiple ways of accessing a service provider that involve different user credentials and different intermediaries. FutureID is also able to chain multiple intermediaries together for a single authentication, either since this is required to achieve interoperability or for improved overall privacy[2]. Which credential shall be used and which of the possible chains of intermediaries shall be used is in complete control of the user. For this purpose, a local or server-based user component receives the FutureID authentication request, analyzes it, and presents the user with options. User policies can automate most of this process and to require user interaction only in certain situations, e.g., if the exposed personal data lies beyond a given threshold. This is similar to Microsoft's identity selector [Cam07] but in addition to selecting the credential to use, it can also select chains of intermediaries and privacy enhancing transformations. In FutureID, the component that supports the user can be either client of server based.

This component representing the user's interests was added primarily for privacy reasons as part of the continuous evaluation of the architecture in a feedback loop. It implements a privacy-friendly information flow [Hor14]. Since this component wasn't foreseen in the budget, it was only implemented by Fraunhofer as a research prototype. Also, a recent master thesis has explored possibilities of applying more advanced user strategies in an easy to use fashion [Bar15]. For stable operational use in a corporate environment, where a single FutureID Broker instance is typical, the identity selector from the SkIDentity project [SkI14] was used.

[2] For example, an intermediary that is trusted by the user can reduce the personal attributes of the user or create a pseudominous identity, before this personal data is revealed to a less trusted service provider or intermediary. Also the implementation of a variation of the "identity federation do not track pattern" [Bjo14] is possible.

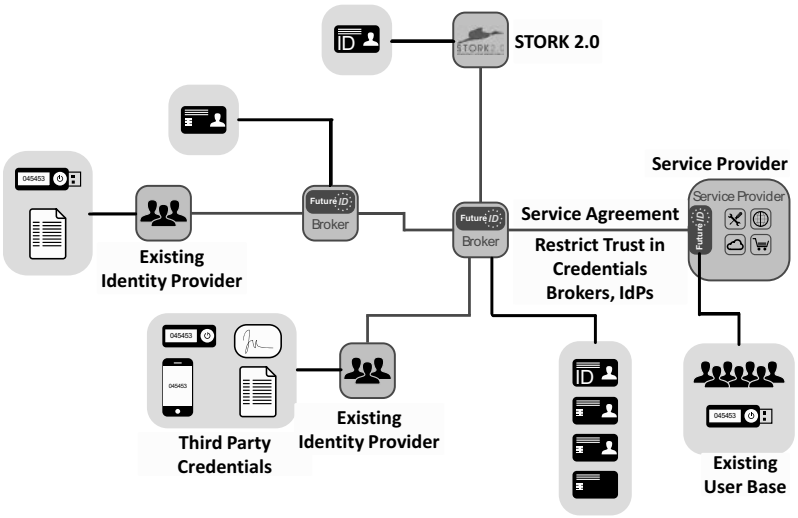

Figure 2: How a Service Provider reaches out to a massive potential user base.

Figure 2 illustrates the FutureID architecture from the perspective of a single service provider who wants to reach out to an as large as possible user base. On the right, it shows the possibility of integrating an installed user base with a locally issued credential via the FutureID "application integration service" component. Then, towards the left, it illustrates how a FutureID broker can make available additional credentials either directly, through existing identity provider of a supported federation technology or through an existing identity management infrastructure such as STORK for which an appropriate broker backend exists. The figure also shows how brokers can be chained to reach out to yet more credentials and thus potential user base for the service provider.

The support for seamlessly integrating direct authentication of locally issued credentials was motivated by the wish to support scenarios that require very high levels of either security[3] or privacy[4]. The integration of broker-based and local authentication was achieved through using the same session library in both the local authentication and the application integration service. The advantage of this approach is that the user has the same experience when using a credential locally or through a broker.

4.2 Scalability

The FutureID approach was specifically designed for very large-scale, potentially global, identity management. Massive scalability was supported through the following:

[3] Note that bearer assertions cannot usually reach the full potential of security [Bur13].
[4] Note that important privacy features of Attribute Based Credentials get lost when an intermediary is introduced.

Support for heterogeneous perceptions of trust: The larger the scale, the more difficult it is to agree among participants on who is considered trustworthy. Most approaches proposed before FutureID mandate that all participants share a single perception of trust. This is very evident in the classical "circles of trust" as implemented by various federation technologies. Also, the eIDAS regulation creates the possibly largest space of homogeneous trust perception by applying the same legislation across all of Europe. Scaling beyond Europe will necessarily render a homogeneous trust perception impossible. A similar effect has support for the private sector where eIDAS is voluntary and trust is closely linked with business risk that varies with business branch and country. A large-scale identity management infrastructure that mandates all participants to share a single perception of trust is therefore incapable of scaling beyond the boundaries of Europe or support the private sector. FutureID therefore accommodates multiple perceptions of trust in the same identity management infrastructure by using Trust Scheme Publication Authorities [Bru151] that a perception of trust and are decoupled from the intermediation services (FutureID "Brokers"). Every service provider can then determine its individual trust policy while still sharing the same intermediation infrastructure.

Support for chains of intermediaries: Intermediation services need intimate knowledge of the issuers of user and/or session credentials[5] they can consume on their input side. They also need to support the necessary technology to consume these credentials. With increasing scale, it becomes ever less likely, that a single intermediary has familiarity of all possible issuers and supports all relevant technologies. For this reason, FutureID supports chaining of intermediation services, for example in support of the subsidiarity principle where intermediaries need to know only issuers close to them.

Design as an open, extensible system: Arbitrary existing or future credential technologies can be supported, as long as there is at least one intermediary who supports it. This renders the architecture future-proof by facilitates the integrations of new technologies such as, FIDO devices. Possibly even more importantly is the organizational approach where new initiatives such as FIDO can add momentum to FutureID much rather than competing with the FutureID infrastructure. In analogy to new credential technologies, new federation technologies and protocols can be integrated simply by providing a new "adaptor" in the intermediation service. By defining the FutureID infrastructure detached from current technologies and making it extensible, the approach promises to continuously augment momentum in order to overcome the significant hurdle of critical mass present in the roll-out of very large-scale identity management solutions.

4.3 Support for a Free Marketplace of Intermediation Services

While other projects and initiatives use the pattern of intermediation for similar

[5] For example, SAML assertions

purposes, what is unique about FutureID is that instead of a single central intermediary or a fixed topology of intermediaries (e.g., one per Member State) intermediation is achieved by an open number of stakeholders who offer intermediation services. This creates a competitive market for intermediation services with the typical benefits: **(i)** Suitability to reach into the private-sector through the use of common offerings (with SLA etc.), reuse of existing well-established and trusted stakeholders without the need to establish new business relations, establish new trust relationships, and negotiate new service contracts possibly with different parameters and business practices. **(ii)** Long term sustainability of the infrastructure since it is controlled by market forces, produces revenue for intermediation providers, and can rapidly react to developments of demand and technologies. **(iii)** Efficiency and innovation through competition that is built into the intermediation concept of FutureID. Multiple vendors of services and software products foreseen by the FutureID approach foster competitive pricing as well as advances through innovation.

4.4 Other Contributions

An impediment to the take up of STORK in the private sector is that stakeholders (such as banks) who need high levels of security typically have already a rolled out base of users with a secure token/credential issued by the stakeholder itself. A seamless integration of these existing users and avoidance of interrupting services is a prime requirement in any evolution of identity management for these stakeholders. Such integration is outside the STORK's scope and leaves this burden to its potential users. The uncertainty and cost of this integration represents a major impediment to uptake. FutureID provides a solution here since it can easily integrate both, the existing credentials and STORK behind a single interface. FutureID has also developed a complete suite in support of eIDAS-compliant electronic signature, including (i) a validation authority for qualified signatures based on trust lists, (ii) signature creation and validation in the FutureID Client, (iii) support for server-based signatures, as well as (iv) a demonstration how to increase security through the use of trusted computing--all complient with the OASIS DSS standard.

FutureID has further developed a universal open source eID client that can be used as a multi-card eID middleware that offers complex authentication functions as required by the German nPA and for signatures. Already, a wide variety of eIDs and other smart cards are supported [Fut15]. Additional smart cards are easy to support through simply providing declarative and standards-compliant CardInfo files. Tools to support creation of such files are available. An add-on framework renders it possible to easily extend the functionality of the FutureID client, e.g., with additional protocols. The client exists both, as PC and mobile version and is easy to install through Java Web Start. Demonstrating its extensibility, the FutureID client has been used to secure authentication of patients and healthcare professionals in the epSOS e-health platform, as well as providing the first legal compliant, signature-based mechanism for patient consent. The FutureID client has been accepted by the eSENS large scale pilot as

integral, officially supported part. To our knowledge, FutureID is the only FP7 project with contributions accepted by eSENS.

The STORK 2.0 CIP-PSP project has officially collaborated with FutureID by providing access to its pre-production infrastructure for cross-border authentication through the official Spanish PEPS (Pan European Proxy Service). It has further provided several test credentials. STORK is fully integrated in FutureID through a specific Broker-backend. This has successfully been demonstrated in the FutureID e-Learning pilot.

Partly to demonstrate the easy of integrating arbitrary credential technologies, FutureID has made a specific effort to integrate so called privacyABCs, i.e., Attribute Based Credential technology that uses advanced cryptography and zero knowledge proofs to put users in control of the personal data they disclose. In particular, FutureID has integrated technology originating from the FP7 project ABC4Trust [ABC16] and that of IRMA Cards [IRM16]. ABC4Trust provides a consistent interface above both, IBM's Idemix technology [IBM16] and Microsoft's U-Prove [Mic12]. To fully integrate privacyABCs the FutureID architecture supports direct presentation of credentials without the need for intermediaries. FutureID has further built support for migration to privacyABC technology and for fostering a critical mass of services for owners of privacyABC credentials by deriving privacyABC credentials from existing government eIDs. This addresses the issue that currently ABC issuers lack high-quality enrolment. FutureID also makes it possible to authenticate to an intermediate FutureID Broker in order to reach services without support for ABCs.

FutureID has made a specific effort to support mobile computing. This includes an Android version of the FutureID client, support for contactless smartcards via NFC, the possibility to use secure elements of mobile devices, and the integration with the Android Security Modules (ASM) framework.

FutureID has also developed tools and methodologies of general interest that will be available beyond the duration of the project. Among them is a terminology for eIDs that was collaboratively authored using a semantic wiki [Med16]. Significant previous and related terminologies have been parsed and loaded in the wiki in order to aid the definition of the FutureID terms without reinventing the wheel. The pre-existing terminologies have also been analyzed to understand the degree of consent on the choice of terms. Web-based tools based on a natural language processing library were developed for use by project partners. The most used is a glossary tool that analysis a deliverable and creates a custom glossary of the terms that were used and defined in the FutureID Terminology Wiki.

FutureID has made a major effort to test all its software components and bring them to a high level of quality and maturity. For this purpose, both, server and client components were continuously tested in an innovative and automated open source test infrastructure that was developed by FutureID based on open source components such as Jenkins, Robot Framework, SoapUI, TestNG, sikuli script, and MediaWiki. The resulting FutureID test infrastructure was also consolidated in a standalone product available for

other projects and is available as a virtual machine for ease of deployment in other contexts.

5 Future Work

The work on FutureID is continuing well beyond the duration of the funded project. There are already several follow-up research projects that exploit and further the results of FutureID, including the nationally funded Fraunhofer Industrial Data Space Initiative [IDS16] and the Horizon 2020 LIGHT*est* project [Bru16] that will start in September 2016. The FutureID experience and reputation are also the basis for several current consulting projects for major industry players. The unique experience of FutureID in very large-scale identity management has also laid the basis for international interest and a first research collaboration with the U.S. National Institute of Standards and Technology [NIST16] (part of the U.S. Department of Commerce), who also operates National Strategy for Trusted Identities in Cyberspace [NSTIC16]. The major results of FutureID have been presented to senior NIST representatives at a specific meeting organized by Fraunhofer IAO in February 2016. As a result, Fraunhofer IAO is currently working with the National Cybersecurity Center of Excellence [NCCoE16] on a related issue[6] and is pursuing further collaboration on FutureID with NIST.

6 Conclusions

FutureID has developed an innovative concept of intermediation between existing credentials on one side and existing services on the other. This intermediation is the key to a successful rollout of both, credentials and services that require high levels of security. What is unique about FutureID, however, is that the number and topology of intermediary components is not fixed and static. FutureID rather adopts an ecosystem-approach by creating a free market for intermediating services. This provides for the flexibility to: scale according to need, adapt to market needs, support special needs of market sectors including niche markets, adapt to established contractual relationships, and easily adapt to various possible business models that render the infrastructure sustainable.

[6] Fraunhofer IAO is working with the NCCoE in the DNS-Based Secured Email Building Block to develop practical, interoperable cybersecurity approaches that address the real-world needs of complex Information Technology (IT) systems. By accelerating dissemination and use of these integrated tools and technologies for protecting IT assets, the NCCoE will enhance trust in U.S. IT communications, data, and storage systems; reduce risk for companies and individuals using IT systems; and encourage development of innovative, job-creating cybersecurity products and services. NIST does not evaluate commercial products under this Consortium and does not endorse any product or service used. Additional information on this Consortium can be found at: https://nccoe.nist.gov/projects/building_blocks/secured_email

7 References

[ABC16] *ABC4Trust Project*. https://abc4trust.eu/, last verified 6.6.2016.

[Bar15] Barta K. (2015): *Design und Evaluierung des FutureID Solvers*. (Masterarbeit) Stuttgart: Hochschule der Medien Stuttgart.

[Bjo14] Bjones R. (2014): *The Identity Federation Do Not Track Pattern*. http://www.beejones.net/the-identity-federation-do-not-track-pattern,

[Bru15] Bruegger B.P. (2015): The Globally Scalable FutureID Trust Infrastructure. In: *World e-ID and Cybersecurity*. Marseille.

[Bru16] Bruegger B.P. und Lipp P. (2016): LIGHTest -- A Lightweight Infrastructure for Global Heterogeneous Trust Management. In: *Open Identity Summit 2016*. Rome, Italy.

[Bur13] Burr W.E.; Dodson D.F.; Newton E.M. et al. (2013): *NIST Special Publication 800*. NIST. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf,

[Cai03] Caillaud und Jullien (2003): Chicken & Egg: Competition among Intermediation. *RAND Journal of Economics*, 34. S. 309–328.

[Cam07] Cameron K. und Jones M.B. (2007): Design Rationale behind the Identity Metasystem Architecture. In: Pohlmann N.; Reimer H. und Schneider W. (Hg.): *ISSE/SECURE 2007 Securing Electronic Business Processes*. Warsaw, Poland: vieweg. S. 117-129.

[eIDAS] EUROPEAN PARLIAMENT AND OF THE COUNCIL (2014): *electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*., DOI 2014/910/EU.

[FID16] *FIDO Alliance*. https://fidoalliance.org/, last verified 6.6.2016.

[Fut16] FutureID Consortium: *Deliverable D21.4*. http://futureid.eu/data/deliverables/ year1 /Public/FutureID_D21.04_WP21_v1.2_Reference%20Architecture.pdf,

[Fut14] FutureID Consortium (2014): D21.4. http://futureid.eu/data/deliverables/year1/Public/ FutureID_D21.04_WP21_v1.2_Reference%20Architecture.pdf,

[Fut15] FutureID Consortium (2015): D32.7. http://futureid.eu/data/deliverables/year3/Public/ FutureID_D32.07_WP32_v1.0_CardInfo_files_for_selected_cards.pdf,

[Fut16] *FutureID*. http://FutureID.eu, last verified 6.6.2016.

[Fut162] FutureID: *FutureID Deliverables*. http://futureid.eu/deliverables, last verified 2016.

[Hor14] Horsch ; Tuengerthal und Wich T. (2014): SAML Privacy-Enhancing Profile. In: *Open Identity Summit 2014*. Stuttgart.

[IBM16] IBM Research: *Identity Mixer*. http://www.research.ibm.com/labs/zurich/idemix/, last verified 2016.

[IDS16] *Fraunhofer Industrial Dataspace*. http://www.fraunhofer.de/de/forschung/fraunhofer-initiativen/industrial-data-space.html#, last verified 6.6.2016.

[IRM16] *IRMA Cards*. https://www.irmacard.org/, last verified 6.6.2016.

[IVE04] IVES B.; WALSH K.R. und SCHNEIDER H. (2004): The domino effect of password reuse. *Communications of the ACM*, 47 (4). S. 75–78.

[MAN07] MANNAN M. und VAN OORSCHOT P.C. (2007): Using a personal device to strengthen password authentication from an untrusted computer. In: DIETRICH S. und DHAMIJA R. (Hg.): *Proceedings of the 11th international Conference on Financial Cryptography and 1st international Conference on Usable Security*. Scarborough, Trinidad and Tobago: Springer. S. 88–103.

[Med16] MediaWiki: *MediaWiki*. https://www.mediawiki.org/wiki/MediaWiki, last verified 2016.

[Mic12] Microsoft Research (2012): *U-Prove*. https://www.microsoft.com/en-us/research/project/u-prove/,

[NCCoE16] *National Cybersecurity Center of Excellence*. https://nccoe.nist.gov/, last verified 6.5.2016.

[NEU94] NEUMANN P.G. (1994): Risks of passwords. *Communications of the ACM*, 37 (4). S. 126.

[NIST16] *National Institute of Standards and Technology*. http://nist.gov/, last verified 6.6.2016.

[NSTIC16] *National Strategy for Trusted Identities in Cyberspace*. http://www.nist.gov/nstic/, last verified 6.6.2016.

[Ope16] *OpenPEPPOL*. http://www.peppol.eu/, last verified 6.6.2016.

[REC06] RECORDON D. und REED D. (2006): OpenID 2.0: a platform for user-centric identity management. In: JUELS A. (Hg.): *Proceedings of the second ACM Workshop on Digital Identity Management*. Alexandria, VA.: ACM Press. S. 11–16.

[SCH06] SCHLÄGER C.; SOJER M.; MUSCHALL B. et al. (2006): Attribute-based authentication and authorisation infrastructures for e-commerce providers. In: BAUKNECHT K.; PRÖLL und WERTHNER (Hg.): *E-Commerce and Web Technologies*. Berlin, Heidelberg: Springer. S. 132–141.

[Sel15] Sellung R. und Roßnagel H. (2015): Evaluating Complex Identity Management Systems--The FutureID Approach. In: Hühnlein D. et al. (Hg.): *Open Idenity Summit 2015*. Berlin: GI-Edition, Lecture Notes in Informatics. S. 133-140.

[SkI14] SkIDentity Consortium: *SkIDentity*. https://www.skidentity.com/en/home, last verified 2014.

[STO16] STORK 2.0: *STORK 2.0*. https://www.eid-stork.eu/, last verified 6.6.2016.