FutureID – Shaping the Future of Electronic Identity

Heiko Roßnagel[1], Jan Camenisch[2], Lothar Fritsch[3], Thomas Gross[4], Detlef Houdeau[5], Detlef Hühnlein[6], Anja Lehmann[2], Jon Shamah[7]

[1]Fraunhofer Institute for Industrial Engineering IAO
heiko.Rossnagel@iao.fraunhofer.de

[2]Zurich Research Lab, IBM Research
{jca,anj}@zurich.ibm.com

[3]Norsk Regnesentral
lothar.fritsch@nr.no

[4]University of Newcastle
thomas.gross@newcastle.ac.uk

[5]Infineon Technologies AG
detlef.houdeau@infineon.com

[6]ecsec GmbH
detlef.Hühnlein@ecsec.de

[7]EEMA
jon.shamah@eema.org

Abstract. The FutureID project builds a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe, which 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 will provide great benefits to all stakeholders involved in the eID value chain. Users will benefit from the availability of a ubiquitously usable open source eID client that is capable of running on arbitrary desktop PCs, tablets and modern smart phones. FutureID will allow application and 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. This will enable service providers to offer this technology to users as an alternative to username/password based systems, providing them with a choice for a more trustworthy, usable and innovative technology. For existing and emerging trust service providers and card issuers, FutureID will provide an integrating framework, which eases using their authentication and signature related products across Europe and beyond. To demonstrate the applicability of the developed technologies and the feasibility of the overall approach FutureID will develop two pilot applications and is open for additional application services who want to use the innovative FutureID technology. This paper provides a short overview of the FutureID project.

Keywords. Identity Management, eID, Identity Broker, Open Source Client

1 Introduction

Identity management (IdM) has emerged as a promising technology to distribute identity information across security domains [1]. In e-business scenarios, federated identity management is increasingly used to connect enterprises along the value chain and enables them to reduce transaction costs significantly [2]. On the web it offers the promise of single sign-on for different domains and service providers, offering a common authentication and authorization infrastructure that eliminates the necessity of managing individual accounts and passwords. On the other hand several EU member states (e.g. Finland, Belgium, Estonia, Austria, Sweden, Italy, Spain, Portugal and Germany) have issued electronic identity cards (eID) to their citizens. Using eIDs for strong authentication in federated identity management scenarios seems to be an obvious and very promising combination. This would on one hand provide improved ease of use for the users and at the same time eliminate problems that are caused by password management issues, password reuse [3], and passwords' security flaws [4]. Therefore, the combination of eID and federated identity management technology promises a major improvement of security on the web and a significant increase of confidence and trust in the use of ICT by EU citizens and business. For the e-government domain, the combination of identity management systems with the strong authentication and signature functionality of identity cards would provide the necessary security infrastructure enabling online services that so far could not have been offered by public administration due to security or legal constraints.

While the strategy to build a trustworthy, comprehensive, user-centric and privacy aware identity management system for Europe based on existing eID and trust infrastructures seems to be compelling and straightforward, there are many unsolved challenges, which prevent the interoperable, secure, ubiquitous, easy and privacy-friendly use of strong authentication mechanisms across Europe. FutureID aims to address these challenges.

The remainder of this paper is structured as follows. We will first provide an overview of the existing challenges in Section 2. In Section 3 we present the approach of FutureID to address these challenges. In Section 4 we discuss the potential impact of the FutureID project before we summarize our findings.

2 Existing Challenges

2.1 No standardized, trustworthy and ubiquitously usable eID client

While the first eID deployments in Europe almost exist for a decade and first member states already have renewed their eID technology, the standardization of the European Citizen Card in CEN TS 15480 [5] and the corresponding international standard ISO/IEC 24727 [6] concluded fairly recently. Therefore, there are many different eID cards in the field and there is no standard conform eID client yet, which would be capable of supporting all the identity cards issued across Europe. While there are some proprietary smart card middleware components and government spon-

sored eID clients, they only support a subset of the issued cards, are only available for certain platforms, lack transparency because they are only distributed as executable and/or do not conform to the relevant international standards such as [5], [6], [7] and [8] for example.

2.2 Complex and costly integration of authentication and identity services

If nothing else because of this lack of standardization it is still very cumbersome to integrate a variety of different authentication devices and services. Therefore, typical service providers only can afford to integrate a limited number of specific authentication services, which in turn only accept a specific set of credentials and authentication tokens. While the Pan-European Proxy Services (PEPS) developed in STORK [9] and the eID-Broker developed in SkIDentity [10] introduce different flavors of eID brokerage, these concepts need to be combined and supplemented by universal authentication and trust services to ease the integration and usage of authentication and identity services.

2.3 No coherent European trust infrastructure for authentication

In addition to the cumbersome technical integration of the different authentication services, the lack of a coherent European infrastructure for trust management imposes additional obstacles, which prevent the easy, reliable and accountable deployment of electronic identity technology. Despite the availability of trust services [11] regulated by the European signature directive 1993/93/EC [12], emerging public key infrastructures for machine readable travel documents [13], trusted certificates shipped with popular browsers [14], several industry driven (e.g. [15], [16], [17]) or academic [18], [19] trust infrastructures and innumerable trust relationships set up and managed in a more or less ad hoc manner, there is no coherent European trust infrastructure for authentication yet. There is an emerging standards for entity authentication assurance frameworks [20] and first authentication related specifications, which use some sort of authentication assurance level (e.g. [21], [22], [23]). However, it is not clear how the different existing and emerging trust infrastructures map to the authentication assurance levels in a traceable manner and how liability issues [24] are regulated among the different stakeholders. Against the background of the forthcoming European regulation on electronic identification and trust services [25] there is an urgent need to provide a comprehensive and coherent trust infrastructure for Europe, which covers services for electronic signatures, authentication and identification and the FutureID project will do its best to support the European Commission and related national institutions in the process of designing and implementing this important piece of infrastructure.

2.4 Privacy threats of real world authentication solutions

Many of the early adopted eID cards contain X.509-based certificates, which can be used for authentication for instance, within the TLS-protocol [26]. The usage of

X.509 certificates allows cryptographically strong User authentication, but at the same time presents considerable privacy concerns. Roughly, Users always have to reveal their full identity and personal data contained in the certificate towards a service provider, even though that amount of information would not be strictly necessary. Furthermore, the signature of the certificate itself already serves as a unique identifier, which allows one to link different transactions of the same User and create extensive usage profiles. This privacy risk is significantly amplified if the authentication result and related identity attributes are transmitted across a complex network of Pan-European Proxy Services (PEPS) as in the STORK approach. Therefore the FutureID project aims at replacing the PEPS-network by universal authentication services, which are able to handle the different eID cards directly.

The German [27] and Austrian [28] eID cards were already designed with privacy protection in mind and include features such as pseudonyms, which shows the awareness of the aforementioned privacy threats. However, those privacy features often require complex infrastructures and come with constraints in terms of security (e.g. the same authentication key is shared among a batch of cards to build anonymity sets) and functionality when compared to standard PKI approaches.

A solution that provides both, i.e. the same or better level of strong authentication as X.509 certificates and preservation of the Users privacy, are privacy-enhancing attribute-based credentials (privacy-ABCs). In a nutshell, privacy-ABCs allow the User to establish several partial and unlinkable identities with each service provider, where they only disclose the information that is minimally required for the purpose at hand. The technology to deploy privacy attribute-based credentials is already available with, for instance, IBM's Identity Mixer [29] and Microsoft's U-Prove [30]. Currently, both are being integrated and used for two real-life pilots in the EU-funded project ABC4Trust project. However, the integration of privacy-ABC technology into large-scale eID environments still remains an interesting and open challenge.

Furthermore, little systematic research has been done on risk analysis and impact assessment of identity technologies. To enable deployment of privacy-friendly identity technologies, its ergonomic and economic parameters will be assessed in a systematic way, especially relating to mandatory risk analysis, risk mitigation and cost-of-ownership. Suggestions have been made in [31] and the topic will be further investigated in the PETweb II privacy risk assessment project that will contribute to FutureID [32].

2.5 Non-technical problems

The technical problems mentioned above seem to be responsible for many of the perceived problems with today's identity management systems, which in turn jeopardize the success in the market. A recent expert survey [33] performed by the SSEDIC thematic network [34] revealed that the most important barriers of using eID technology include the poor usability, the low perceived usefulness, the low awareness that the technology exists and the lack of applications.

From an economic point of view the interrelation between the perceived problems at the surface and the source problems at the root can be clearly explained: The challenge identity management and eID solutions are facing is that the market for this technology is a multi-sided market. According to [35] and [36], "A market is said to be two-sided if firms serve two distinct types of customers, who depend on each other in some important way, and whose joint participation makes platforms more valuable to each. In other words, there are indirect network externalities between the two different customer groups."

In multi-sided markets, when a system mediates between several parties, the "chicken or egg" problem is quite common [37]. When no services are supporting it, the usefulness for the user is presumably low. On the other hand, when no users have adopted the product yet, service providers' motivation to implement it is quite minimal. For a user to perceive a meaningful benefit, a system has to be widely adopted, and its underlying protocols implemented by a wide range of service providers [2]. On the other hand a service will hardly implement a certain identity management protocol if there is no broad support on the user side, as supporting too many unsuccessful protocols would mean cluttering its user interface and facing sunk implementation costs [2]. The utility for both participants of eIDs partially depends on the adoption by agents on the other side, indicating indirect network effects [38] with positive feedback: if more users adopt a SSO system, more services will adopt, and the other way around.

In order to utilize the full potential of eIDs, the technology needs to be adopted on a wide basis. As it is a multi-sided market, this will only be achieved if all participating parties perceive a benefit in adopting the technology. Therefore, FutureID will consider the interests of all the stakeholders involved in the eID ecosystem to facilitate economic conditions for wide take-up of its results. This includes the provision of a trustworthy and usable open source eID client and several components and services, which ease eID deployment on the back end side.

3 The FutureID Approach

The rationale for the objectives of FutureID is to address these challenges by developing the novel, integrative, secure, yet market-compliant FutureID infrastructure. FutureID will consider the interests of all involved stakeholders to ensure that the solution is compliant with market demands and privacy regulation. It will address the challenge of the two sided market by providing on one hand a trustworthy and usable open source client that supports multiple platforms and on the other hand by developing a service environment that allows for the smooth integration of eID technology on the back end side. Furthermore, FutureID will demonstrate the applicability and feasibility of the approach by developing two pilot applications. Figure 1 provides an overview of the envisioned FutureID Infrastructure.

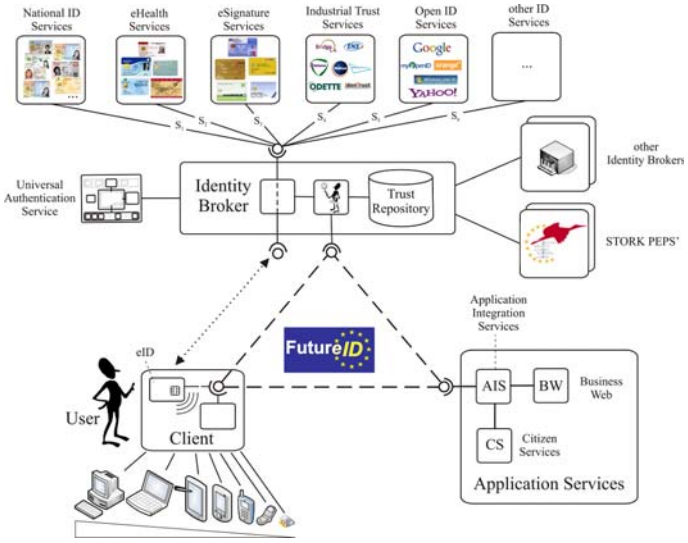

Fig. 1. The FutureID Infrastructure

The FutureID Infrastructure in particular comprises the following components, which are briefly described in the following subsections:

- Client
- Identity Broker
- Universal Authentication Service
- Trust Repository
- Application Services

3.1 Client

The User is equipped with an eID token and a corresponding client application. In order to facilitate the broad application of the FutureID technology, the FutureID Client is designed to support all popular PC platforms and diverse mobile devices including notebooks, tablet PCs, PDAs, smart phones, other mobile phones and even other embedded devices and will be distributed under a suitable open source license.

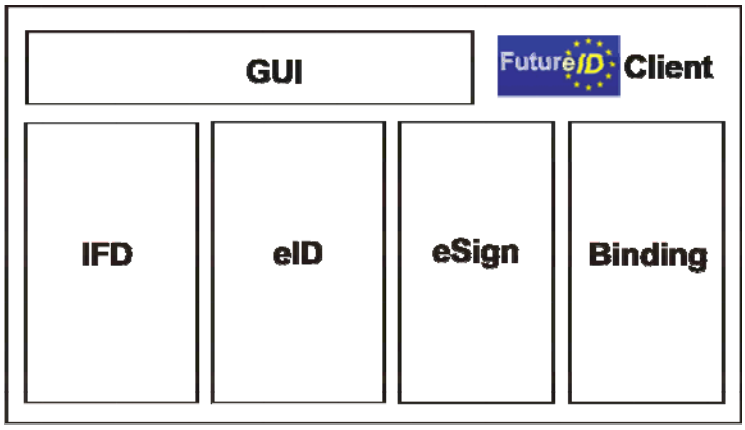

Fig. 2. Rough outline of the FutureID Client

As sketched in Figure 2 the FutureID Client roughly consists of the following building blocks:

- **Interface Device (IFD)** implements the IFD Layer as specified in ISO/IEC 24727-4 [20] such that a variety of smart card terminals, smart cards and similar hardware tokens can be accessed by the FutureID Client.
- **Electronic Identity (eID)** in particular implements the Service Access Layer as specified in ISO/IEC 24727-3 [20], such that arbitrary authentication tokens can be supported as long as they are described by a suitable `CardInfo` file according to CEN 15480 [5]. This component also contains support for federated identity management protocols, such as SAML [39] including the ECP (Enhanced Client and Proxy) profile [7] for example, and attribute-based credential technologies according to Idemix [29], U-Prove [30] or alternative credential technologies such as [40] or [41] for example.
- **Electronic Signatures (eSign)** allows to create advanced electronic signatures according to CAdES [42], XAdES [8], PAdES [43] using the standardized OASIS DSS interface [44].
- **Binding** contains functionality to support various message bindings such as SOAP [45], PAOS [28] and alternative transport protocols such as the Austrian Security Token Abstraction Layer (STAL) [46] or the eID applet protocol used in Belgium [47]. This component also contains means for a smooth integration of the FutureID Client core into browsers via interfaces such as PKCS#11 [48] for example.
- **Graphical User Interface (GUI)** will exist for each platform, which is supported by the FutureID Client and provides an easy to use interface for the User.

Furthermore there will be a comprehensive FutureID Client Testbed and additional research and development to provide trustworthy platforms for the FutureID Client.

3.2 Identity Broker

A major objective of the Identity Broker is to make it easy for Service Providers to connect to the FutureID infrastructure and use the various authentication tokens (national eID cards, electronic health cards, electronic signature cards etc.) connected to the FutureID Client in conjunction with associated external authentication services, the Universal Authentication Service developed within the FutureID project or other Identity Brokers, such as the Pan European Proxy Services (PEPS) developed in STORK [9] or the eID-Broker developed in SkIDentity [10] for example. There are two general operation modes for the Identity Broker:

- **Dispatcher Mode:** In a first and simple operation mode the Identity Broker only serves as dispatcher and determines an appropriate authentication service, which performs the authentication of the User and/or its associated platform and generates an appropriate assertion which can be consumed by the Service Provider.

- **Claims Transformer Mode:**In a more sophisticated scenario, the Identity Broker performs the authentication itself (together with the attached Universal Authentication Service) and then transforms the claims to an appropriate protocol and credential, requested by the Service Provider. The issued credential may either be a
  - *Session Credential* (e.g. a SAML [39] or OpenID [49] assertion), which has a short time to live and is (more or less) directly presented to the Service Provider or it may be an
  - *Privacy-Enhancing Attribute-based Credential* (e.g. Idemix [29], U-Prove [30] or alternative constructions that can be used to instantiate Privacy-ABCs as defined in [50]), which has a long-term validity and is issued to the User, who can in turn derive unlinkable presentation tokens from her credential portfolio which only reveal the information that is minimally necessary for the Service Provider.

3.3 Universal Authentication Service

In order to provide an optimized message flow and enable the Claims Transformer Mode mentioned above, the FutureID project will develop a Universal Authentication Service, which is able to support all authentication protocols implemented by the various authentication tokens deployed across Europe.

As the existing eID cards, eHealth cards, electronic signature cards already support a large variety of different authentication protocols and it may be expected that future authentication tokens will support other credentials and authentication protocols, it would be close to impossible to implement all required protocols using a conventional approach, because this would require a specialized program module for each and every authentication protocol. In order to solve this problem, the FutureID project introduces a novel approach for realizing a Universal Authentication Service, which makes it possible to support arbitrary authentication protocols in a very efficient manner. As depicted in Figure 3 the Universal Authentication Services contains a generic Execution Environment, which is capable of executing arbitrary protocols, which are described by appropriate Authentication Protocol Specification (APS) files.

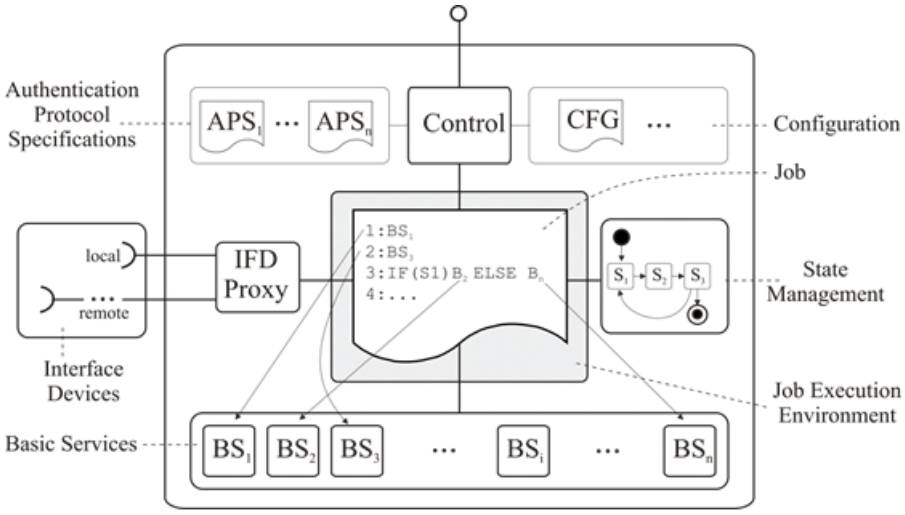

Fig. 3. High Level Design of the Universal Authentication Service

The APS-descriptions of the authentication protocols in turn refer to appropriate Basic Services, such as cryptographic primitives or smart card commands according to ISO/IEC 7816 [51]. As the different authentication protocols are all composed of a rather limited set of Basic Services, the problem of supporting arbitrary authentication protocols is reduced to providing this limited set of basic functionality and providing appropriate APS-descriptions for the different authentication protocols.

3.4 Trust Repository

The Trust Repository is attached to the Identity Broker and provides a comprehensive repository for trusted certificates and services [52], SAML meta data for trusted providers [53] and other trust related information. It can provide standard policies for the stakeholders such as signature policies and privacy policies, and archive these with a unique URI for later reference. In addition, it provides an audit trail for forensic analysis or billing purposes.

.

3.5 Application Services

The Application Services are consumed by the User and integrated into the FutureID infrastructure via the Application Integration Services (AIS). To demonstrate the broad applicability of the developed technologies, the FutureID project will address services for citizen as well as business services, which can be used by large and especially also small enterprises. To demonstrate the practical value of the envisioned FutureID infrastructure for the provision of secure services for European citizen, it is planned to integrate the FutureID infrastructure with the European electronic health large scale pilot project epSOS [54].

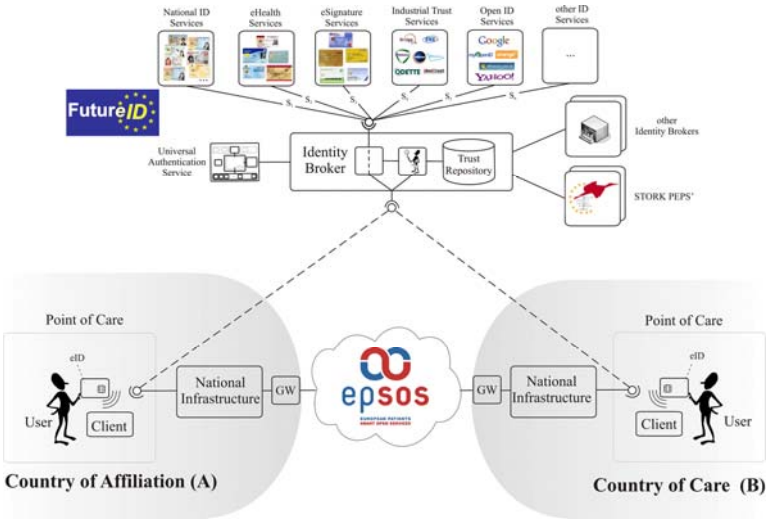

Fig. 4. FutureID based cross-border citizen services for epSOS

As depicted in Figure 4, this will involve Users of the FutureID infrastructure, which are located in different countries (Country of Affiliation (A) and Country of Care (B)) and act in different roles (e.g. as patient, administrative staff or health-professional). Among the current use cases for epSOS is the provision of a patient summary, which is provided in the home country (Country of Affiliation (A)) and can be accessed in case of a medical need in the foreign country (Country of Care (B)). In a similar manner there are first pilots for the exchange of electronic prescriptions across cross-borders. In order to demonstrate the applicability of the FutureID technology it is planned to provide eID-based security safeguards, which may serve as long-term replacement for the currently developed enhanced security safeguards for epSOS [55], which provide end-to-end-security but still rely on rather weak password-based cryptographic mechanisms. The signature services within the FutureID project may be used for the electronic provision of the patient's consent (e.g. for a patient summary) and the end-to-end protection of the authenticity and integrity of electronic documents (e.g. electronic prescriptions). Furthermore the different eID cards will be used for purposes of strong authentication and - whenever technically possible – for the encryption of the medical data.

4 Potential Impact

4.1 Specific impacts on eID stakeholders

The FutureID infrastructure will provide benefits to all stakeholders involved in the eID value chain. **Users** will benefit from the availability of ubiquitously usable open source eID client that is capable of running on arbitrary desktop PCs, tablets and modern smart phones. FutureID will pay special attention to ensure the user-

friendliness of this client. The absence of a user-friendly client has been identified as a major barrier towards the wide application of eID technology [34] [56], which will be addressed by the FutureID Client. Since the utility of eID is dependent on the availability of services that provide a perceivable benefit to the users, FutureID will further provide application integration services that allow an easy integration of existing services into the FutureID infrastructure. This will in turn also provide benefits to **application and service providers**, enabling them to use trustworthy authentication services without the necessity of making large up-front investments in eID technologies or to meet legal obligations. This will also provide new business opportunities to application and service providers and allow them to address new consumers segments, which have avoided the use of those services due to trust issues or privacy concerns. For the **e-government** domain, the combination of identity management systems with the strong authentication and signature functionality of identity cards will provide the necessary security infrastructure enabling online services that so far could not have been offered by public administration due to security or legal constraints. Furthermore, the ability to use the FutureID infrastructure will reduce cost for **businesses** to setup or migrate to use of eID in their standard business activities and avoid high (prohibitive) transaction costs in many cases. **Identity service providers** will benefit from the increased pool of potential customers of their services. The FutureID infrastructure allows for an easy integration of existing identity services into the universal authentication service. Through the specific focus on privacy risk analysis, the stakeholders will obtain increased awareness of the risks created by high-assurance electronic identities.

4.2 Specific impacts on the eID market

In its report on the "Electronic Identity Management Infrastructure for trust worthy services" [56] the ELSA Thematic Working Group on Electronic Identity Infrastructure has provided a comprehensive list of barriers to the widespread uptake of eID including technological, societal, legal, economic and organizational barriers. Many of those will be addressed by FutureID.

On the technological side FutureID will contribute to improve the interoperability of eID systems and to overcome the fragmentation and complexity of the eID standards landscape. It will deliver a framework to provide expected (and uniform) levels of security and privacy protection and to manage the complexity of multiple electronic identities. Furthermore, FutureID will provide harmonized eID middleware implementation that allows an easy integration of services. The universal authentication service architecture will enable the integration of different channels and eID types/sources while the application integration service will allow integrating services covering the public and the private sector.

Regarding the societal barriers, FutureID will remove the lack of ease of use of eID with the user-friendly and ubiquitously usable client and address the lack of citizen awareness of benefits of the use of eID with the ability to rapidly include useful services and the development of convincing pilot applications. The lack of trust citizens have in areas of privacy (loss of anonymity, persistence of activity traces) will be

addressed by the development of guidelines for privacy friendly identifier systems and the integration and extension of privacy-friendly technologies, such as privacy-enhancing attribute-based credentials, which are compatible with the currently existing and emerging eID landscape.

On the economic side, FutureID will eliminate the need for large up-front investments in leading edge technologies and reduce the cost for businesses to use eID in their standard business activities. Furthermore, FutureID will address the “chicken or egg” problem of a two-sided market, by providing solutions for both ends.

With the activities concerning Privacy Impact Analysis (PIA) and privacy risk analysis, FutureID will widen the focus from security properties and identity assurance to a broader conception of risks for all stakeholders depending on the choice and application of eID technology.

4.3 Added Value of European Approach

The Digital Agenda for Europe aims to deliver sustainable economic and social benefits from a digital single market based on interoperable applications. Providing a ubiquitously usable identity management infrastructure is at the heart of creating a more unified digital market, leveraging the advantages of fast EU-wide computer networks. FutureID aims to build a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe. Obviously this requires a European approach. FutureID will bring together leading industrial and academic experts from Europe to collaboratively work on achieving this challenging goal. The existing barriers for a common ubiquitous European eID framework apply to all member states and therefore should best be addressed in a concentrated and European effort. In particular in multi-sided markets where network effects play a dominant role, reaching a critical mass of users and service providers is essential for the success of the envisioned technology. Reaching such a critical mass will be much more promising on the single European market than on a national level. In addition, considerable potential for substantial savings exists through cross-border e-commerce for EU citizens. Furthermore, 85% of the experts questionaired during the SSEDIC survey [34] agree "that digital identities should be interoperable across borders". Such interoperability can only be achieved with a European approach. By engineering compliance to European regulator frameworks for privacy and data protection, the FutureID approach will help building a competitive approach for the European information industry compared to vendors from other legislative areas.

5 Conclusion

The FutureID project builds a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe. FutureID will combine expertise, experience and skills of partners with multidisciplinary and complementary competencies. Nineteen participants from eleven European countries constitute the FutureID Consortium.

Acknowledgments

The authors gladly acknowledge this research was funded in part by the European Commission under the seventh Framework Programme (Grant agreement no: 318424, FutureID). However, the results presented here reflect the views of the authors only.

References

[1] E. Maler and D. Reed, "The Venn of Identity: Options and Issuers in Federated Identity Management," *IEEE Security & Privacy*, vol. 6, no. 2, pp. 16–23, 2008.

[2] D. Hühnlein, H. Roßnagel, and J. Zibuschka, "Diffusion of Federated Identity Management," in *Sicherheit 2010*, F. C. Freiling, Ed. Bonn: Köllen Druck + Verlag GmbH, 2010, pp. 25–36.

[3] B. Ives, K. Walsh, and H. Schneider, "The Domino Effect of Password Reuse," *Communications of the ACM*, vol. 47, no. 4, pp. 75–78, 2004.

[4] P. G. Neumann, "Risks of Passwords," *Communications of the ACM*, vol. 37, no. 4, p. 126, 1994.

[5] CEN 15480, "Identification card systems - European Citizen Card," Technical Specification, Part 1-4.

[6] ISO/IEC 24727, "Identification cards- Integrated circuit cards programming interfaces," International Standard, Part 1-6.

[7] S. Cantor, "SAML V2.0 Enhanced Client or Proxy Profile Version 2.0," OASIS, Working Draft 02, Feb. 2011.

[8] ETSI, "Technical Specification XML Advanced Electronic Signatures (XAdES), Version 1.4.1," ETSI, ETSI TS 101 903, Jun. 2009.

[9] BioP@ss - Consortium, "BioP@ss - Project." [Online]. Available: http://www.biopass.eu.

[10] D. Hühnlein, G. Hornung, H. Roßnagel, J. Schmölz, T. Wich, and J. Zibuschka, "SkIDentity: Vertrauenswürdige Identitäten für die Cloud," presented at the D-A-CH Security 2011, Oldenburg, 2011, pp. 296–304.

[11] European Commission, "European Commission: List of pointers to national trusted lists (provided by EU)," 2011. [Online]. Available: https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml.

[12] European Commission, *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*. .

[13] ICAO, "Regulations for the ICAO Public Key Directory," http://www2.icao.int/en/MRTD/Downloads/PKD%20Documents/PKD%20Regulations.pdf, Jul. 2009.

[14] Mozilla, "Included Certificate List," Jun-2009. [Online]. Available: http://www.mozilla.org/projects/security/certs/included/.

[15] Odette, “Odette Trust Service.” [Online]. Available: https://forum.odette.org/sevrice/tsl.service.
[16] tScheme, “tScheme Website,” Nov-2011. [Online]. Available: http://www.tscheme.org.
[17] TeleTrust, “EBCA - European Bridge CA,” 2011. [Online]. Available: https://www.ebca.de/en/.
[18] EUGridPMA, “European Policy Management Authority for Grid Authentication,” *EUGridPMA - Building Trust for Authentication in e-Science*. .
[19] EuroPKI, “EuroPKI,” *EuroPKI - home*. [Online]. Available: http://www.europki.org.
[20] ISO/IEC 29115, “Information technology - security techniques - Entity authentication assurance framework,” Committee Draft, 2010.
[21] Bob Morgan, Paul Madsen, and Scott Cantor, “SAML V2.0 Identity Assurance Profiles Version 1.0,” OASIS Committee Specification, Nov. 2010.
[22] Odette, “Odette: Federated Identity Management Service Standards for Automotive (SESAM), Version No 1R0.” Mar-2010.
[23] D. Recordon, M. Jones, J. Bufu, J. Daugherty, and N. Sakimura, “OpenID Provider Authentication Policy Extension 1.0,” Dec-2008. .
[24] J. Alcalde-Morano, J. L. Hernández-Ardieta, A. Johnston, D. Martinez, and B. Zwattendorfer, “Interface Specification,” Deliverable D5.8.1b, Sep. 2009.
[25] European Commission, “Regulation of the european parliament and of the council on electronic identification and trust services for electronic transactions in the internal market,” Brussels, Proposal COM(2012) 238/2, 2012.
[26] T. Dierks and E. Rescorla, “The Transport Layer Security (TLS) Protocol, Version 1.2,” RFC 5246.
[27] BSI, “Advanced Security Mechanism for Machine Readeable Travel Documents - Extended Acess Control (EAC), Password Authentication Connection Establishment (PACE), and Restricted Identification (RI),” Technical Directive (BSI-TR-03110) Version 2.05, 2011.
[28] Liberty Alliance Project, “Liberty Reverse HTTP Binding for SOAP Specification,” Version v2.0.
[29] J. Camenisch and E. van Herreweghen, “Design and implementation of the idemix anonymous credential system,” presented at the ACM conference on Computer and communications security, New York, 2002.
[30] Microsoft Inc., “Microsoft U-Prove Community Technology Preview R2.” [Online]. Available: https://connect.microsoft.com/site1188. [Accessed: 31-Dec-2011].
[31] L. Fritsch and H. Abie, “A Road Map to the Management of Privacy Risks in Information Systems,” in *Konferenzband Sicherheit 2008*, 2008, vol. 128, pp. 1–15.
[32] E. Paintsil and L. Fritsch, “A Taxonomy of Privacy and Security Risks Contributing Factors,” in *IFIP Advances in Information and Communication Technology*, Helsingborg, Sweden, 2011, vol. 352, pp. 52–63.
[33] Hugo Kerschot, “eID Adoption Survey,” SSEDIC Deliverable Report YEAR 1, Nov. 2010-Nov. 2011.

[34] SSEDIC-Consortium, “SSEDIC (Scoping the Single European Digital Identity Community) Project.” [Online]. Available: http://www.eid-ssedic.eu/.
[35] D. Evans, “The Antitrust Economics of Multi-Sided Platform Markets,” *Yale Journal on Regulation*, vol. 20, no. 2, pp. 235–294, 2003.
[36] A. Hagiu, “Merchant or Two-Sided-Platform?,” *Review of Network Economics*, vol. 5, no. 2, pp. 115–133, 2007.
[37] B. Caillaud and B. Jullien, “Chicken & Egg: Competition among Intermediation Service Providers,” *RAND Journal of Economics*, no. 34, pp. 309–328, 2003.
[38] M. L. Katz and C. Shapiro, “Systems Competition and Network Effects,” *Journal of Economic Perspectives*, vol. 8, no. 2, pp. 93–115, 1994.
[39] P. Hallam-Baker and E. Maler, *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)*. 2002.
[40] D. Bauer, D. Blough M., and D. Cash, “Minimal information disclosure with efficiently verifiable credentials,” presented at the 4th ACM workshop on Digital identity management (DIM ’08), New York, 2008, pp. 15–24.
[41] R. E. Verheul, “Self-Blindable Credential Certificates from the Weil Pairing,” in *Advances in Cryptology*, vol. 2248, pp. 533–551.
[42] ETSI, “CMS Advanced Electronic Signatures (CAdES), Version 1.8.1,” ETSI, ETSI TS 101 733, Dec. 2009.
[43] ETSI, “PDF Advanced Electronic Signature Profiles, Part 1 - 5,” ETSI, ETSI TS 102 778, 2009.
[44] OASIS, “Digital Signature Service Core Protocols, Elements, and Bindings, Version 1.0.” .
[45] W3C Note, “Simple Object AccessProtocol (SOAP) 1.1.” 08-May-2000.
[46] MOCCA, “Modular Open Citizen Card Architecture Project.” [Online]. Available: http://mocca.egovlabs.gv.at/.
[47] F. Cornelis, “eID-Applet Project.” [Online]. Available: http://code.google.com/p/eid-applet/.
[48] RSA Laboratories, “PKCS #11 Base Functionality v2.30: Cryptoki - Draft 4.” 10-Jul-2009.
[49] O. Foundation, *OpenID Authentication 2.0*. .
[50] J. Camenisch, I. Krontiris, A. Lehmann, G. Neven, C. Paquin, K. Rannenberg, and H. Zwingelberg, “Architecture for attribute-based credential technologies,” Deliverable D2.1, 2011.
[51] ISO/IEC 7816, “Identification cards - Integrated circuit cards,” International Standard, Part 1-15.
[52] ETSI, “Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information,” ETSI, ETSI TS 102 231, V3.1.2, Dec. 2009.
[53] S. Cantor, J. Moreh, R. Philpott, and E. Maler, “Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0,” OASIS Standard, Mar. 2005.
[54] epSOS-Consortium, “epSOS (Smart Open Services for European Patients) Project.” [Online]. Available: http://www.epsos.eu.

[55] Fraunhofer, “epSOS Enhanced Security Safeguards (epSOS ESS) Project.” [Online]. Available: http://www.isst.fraunhofer.de/geschaeftsfelder/eHealth/refpro/epsos/.

[56] INFSO H2, “European Large Scale bridging Action (ELSA) - Electronic Identity Management Infrastructure for trust worthy services,” European Commission, Jan. 2010.