Recommendations and Future Work

D12.9

Document Identification	
Date	26/11/2015
Status	Final
Version	1.0

Related SP/WP	all	**Document Reference**	D12.9
Related Deliverable(s)		**Dissemination Level**	PU
Lead Participant	UNEW	**Lead Author**	Thomas Gross (UNEW)
Contributors	Thomas Gross (UNEW) Kovila Coopamootoo (UNEW Paolo Modesti (UNEW) Nuria Ituarte Aranda (ATOS Jessica Schroers (KUL) Hannah Obersteller (ULD) Meiko Jensen (ULD) Lothar Fritsch (NRS) Bud P. Bruegger (FHG)	**Reviewers**	Heiko Roßnagel (FHG) Janina Hofer(USTUTT)

This document is issued within the frame and for the purpose of the *FutureID* project. This project has received funding from the European Unions Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318424.

1 Executive Summary

Major Achievements

- **Design and development of a complement to STORK** whose function is to
  - integrate arbitrary identities, token and federation technologies beyond just government notified eIDs
  - create an open market for governmental and private-sector intermediation services that stimulates efficiency, quality of service and innovation through competition and is designed for long-term economic sustainability
  - support service providers who already have an installed base of their own credentials
  - help the adoption of STORK in the private sector

- **Pioneer the first practical architecture and technology for very large-scale meta-federation** featuring
  - architecture without any need for central components or restrictions on possible topologies
  - interoperability across federation dialects
  - an architecture and trust infrastructure that concurrently supports multiple perceptions of trust
  - user-centric and privacy-friendly information flows
  - accountability and privacy-friendly logging
  - support for chains of intermediaries
  - patterns to avoid profiling of users
  - possibility of abstract in multiple steps from the complexity of participating federations and trust domains

- Detailed legal study of large-scale identity management issues

- Integration of the requirement of a wide range of non-technical disciplines including legal, socio-economic aspect, privacy, usability, and inclusion into its architecture and implementation.

Remaining Gaps

- mature open source version of all components
- formal standardization
- easier to use identity selector that
  - supports user-enforced privacy and

  - scales to the enormous number of possible credentials of a very large-scale deployment without losing ease of use.

- implementation and integration of new key-based FutureID federation protocol in support of accountability and privacy-friendly logging, including its integration with current browsers
- Research on how to render FutureID highly resilient.

Overall Recommendations

- Foster the long-term sustainability of the FutureID results beyond the duration of the project.
- Use eSENS to further mature FutureID components, particularly the open source versions.
- Integrate FutureID into CEF as a complement to STORK for reaching out to the private sector and services that need to integrate non-notified electronic identities.
- Support research and development to fill the gaps identified by FutureID that are necessary for operational use at very large scales.
- Promote FutureID as the first generic solution for very large-scale identity management:
  - beyond Europe by:
    * engaging with North-America and other regions in a discussion of a common vision and conceptual framework for global identity-management
    * support of international standardization of FutureID concepts and technologies
    * foster a global open-source community around an open source reference implementation of FutureID
  - to the Private Sector by:
    * providing an off-the-shelf open source solution based on FutureID and STORK for service providers who need support for notified and additional eIDs
    * support high-profile champions to deploy and demonstrate FutureID technology
    * create awareness of the opportunity of providing commercial intermediation services and its market potential

Legal Recommendations

- National eIDs should be usable also in the private sector. For this purpose, appropriate legislation is needed.
- A system such as FutureID should be used for data minimization and pseudonymous (service-specific) identifiers, particularly in private sector use.
- The use of non-notified eIDs is important and should be supported by legislation (e.g. determine application of the eIDAS Regulation concerning assessment of the level of assurance).
- Standard contractual clauses should be developed that regulate responsibilities of parties in large-scale identity management systems.

- With respect to the eTrust Services regulated in the eIDAS Regulation, a legal obligation for Member States to introduce these services should be considered.
- The interoperability framework introduced by the eIDAS Regulation needs to be ready to process any kind of data in a lawful way. With respect to sensitive data this will require the system's ability to provide end-to-end-encryption.
- Privacy by design is an important principle, which needs, however, to be more defined. An approach to list concrete requirements has been elaborated in D22.3.
- In (privacy-friendly) decentralized systems is it necessary to ensure appropriate liability allocation/redress mechanisms. Legally essential evidence preservation can be done via a privacy friendly logging solution, that allows finding the liable party.

Research Recommendations

- Transfer results and insights of FutureID into other domains, such as the Internet of things.
- Adaptation and Integration of FutureID result and components into complex interorganizational systems such as Fraunhofer's "Industrial Data Space".
- Qualitative and quantitative research on socio-economic aspects of federations and the sustainable evolution of ecosystems of very large-scale identity management systems.
- Privacy-preserving identity federation and attribute-based authentication are key research areas to pursue and substantiate.
- As outlined in the legal recommendations, the research and technical primitives enabled by it should enable strong end-to-end privacy-by-design.
- FutureID identified the privacy-preserving accountability as a key research area to follow from the advances made in privacy preserving audits.
- Substantial research and development into highly resilient and fault-tolerant identity federation systems is required.
- Future identity federation systems should be established on a trusted computing base and attestation to protect their integrity and demonstrate it to others.

Roadmap

FutureID has been highly successful and has produced a wealth of important results. The following describes how to use the FutureID results to roll out a Europe-wide identity management system in support of the single market of services.

- open source reference implementation of all components
- formal standardization of protocols
- fill the identified gaps to support operational use at very large scales:
  - new, key-based federation protocols that support accountability, privacy-friendly logging, and strong security

  - easy to use identity selector that empowers users to control the authentication process and enforce their own privacy

- first high-profile deployments of the technology:
  - service providers who need to support additional credentials in addition to those supported by STORK
  - academic networks such as Geant with its eduroam
  - meta-federations in fields such as banking or automotive operated by existing organizations dealing with inter-banking issues or industry-wide data and trust networks.

- encourage uptake by software industry and integrators to implement the new FutureID standard in commercial products

- build a FutureID community beyond Europe
  - The United States government is currently looking to develop a vision and conceptual framework for very large-scale (and potentially global) identity management

2 Document Information

2.1 Contributors

Name	Affiliation
Thomas Gross	UNEW
Kovila Coopamootoo	UNEW
Paolo Modesti	UNEW
Nuria Ituarte Aranda	ATOS
Jessica Schroers	KUL
Hannah Obersteller	ULD
Meiko Jensen	ULD
Lothar Fritsch	NRS
Bud P. Bruegger	FHG


FutureID

2.2 History

0.1	14/10/2015	Thomas Gross	initial version
0.1.1	15/10/2015	Bud Bruegger	comments, lessons learnt overall project
0.1.2	15/10/2015	Jessica Schroers	legal background material
0.1.3	16/10/2015	Lothat Fritsch	recommendations for stakeholders
0.1.4	16/10/2015	Thomas Gross	lessons learnt, security, distribution of work
0.2	23/10/2015	Paolo Modesti	lessons learnt from security evaluation
0.2.1	25/10/2015	Thomas Gross	lessons learnt from technical evaluation
0.2.2	26/10/2015	Thomas Gross	research implications
0.2.3	26/10/2015	Nuria Ituarte	strategic benefits
0.3	28/10/2015	Jessica Schroers,	legal implications
		Hannah Obersteller	legal implications
0.4	29/10/2015	Hannah Obersteller,	privacy recommendations
		Meiko Jensen	privacy recommendations
0.5	05/11/2015	Kovila Coopamootoo	editorial, usable privacy, recommendations
0.6	08/11/2015	Thomas Gross	lessons learnt from socio-economic evaluation
0.7	09/11/2015	Lothar Fritsch	privacy recommendation
0.7.1	09/11/2015	Thomas Gross	background material for further analysis
0.7.2	09/11/2015	Bud Bruegger	editorial
0.7.3	10/11/2015	Lothar Fritsch	recommendations for stakeholders
0.7.4	10/11/2015	Kovila Coopamootoo	editorial
0.8	08/11/2015	Thomas Gross	refined structure, background material
0.9	12/11/2015	Kovila Coopamootoo	user-centric and privacy by design
0.10	12/11/2015	Bud Bruegger	transfer to LaTeX-able deliverable production
0.10.1	12/11/2015	Bud Bruegger	final structure, first draft executive summary
0.10.2	13/11/2015	Kovila Coopamootoo	privacy-by-design/usability for exec summary
0.10.3	13/11/2015	Thomas Gross	integration of lessons learnt from evaluations
0.10.4	16/11/2015	Bud Bruegger	integration of key characteristics
0.10.5	17/11/2015	Jessica Schroers	legal recommendations for executive summary
		Hannah Obersteller	legal recommendations for executive summary
0.11	18/11/2015	Thomas Gross	cross-linking and introduction
0.11.1	19/11/2015	Thomas Gross	organisation
0.11.2	19/11/2015	Bud Bruegger	Recommendations
0.11.3	19/11/2015	Thomas Gross	key characteristics: privacy-by-design, resilience
0.11.4	19/11/2015	Bud Bruegger	Roadmap, Strategic Benefits
0.11.5	19/11/2015	Bud Bruegger	Improvement of key characteristics
0.11.6	19/11/2015	Thomas Gross	Integration of research implications
0.11.7	19/11/2015	Bud Bruegger	Spelling Corrections
0.12	24/11/2015	Bud Bruegger	Editing, integration of figure, improvements
0.99	24/11/2015	Thomas Gross	Introduction, research recommendations, review candidate
1.0	26/11/2015	Bud Bruegger	Fixed comments by internal reviewers

2.3 Table of Contents

1 Executive Summary **1**

2 Document Information **5**

2.1 Contributors 5

2.2 History 7

2.3 Table of Contents 8

2.4 List of Figures 12

3 Introduction **14**

3.1 Methodology 14

3.2 Organisation 15

4 Key Characteristics of Large-Scale Identity Management in Support of a Single Market **16**

4.1 Reuse of all Existing Momentum, Initiatives, Infrastructure, and Technology . . . 16

4.2 Reaching Critical Mass through Intermediation 16

4.3 Need for a Competitive Market for Services that Compose the Overall System . . 16

4.4 Need to Support Diverse Perceptions of Trust while still Sharing Infrastructure Components 17

4.5 Need to be Designed as an Open System 17

4.6 Need for User-Centric Design 17

4.7 Need to Protect Privacy by Design 18

4.8 Need for Resilience 18

4.9 Need to Reuse Established Trust and Business Relationships 19

4.10 Need to Go Beyond Existing Federation Technologies 19

4.10.1 Need for Privacy-Friendly Information Flows 19

4.10.2 Need to Avoid Assertion Formats that Facilitate Profiling 20

4.10.3 Importance of Accountability 20

4.10.4 Privacy-Friendly Logging 20

4.10.5 Need to Support Chains of Multiple Intermediaries 21

4.10.6 Need to Support Multiple Credential Types and Direct Presentation of Credential to Service Provider . . . 21

5 Legal Implications **23**

5.1 Use of national eIDs . . . 23

5.1.1 National Identifiers . . . 23

5.1.2 Other authentication means . . . 24

5.1.3 Remuneration for the use of eIDs . . . 24

5.2 Responsibilities of parties . . . 24

5.3 Company authentication . . . 25

5.4 Man in the middle . . . 25

5.5 Logging . . . 25

5.6 Sensitive Data . . . 26

5.7 Privacy by Design . . . 26

6 Strategic Benefits of FutureID **28**

6.1 Users . . . 28

6.2 Service Providers . . . 28

6.3 Credential Issuers and Identity Providers . . . 29

6.4 Providers of Broker Services . . . 29

6.5 Trust Scheme Authorities . . . 30

6.6 Policy Makers . . . 30

7 Lessons Learnt from the FutureID Evaluation **31**

7.1 Overall Project . . . 31

7.1.1 Recommendations . . . 32

7.2 Security . . . 33

7.2.1 Lessons Learnt and Recommendations . . . 33

7.2.2 Future Work . . . 36

7.2.3 Audience/Stakeholders . . . 36

7.3 Privacy . . . 37

7.3.1 Utilization of Multiple Brokers . . . 37
7.3.2 Specific evaluation . . . 39
7.4 Usability . . . 41
7.5 Socio-Economic . . . 41
7.5.1 Recommendations . . . 42
7.6 Legal . . . 43

8 Research Implications **44**
8.1 Compositional Reasoning . . . 44
8.1.1 Recommendations . . . 44
8.1.2 Future Work . . . 44
8.1.3 Audience/Stakeholders . . . 44
8.2 Methods and Languages for Privacy Goals . . . 44
8.2.1 Recommendations . . . 45
8.2.2 Future Work . . . 45
8.2.3 Audience/Stakeholders . . . 45
8.3 Privacy-Preserving Audits . . . 45
8.3.1 Recommendations . . . 45
8.3.2 Future Work . . . 46
8.3.3 Audience/Stakeholders . . . 46
8.4 Privacy-Preserving Revocation . . . 46
8.4.1 Recommendations . . . 46
8.4.2 Future Work . . . 46
8.4.3 Audience/Stakeholders . . . 46
8.5 Usable Privacy . . . 47
8.5.1 Recommendations . . . 47
8.5.2 Future Work . . . 47
8.5.3 Audience/Stakeholders . . . 47

9 Recommendations **48**

10 Roadmap

2.4 List of Figures

1 The Federated Identity Do-Not-Track Pattern against Profiling. 37


FutureID

3 Introduction

This deliverable offers recommendations and identifies areas of future work after the completion of FutureID. The executive summary in the beginning of this deliverable highlights the most important points, whereas the body of the document provides supporting evidence and arguments.

3.1 Methodology

The work for this deliverable was facilitated with an interdisciplinary group of researchers, including the FutureID technical coordinator and experts in security, privacy, legal aspects and technical realisation of reference implementation and pilots.

The work of this deliverable followed a staged bottom-up approach. First, we analysed the outcomes of FutureID as expressed in the different evaluation deliverables, D12.1-D12.8. We considered the requirements originally proposed for the respective areas and the immediate outcome of the evaluation. From these observations, we derived lessons learnt, future work and a projection towards key stakeholders. This bottom-up work yields the Section Section 7, which in turn includes dedicated sections for the overall project lessons learnt, security, privacy, usability, socio-economic and legal lessons learnt. The remaining gaps of FutureID are founded in this evaluation.

We decided to establish dedicated broader lessons learnt for two key areas: Section 5 and Section 8. These evaluations were performed by legal and research experts respectively, considering observation made throughout the project. Hence, Section 5 contains expert recommendations on the legal environment of FutureID and identity federation, in general. Legal implications are naturally focused on policy and law makers.

Section 8 evaluates the advances made in the research of WP2.4 and identifies which research areas have shown to be promising or feasible. This yields recommendations for promising areas of future work, which could be included in future EU projects.

Separately from the investigation of lessons learnt and implications in these areas, we took a strategic perspective for FutureID as a whole. This perspective is taken into account in two ways. First, we identified the strategic benefits of FutureID as a paradigm as well as as a reference architecture with a set of components. The strategic benefits are grounded in a bottom-up analysis, collecting outcomes of the exploitation plan, the benefits of individual components, and benefits for stakeholders. Subsequently, we established strategic benefits with a high-level perspective. Section 6 contains the outcome of this analysis.

Secondly, we identified key characteristics of large-scale identity federation systems that are to thrive in actual markets. These key characteristics are influenced by the socio-economic evaluation, but also by the overall experience gathered throughout the project. Section 4 outlines these characteristics concisely.

Finally, we synthesised recommendations and future work proposals from this process, especially

a roadmap ahead.

3.2 Organisation

As a principle, this document is structured such that the most important information comes first and more detailed supporting evidence is provided subsequently. The reason for this structure is that key insights can be accessed quickly.

Hence, this deliverable starts with three high-level strategic analyses of identity management in the spirit of FutureID. Section 4 takes the lead. Whereas the key characteristics focus on technical and socio-economic characteristics, the following Section 5 offers the legal analysis for large-scale identity management and what legal frameworks need to be in place to enable those systems. Section 6 follows this argument, outlining the strategic benefits of FutureID.

The following two sections substantiate the argument, with more fine-grained Section 7 and Section 8. The lessons learnt section targets stakeholders establishing similar projects, that is identity and service providers as well as industry, considering a variety of angles from overall project management to requirements domains. The research implications target academic stakeholders, highlighting research outcomes and open questions to pursue.

This deliverable closes with forward-looking Section 9 and Section 10.

4 Key Characteristics of Large-Scale Identity Management in Support of a Single Market

Based on the experience of the FutureID project, the following section describes key characteristics of solutions for very large-scale identity management in support of a (single) market of online services. The recommendations are abstracted from FutureID itself but contain a *status* section that states FutureID's contribution.

4.1 Reuse of all Existing Momentum, Initiatives, Infrastructure, and Technology

Considering the daunting effort of a very large-scale identity management system, the only realistic way of implementation is to reuse existing initiatives, infrastructures, technologies, identities and momentum as much as possible. While this support of *legacy* complicates the system from a technical point of view, it significantly eases the much more challenging task of actually getting electronic identities used by a large number of users and service providers.

Status: FutureID is designed to integrate all existing assets while keeping the way open to incorporate cutting-edge and *revolutionary* technologies such as the privacy-friendly attribute-based credentials.

4.2 Reaching Critical Mass through Intermediation

The possibly most critical success factor for a large scale identity management system is its (voluntary) uptake by users and service providers. The very best system fails if it is not used. To be worth-while, the system needs to offer a critical mass of services to users and of potential users to service providers, respectively. This can be reached through (a) component(s) (sometimes called hubs, proxies, gateways, or brokers) that interface between diverse electronic identities and identity providers on one hand and service providers on the other. The intermediary takes care of the complexity of diverse technologies, trust levels, etc. and renders participation easy for identity and service providers.

Status: FutureID is designed to implement the intermediation pattern.

4.3 Need for a Competitive Market for Services that Compose the Overall System

A long-term sustainable solution must remain cost-effective, provide high-quality service to all stakeholders, incorporate new and innovative technologies, adapt to special needs of stakeholders, and cater to branch-specific and niche-markets. This is only achievable if there are multiple vendors for each system component and service. Most prominently, vendors include identity providers and intermediation service providers.

Status: The FutureID architecture supports an open marketplace of such services by avoiding the need for central components and control or a fixed topology of intermediaries and providing an *auto-configuration* when new services enter the market place. The avoidance of any centralized component or registration is crucial to prevent restrictions of free market forces.

4.4 Need to Support Diverse Perceptions of Trust while still Sharing Infrastructure Components

Perception of trust is closely linked to the perception of risk. Different entrepreneurs from different business-sectors, operating in different locations, and addressing different market segments cannot possibly agree on a single shared perception of trust. Trust fails to scale. Legal certainty that may apply to a whole region (e.g., eIDAS in Europe) is only one of many aspects of trust and fails to scale beyond the boundaries of the region while processes of the market are typically global.

A successful large-scale identity management system therefore needs to be able to support multiple perceptions of trust while still permitting the sharing of identities and identity services among stakeholders with different perceptions of trust.

Status: The FutureID architecture allows trust-perception-specific intermediaries to combine existing identities and identity providers in different ways from other intermediaries. The FutureID trust infrastructure was specifically designed to support diverse perceptions of trust and different trust assessments of the same identities and identity services.

4.5 Need to be Designed as an Open System

In order to be successful, a large-scale identity management system must be able to incorporate new initiatives, stakeholders, and technologies as they evolve. Failing to do so would create competing efforts that contradict the objective of reaching a critical mass. Failing to incorporate innovative new technologies would also render the solution obsolete.

Status: FutureID is designed as an open system that can incorporate new technologies (as demonstrated with Attribute-Based Credentials) and is not threatened by new initiatives such as *FIDO*.

4.6 Need for User-Centric Design

To support end user adoption, we recommend that identity federation systems incorporate user-centric design and that the European Union advocates user-centric design. First, user-interface design shall take into account the user all the way ensuring usability as key feature through-out. Second, identity federation systems and deployments for Europe shall support a user-centric mode of operation, which puts the component that represents the user's interests in the centre of transactions. This is a necessary condition for strong privacy-enhancing technologies, such

as attribute-based authentication, by which architectural design decisions need to enable future adoption of such technologies.

Status: FutureID is designed to support user-centric operation and has received significant usability consideration, from the requirements stage onwards.

4.7 Need to Protect Privacy by Design

To protect citizens from identity theft and mass surveillance of organised crime or nation-state actors, we recommend to make privacy-by-design a priority for identity federation system. Privacy-by-design provides and overarching framework for integrating privacy and data protection early and effectively into technologies, organisational processes and networked architectures. It provides multidisciplinary considerations into

- The right legal framework in the European Union, contractual agreements that highlight responsibilities of each party within FIM and privacy friendly logging solutions.
- Technical compliance with and beyond principles of data minimisation and purpose limitation as well as protection goals of transparency and intervenability.
- Re-usable software engineering methods that weaves user-centric privacy-by-design within the system design and development process.
- To enable realisation of legal propositions in practice, privacy should not be considered separately from privacy during design. User-centric privacy would involve shifting control to users, who may not always be in a position to fully assess risks. Improving user experience does not provide a one-size-fits-all solution.

Status: FutureID included privacy principles in its genesis and supports attribute-based authentication. Requirements for privacy-preserving brokering and identity provisioning were included.

4.8 Need for Resilience

Identity federation systems like FutureID stand to become a lynchpin for the digital economy, its identity backbone. To protect the system and the service providers as well as users who depend on the identity federation system, identity federation needs to be highly resilient. We recommend that the European Union makes the research and deployment of highly resilient identity federation a priority. FutureID's evaluation highlights three properties to include: a) privacy-preserving accountability, b) security assurance and system integrity of the identity federation system itself, and c) dependability and fault tolerance.

Status: FutureID specified requirements for system resilience based on today's state-of-the-art. Since out of scope of the DoW, they were not realised in the implementation though. Further research is required to solve highly resilient identity federation conceptually.

4.9 Need to Reuse Established Trust and Business Relationships

In many business areas, trust and business relationships to stakeholders with a specific role in the field have grown over extended periods of time. Prime examples are organizations dealing with inter-banking tasks or organizations who operate networks and trust frameworks in the automotive industry. For ease of deployment, uptake, and acceptance, any large-scale identity management solution should reuse these existing trust relationships and permit the existing organizations to act as intermediaries or authorities for the definition of trust schemes. By forcing a replacement of these existing organizations with different stakeholders due to a rigid topology or architecture would be very time consuming and bear a high risk of failure.

Status: The FutureID architecture avoids placing any restrictions on the topology of intermediaries and its open market approach. The infrastructure encourages that already established organizations act as intermediaries and/or trust scheme authorities.

4.10 Need to Go Beyond Existing Federation Technologies

While a wealth of well-established federation technologies already exist and are implemented in readily available products, these are insufficient compared to the needs of very large-scale identity management. The following provides an incomplete list of shortcomings of current federation technologies:

4.10.1 Need for Privacy-Friendly Information Flows

Current federation technologies have major shortcomings from a privacy point of view. One of these concerns information flows. When service providers issue an authentication request to the identity provider/intermediary of their choice, users may not even be aware of being redirected to another party. They thus lack the possibility of giving preference to the identity providers/intermediaries they trust and avoid untrusted ones. Users further lack the possibility to intervene in order to avoid the redirection to an undesired third party. Such a third party, i.e. and identity provider or intermediary, can learn a lot of privacy-critical meta-information about the user. For example, it can know who (e.g., established through browser-fingerprinting) accesses which service when. Third parties that users are forced to visit therefore present a risk of becoming big brothers. To solve this problem, new federation technologies are required that give users control of the information flow and let them chose third parties that are trustworthy.

Status: For this reason, FutureID uses a locally installed or server/cloud-based identity selector that represents and protects the users' interests. Since this component was not foreseen in the description of work, only a minimal solution could be implemented in the projects main implementation. To complement this, research has been conducted that prototyped the possibilities of privacy-protection and a master thesis was concentrating on the user-interface design to render this powerful component easy to use and understand by ordinary users. More work is required to bring this to an operational status.

4.10.2 Need to Avoid Assertion Formats that Facilitate Profiling

Another shortcoming in privacy protection are bearer assertions that typically contain both, information about the identity of the user and the intended recipient of the assertion. While the latter piece of information serves to avoid certain attacks on bearer assertions, listing identity and the service that consumes the assertion together obviously facilitates the profiling of users. New federation technologies need to avoid this privacy pitfall.

Status: FutureID has addressed this problem in two ways: (i) It has shown how the "Do Not Track Pattern" can be applied through the use of two intermediaries (brokers), one of which knowing the full identity but not the intended service, the second knowing the intended service but only an unlinkable pseudonymous identity. (ii) DTU has further developed a more advanced key-based federation protocol that avoids the need of listing intended recipients in bearer assertions. Both approaches need additional work to come to an operational state.

4.10.3 Importance of Accountability

Liability is an important issue in large-scale identity management. Since authentication in large-scale (meta-) federations typically involve a number of parties, if something goes wrong, it becomes crucial to be able to determine which of these parties has failed and is thus liable. Was it the fault of the credential issuer, of the identity provider, of one of the intermediaries (brokers, PEPS, etc.), or even of some hostile attacker? Current federation technologies fail to support this kind of accountability; new technologies are needed that support accountability by design.

Status: FutureID (DTU and FHG) has designed an advanced federation protocol based on formal proofs to support accountability.

4.10.4 Privacy-Friendly Logging

Further, identity providers and intermediaries (brokers, PEPS, ...) typically require logging in order to proof the absence of wrong-doing and thus defend themselves from liability claims. Storing personal information indefinitely in a log competes with the requirements of privacy to delete personal data as soon as possible, preferably right after issuing a derived assertion. Current federation technologies require to choose from privacy-unfriendly logging to protect against liability claims and privacy-friendly absence of logging that forfeits any protection against liability claims.

Status: In FutureID, the advanced federation protocol developed by DTU and FHG combines both, accountability and privacy-friendly logging.

4.10.5 Need to Support Chains of Multiple Intermediaries

In large-scale identity management systems, intermediation is used as a point of abstraction. It is used to encapsulate complexity and hide it from users of the intermediation service. This includes the following:

- Abstraction of multiple (token, authentication, federation) technologies behind a single interface,
- Classification of a potentially large number of issuers to few levels of assurance according to a selected trust scheme.

At very large scale, it is unrealistic to expect abstraction to always happen in a single step, i.e. to assume that there is only a single point of intermediation. New federation protocols are therefore required that can handle chains of intermediation.

Status: The FutureID architecture foresees the possibility of chaining intermediaries (brokers, PEPS, etc.). This chain is controlled by the identity selector. Since this requirement was lacking in the description of work, only the research prototype of the identity selector can handle more than one intermediary. More work is needed to reach an operational status.

4.10.6 Need to Support Multiple Credential Types and Direct Presentation of Credential to Service Provider

Certain credential types must be presented directly to the service provider, i.e., without any intermediary, in order to preserve their key properties. Two examples shall illustrate this:

- Attribute-Based Credentials preserve their unprecedented privacy features only if they are presented directly to the service provider,
- A translation of an X.509 credential in a bearer assertion by an intermediary drastically lowers the security level of authentication.

It is therefore beneficial, if service providers can accept certain credentials directly. If they accept both, directly presented credentials and assertions from intermediaries, they need to maintain multiple "credential consumers".

Current federation technologies fail to integrate the possibility of direct presentation of credentials to service providers. They also limit the kinds of credentials to assertions of a single federation technology. To support multiple types of credential consumers, including those for direct presentation, service providers need to offer their own "identity selectors", leaving users with an inconsistent experience across services and with different credentials, as well as with multiple identity selection steps that may be confusing. New federation approaches should integrate the possibility of service providers operating multiple credential consumers in parallel that are integrated in a single consistent user experience.

Status: FutureID's service provider component permits the use of multiple credential consumers of differing technology that all share the same session concept. FutureID thus also allows direct presentation of credentials for security or privacy reasons. Direct presentation credentials are one of the options to chose from in the single identity selector that also handles "federated credentials".

5 Legal Implications

The legal tasks in the FutureID project – from assessing the general legal framework to specific legal requirements – yielded several remaining open questions and missing instruments in the existing framework with regard to identity management and authentication mechanisms. In this section, we strive to collect important aspects from a legal point of view. Not all points can be solved by lawyers and policy makers (alone), however, this section is to be read as law- (and policy-)inspired analysis, but addressing all stakeholders of identity management systems. The findings mostly name the issue and its consequences, before recommending a way to handle it. This can be a concrete solution but also the recommendation of further research on a specific topic. As FutureID was dealing with eIDs as well as with electronic signatures, the interpretation and enforcement of the eIDAS Regulation – entered into force during the project runtime – was an important point to be discussed. Consequently, many recommendations in this section deal with the Regulation and its consequences. Others are directly derived from data protection law and mainly highlight the potential of developed (or upcoming) technical solutions to enhance the level of data protection in online authentication contexts.

5.1 Use of national eIDs

The focus of national eIDs lies on public services. The eIDAS Regulation allows the cross-border use of eIDs, but the provisions consider only public services. Therefore it is for the Member State to decide whether it is possible to use national eIDs for private services, or not. Considering the costs of the implementation of national eID schemes, and the benefit of the usage of national eIDs on a broader scale, policy makers should open the possibility to use national eIDs in a privacy friendly way also for private services. This might require some changes in law and/or administrative policies.

5.1.1 National Identifiers

However, in this regard one legal hurdle becomes obvious, as many national eIDs use unique national identifiers, which could be a reason not to make eIDs available to private services. Persistent identifiers as introduced in the implementing act to art. 8 eIDAS are not possible if an eID is used for private Service Providers as well. In general it is not desirable to generate one big usage pattern "cross-border", involving the private sector would make it worse (e.g.: could be linked between a financing request at a private bank and the participation in a public tender by the same entrepreneur). The content of the minimum data set can be determined by Member States (within the borders set by the implementing act), therefore, if a MS decides that the minimum data set it wants to work with is comparatively large, it might be justifiable for public purposes – but hardly for any arbitrary kind of private sector purpose. These arguments show that data minimisation is necessary, especially for a private sector use of national eIDs. The FutureID system could be helpful in this regards, as even if the eID of Member States does not have a data minimisation functionality and therefore provides a lot of data, the FutureID ecosystem can solve this (reduce and integrate it to a federated IdM system). Additional possibilities are

that although an eID may not be part of e.g. a system like the nPA, which works with domain specific identifiers, the FutureID infrastructure can add domain/service specific identifiers, and can take out/replace unique national identification numbers. (See also section 7 below.)

5.1.2 Other authentication means

Another factor is that customers might have a large interest in not always authenticating themselves using their national eID (even if data minimisation is possible). If they come from countries which did not notify other eID means, they would under the current legislation have no choice but to use eID means different from notified ones. To provide more user choice the interoperability of different eID means should be fostered. FutureID can help in this regard, as it provides interoperability of different eID means. Levels of Assurance (LoA) can also be helpful. For self-determination one common LoA system (preferably eIDAS, as it already exists and Member States have to indicate the LoAs when notifying) should be used and customers should be clearly informed which LoA their identification means have and which LoAs are required to access a certain service. Every service should indicate which the lowest necessary LoA is, and accept all identification means that possess this or a higher LoA. This fosters self-determination, as the customer can autonomously decide which eID means they want to use for which service. In future this would require a broader applicability of a single system of LoAs. A standard assessment and a way to verify that specific eIDs indeed have that LoA would be useful.

5.1.3 Remuneration for the use of eIDs

The eIDAS Regulation leaves the choice to the Member States whether to allow private services the use of national authentication schemes or not, including possible terms of access. This could possibly result in many different terms and costs of access. In this regard, the FutureID Broker system might be additionally useful, as it could negotiate terms of access, and possibly flatrates, for the authentication service. Such a negotiation is out of the reach of single SPs which do not have a high amount of authentication requests, could not request. Additionally it would simplify the use of national eIDs for SPs, as they do not have to contract with every Member State, but can simply have one contract with a FutureID Broker, which will have the appropriate contracts with the different Member States to ensure that the Broker can use their service.

5.2 Responsibilities of parties

The responsibilities of the different parties within identity federations are not specified by law. Therefore contractual agreements are necessary. However, these require negotiations, using time and money, and might be disadvantageous for certain parties. A solution could be standard contractual clauses as they exist for data processing between MS and third countries. These could for example address jurisdiction agreements and (if the GDPR is coming) agreements on the competent DPA.

5.3 Company authentication

The eIDAS Regulation allows for the use of eSeals (signatures of legal persons), but factually employees often need to use their private eID to sign, as legal persons usually do not have eIDs. This enables links between private and professional use of the eID of employees. Therefore it is desirable to have other means. The employee IDs already existing in many bigger companies could have such functionality and be connected to the existing infrastructure by using FutureID. The eIDAS Regulation lays the legal foundation by introducing "eSeals". From a labour law point of view with the introduction of eSeals it is doubtable whether employers can oblige their employees to use their private eIDs for professional purposes, i.e. sign documents on behalf of the employer. Having said this, the provision of eSeal means bound to legal persons lays the (legal and factual) foundation for fostering the use of eTrust services in cross-border business. Additionally, from a data protection point of view, in some cases it is irrelevant for the recipient to identify the employee who signed, if he just can be sure that the document is signed in a legally binding manner. The disclosure of the employee's name, consequently, is an unnecessary disclosure of personal data. The provision of eSeal means for legal persons is a market, too. Contrary to the situation with eIDs for citizens, the Member States are not competent to issue "eIDs for enterprises". However, such registers or services already exist in some regions or countries, e.g. the eHerkenning system in the Netherlands. In this context, a future research topic could be to develop a technique which allows internal identification of the signee without revealing his identity to the recipient.

5.4 Man in the middle

The threat of creating a big "man in the middle" is a principal problem in IdM solutions. FutureID provides the possibility of employing multiple brokers, therefore diminishing the information every single Broker can have about the user. It should be ensured that the system, when deployed, will not rely on one single broker. The issue and a technical solution have been explained in detail in section 7.3 (Lessons Learnt from the Privacy Evaluation). From a legal point of view, the recommended decentralised system will require a contractual chain of liability. Here it is important that the broker that is in contact with the user cannot completely exclude liability for failures.

5.5 Logging

Logging is necessary, especially to be able to provide proof in case of claims. However, logs can include personal information and are therefore seen critical from a privacy point of view. At the same time, in order to be able to use logs as evidence, is it important to be able to prove that the logs have not been tampered with. Therefore, future research should consider privacy friendly logging solutions.

5.6 Sensitive Data

In the FutureID project one pilot application was extending the pre-existing epSOS network by two additional functionalities: authentication to the system with different eIDs and electronic signing of consent forms. The personal data processed in electronic health care systems in general is sensitive data and additional protection is required, e.g. by implementing at least a two-factor-based authentication like done in FutureID. Due to the sensibility of the data, the transmission necessarily needs to be end-to-end-encrypted. However, for the implementation of the interoperability framework as set up by the eIDAS Regulation, end-to-end encryption should be mandatory. Otherwise, the framework will not be suitable for health related data or for any other sensitive data (in terms of art. 8 Dir. 95/46/EC). This would needlessly limit the possible cross-border use cases, but could be solved by setting end-to-end-encryption as standard instead of just "facilitating" end-to-end-encryption. Furthermore, art. 6 (1) Commission Implementing Regulation (EU) 2015/1501 (on the interoperability framework) provides that the data exchange and the maintenance of data integrity between the national nodes shall be ensured by using best available technical solutions and protection practices. This cannot be less than end-to-end-encryption at this point in time. A respective clarification could be made by the Cooperation Network, based on art. 12 (1) (EU) 2015/1501.

5.7 Privacy by Design

All the aspects described above can more or less be summarized to the principle of "privacy by design", which – without going into detail – stands for system engineering with privacy in mind. It means to technically comply with data protection law (with its principles of data minimisation and purpose limitation as well as protection goals like transparency and intervenability), and even go beyond the (minimum) standards. Art. 12 (3c) eIDAS Regulation states that the interoperability framework for the European cross-border use of eIDs shall facilitate the implementation of the principle of privacy by design. In fact, the principle should be observed during the design of the framework itself. In the draft General Data Protection Regulation, the principle of "data protection by design and by default" is mentioned in art. 23. While the final wording of this article, putting a general obligation on the controller to respect the principles, is not agreed yet, the wording of rec. 61 apparently is undisputed: Rec. 61 states that the protection of the rights and the freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organisational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of the Regulation are met. In order to ensure and demonstrate compliance with the Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default. Although at this point time the legal text is only a draft, the consequences should be envisaged. From a recital – in contrary to an article of a Regulation – no legal rights can be derived directly. However, the articles have to be interpreted in the light of the recitals. An illustrative example in how far FutureID results are relevant in this respect: Art. 5 (1 c) draft General Data Protection Regulation provides that personal data must be adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed;

they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data. Read together with rec. 61 (privacy by design) this means, that the service provider – as data controller – has to justify and document which data he needs, and may not process any data beyond. If the user's eID is unable to provide only the appropriate data (a functionality which would be an excellent example for privacy by design), the service provider may make use of a Broker Service which is able to strip off all irrelevant data and still ensure the trustworthy origin of the information. This would require that the Broker (as a third, independent party in this scenario), which is trusted by the user and the service provider, will delete all the information received immediately after the information is not needed anymore for the transfer. This can also, in accordance with the principle of privacy by design, be implemented as an automatic deletion function. Like this, at least the shortcomings of "traditionally designed" systems could be mitigated.

6 Strategic Benefits of FutureID

The following describes the strategic benefits for various stakeholders:

6.1 Users

- Thanks to the intermediation patterns of FutureID, users can reach a critical mass of services with a single credential. This renders the possible effort of obtaining, installing (e.g. a card reader), using (e.g., remember a PIN), and renewing a credential worth-while.
- Users can therefore use fewer credentials to reach the services they need.
- By rendering trustworthy credentials interoperable with a wide range of services, users can reduce their reliance on passwords that render them vulnerable to attacks and potentially permanent damage resulting from identity theft.
- The user-centered information and interaction flows of FutureID put users in control of the authentication process and empower users to give preference to trusted identity providers and brokers and avoid untrusted ones, optionally by cancelling the authentication process before untrusted parties receive any personal information or meta data.
- FutureID has developed the concept where users can enforce their own privacy protection by requesting brokers to create pseudonymous identities, minimize the exposed data even when using "full-disclosure" eIDs, and applying patterns that render profiling impossible.
- FutureID renders more services accessible to owners of privacy-friendly attribute-based credentials through the possibility of using broker services that interface privacy ABCs to traditional service providers who lack support for this technology.
- FutureID provides users with a consistent user experience across a very large number of credential types and across all service providers. This renders much more transparent to users what happens, who gets to see personal information, and how the process can be controlled.

6.2 Service Providers

- Service providers can use the intermediation capability of the FutureID infrastructure to reach out to a virtually unlimited user base and arbitrary credential types.
- Service providers have full control of which credential issuers, identity providers and broker services they trust at what level of assurance.
- Service providers faced with needing to support a wide range of digital identities, multiple authentication protocols, and multiple federation dialects can outsource this complexity to broker services.
- FutureID creates an open marketplace for such broker services such that service providers benefit from competition and avoid lock-in.
- FutureID permits contractual agreements with broker services that can integrate service level agreements and regulate liability.
- In business branches where trusted third parties already exist, these can operate FutureID

broker services and act as trust scheme authorities. This avoids the need that service providers are forced to disregard established trust relationships since the required service can only be offered by new, unknown entities.
- Since the operation of broker services is market-motivated and no central control, registration, or third-party infrastructure configuration is needed, also service providers operating in niche markets are likely to find the necessary offerings of broker services.
- Due to the market-oriented nature of the FutureID infrastructure and its avoidance of lock-in to specific broker services, service providers' investment is much better protected.
- Mission-critical services can contract multiple distinct broker services in order to guarantee availability of the service.
- Service providers in need of using government notified eIDs while still needing to support an existing user base with non-notified electronic identities can use FutureID to access both, notified identities through STORK and non-notified ones through direct authentication or external identity providers.
- For security and privacy reasons, service providers can integrate non-federated direct authentication of credentials with authentication through a broker while integrating both in the same look and feel for the user.

6.3 Credential Issuers and Identity Providers

- The value of credentials and federated identities to users and service providers is drastically increased through the intermediation pattern used by FutureID.
- Profitability of credential issuance and federation is thus broken out of service-specific silos and can be provided through a much wider market.
- This renders the business of credential issuance and identity federation more attractive and easier sustainable.

6.4 Providers of Broker Services

- FutureID creates a new market for broker services that support the need of service providers to support a wide range of electronic identities that are usually accessible through a range of different circles of trust, federation technologies, and trust schemes.
- Due to the open nature of the FutureID marketplace, broker services can specialize on specific market segments and be competitive by targeting specific legal needs (e.g., a given legislation and place of court), language of services (both online and in documents), technical requirements (e.g. integration with given application server technologies), or branch-specific business practices (e.g., liability or SLA schemes).
- Broker services can operate without the need for a third party approval, registration or enabling service. This protects the investment and allows rapid adaptation to changes in the market.
- Broker services can collaborate with other broker services and identity providers in order to increase their offering of supported electronic identities beyond what would be possible within the limits of their own capacity.

- Broker services can operate farms of "virtual brokers" to adapt to the trust perception and needs of individual service providers and provide custom services.

6.5 Trust Scheme Authorities

- Trust Scheme Authorities, i.e. publishers of trust lists or lists of lists, can use the FutureID trust infrastructure to make trust lists easier to use by verifiers. This is comparable to certificate revocation management, where it is cumbersome for verifiers to download complete revocation lists and easy to query the revocation status of individual certificates. A patent application has been filed for the FutureID trust infrastructure and the LIGHTest proposal (Horizon2020 DS-5-2015) attempts to bring it to technology readiness level 7.

6.6 Policy Makers

- FutureID has complemented STORK to:
  - provide interoperable identity management for electronic identities that are not notified (e.g., health and health-professional cards)
  - make it easy for service providers to use notified, non-notified and self-issued electronic identities in parallel.
- With this and many other properties, FutureID significantly helps to foster the use of eIDs and other electronic identities in the private sector.
- Thanks to the market-oriented approach and the avoidance of centralized components or centralized governance, FutureID is arguably the first identity management infrastructure that can scale globally. This can potentially put Europe in a leadership role for conceiving very-large scale identity management concept that are interoperable beyond the borders of Europe itself. A prime opportunity in this area is a potential collaboration with the United States to develop a common vision and conceptual framework for interoperable identity management. Trade agreements such as TTIP will require interoperability of identities across the Atlantic in order to support the market of online services. This is a field where Europe can be highly competitive.

7 Lessons Learnt from the FutureID Evaluation

This section provides an exposé with the lessons learnt derived across evaluations, including general lessons to more specific ones under technical, security, privacy, usability, socio-economic and legal criteria.

7.1 Overall Project

This section describes the lessons learnt for the FutureID project as a whole. The discussion is also important to put the aspect-specific lessons learnt in the right context and explains certain lessons by making the impredance mismatch explicit that exist inherently between the project's work plan and the approach of requirements analysis, design and implementation, and evaluation.

A proposal for a European project, to be fundable, must include a detail plan of work. In a technical project such as FutureID, such a plan of work is closely linked to an initial solution of the problem addressed by the project. In particular, in FutureID the work package and tasks follow the structure of a preliminary architecture and its components. The description of work thus fixes the main components and their overall functionality.

Evaluation, on the other hand, usually assumes a sequence of defining requirements, then finding a solution that satisfies them, and finally explicitly comparing the solution to the stated requirements.

The difficulty of embedding an evaluation approach into a European project stems from the fact that there the step of finding a solution fails to be free but is significantly restricted by the pre-existing structure of the work plan and its allocation of resources. In particular, the introduction of additional architectural components is difficult since they lack a corresponding work package and/or task in the description of work. The situation is similar when the functionality of a foreseen component is changed significantly compared to the plan created in the proposal phase.

FutureID has experienced this exact difficulty that is inherent for such projects. Namely, the preliminary architecture of the proposal and thus description of work failed to satisfy some major requirements that were only defined in the first phase of the project. This is not surprising also considering the multi-disciplinary composition of the requirements team that contrasts with the reality of proposal writing where typically a single person is responsible for the preliminary architecture.

The FutureID project therefore made a major interdisciplinary effort for reviewing and revising the preliminary architecture in order to satisfy the stated requirements. The resulting "new" architecture was certainly a big progress but also introduced an additional architectural component (namely the Solver and Executor) with functionality that was not foreseen in the proposal. It also changed and increased the functionality and thus complexity of the Broker Service component significantly.

As expected, a full implementation of the new, improved, and more ambitious FutureID ar-

chitecture was impossible with the available resources of the project. FutureID addressed this difficulty as follows:

- The new architecture was described in all its potential and distinct evaluation efforts looked at the architecture and its implementation.

- A subset of the architecture was chosen for implementation. It maximized its value on the directly accessible market segment of smaller-scale identity management and lacks certain functionality that is only necessary for very-large-scale deployments--a market that yet has to be rendered accessible.

- The FutureID consortium has invested additional effort beyond the description of work to prototype functionality that could not be implemented in the mature main components of FutureID. This includes a prototype of an additional implementation of the Broker Service by FHG that serves as a vehicle of experimentation and of delivering proofs of concepts for advanced functionality. This was complemented by a prototype implementation of the Solver and Executor component by FHG and a master thesis that explored approaches that maximize the usability of this component.

- The FutureID implementation focuses on legacy protocols such as SAML. This greatly maximizes the ease of deployment through reuse of existing infrastructures and systems. In addition, the FutureID architecture also opens opportunities for new protocols with previously unreached characteristics of accountability, privacy, and security. While these protocols were not implemented, they were formally designed under the lead of DTU and limited prototyping explored their feasibility with current browsers.

In summary, the FutureID consortium has found a tradeoff that both, delivers a mature implementation for the currently accessible market and describes a more ambitious solution for very-large-scale identity management for which all major uncertainties have been addressed explicitly. The actual implementation is a key enabler for successful exploitation and sustainability of FutureID; the design of a very-large-scale solution significantly advances the field and provides a solid basis for a road map and the identification of necessary future work.

7.1.1 Recommendations

Projects that follow a structure of requirements assessment, design, implementation, and evaluation should make it explicit to all participants that the fixed resources and work plan of the project limit the possibilities to satisfy all requirements. Without such awareness, particularly project partners who are not involved in the implementation tasks may have unrealistic expectations of what can actually be implemented and may therefore experience considerable frustration.

The approach taken in FutureID to address this difficulty seems to be a good practice that is recommended to be used in other projects. FutureID has attempted to address all requirements

in its conceptual framework and architecture, while restricting the implementation to a realistic subset that is oriented to the currently accessible market.

7.2 Security

One of the requirements of FutureID was to building a scalable, robust and secure identity federation system on European Scale.

7.2.1 Lessons Learnt and Recommendations

Eventually, entire economies will depend on the operation of identity federation systems.

- The security evaluation shows that mostly functional requirements are applicable to the reference architecture.
- The security requirements (D22.2) that provided the main input for the analysis were mostly inapplicable at architecture level. In fact, many requirements are related to a specific implementation or to a specific technical environment and they cannot be captured at the level of abstraction of the reference architecture. The reference architecture relies on legacy protocols such as that described in the SAML 2.0 POST/POST profile. Beyond that, it does not specify the fault-error-failure behaviour of FutureID components or subsystems, which might affect security strongly. In particular, the Reference Architecture does not specify 'abort' or 'go-ahead' conditions for its protocol runs, beyond what is specified in the used legacy protocols. Since some security requirement are built upon 'abort' and 'go-ahead' conditions, these should be considered conceptually at Reference Architecture level and not left to implementation decisions.
- More tests implemented in the testbed could have been used during the evaluation. However, it turned out that the mapping between requirements and the test cases was not feasible. One of the main reasons was that, in the development process, there was not an explicit mechanism to account for how the requirements were implemented in the software. Missing the first link it was not possible to have a clear path connecting requirements, software artefacts and test cases. Our recommendation is to use a rigorous software development methodology that would allow to document clearly and effectively the dependencies between input (requirements) and outputs (software artefacts and functionalities). Automatization would have allowed to repeat the test multiple times in a systematic manner, as the manual assessment could not completely synchronize with the evolution of the software development of the components.
- The evaluation was performed mostly during the last year of the project. Apart from the reference architecture that was defined at the end of the first year of the project, the implementation and the development of pilots evolved significantly during the period of the evaluation. This caused difficulties and uncertainties that could be partially overcome with the help of developers. Nevertheless, especially in the last few months of the project, when software components and pilots were released, the synchronization became increasingly difficult. Again, the collaboration of the project partners was useful, but from the

evaluators' point of view would have been preferable to have more time to evaluate the final, stable and finalized product after the end of the project.

- Regarding the reference implementation, three key areas were identified in need of a substantial improvement with respect to the current situation, in case an operational identity management infrastructure would be deployed. It should be underlined, that the construction of such large infrastructure was beyond the scope of the FutureID project, which was rather aimed at demonstrating the benefits and the technical feasibility of building such infrastructure. The requirements on accountability, integrity and resilience were deemed 'not applicable' for FutureID reference architecture and implementation, however will be crucial for sustainable systems.
- **Accountability** means that the system keeps unalterable and unforgettable evidence of its transactions, yielding non-repudiation, and hence creating the technical foundations for liability in the business ecosystem that builds on the identity federation.In identity federation systems accountability is a crucial factor, as undeniable evidence needs to be given, in several situations, including resolving disputes of any kind and criminal investigations, to all the participants (users, identity providers, service providers, certification authorities, public authorities). With respect to specific requirements:
  - Components must ensure that any security relevant data like authentication data, eID data, assurance level or log files are protected against unauthorized modification, substitution, re-ordering, or deletion.
  - Audit records by FutureID components or system administrators should be stored with integrity protection in an access-restricted storage space.
  - For audit events, resulting from actions of identified users, all FutureID backend components must be able to associate each event with the identity of the user that caused the event, in compliance with the FutureID privacy requirements.
  - The FutureID backend components must be able to apply a set of rules to monitor the audited events and based upon these rules indicate a potential security violation.
  - All FutureID components that generate audit records must prohibit all entities read access to the records except for those entities that have been granted explicit access.
  - Access to all audit records by FutureID components or system administrators should be recorded and stored with integrity protection in an access-restricted storage space.

- **Integrity** refers to the capacity of the FutureID sub-systems to establish the sound configuration and state of its components and attest to this to other parties based on trusted computing. A set of requirements requested that the components should have been able to handle security relevant data like authentication data, eID data, assurance level, log files, audit records in a way that would allow their protection against unauthorized modification, substitution, re-ordering, or deletion. Another class of requirements prescribe integrity checks of software components, at bootstrap and in case of restart, that were not deemed necessary for demonstrating a proof of concept but cannot be ignored in the production environment. In detail:
  - Components should be able to verify their own integrity during start up and re-start.
  - Components must ensure that any security relevant data like authentication data,

eID data, assurance level, log files are protected against unauthorized modification, substitution, re-ordering, or deletion. The component should provide evidence, if any of these data have been modified, substituted or re-ordered.
  - The Universal Authentication Service must check the consistency of all its modules and libraries with its APS language repository, including matching versions. The Universal Authentication Service should check the consistency of specifications in APS language with the general security policies, including key lengths, cryptography parameters, and allowed protocol suites.

- **Resilience** refers to the capacity of FutureID to protect itself against adversarial action. A set of requirements considers the resilience of the entire system and its fail-over behaviour. They are meant to be applicable to an operational identity management infrastructure deployed at the continental level, and therefore, again, cannot be applied to a reference implementation, which cannot be compared in terms of hardware and software resources with an operational identity management infrastructure serving a large base of users. However, for the real infrastructure they would be crucial. These improvements will need to be taken into account:
  - Components must assign a priority to each subject in the security functionality. It must ensure that access to all sharable resources is mediated based on the assigned priority.
  - The system must enforce maximum quotas for memory space, storage space and CPU load that each authentication session can use during the identity federation procedure.
  - The system should provide sufficient throughput to offer its services under high load, with significant contingency to spare for unexpected events.
  - The system must provide sufficient resistance against denial-of-service attacks.
  - The components must integrate with intrusion detection systems and react adequately upon detection of a potential security. For example, session termination, residual data deletion, key destruction and security attribute expiration.
  - Components must be resistant against run-time attacks that could violate their integrity.
  - The FutureID backend components should be able to maintain profiles of system usage in compliance with the privacy requirements that allow the detection of any suspicious user activity. In case of detection of a suspicious activity, an alert to the system administrator should be triggered. Depending on the level of severity, a user authentication may be blocked until the detected issue is resolved.
  - The FutureID backend components should have available a heuristic method to detect well-known attacks and intrusion scenarios. Upon detection, the affected component should inform the other components about the security violation and terminate further service activities. Additionally, it should trigger an alert to the system administrator.
  - Any confidentiality loss within one system component must not lead to confidentiality issues in other system components.
  - The system of systems that makes the FutureID infrastructure must not exhibit a

single-point-of failure.
- The FutureID Infrastructure must implement well-defined failure modes and modes of reduced functionality.
- The FutureID infrastructure must provide a fail-over mechanism in case of a failure.
- In case of a failure, the FutureID infrastructure must offer a graceful degradation to an emergency mode that maintains critical functions.
- The FutureID infrastructure must provide redundancy for key components, such as the Broker Service.
- A loss of integrity within one system component must not lead to an integrity loss in another component or to the loss of overall system integrity.
- The FutureID infrastructure components must establish a mutual synchronization of system timers to ensure that timeouts and time-restricted token validities are enforced correctly.
- The integrity of system time should be checked regularly to detect any tampering with time settings.

7.2.2 Future Work

- Scalability and dependability methods for identity federation.
- Privacy preserving accountability (related to privacy-preserving audit)
- Thus the topics of 'Accountability', 'Integrity' and 'Resilience' need to be addressed in future projects in identity federation.
- Accountability is at a tension with privacy and intractability requirements, highlighting open problems for research.
- Privacy-preserving accountability and integrity should be topics researched.
- Resilience as been neglected for too long.
- Future architectures need to include a focus on error cases, faults, errors and failures.
- Design identity federation with high resilience and fault tolerance.
- Infuse identity federation research with insights from dependability, fault-tolerance.
- Create dedicated research for high resilience against adversarial influence on the overall system and components.

7.2.3 Audience/Stakeholders

- Academia
- Industry
- Policy makers to establish focus on resilience.

7.3 Privacy

We first provide a discussion of a scenario with multiple, specialized brokers that can improve privacy. This scenario was not used in the FutureID pilots, however it illustrates the potential of the architecture. We follow the discussion up with a review of the privacy evaluation process, the presentation of the lessons learnt, and some recommendations.

7.3.1 Utilization of Multiple Brokers

At the core of the FutureID Reference Architecture lies the central design decision to allow for utilization of multiple brokers. Moreover, the choice and arrangement of these brokers is controlled by the user with support from a local or remote software component. This central design decision has caused a large amount of discussion among the FutureID project partners which was analysed in detail in D.12.4, section 7.1.1.5. As can be seen from these discussions, the approach of utilizing multiple brokers in a single authentication process, especially when arranged according to the choice of the concerned user herself, needs to be analyzed in depth, way beyond the results that were achievable within the scope of the FutureID project.

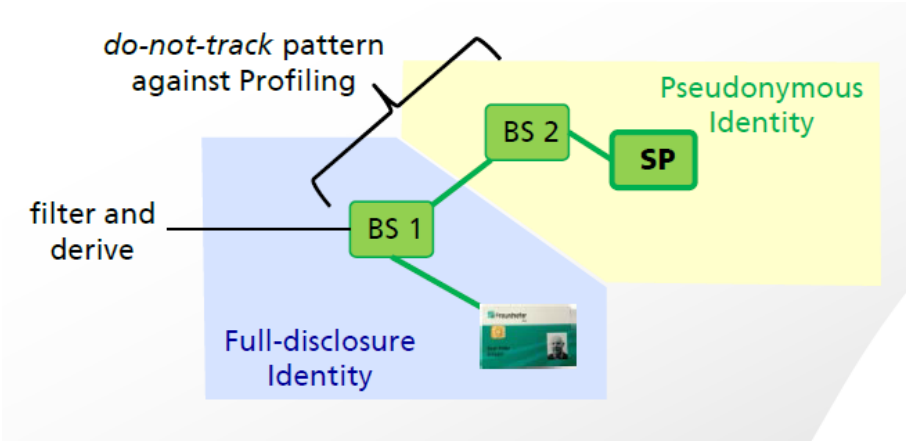

Figure 1: The Federated Identity Do-Not-Track Pattern against Profiling.

An early discussion on benefits and issues with the flexibility of this design decision in the FutureID Reference Architecture can be found in FutureID deliverable 12.4: Privacy Evaluation, which also outlines the so-called Do-Not-Track-Pattern approach to the utilization of multiple brokers (cf. Figure 1). What can definitely be said given the results from the FutureID project is that the flexibility introduced by the utilization of multiple brokers definitely has the potential to be used in both ways: for good and for bad. The discussion on this issue was intensified by the current developments on the legal basis of authentication of human individuals in Europe, e.g. based on the eIDAS regulation (see below). **Here, the concept of utilizing multiple brokers is considered superior to existing authentication infrastructures with centralized, single broker services**. This observation is also inline with the socio-economic

perception of the landscape of identity management systems, which does see potential for a market of identity broker services in Europe. Moreover, existing identity management systems, e.g. within major companies, can be utilized as brokers in a FutureID environment and context, which is not directly feasible with any of the well-known pan-European identity and access management infrastructures of today. As a general result, it was identified within the FutureID project's discussions on the Reference Architecture that additional efforts are required in order to understand the impact and consequences of different use cases of the FutureID Reference Architecture. These efforts range over all of the FutureID requirements domains, i.e. concerning technical, security-related, privacy-related, socio-economic, usability-related, legal, and accessibility-related research questions.

(Semi-)Automated Support of Data Minimization and Attribute Derivation Along with the flexibility in terms of the FutureID Reference Architecture comes its ability to include attribute-filtering and attribute-deriving broker services. In such scenarios, the authentication tokens issued by the identity provider (e.g. stored on the eID token) contain more information than are necessary at the service provider. In other authorization contexts, this would always lead to the service provider learning about those additional attributes of the human individual without the need to do so. Here, the FutureID Reference Architecture allows for utilization of a feature of FutureID broker services: **attribute filtering and attribute derivation**. Attribute filtering refers to the technique of an identity broker receiving an authentication token with many attributes, then selecting a subset of these attributes (according to what the service provider needs to know), and issuing a new authentication token (with the FutureID broker service being the issuer) that contains only the required attributes. Hence, in such a scenario, all other information from all other attributes is filtered out before the authentication token is disclosed to the service provider. Attribute derivation goes beyond pure attribute filtering, as it refers to the technique of generalization of attribute values. Similar to common anonymization techniques, attribute derivation techniques take precise attribute values (like location, birthdate, etc.) as input, and derive information from these attributes that exactly match the corresponding information needs of the receiving side (i.e. the service provider). For the example of location, such attribute derivation may take GPS coordinates as input, and derive the country (and thus legislational context) of the user as output, sent to the service provider. Similarly, attribute derivation may be used to decide whether the user is over 18 years old, based on the information of the exact birthdate. Both attribute filtering and attribute derivation allow for strong implementations of the principle of data minimization, which is a key requirement in both security and privacy domains, and also often plays a major role in business-to-business interactions. Here, the FutureID project was one of the first that identified the capabilities of such attribute filtering and attribute derivation techniques, and hence we consequently embedded the use of these techniques into all of the FutureID artifacts. However, during the project phase, we identified a lot of open issues associated with the utilization of attribute filtering and attribute derivation techniques in real-world contexts. For instance, the use of unique identifiers in authentication tokens allows for linkability of attributes to a degree that may render the whole idea of attribute filtering useless, e.g. if the authentication token can be linked to an existing dataset at the service provider that already contains the same attribute values that should have been protected. Moreover, it is not yet clear what approach is best to match the

attribute information needs of the service provider with the attribute disclosure incentives of the user and the technically typically fixed attribute disclosure policies of the identity providers. Here, many different scenarios arise, ranging from an empty set of policy options (e.g. if the information needs of the service provider directly collide with the confidentiality needs of the user) to a huge set of viable authentication options, in which case the problem of selection of optimal authentication plans arises. In this context, the FutureID project has come up with an early analysis and a set of strategies, as is described in the FutureID Reference Architecture documentation of the Solver&Executor component, yet we identified a set of open challenges associated with the use of this component that could not be addressed properly within the scope of the FutureID project. Here, additional efforts in terms of analysis of different scenarios and policy options is required in the future.

7.3.2 Specific evaluation

The challenge of the privacy and data protection work in FutureID was the asynchronous activities that were taken place in distributed design, development and integration all over the project. Resulting from the evaluation and the intense discussions with designers, developers, domain experts and evaluators, we came to the overall conclusion that FutureID components can be configured to support scenarios and business models with strong respect for end user privacy. However, in the evaluation work that was supposed to connect the requirements to architecture, implementation and pilot applications, we ran into a number of dilemmas and difficulties. On architecture level, many of the important data protection questions from the legal and the PET domain were undecidable due to the architecture's generic approach independent from particular business models and roles. While the components and architecture provide flexibility to implement strict privacy regimes with FutureID, the chosen demonstrators and their underlying scenarios where not requesting and therefore not taking in use much of FutureID's potential. **As the architecture and component level is implemented very flexible, we are convinced that it can be used to implement state-of-the-art privacy**. However, the particular use case, component integrator and operator will have to configure and implement for high privacy to reach this goal. Hence follows the objective below from this experience.

Objective/Requirement

- Prepare documentation for privacy evaluation including business model and stakeholder roles

To enable the evaluation of all requirements, a particular business case has to be specified both on the administrative/legal and the technical level. Stakeholders, their specific roles with respect to the Data Protection Directive, their handling of personal information in relation to the business model, and their particular implementation ideas including a specification of the technologies to be used are necessary for a complete evaluation round.

We must, in addition, conclude that the available budget for project-internal evaluation did not accommodate for in-depth analysis of the 150 privacy requirements against all pilots. Should

a combined legal/privacy analysis succeed, the project must rely on the submission of highly standardized contracts, service level agreements, and policies.

Lessons Learnt During development, the specific business configuration of the FutureID components were not yet defined. However, a large number of the privacy requirements need documentation about the particular business configuration, legal roles, and business practices of the participants in an application of FutureID.

In addition, the integration of existing background from pre-FutureID development proved to create further challenges, as such components were not developed with the FutureID privacy requirements in mind. In future projects, it is strongly recommended to include a project milestone "Evaluation of background technology" into the project plan. This should happen before any new components or specifications based on background components are performed.

Recommendations

- Document very well from the beginning of any FutureID application/exploitation project the business configuration, the stakeholder roles, contracts and policies that establish the business using FutureID components!
- Include a real-world application subproject with a well-specified pilot from the beginning!
- Check background technologies against the project's objectives and the project's internal requirements!
- Seek exploitation projects for FutureID that have a strong privacy focus to demonstrate the architecture's potential!
- Develop and use highly standardized contracts, service level agreements, and privacy policies that accommodate evaluation and reduce complexity!

Future Work

- Legal: develop contractual framework.
- Privacy: Develop catalog of best-practice configurations based on "top 10 business models"
- Technology: Develop default configurations with explicit support for best-practice configurations.

Audience/Stakeholders Audience: FutureID core vendors/developers. FutureID future users/customers. Supervision and certification authorities.

7.4 Usability

One of the objectives of FutureID involved building a user-centric identity federation system on European Scale that provide user support for privacy. The usability lessons concerns specific evaluation lessons, user support related to privacy requirements and project organisation to facilitate testing

- Project Management: Final deadlines for technical work should be earlier than evaluation, to ensure readiness of the technical developments. A constantly stable, integrated, running versions of the client in a certain environment should be ensured, to be able to test things at all times.
- A user-centric HCI process that foresees two more iteration circles for testing the system with end users (could be mockups) and incorporates the Usability and User Experience assessment for the service side (i.e. being a client of FutureID).
- Defining real world/situational scenarios such that we can anticipate more real use cases apart from the Pilots. I addition, as much real and realistic information as possible (e.g. about privacy statements, etc.) would be an advantage.
- eID systems need to adopt a user-centric privacy-by-design infrastructure with user-centric protocols that provides privacy goals of unlinkability, transparency and intervenability.

Specific Recommendations for Future Systems

- Create information material around eID systems: e.g. Tutorials or short Videos on accompanying websites, explaining the general idea behind FutureID. Users would expect this information, but rather not directly in the client (apart from first usage). Furthermore it should be available without the need to install software. This would even more create understanding about FutureID and facilitate further usage. This also involves investigating user understanding of information provided to them and how to translate the information in a format the user understands and that is that matches their models of privacy.

- Future Systems should identify and tackle a broad range of Use Cases that can be later evaluated with users. During usability Tests users often said, that they were willing to use such systems, only if the service and benefit would be worth it. Simple, uncritical (in terms of security) use cases were not seen to be worth the effort of going beyond existing solutions. Some of the mentioned services were government services, contracts, and online payments – things that now require postal communication, access in person or other special considerations.

7.5 Socio-Economic

The challenge identity management and eID solutions are facing is that the market for this technology is a multi-sided market. The utility for all participants of eIDs partially depends on the adoption by agents on the other side, which is caused by indirect network effects with

positive feedback: if more users adopt an identity management system, more services will adopt, and the other way around.

In order to utilise 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 considered the interests of all the stakeholders involved in the eID ecosystem to facilitate economic conditions for wide take-up of its results.

Ultimately, a FutureID ecosystem shall be viable for all stakeholders involved to support the creation of the ecosystem. Consequently, FutureID seeks to offer low ecosystem entry costs and to provide benefits to all stakeholders involved in the eID value chain. Hence, the FutureID socio-economic requirements ask for the support of

- different business cases and forms of revenue generation,
- various (mobile) deployment models,
- interoperability, platform independence, and global applicability,
- value-add for all stakeholders (revenue, cost savings, usability, security or privacy benefits), and
- price differentiation.

The FutureID socio-economic evaluation has shown that the FutureID reference architecture fully satisfies the socio-economic requirements.

7.5.1 Recommendations

- Socio-economic viability should be a key concern for future identity federation systems. This recommendation is rooted in the network effect and the necessity to read critical mass to build an ecosystem with a positive network effect. This entails keeping the cost for early adopters low and offering benefits for all stakeholders involved.
- The requirements expressed for the FutureID reference architecture should be a benchmark for new systems. FutureID has proposed a set of socio-economic requirements that support ecosystem creation and shown that these requirements can be realised in a reference architecture. Hence, this research should inform future identity federation research projects as well industry deployments.
- The actual impact of the requirements on socio-economic ecosystems asks for further investigation and quantification as future work. At this point, we don't know yet, which of the requirements put forward by FutureID impact the adoption and ecosystem creation to what extent. FutureID advocates to include research work packages in future identity federation projects to investigate these factors quantitatively.

7.6 Legal

In a research project, the lawyers' role hardly can go beyond general recommendations and guidance whether a certain technique/application is compliant to the existing legal framework (or where the trouble begins). In a final deployment many additional legal requirements might arise. These requirements depend on the exact deployment, including how, to whom, and where an online service or a technical component will be deployed, which at the beginning and even during the project (except if a project would have a very limited and specific focus including the country and service, unlike FutureID) cannot be assessed. We propose general recommendations followed with specific ones emerging from evaluations

- For future projects it might be beneficial to decide upon a 'most likely' use case how the technology might be deployed, including concrete countries, stakeholders, etc., which then can be completely assessed from a legal perspective. This would lead to a concrete result instead of mainly highlighting legal challenges and questions and discuss theoretical consequences, without being able to answer them fully.
- When drafting legal requirements, this should be done separately for the different levels of evaluation. In FutureID, the architecture, the implementation and finally the pilots were evaluated separately. However, legal requirements that are applicable to all these stages of development are hardly thinkable. Therefore it is recommended to draft specific legal requirements for each artefact. Especially for architecture (and maybe implementation). Privacy by Design might be considered a requirement (e.g. based on art. 12 (3c) eIDAS Regulation for interoperability framework or the principle of data protection by design included in the draft General Data Protection Regulation). However, this could result in a significant overlap between the legal and the privacy evaluation and should be coordinated accordingly.
- Another role can be to bring newly developed techniques to the minds of those who make the political decisions; typically the law is referring to "best available" or "state of the art" techniques. However, the technical development is comparatively fast and a "state of the art" of today can cause the security breach of tomorrow. Research projects – and especially lawyers in research projects – have the potential to bridge between policies and technical development, and thereby help to make improved technology known to and used by a broad public – in consequence: help to make it become "state of the art".

8 Research Implications

This section details our research progress in WP2.4 and its implications for the future in particular how theoretical and scientific findings can be used.

8.1 Compositional Reasoning

FutureID sought to establish a reasoning over the compositionality of cryptographic and security protocols and more generally languages and tools that allow the analysis of complex systems that are composed of multiple components. In scientific terms this yielded two relative soundness results or typing and parallel composition. The research in Task 24.1 is complemented by the development of the Authentication Protocol Specification (APS) Language. The task showed feasibility of compositional reasoning, provided the first consideration of formats in formal models of security protocols, showed compositionally for protocols relevant for eID, such as Extended Access Control, and investigated vertical protocol composition for multiple layers of security and application protocols.

8.1.1 Recommendations

As recommendations we propose

- Further research into compositional reasoning.
- To be extended to include the identity federation standards as well.
- Extend composition from protocols to systems.
- Include a systems-of-systems methodology.

8.1.2 Future Work

- Formal verification for entire identity federation systems and their protocols.

8.1.3 Audience/Stakeholders

- Academia
- Industry to pick up tools

8.2 Methods and Languages for Privacy Goals

A research objective of FutureID was to establish methods and language for the analysis of privacy goals with formal methods, as alternative to established methods such as differential privacy or k-anonymity. The work by DTU and UNEW with King's College London on alpha-beta privacy showed that new approaches to reasoning over privacy goals are possible. This

methodology is applied to the FutureID architecture. Further, the concepts of privacy-preserving attribute-based credentials were unified and complemented with a language framework and formal semantics to describe the effects of their transactions.

8.2.1 Recommendations

- The research in FutureID suggests that further research should be pursued to explore mechanised reasoning over privacy properties.
- The consequences of the user's and service provider's actions over time on the user's privacy are extremely hard to predict. Formal methods techniques can help there.
- There is the possibility that big data techniques could be turned on the problem of privacy-implications of (extrapolated) actions.

8.2.2 Future Work

- Alpha-beta privacy is a promising primitive that asks for further investigation.
- Research into privacy implications of actions of multiple-actor systems of systems.
- Risk analysis for long-term privacy risks.

8.2.3 Audience/Stakeholders

- Academia

8.3 Privacy-Preserving Audits

Task 24.3 investigated privacy-preserving audit and data handling methods, early activities focused on audits themselves, which included new mechanisms on graph signatures and topology certification. Later activities included data handling in the sense of how data is managed by the service provider. This involves authentication, signatures and computations on signed data. Furthermore, this task included a new threshold password-authenticated secret sharing protocol and efficient constructions for blind signature schemes. This research further involved design strategies for a privacy-preserving Austrian eID system. Altogether, the privacy preserving audit and data-handling research area has proven very fruitful.

8.3.1 Recommendations

Privacy-preserving audit and data handling seemed like an area with potential that vouches for further investigation. Based on the recommendations from the security evaluation, we further recommend to establish further research to overcome the tension between privacy and accountability. This recommendation is rooted in the need of identity federation systems to account

of authentications for liability purposes, however, therein lies a privacy risk of profiling and tracking of the users. Hence, we recommend to investigate privacy-preserving accountability.

8.3.2 Future Work

- Investigate privacy-preserving accountability.

8.3.3 Audience/Stakeholders

- Academia

8.4 Privacy-Preserving Revocation

Task 24.5 was to establish multiple privacy-preserving revocation mechanisms. Those are crucial to enable privacy-enhancing authentication methods, such as anonymous credential systems, and be able at the same time to revoke lost or stolen credentials. FutureID proposed a new privacy-preserving revocation mechanism for attribute-based credentials that allows the system to effectively handy multiple revocation lists. This study further includes the enabling primitive of cryptographic accumulators. Furthermore, FutureID proposes means to use epochs to gain a balance between practical revocation and reasonably strong privacy guarantees.

8.4.1 Recommendations

FutureID made advances to the field, yet privacy-preserving revocation remains a daunting topic. We recommend to pursue further research on this topic to seize the ultimate prize of a privacy-preserving revocation scheme that works on a European scale and can accommodate the likely revocation rates of such a system.

8.4.2 Future Work

- Large-scale privacy preserving recommendation systems with high revocation rates.
- Research in alternative mechanisms to revocation, apart from dynamic accumulators and epochs.

8.4.3 Audience/Stakeholders

- Academia

8.5 Usable Privacy

An objective of FutureID was establishing human dimensions of security and privacy in relation to identity federation in the widest sense. Within our research, we investigated of cognitive and affective factors as well as personality traits on security decision making. This showed cognitive effort requirements of privacy decisions, showed impact of cognitive depletion and traits on password choice. We elicited user models of privacy and observed the influence of affect (expressed or observed emotions) in user models of privacy vs. sharing. We also assessed the feasibility of psycho-physiological measurement methods for security and privacy. Furthermore, we have designed a two-factor authentication scheme for usable server-based eID and signature solutions, based on a challenge-response approach

8.5.1 Recommendations

- Human dimensions are crucial for security and privacy of identity federation because they have a high impact on decisions and behaviour and need further research.
- Need more research in evidence-based methods in human dimensions of security and privacy. There is currently a gap in rigorous, reproducible and re-usable components in the area and foremost requires foundational research.
- Support research for cognitive, affective and trait aspects of security and privacy as these human states are seen to influence decisions and place users in a vulnerable state.
- Infuse usable privacy with psycho-physiological measurements and eye tracking which provides a complement to self-reports that depends on user interpretations.

8.5.2 Future Work

As future work we propose investigation of:

- What influences the user's trust in an identity federation system?
- What human dimensions make a difference for the usability of privacy-enhancing technologies?
- How can PETS and identity federation systems be designed accounting for those human factors?
- How to to make usable privacy and security a dialogue between systems and users rather than a monologue?

8.5.3 Audience/Stakeholders

- Academia
- Industry to pick up recommendations on policies

9 Recommendations

While FutureID has produced mature products for smaller-scale identity management that can be sustainably exploited by Partners, **arguably its most important result** is probably its architecture and **unique experience of very large-scale identity management**. This experience distinguishes itself with unprecedented, potentially global, scalability. In comparison to pilot projects of the U.S. NSTIC initiative that were all limited in scale, FutureID attempts to provide the flexibility and scalability to reach much further; in comparison to STORK, FutureID provides the characteristics necessary for private-sector uptake, supports all potential current and future credentials, and avoiding central control or agreements, can scale well beyond the boundaries of Europe.

This most precious result of FutureID, due the current lack of a market that can sustainably support it, requires support by policy makers in order to be exploited to its fullest potential. Different kinds of support actions are described in the following:

- FutureID technology has already be included in the **eSENS** large scale pilot as part of the epSOS e-health component. But this does not cover all components of FutureID that are necessary for its approach to very large-scale identity management. Most importantly it doesn't include the mature broker service component that is, as determined by the DoW, a proprietary component owned by a project partner. The FutureID projects has however produced less mature open source implementations of all components, including the broker service. eSENS's mandate to render components more mature for later use in CEF could very well be applied to **bring the open source version of all components to an operational level of maturity**. This work item could be seamlessly integrated into the extension of eSENS that is currently being discussed and without the need to add additional partners to the eSENS consortium since the existing partner Fraunhofer-Gesellschaft is also copyright holder of these open source FutureID components. The resulting open source implementation is a prerequisite for several of the following recommendations.

- The main identity management component in **CEF** is STORK. We propose that **FutureID is a necessary complement to STORK** to deploy an interoperable identity management solution in all strategically important sectors. In particular, the **integration of FutureID as an complementary identity management component in CEF** would, among others, identity-enable the following sectors:
  - **e-Health**: While several member states issue electronic health professional cards and/or electronic health cards to their citizens, these are unlikely to be notified within eIDAS and thus be supported by STORK. Since interoperable use of health-related electronic identities is crucial to applications such as epSOS, FutureID would be an ideal solution to bring Europe-wide interoperable management of health-related identities.
  - **private-sector** uses: Certain private-sector players, such as banks, have a strong need for secure and trusted identities and are therefore ideally suited to use eIDs via STORK. Since their need predates the availability of STORK however, and to cover

customers not in possession of some notified eID, these private-sector players have typically already rolled out their own identity tokens. A simple replacement of this existing solution with STORK is not possible, since it would disrupt service for the existing user base. These private-sector players will therefore only take up STORK if it comes with an vehicle to support the existing electronic identities in parallel. FutureID is an ideal vehicle for this need since it can support arbitrary credentials and already integrates STORK.

- FutureID has conducted pioneer work with its **multidisciplinary** team designing a **solution for very large-scale identity management** that integrates a wide range of viewpoints. Particularly non-technical viewpoints like socio-economic aspects, legal aspects, privacy-aspects, usability and inclusion received ample attention. All these points of view were integrated in a shared vision across participating disciplines and were formalized in the FutureID architecture that was created in several revisions until all major concerns were satisfied.
  This multidisciplinary work **identified remaining gaps** between the current implementation of FutureID and the demanding needs of very large-scale identity management. Since not foreseen in the DoW, resources were insufficient to fully implement these unforeseen items within the project. **FutureID has already conducted research** and where possible even implemented research prototypes **to better understand these remaining issues** and specify in detail how the remaining gaps have to be filled.
  In this context, we **recommend to support the necessary work to close these few remaining gaps and thus significantly increase the overall value** and obtain a system with full support of the stringent requirements of very large-scale identity management.

- **Arguably, the FutureID architecture and implementation define the cutting-edge in very large-scale identity management**. In particular, we believe to have been the first initiative to find ways to achieve certain key characteristics that are for example (i) necessary to deploy such a system interoperably also in regions beyond Europe or (ii) to be attractive in private-sector business environments. An example for such a characteristics is the absence of central components or control--a prerequisite for the acceptance in more than one region (e.g., North-America); another example the "self-configuration" of the FutureID infrastructure without the need of registration or approval--a prerequisite to attract private-sector investments by avoiding risky dependency on third parties.
  Very large-scale identity management is inherently a global problem and no single regional solution will be able to survive in isolation. To fully exploit the potential of FutureID's pioneering work, its results have to be promoted beyond Europe and contribute to a common solution that involved other regions.
  We therefore **recommend to support the promotion of FutureID results beyond the borders of Europe**. The following illustrates how this could be done with the United States:

  – The United States, like Europe, perceives very large-scale identity management as a key enabler for societal and economic development.

  - Through the NSTIC initiative and other efforts, this topic already receives ample attention.
  - Initial verifications show a significant interest by the United States to discuss a common vision and conceptual framework for very large-scale identity management with Europe.
  - The FutureID experience represents an ideal basis for contributing to a common vision and conceptual framework.
  - We therefore recommend to exploit this current interest and **support the creation of an adequate forum between the United States and Europe to create a common vision and conceptual framework for an interoperable large-scale identity management across these regions**.
    * This could prepare for a later joint standardization of these concepts and corresponding architectural components.
    * The open source implementation of FutureID may be a suited vehicle to prototype and verify such a standard.

- FutureID represents a high potential for private-sector identity management, typically in combination with STORK that provides support of government notified eIDs. We recommend to **support an explicit effort to promote the uptake of FutureID/STORK in the private sector**. This could include the following actions.
  - Provide an off-the-shelf open source distribution of FutureID and STORK components, including the necessary promotional and training resources, that is specifically geared to the needs of private-sector players. This could for example, be done in CEF (see above).
  - Identify high-profile champions where this solution can be verified, improved, and fine-tuned.
  - Support the first high-profile private-sector players to deploy this FutureID/STORK solution and thus create success stories.
  - Use these success stories for promoting general uptake of the solution in the private sector.

10 Roadmap

FutureID has been highly successful and has produced a lot of important results. The following describes steps necessary to roll out a Europe-wide identity management system in support of the single market of services based on FutureID results.

- For a large-scale uptake across business sectors, provision of an **open source reference implementation of all FutureID components** is crucial. In accordance with the DoW, some major FutureID components such as the broker service have been implemented as proprietary solutions. Beyond the DoW, FutureID has also produces less mature open source versions of all components. To evolve them to an operational maturity level and render them downloadable from the FutureID portal would be a major milestone in the general rollout of FutureID in the large-scale identity management market.
  Among the benefits of an open source version of all FutureID components are the following:
  - independence of a single vendor / competition
  - easy systems integration
  - easy extension to meet specific needs (such as broker backends for yet unsupported federation dialects)

- **Fill the few remaining gaps to fulfill the requirements specific to very large-scale deployments**. (See Section 4). Examples for these gaps include the following:
  - Support for full accountability that is an enabler for liability management in large-scale situations where several actors could be responsible for wrong doing in a single transaction.
  - Support for privacy-by-design as protection for European citizens and mitigation of large-scale tracing and profiling.
  - An identity selector strategy that remains easy to use in presence of a massive number of potential credentials.
  - An identity selector that informs user about privacy implications of their choices in an easily understandable and usable way.

- To further ease large-scale rollout, a formal and desirably **international standardization** of all FutureID components will provide the following benefits:
  - Significantly increase acceptance by the various stakeholders.
  - Facilitate commercial software vendors to offer proprietary implementations of FutureID components.
  - Foster acceptance of FutureID beyond the boundaries of Europe.

- Build a **European community to support FutureID** beyond the current consortium. This community shall support the roll-out of FutureID/STORK solutions and govern its further development. The community includes the following groups of stakeholders:

  - Public and private-sector service providers
  - Commercial software vendors and integrators
  - An open source community in support of the open source reference implementation

- **Integrate the FutureID experience and results into a global vision of interoperable large-scale identity management**. This requires the involvement of key extra-European stakeholders.

- **Support first high-profile deployments of the technology** addressing:
  - service providers who need to support additional credentials in addition to those supported by STORK
  - academic networks such as Geant with its eduroam
  - meta-federations in fields such as banking or automotive operated by existing organizations dealing with inter-banking issues or industry-wide data and trust networks.

- Encourage uptake by software industry and integrators to implement the FutureID standard in commercial products

- Establish **privacy-preserving and highly resilient identity federation research** to complement the FutureID Framework. This research shall enable key ingredients for for future identity federation systems:
  - advanced privacy-preserving accountability, integrity of all FutureID components, and high resilience against adversarial action.
  - full integration of privacy-enhancing attribute-based credentials towards end-to-end privacy-by-design.