Gesellschaft für Informatik e.V. (GI)

publishes this series in order to make available to a broad public recent findings in informatics (i.e. computer science and information systems), to document conferences that are organized in cooperation with GI and to publish the annual GI Award dissertation.

Broken down into
- seminars
- proceedings
- dissertations
- thematics

current topics are dealt with from the vantage point of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure high quality contributions.

The volumes are published in German or English.

Information: http://www.gi.de/service/publikationen/lni/

ISSN 1617-5468
ISBN 978-3-88579-658-9

Open standards and interfaces as well as open source technologies play a central role in the current identity management landscape as well as in emerging future scenarios such as Internet of Things enabled healthcare and global infrastructures for trust management. While there are already plenty of successful applications in which those techniques are used to safeguard the authenticity, integrity and confidentiality, there are still many closely related areas which demand further research. The aim of the "Open Identity Summit 2016" is to link practical experiences with academic innovations. Focus areas of this event are research and applications in the area of Identity Management, Policy Implementation, Privacy by Design, Trust Services, and Mobile ID.

D. Hühnlein, H. Roßnagel, C.H. Schunck, M. Talamo (Eds.): Open Identity Summit 2016

264

GI-Edition

Lecture Notes in Informatics

Detlef Hühnlein, Heiko Roßnagel,
Christian H. Schunck, Maurizio Talamo (Eds.)

Open Identity Summit 2016

der Gesellschaft für Informatik e.V. (GI)

13.–14. October 2016
Rome, Italy

Proceedings

Detlef Hühnlein, Heiko Roßnagel,
Christian H. Schunck, Maurizio Talamo (Eds.)

Open Identity Summit 2016

13. - 14.10.2016
Rome, Italy

Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-264

ISBN 978-3-88579-658-9
ISSN 1617-5468

Volume Editors
Detlef Hühnlein
ecsec GmbH
Sudetenstr. 16, D-96247 Michelau, Germany
detlef.huehnlein@ecsec.de
Heiko Roßnagel
Fraunhofer Institute for Industrial Engineering IAO
Nobelstr. 12, D-70569 Stuttgart, Germany
heiko.rossnagel@iao.fraunhofer.de
Christian H. Schunck | Maurizio Talamo
Fondazione Universitarià INUIT – Tor Vergata
Via Orazio Raimondo 18, 00173 Rome, Italy
{christian.schunck|maurizio.talamo}@inuitroma2.it

printed by Köllen Druck+Verlag GmbH, Bonn

Preface

Welcome to the "Open Identity Summit 2016" (OID2016), which has been jointly organized by the special interest groups BIOSIG within the German Informatics Society (Gesellschaft für Informatik e.V. (GI)), the EU-funded FutureID project, the Open eCard project, the SSEDIC.2020 initiative, the PICASO project, the LIGHTest project, the FutureTrust Project, and last but not least by Fondazione Universitarià INUIT Tor Vergata.

The international program committee performed a strong review process according to the LNI guidelines. At least three reviews per paper and 47 percent accepted papers of the 21 submitted papers as full scientific papers guarantee the high quality of presentations. These proceedings cover the topics of ecosystems and architectures for digital identity, mobile electronic identity, trust services, open source, and cloud and data management.

Furthermore, the program committee has created a program including selected contributions of strong interest (further conference contributions) for the outlined scope of this conference.

We would like to thank all authors for their contributions and the numerous reviewers for their work in the program committee.

Rome, October 2016

Detlef Hühnlein
ecsec GmbH

Heiko Roßnagel
Fraunhofer IAO

Christian H. Schunck
Fondazione INUIT

Maurizio Talamo
Fondazione INUIT

Conference Chairs

Detlef Hühnlein, ecsec GmbH
Heiko Roßnagel, Fraunhofer Institute for Industrial Engineering IAO
Christian H. Schunck, Fondazione Universitarià INUIT Tor Vergata
Maurizio Talamo, Fondazione Universitarià INUIT Tor Vergata

International Program Committee

Franco Arcieri, Italy
Moez Ben MBarka, France
Arslan Broemme, Germany
Bud Brügger, Germany
Christoph Busch, Germany
Victor-Philipp Busch, Germany
Andrea Caccia, Italy
Jörg Caumanns, Germany
Juan Carlos Cruellas, Spain
Roger Dean, United Kingdom
Jos Dumortier, Belgium
Simone Fischer-Hübner, Germany
Lothar Fritsch, Germany
Jens Fromm, Germany
Walter Fumy, Germany
Igor Furgel, Germany
Robert Garskamp, Netherlands
Ulrich Greveler, Germany
Thomas Gross, United Kingdom
Marit Hansen, Germany
Olaf Herden, Germany
Oliver Hinz, Germany
Gerrit Hornung, Germany
Moritz Horsch, Germany
Detlef Houdeau, Germany
Detlef Hühnlein, Germany
Tina Hühnlein, Germany
Klaus Junker-Schilling, Germany
Jan Jürjens, Germany
Ulrike Korte, Germany
Michael Kubach, Germany
Andreas Kuckartz, Germany
Raik Kuhlisch, Germany
Andreas Kühne, Germany
Sebastian Kurowski, Germany
Herbert Leitold, Germany
Peter Lipp, Austria
Luigi Lo Iacono, Germany
Johannes Loxen, Germany
Milan Markovic, Serbia
Tarvi Martens, Estonia
Gisela Meister, Germany
Daniela Merella, Italy
Axel Nennker, Germany
Alexander Nouak, Germany
Sebastian Pape, Germany
Sachar Paulus, Germany
René Peinl, Germany
Henrich Pöhls, Germany
Kai Rannenberg, Germany
Alexander Rossnagel, Germany
Heiko Roßnagel, Germany
Carlos Sanchez, United Kingdom
Aleksandr Sazonov, Russia
Ivonne Scherfenberg, Germany
Christian H. Schunck, Italy
Steffen Schwalm, Germany
Jörg Schwenk, Germany
Jon Shamah, United Kingdom
David Simonsen, Denmark
Maurizio Talamo, Italy
Don Thibeau, United States
Thomas Uhl, Germany
Tobias Wich, Germany
Thomas Wieland, Germany
Alex Wiesmaier, Germany
Jan Zibuschka, Germany
Jan Ziesing, Germany
Frank Zimmermann, Switzerland

Invited Speakers

Robin Wilton, United Kingdom

Partners

BIOSIG – Biometrics and Electronic Signatures (http://www.biosig.org/)
The special interest group “Biometrics and Electronic Signatures” (BIOSIG) within GI e.V. is dedicated to the fundamentals, methods, techniques, processes and implementations used to guarantee the authenticity and integrity of entities.

SSEDIC.2020 (http://www.ssedic2020.com/)
The objective of SSEDIC.2020 is to provide a platform for all the stakeholders of eID (electronic identity) to work together and collaborate. SSEDIC.2020 builds on the success of the EU funded SSEDIC thematic network.

FutureID Project (http://www.futureid.eu/)
The EU-funded FutureID project builds a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infra-structure for Europe, which integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims.

Open eCard Team (http://www.openecard.org/)
The Open eCard Team is an open community, which aims at providing an open source and cross platform implementation of the eCard-API-Framework (BSI-TR-03112) and related international standards such as ISO/IEC 24727 and OASIS DSS through which arbitrary applications can utilize authentication and signatures with arbitrary smart cards.

PICASO Project – (http://www.picaso-project.eu)
The PICASO project aims to develop an ICT platform which will support the coordination of care plans across different sectors for people diagnosed with co-occurring chronic diseases. The PICASO platform is a service oriented, ICT based integration platform based on dynamic and personalized orchestration of care services. The method for sharing patient information between all relevant formal and informal care providers is by using a unique, trust federated solution, thereby overcoming the problem of data privacy in cloud based health systems.

LIGHTest Project – (http://cordis.europa.eu/project/rcn/203437_en.html)
The objective of LIGHTest is to create a global cross-domain trust infrastructure that renders it transparent and easy for verifiers to evaluate electronic transactions. By querying different trust authorities world-wide and combining trust aspects related to identity, business, reputation etc. it will become possible to conduct domain-specific trust decisions. This is achieved by reusing existing governance, organization, infrastructure,

standards, software, community, and know-how of the existing Domain Name System, combined with new innovative building blocks.

FutureTrust Project – (http://www.futuretrust.eu/)
Against the background of the regulation 2014/910/EU on electronic identification (eID) and trusted services for electronic transactions in the internal market (eIDAS), the FutureTrust project aims at supporting the practical implementation of the regulation in Europe and beyond. For this purpose, FutureTrust will address the need for globally interoperable solutions through basic research with respect to the foundations of trust and trustworthiness, actively support the standardisation process in relevant areas, and provide Open Source software components and trustworthy services which will ease the use of eID and electronic signature technology in real world applications.

Cooperation

Supported by

Gesellschaft für Informatik e.V.
http://www.gi.de/

Table of Contents

Open Identity Summit 2016 – Regular Research Papers

Open Identity Summit 2016 – Further Conference Contributions

Open Identity Summit 2016

Regular Research Papers

LIGHT^{est} -- A Lightweight Infrastructure for Global Heterogeneous Trust Management

Bud P. Bruegger[1], Peter Lipp[2]

Abstract: LIGHT^{est} is a project that is partially funded by the European Commission as an Innovation Action as part of the Horizon2020 program under grant agreement number 700321. LIGHT^{est}'s objective is to create a **L**ightweight **I**nfrastructure for **G**lobal **H**eterogeneous **T**rust management in support of an open **E**cosystem of **S**takeholders and **T**rust schemes. We show supported scenarios, motivate the necessity for global trust management and discuss related work. Then we present how LIGHT^{est} addresses the challenges of global trust management, its reference architecture and the pilot applications.

Keywords: trust management, trust decisions, trusted lists, global trust infrastructure

1 On Trust and Trust Decisions

There are many possible definitions of trust [Gefen]. In LIGHT^{est}, a trust decision determines whether a verifier should act on an electronically received transaction. This is illustrated in Figure 1a.

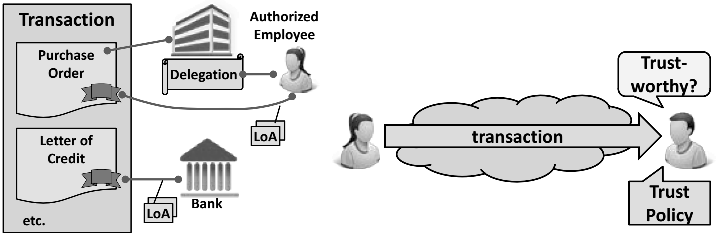


Figure 1: (a) The evaluation of trustworthiness of a transaction based on a trust policy, and (b) a prototypical transaction consisting of multiple parts and involving delegation.

A trust decision depends on the verifier's perception of risk, i.e. the probability and extent of possible damage and the availability of mitigation measures such as legal enforceability or insurance. This can be expressed in the verifier's trust policy.

Since verifiers often lack direct acquaintance of the partners involved in the transaction, they rely on authorities asserting their electronic identities as well as other trust-relevant

[1] Fraunhofer IAO, Identity Management, Nobelstr. 12, 70569 Stuttgart, bud.bruegger@iao.fraunhofer.de
[2] Technische Universität Graz, Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie, Inffeldgasse 16a, 8010 Graz, peter.lipp@iaik.tugraz.at

properties. These authorities manage *trust schemes* that assign Levels of Assurance (LoAs) to identities. Scheme information can, for example, be published in the form of a *Trusted List* (or Trust Status List) as defined, for example, by ETSI [ETSI16].

Figure 1b shows, by example of electronic trade, how a transaction involves multiple data records, each of them being associated with some identity[3]. For example, the purchase order in the figure is associated with the authorized employee who signed it; the letter of credit is associated with its issuing bank. The association can be either direct or indirect through a mechanism of delegation [Mod05] [Van09] [Eur09] [STO] [Lei14].

Trust in transaction data is derived from the LoA of the identities that are linked to the various records. The LoA of a single identity can be rated differently by different authorities issuing trust lists. It is important for a globally scalable trust infrastructure such as LIGHT^{est} that multiple, potentially conflicting perceptions of trust can co-exist and avoiding the need for all verifiers to share a single perception in order to participate.

It is up to verifiers to determine in their trust policies which trust schemes (lists) are to be applied. The trust policy also states the minimal levels of assurance required for each data record in order to consider the transaction trustworthy.

1.1 Different Trust Schemes for Different Aspects of Trust

Many real-world applications require a variety of trust schemes, focusing on different aspects of trust influencing the transaction risks. Examples include:

- **Identity-centric**: This type of trust, also addressed by eIDAS [eIDAS], focuses on the certainty that an electronic entity represents a certain legal entity. This identity-centric type of trust is the basis for legal validity and enforcement.
- **Reputation-centric:** This includes properties such as customer satisfaction ratings in “electronic shopping”.
- **Business-centric**: This includes properties such as credit ratings, the capital that is backing liability, etc. Business-centric ratings are often specific to a business area and/or a type of transaction.
- **Quality-centric**: This includes ratings of the quality of offered merchandize or services that is verified and certified by some authority.
- **Compliance-centric**: Compliance-centric trust schemes typically use Boolean levels of assurance (compliant/non-compliant) and include things such as compliance with regulations on the protection of personal data, compliance with export regulations, or the Italian anti-mafia certification.
- **Based on direct experience**: A trust scheme may also be based on direct experience with the transaction participants and could, for example, be expressed in the form of black- and whitelists.

[3] Such an association can, for example, be established by electronic signatures.

1.2 Types of Trust Schemes

To cater to different requirements of trust management, LIGHT^{est} supports a variety of different trust scheme types. They include the following: **(i) Boolean** trust schemes, for example indicating whether an issuer is **qualified**, **(ii)** Trust schemes using **levels of assurance** and **(iii)** Trust schemes certifying **arbitrary sets of attributes**.

While most common trust schemes and the data certified will be public, LIGHT^{est} technology can also be used for certifying potentially sensitive data through the use of **sensitive trust schemes**. They avoid linkability to the entities it describes and optionally supports selective disclosure of attributes under the control of these entities.

2 Previous and Related Work

LIGHT^{est} can be seen as an extension and evolution of the trust infrastructure of the now completed FP7 project *FutureID* [Fut][Bru15]. The following shows how LIGHT^{est} advances the state of the art:

2.1 Trust Lists

Probably the most common way to express trust schemes is in the form of signed trust lists. Among the best known are ETSI's TS 119 612 [ETSI16] with its update that is expected as basis for an eIDAS implementation act and SAML V2.0 Identity Assurance Profiles [SAML10] used, for example, by the Kantara initiative [Kan].

The direct use of trust lists by verifiers is very onerous. It is comparable to the direct use of certificate revocation lists that have been largely replaced by OCSP [RFC6960] providing a way to use simple queries of the status of individual certificates.

To use trust lists directly, verifiers are responsible for the following tasks: **(i)** Securely provision the list's trust anchor (the certificate used to validate the list's signature) and location, **(ii)** download the list, **(iii)** verify the list's signature, **(iv)** parse the list, **(v)** load the list data in some local storage that permits querying of individual entries, **(vi)** repeat some of the above tasks every time the list is updated or its trust anchor expires and has to be renewed. Since such a procedure is too cumbersome for normal verifiers, this complexity and responsibility will typically be offloaded to Validation Authorities.

LIGHT^{est} provides an alternative solution to Validation Authorities that is conceptually equivalent to that of OCSP: It enables verifiers to query individual trust list entries over the network at the authority who issued the trust list[4].

Figure 2 illustrates the difference between the direct use of trust lists by verifiers and the

[4] Or a trusted third party who publishes the trust list in representation of this authority.

much more convenient querying of trust list items through the LIGHT*est* trust infrastructure. It shows how the verification of the trustworthiness of a single certificate is managed in the two cases.

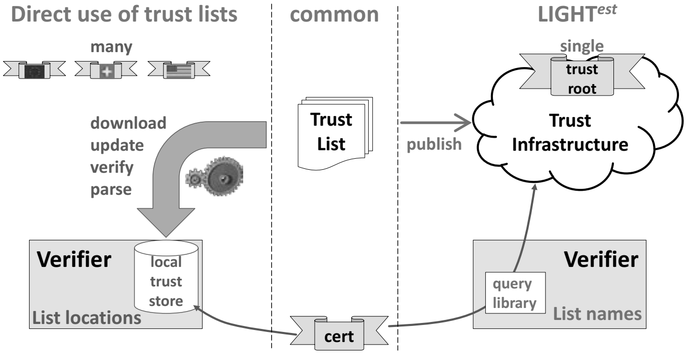


Figure 2: Comparison of direct use of a trust lists vs. the querying of a list item in LIGHT^{est}.

The following advantages of the LIGHT*est* approach are evident: A single trust root covers all current and future trust lists in LIGHT*est*, while verifiers need to provision and update one trust anchor per list in case of direct use. LIGHT*est* replaces the cumbersome tasks or setting up and continuously updating a local trust store with simple queries of list items.

2.2 Validation Authorities

Validation authorities (VAs) relieve verifiers from the burdensome management of trust lists. Prime examples are the VAs operated by member states for qualified signatures. Figure 3 illustrates how a VA interfaces between verifiers and trust lists, offering a query interface. Evidently, all verifiers share the same perception of trust.

Figure 4 shows the alternative approach taken by LIGHT*est*. Here, every trust list is rendered queryable through its publication in the LIGHT*est* trust infrastructure. Shifting the point of publication to the trust lists allows different verifiers to apply different perceptions of trust, i.e., different sets of trust lists.

Another difference between validation authorities and LIGHT*est* is also illustrated in these figures: In LIGHT*est*, verifiers send queries that are very small, typically a single network packet[5,] containing only a hash of the certificate to verify.

The LIGHT*est* approach is thus by several orders of magnitude more efficient in the required network resources and the possible response times. When planning for global scalability, such efficiency becomes important.

[5] DNS queries preferentially use a single UDP packet.

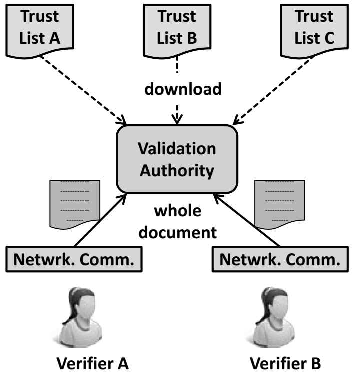


Figure 3: Validation authorities as interface between verifiers and trust lists.

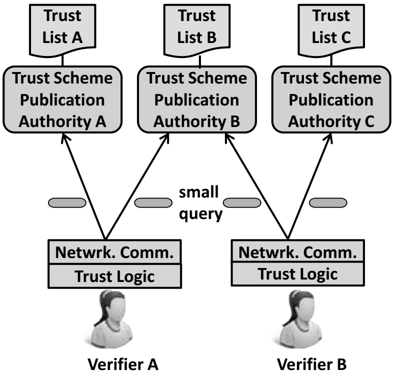


Figure 4: Different verifiers use different combinations of trust schemes as defined in their trust policy.

In many application areas, confidentiality and privacy may be a bigger issue than efficiency. For example, in the field of e-procurement, neither purchaser nor supplier may be willing to send the full data to a validation authority operated by a national authority. Since LIGHT^{est} offers the same convenience to verifiers as VAs without requiring access to signed documents, its range of application is much wider.

LIGHT^{est} avoids introducing intermediaries such that every involved stakeholder is directly responsible for the data it publishes. It is therefore better suited for cross-jurisdiction settings.

3 The European LIGHT^{est} Project

LIGHT^{est} is a project that is partially funded by the European Commission as an Innovation Action as part of the Horizon2020 program under grant agreement number 700321. Its start date is September 1, 2016 and its duration 36 months. The estimated project cost is 8.7 Mio Euros.

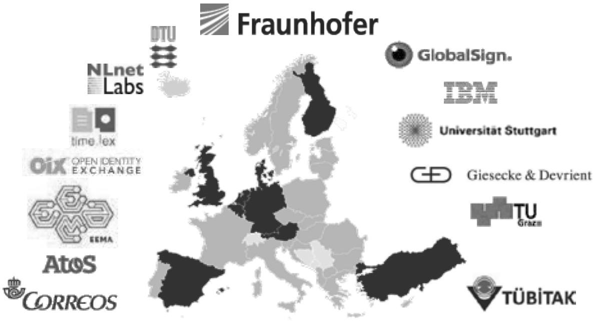


Figure 5: The LIGHT^{est} consortium.

The LIGHT^{est} consortium is consists of 14 partners from 9 countries, namely Austria, Belgium, Denmark, Finland, Germany, Spain, The Netherlands, Turkey, and the United Kingdom. The project is coordinated by Fraunhofer. The partners are shown in Figure 5.

Our objective is to build a global infrastructure. For this reason, the consortium of the EC-funded project includes the European branches of organizations that operate globally, namely the Open Identity Exchange and GlobalSign, IBM, and G&D. Further outreach beyond Europe will be implemented through the composition of the advisory board and the associate partner program.

4 How LIGHT^{est} Addresses Challenges of Global Trust Management

The following describes some major challenges of global trust management and how LIGHT^{est} addresses them.

4.1 Creation of a Global Trust Infrastructure at Feasible Effort

The effort required to create a global infrastructure is enormous and in most cases well out of reach of an EC-funded project with a very limited budget. This becomes even more evident when considering some of the requirements of the infrastructure: **(i)** Global agreement on the governance of the single trust root. **(ii)** Global organization to register unique names of trust schemes. **(iii)** A highly available and efficient global infrastructure for scheme location and queries. **(iv)** Design of the necessary protocols and their international standardization. **(v)** Development and maturation of software implementations of these protocols. **(vi)** Detailed security analysis of the infrastructure and of specific software products. **(vii)** Registration of trust schemes at the global registry. **(viii)** Training of staff to operate servers that publish trust schemes.

LIGHT^{est} addresses this possibly most difficult challenge through reuse of the existing Domain Name System (DNS. In particular, LIGHT^{est} employs the global DNS system as-is. Only marginal additions render it usable as a global trust infrastructure. It does so by following well-established strategies of other kinds of trust management[6].

4.2 Global Acceptance of the Approach Beyond Europe

A trust infrastructure that is global in a technical sense is only useful if it is actually accepted by at least the majority of stakeholders. Such a trust infrastructure needs to

[6] Namely, LIGHT^{est} adds to an existing family of trust management approaches in the family of IETF RFCs around DANE (DNS-based Authentication of Named Entities).

support global interoperability of trust schemes and trust queries.

LIGHT^{est} addresses this challenge by embedding its technical innovations into an inclusive and collaborative strategy that positions LIGHT^{est} from the start as a global initiative, open to extra-European collaboration.

4.3 Support for Heterogeneous Trust Models, since Homogeneous Models Fail to Scale Globally

Most current approaches assume that all participants share a single homogeneous perception of trust. Prime examples are "circles of trust". In a global setting, this assumption fails to apply. A global infrastructure therefore has to support heterogeneous trust models where stakeholders without a common perception of trust can collaborate.

LIGHT^{est} supports heterogeneous models of trust by moving the decision point for who is trusted to the verifier's trust policy. It typically selects and combines few existing large scale trust schemes (such as that of EU qualified signature) and can further personalize it with local black- and white-lists.

4.4 Automatic Handling of Subsidiarity Principle in Trust Schemes

Many existing trust schemes are constructed based on the subsidiarity principle. A global trust infrastructure must support such schemes automatically and transparent to verifiers. An example for this is the trust scheme of European qualified signatures where the European Commission uses a "*list of lists*" to delegate national portions of this trust scheme to the *trusted lists* created by Member States. While it may be easy to define hierarchical trust schemes, the challenge is to make it easy for verifiers to seamlessly follow all delegations to lower hierarchical nodes.

LIGHT^{est} addresses this challenge by using the native and massively proven DNS mechanism to delegate the management of sub-domains to third parties. The mechanism can support an arbitrary depth of the hierarchy and the LIGHT^{est} client libraries render the hierarchical structure of trust schemes transparent to verifiers.

4.5 Access to Trust Schemes based on Human-Readable Names

To enable non-technical decision makers understanding and authoring their trust policies, trust schemes must have globally unique but human-readable names. Accessing trust scheme data solely based on this name avoids error-prone configuration and removes significant vectors of attack. Enterprises operating on a global market have to accept signatures from customers world-wide and thus deal with a large number of trust schemes.

Technically, the use of current trust schemes typically requires two elements: **(i)** The location from where some trust list can be downloaded and **(ii)** the certificate that has signed the trust list and is required for verification.

A manual assignment of names to location/certificate pairs during configuration of a system is highly cumbersome and error prone. A global trust infrastructure should therefore render it possible to identify trust schemes with simple names suited for use by non-technical decision makers who define the organization's trust policy. These names should directly be usable to technically access and verify the actual data of the corresponding trust scheme.

LIGHT^{est} addresses this challenge by using DNS domain names to identify trust schemes. For example, the European trust scheme of qualified signatures may be named "*qualified.TRUST.ec.eu*". Here, *qualified* is the scheme name, *ec.eu* the authority responsible for the scheme, and *TRUST* a standardized constant word used across the trust infrastructure. Using the existing DNS, this name can then be used by software to locate and access the data that is contained in the named trust scheme.

4.6 Use of a Single Trust Root to Replace a Multitude of trust Anchors

On a global market, automatic verification of trust requires that the certificates of all trusted scheme operators issuing trusted lists must be loaded into the configuration of the system. These certificates are required to validate that the content of the trust scheme (list[7]) originates from a trusted source and not from some hostile attacker.

Provisioning such trust anchors is a highly security sensitive task and an attractive attack vector. An easy solution is the use of a single trust root from which all trust is derived.

LIGHT^{est} addresses this challenge by applying the existing, unique, and globally accepted trust root of the DNS. The standard mechanism of the DNS (with DNSSEC extension) allows to derive trust in trust scheme data from this single trust root and the (domain) name of the trust scheme.

4.7 Integration of Multiple Types of Trust Schemes in a Single Infrastructure

Real world trust decisions on electronic transactions typically require taking several different aspects of trust into account. A global trust infrastructure must be able to support all these aspects to avoid that verifiers need to access many different trust infrastructures and manage interoperability issues.

For example, to validate a purchase order with attached letter of credit, the following trust aspects may be involved: **(i)** Are the seals of the purchaser and bank qualified and

[7] While a "list" is mentioned here, the same reasoning applies also to possible Validation Authorities.

thus legally valid? **(ii)** Is the capitalization of the purchaser sufficient for the total amount of the order? **(iii)** Is the bank who issued the letter of credit trusted for the amount guaranteed?

The example illustrates that this involves different authorities using different trust schemes with different levels of assurance. It is evident that requiring multiple trust infrastructures would make validation very difficult and complex and multiply the cost as well. We therefore believe that the only viable way to enable electronic transactions on the single market is the conception of a single trust infrastructure that can support arbitrary current and future trust schemes.

LIGHTest addresses this challenge by using a very generic model of trust scheme and supporting an open number of trust schemes to coexist concurrently.

5 The LIGHT^{est} Reference Architecture

Figure 6 shows the LIGHT^{est} reference architecture with all the major software components. It illustrates how a verifier can validate a received electronic transaction based on her individual trust policy and queries to the LIGHT^{est} reference trust infrastructure.

Verifiers use Policy Authoring and Visualization Tools to state their individual trust policy. These tools support non-technical decision makers understanding and creating trust policies that can be applied by the Automatic Trust Verifier component (ATV).

In a cross-jurisdiction setting, different trust schemes are used to describe conceptually equivalent aspects. To make it easy to verifiers, Trust Translation Authorities (TTAs), provide the necessary translation data to map the levels of assurance of the foreign trust scheme to its equivalent in the domestic trust scheme. For example, an American authentication security of Level 3 could be mapped to the eIDAS level *substantial*.

Very often, data records that compose an electronic transaction are not directly signed by the legal entity responsible for it (e.g., using a company seal), but by a natural person that acts as an authorized representative for the former based on a delegation. The architecture therefore foresees the component of Delegation Publishers (DPs) that permit verifiers to query delegations and mandates.

All server components are implemented as DNS name servers. Organizations intended to publish trust schemes, translations schemes, and/or delegations can reuse their existing DNS servers (with security extension) or the existing outsourcing of this functionality.

In the same way as the DANE (DNS-based Authentication of Named Entities) standard [rfc7671] uses the DNS security extension to derive trust in TLS server certificates, LIGHT^{est} derives trust in trust scheme, translation, and delegation data. Chains of trust can be stored as receipts that can be validated at a later point in time.

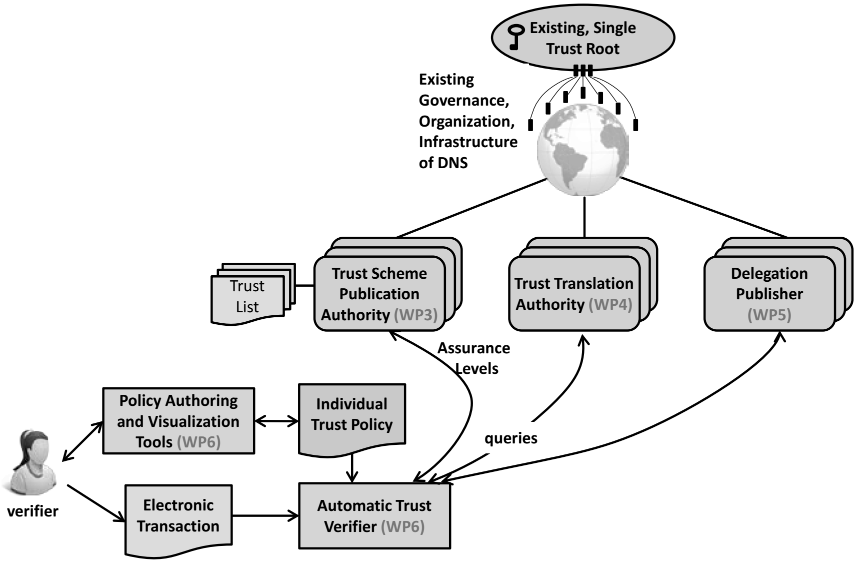

Existing, Single Trust Root
Existing Governance, Organization, Infrastructure of DNS
Trust List
Trust Scheme Publication Authority (WP3)
Trust Translation Authority (WP4)
Delegation Publisher (WP5)
Assurance Levels
Policy Authoring and Visualization Tools (WP6)
Individual Trust Policy
queries
verifier
Electronic Transaction
Automatic Trust Verifier (WP6)

Figure 6: The LIGHT^{est} Reference Architecture.

6 The LIGHT^{est} Pilot Applications

Two pilots to demonstrate LIGHT^{est} in an operational environment. They demonstrate the ease of integration of LIGHT^{est} components in existing systems and the benefits provided by the LIGHT^{est} functionality in real world usage scenarios.

One pilot uses LIGHT^{est} for all trust management in the cloud-based e-Correos platform that provides trustworthy communication services to citizens and businesses at a national scale. The other pilot focuses on e-invoicing in the OpenPePPOL [Ope]environment to establish trust in the various signatories and demonstrate the delegation-enabling of applications through LIGHT^{est}.

7 The LIGHT^{est} Approach for Going Global

To achieve acceptance also beyond Europe, as is necessary for a truly global trust infrastructure, LIGHT^{est} uses an open and inclusive process that involves as much as possible also non-European stakeholders:

(i) LIGHT^{est} considers also extra-European existing schemes in its inventories and attempts to assess also the requirements of non-European stakeholders. **(ii)** LIGHT^{est}

encourages participation of non-European stakeholders through global players in the consortium, the advisory board, and an associate partner program. **(iii)** LIGHT^{est} attempts international standardization of key elements, for example in the IETF. This process is by definition open to stakeholders world-wide. **(iv)** All DNS-related key components of LIGHT^{est} will be open source. The developed code will be hosted on an existing project portal such as Joinup, inviting contributions from outside the project from the beginning.

To support building up a global community, LIGHT^{est} applies a community-based dissemination strategy. For this purpose, a community is built around a vision of *universal, global, and interoperable trust management through the single standard solution offered by LIGHT^{est}*. This vision can be shared by stakeholders with different and potentially competing economic interests and is supported by the fact that the growth of the community in support of this vision will benefit every single member.

To achieve the above objectives, communication activities are integrated in a systematic strategy of community building. The big difference between community-based, and the "standard" dissemination strategies of projects lies in the amplification factor. In "standard" dissemination, the effort is carried solely by the project partners and is therefore necessarily limited, for example compared to global ambitions. In contrast, a community-based approach empowers project-external community members to disseminate the community's vision independently of the project and without funding through the project. In the ideal case, a vision can "go viral". This approach can adapt the dissemination to local languages and cultural settings, exploit opportunities that project partners could not possibly know about, and can access additional funding sources and support in other parts of the world.

8 Conclusions

This paper has described the major characteristics of the EC-funded LIGHT^{est} project. It promises a high impact through its wide range of applicability, its flexible support for a variety of trust schemes and trust aspects, and its global design both technically and through its planned community. The far-reaching use of the existing, globally implemented domain name system makes a global roll out at all possible. The use of the single trust root of the DNS is a key for real-world usability of the infrastructure.

While the partial funding by the European Commission is limited to its Consortium, LIGHT^{est} plans to build up a global community that promotes the implementation of the global trust infrastructure well beyond Europe. International standardization and the planned availability of open source implementations of all necessary components facilitates large-scale uptake.

The LIGHT^{est} project invites all interested parties, including non-European stakeholders, to participate in various ways in the project. Possibilities include contribution of one's trust schemes to the inventory of the project to ascertain its support in the produced standards and software, serving on the advisory board to represent regional or sectorial requirements, participation in standardization, promoting and disseminating the vision of LIGHT^{est} , and setting up of additional demonstrators and pilots. Interested parties are asked to contact the authors.

9 References

[Bru15] Bruegger B.P. (2015): The Globally Scalable FutureID Trust Infrastructure. Marseille, France.

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

[ETSI16] ETSI (2016): *TS 119 612: Electronic Signatures and Infrastructures (ESI); Trusted Lists.* http://www.etsi.org/deliver/etsi_ts/119600_119699/119612 /02.02.01_60/ ts_119612v020201p.pdf,

[Eur09] European Commission (2009): *Study on eID Interoperability for PEGS: Update of Country Profiles*. IDABC Programme.

[Fut] *FutureID*. http://FutureID.eu,

[Gefen] Gefen ; Rao V.S. und Tractinsky (2002): The Conceptualization of Trust, Risk and Their Relationship in Electronic Commerce: The Need for Clarification. In: *36th Hawaii International Conference on System Sciences (HICSS'03)*. Big Island, HI, USA: IEEE. S. 1-10.

[Kan] *Kantara*. https://kantarainitiative.org/trust-registry/ktr-trust-validation/,

[Lei14] Leitold H.; Lioy A. und Ribeiro (2014): STORK 2.0: Breaking New Grounds on eID and Mandates. Mesago Messe Frankfurt GmbH. S. 1-8.

[Mod05] Modinis study on identity management in eGovernment (2005): *Common Terminological Framework for Interoperable*. https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf,

[OASISDSS] OASIS: *Digital Signature Services*. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss,

[Ope] *OpenPEPPOL*. http://www.peppol.eu/,

[RFC2560] *RFC2560*. https://www.ietf.org/rfc/rfc2560.txt,

[SAML10] OASIS: *SAML Assurance Profile*. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.html,

[STO] STORK 2.0: *D2.1: Existing e-ID infrastructure analysis*. (Delivarable).

[Van09] Van Alsenoy ; De Cock ; Simoens K. et al. (2009): Delegation and digital mandates: Legal requirements and security objectives. *Computer Law & Security Review*, 25 (5). S. 415-432.

FutureTrust – Future Trust Services for Trustworthy Global Transactions

Detlef Hühnlein[1], Tilman Frosch[2], Jörg Schwenk[2], Carl-Markus Piswanger[3], Marc Sel[4], Tina Hühnlein[1], Tobias Wich[1], Daniel Nemmert[1], René Lottes[1], Stefan Baszanowski[1], Volker Zeuner[1], Michael Rauh[1], Juraj Somorovsky[2], Vladislav Mladenov[2], Cristina Condovici[2], Herbert Leitold[5], Sophie Stalla-Bourdillon[6], Niko Tsakalakis[6], Jan Eichholz[7], Frank-Michael Kamm[7], Jens Urmann[7], Andreas Kühne[8], Damian Wabisch[8], Roger Dean[9], Jon Shamah[9], Mikheil Kapanadze[10], Nuno Ponte[11], Jose Martins[11], Renato Portela[11], Çağatay Karabat[12], Snežana Stojičić[13], Slobodan Nedeljkovic[13], Vincent Bouckaert[14], Alexandre Defays[14], Bruce Anderson[15], Michael Jonas[16], Christina Hermanns[16], Thomas Schubert[16], Dirk Wegener[17], and Alexander Sazonov[18]

[1] ecsec GmbH, Sudetenstraße 16, 96247 Michelau, Germany, {firstname.name}@ecsec.de

[2] Ruhr Universität Bochum, Universitätsstraße 150, 44801 Bochum, Germany, {firstname.name}@rub.de

[3] Bundesrechenzentrum GmbH, Hintere Zollamtsstraße 4, A-1030 Vienna, {firstname.name}@brz.gv.at

[4] PwC Enterprise Advisory, Woluwedal 18, Sint Stevens Woluwe 1932, Belgium, {firstname.name}@be.pwc.com

[5] A-SIT, Seidlgasse 22/9, A-1030 Vienna, Austria, {firstname.name}@a-sit.at

[6] University of Southampton, Highfield, Southampton S017 1BJ, United Kingdom, {S.Stalla-Bourdillon, N.Tsakalakis}@soton.ac.uk

[7] Giesecke & Devrient GmbH, Prinzregentestraße 159, 81677 Munich, Germany, {firstname.name}@gi-de.com

[8] Trustable Limited, Great Hampton Street 69, Birmingham B18 6E, United Kingdom, {kuehne,damian}@trustable.de

[9] European Electronic Messaging Association AISBL, Rue Washington 40, Bruxelles 1050, Belgium, {r.dean, jon.shamah}@eema.org

[10] Public Service Development Agency, Tsereteli Avenue 67A, Tbilisi 0154, Georgia, mkapanadze@sda.gov.ge

[11] Multicert – Servicos de Certificacao Electronica SA, Lagoas Parque Edificio 3 Piso 3, Porto Salvo 2740 266, Portugal, {firstname.name}multicert.com

[12] Turkiye Bilimsel Ve Tknolojik Arastirma Kurumu, Ataturk Bulvari 221, Ankara 06100, Turkey, cagatay.karabat@tubitak.gov.tr

[13] Ministarstvo unutrašnjih poslova Republike Srbije, Kneza Miloša 103, Belgrade 11000, Serbia, {firstname.name}@mup.gov.rs

[14] Arηs Spikeseed, Rue Nicolas Bové 2B, 1253 Luxembourg, Luxembourg, {firstname.name}@arhs-developments.com

[15] Law Trusted Third Party Service (Pty) Ltd. (LAWTrust), 5 Bauhinia Street, Building C, Cambridge Office Park Veld Techno Park, Centurion 0157, South Africa, bruce@LAWTrust.co.za

[16] Federal Office of Administration (Bundesverwaltungsamt), Barbarastr. 1, 50735 Cologne, Germany, {firstname.name}@bva.bund.de

[17] German Federal Information Technology Centre (Informationstechnikzentrum Bund, ITZBund), Waterloostr. 4, 30169 Hannover, Germany, {firstname.name}@itzbund.de

[18] National certification authority Rus CJSC (NCA Rus), 8A building 5, Aviamotornaya st., Moscow 111024, Russia, sazonov@nucrf.ru

Abstract: Against the background of the regulation 2014/910/EU [EU1] on electronic identification (eID) and trusted services for electronic transactions in the internal market (eIDAS), the FutureTrust project, which is funded within the EU Framework Programme for Research and Innovation (Horizon 2020) under Grant Agreement No. 700542, aims at supporting the practical implementation of the regulation in Europe and beyond. For this purpose, the FutureTrust project will address the need for globally interoperable solutions through basic research with respect to the foundations of trust and trustworthiness, actively support the standardisation process in relevant areas, and provide Open Source software components and trustworthy services which will ease the use of eID and electronic signature technology in real world applications. The FutureTrust project will extend the existing European Trust Service Status List (TSL) infrastructure towards a "Global Trust List", develop a comprehensive Open Source Validation Service as well as a scalable Preservation Service for electronic signatures and seals. Furthermore it will provide components for the eID-based application for qualified certificates across borders, and for the trustworthy creation of remote signatures and seals in a mobile environment. The present contribution provides an overview of the FutureTrust project and invites further stakeholders to actively participate as associated partners and contribute to the development of future trust services for trustworthy global transactions.

Keywords: Trust, eID, Trust Services, Global Trust List, electronic Signatures and Seals, Validation, Preservation, eID-based enrolment of Qualified Certificates, remote and mobile Signing and Open Source.

1 Background and Motivation

There are currently around 150 trust service providers across Europe[19], which issue qualified certificates and/or qualified time stamps. Hence, the "eIDAS ecosystem" with respect to these basic services is fairly well developed. On the other hand, the provision of qualified trust services for the validation and preservation of electronic signatures and seals as well as for registered delivery and the cross-border recognition of electronic identification schemes have been recently introduced with the eIDAS regulation [EU1]. However, these services are not yet available in a mature, standardised, and interoperable manner within Europe.

In a similar manner, the practical adoption and especially the cross-border use of eID cards, which have been rolled out across Europe, is – despite previous and ongoing research and development efforts in pertinent projects, such as STORK, STORK 2.0, FutureID, e-SENS, SD-DSS, Open eCard, OpenPEPPOL and SkIDentity – still in its infancy. In general there is no opportunity to use national eID means in foreign environment. In particular, it is often not yet possible in practice to use an eID card from one EU Member State to enrol for a qualified certificate and secure signature creation device (SSCD) in another Member State.[20]

[19] See [EUTL], [DIR] and [3xA16] for example.

[20] Note, that such a cross-border enrolment for qualified certificates may become especially interesting in combination with remote and mobile signing services, in which no physical SSCD needs to be shipped to the user, because the SSCD is realized as central Hardware Security Module (HSM) hosted by a trusted service

In particular the following problems seem to be not yet sufficiently solved and hence will be addressed in the FutureTrust project:

P1. No comprehensive Open Source Validation Service

Multiple validation services are available today. They range from offering revocation information to full validation against a formal validation policy. These services are operated by public and private sector actors, and allow relying parties the validation of signed or sealed artefacts. However, there is currently no freely available, standard conforming and comprehensive Validation Service, which would be able to verify arbitrary advanced electronic signatures in a trustworthy manner. To solve this problem the FutureTrust project will contribute to the development of the missing standards and the development of such a comprehensive Validation Service.

P2. No scalable Open Source Preservation Service

The fact that signed objects lose their conclusiveness if cryptographic algorithms become weak induces severe challenges for applications, which require maintaining the integrity and authenticity of signed data for long periods of time. Research related to the strength of cryptographic algorithms is addressed in many places, including ECRYPT-NET[21], and does not fall within the scope of FutureTrust. Rather, the FutureTrust project will aim at solving this problem by contributing to the development of the missing standards and the implementation of a scalable Open Source Preservation Service that makes use of processes and workflow to ensure preservation techniques embed the appropriate cryptographic solutions.

P3. Qualified electronic signatures are difficult to use in mobile environments

Today, applying for a qualified certificate involves various paper-based steps. Furthermore, to generate a qualified signature, typically a smart card based signature creation device has to be used, which is complicated in mobile environments due to the need for middleware and drivers that are often not supported on the mobile device. The FutureTrust project will aim at changing this by creating a mobile Signature Service, which supports eID-based enrolment for qualified certificates and the remote creation of qualified electronic signatures initiated by using mobile devices.

P4. Legal requirements of a pan-European eID metasystem

The first part of the eIDAS-regulation that deals with eIDM systems aims to create a standardized interoperability framework but does not intend to harmonize the respective national eIDM systems. Instead it employs a set of broad requirements, part of which is the mandatory compliance of all systems to the Data Protection Directive [EC2]. The

provider, which fulfils the requirements of [CEN1], and against the background of the eIDAS-regulation (see e.g. Recital 51 of [EU1]) one may expect that such a scenario may soon become applicable across Europe and beyond.

[21] https://www.cosic.esat.kuleuven.be/ecrypt/net/

Directive will soon be replaced by the General Data Protection Regulation (GDPR) [EU3], which introduces new concepts and safeguards for data protection. To facilitate compliance with the GDPR, the FutureTrust project will conduct desk research to analyse how the newly emerged privacy and data protection legislation impacts on existing laws and derive a list of necessary characteristics that an EU eID and eSignatures metasystem should incorporate to ensure compliance.

P5. Legally binding electronic transactions with non-European partners are hard to achieve

While the electronic signature directive [EC1] and the eIDAS-regulation [EU1] define the legal effect of qualified electronic signatures, there is no comparable global legislation and hence electronic transactions with business partners outside the European Union are challenging with respect to legal significance and interoperability. To work on a viable solution for this problem the FutureTrust project will conduct basic research with respect to international legislation, contribute to the harmonization of the relevant policy documents and standards and build a “Global Trust List”, which may form the basis for legally significant electronic transactions around the globe.

P6. Scope of eIDAS interoperability framework is limited to EU

In a similar manner, the scope of the interoperability framework for electronic identification according to Article 12 of [EU1] is limited to the EU. There are many aspects of an international interoperability framework that need to be assessed, especially in regard of to the changes in privacy and data protection highlighted above.[22] Against this background, the FutureTrust project will extend the work from pertinent research and large-scale pilot projects to integrate non-European eID-solutions in a seamless and trustworthy manner, after defining the requirements and assessing the impact of data transfers beyond the European Union.

P7. No formal foundation of trust and trustworthiness

To be able to compare eID solutions on an international scale, there is no international legislation which would allow to “define” trustworthiness. Instead, scientifically sound formal models must be developed which describe international trust models, and especially model to compare the trustworthiness of different eID services.

To demonstrate the viability and trustworthiness of these formal models, and show that the developed components can be used in productive environments, the FutureTrust project will implement real world pilot applications in the area of public administration, eCommerce, eBusiness and eBanking.

[22] For example, data transfers to the US are currently not clearly regulated after the invalidation of the ‘Safe Harbor’ agreement by the EUCJ (C-362/14). The EU officials are currently in negotiations on a new arrangement, named ‘EU-US Privacy Shield’ which was halted after a contradictory opinion from the WP29 (WP238).

2 The FutureTrust Project

In order to solve the problems mentioned above, the FutureTrust partners (see Section 2.1) have sketched the FutureTrust System Architecture (see Section 2.2), which includes several innovative services, which are planned to be used in a variety of pilot projects (see Section 2.8).

This will in particular include the design and development of a Global Trust List (gTSL) (see Section 2.3), a Comprehensive Validation Service (ValS) (see Section 2.4), a scalable Preservation Service (PresS) (see Section 2.5), an Identity Management Service (IdMS) (see Section 2.6) and last but not least a mobile Signature Service (mSignS) (see Section 2.7).

2.1 FutureTrust Partners

The FutureTrust project is carried out by a number of core partners as depicted in Figure 1, which includes Ruhr-Universität Bochum (Germany), ecsec GmbH (Germany), Arhs Spikeseed (Luxembourg), EEMA (Belgium), Federal Computing Centre of Austria (Austria), Federal Office of Administration Germany (Germany), Price Waterhouse Coopers (PWC) (Belgium), University of Southampton (United Kingdom), multicert (Portugal), Giesecke & Devrient GmbH (Germany), Trustable Ltd. (United Kingdom), Secure Information Technology Center – Austria (Austria), Public Service Development Agency (Georgia), Türkiye Bilimsel veTeknolojik Araştırma Kurumu (Turkey), LAW Trusted Third Party Services (Pty) Ltd. (South Africa), Ministry of Interior Republic of Serbia (Serbia).

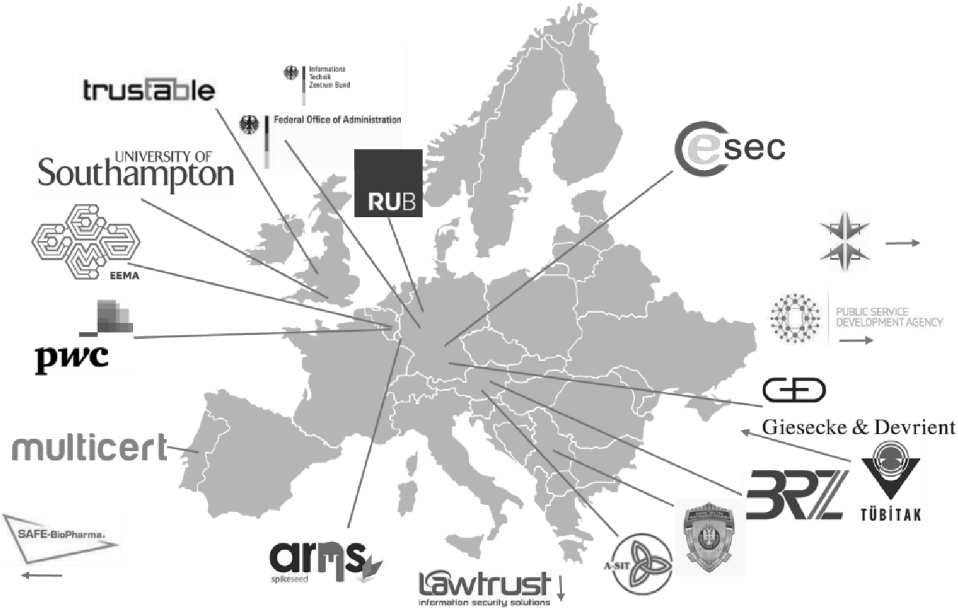

trustable
Informations Technik Zentrum Bund
Federal Office of Administration
UNIVERSITY OF Southampton
RUB
EEMA
pwc
multicert
SAFE-BioPharma.
arms spikeseed
lawtrust information security solutions
A-SIT
esec
PUBLIC SERVICE DEVELOPMENT AGENCY
Giesecke & Devrient
BRZ
TÜBITAK

Figure 1: FutureTrust Partners

Furthermore the FutureTrust project is supported by selected subcontractors and an unlimited number of associated partners, which currently includes the German Federal Information Technology Centre (Informationstechnikzentrum Bund (ITZBund)), A-SIT Plus GmbH (Austria), the SAFE Biopharma Association (USA) and the National Certification Authority Rus (NCA Rus) (Russia).

Note that the FutureTrust project is open for collaboration with additional associated partners and especially invites **Trust Service Providers** according to [EU1] or similar policy frameworks to participate in the FutureTrust project and benefit from the envisioned research and development.

2.2 FutureTrust System Architecture

As shown in Figure 2, the FutureTrust system integrates existing and emerging eIDAS Trust Services, eIDAS Identity Services and similar Third Country Trust & Identity Services and provides a number of FutureTrust specific services, which aim at facilitating the use of eID and electronic signature technology in different application scenarios.

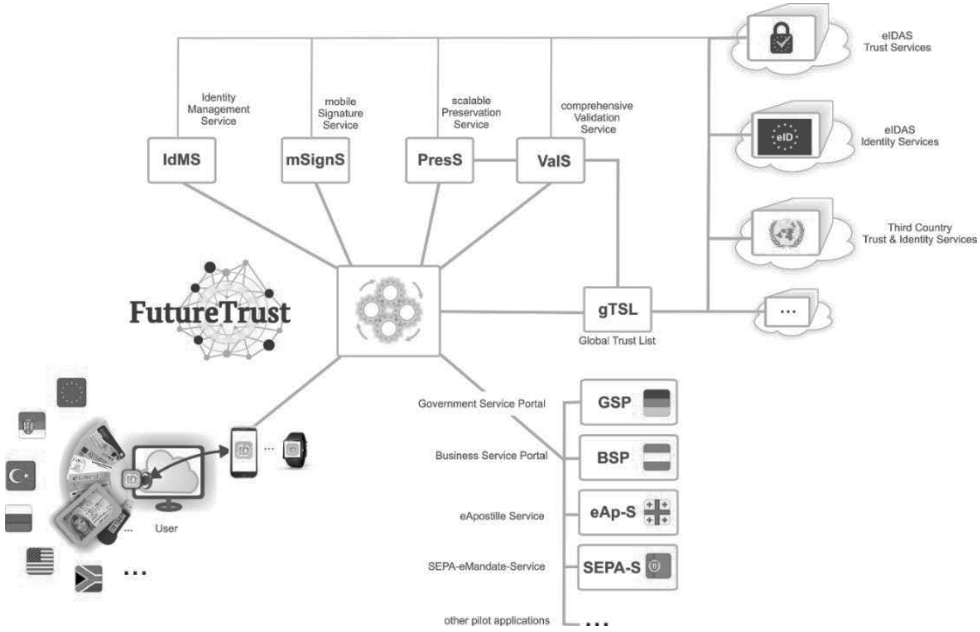


Figure 2: FutureTrust System Architecture

2.3 Global Trust List (gTSL)

The gTSL is envisioned to become an Open Source component, which can be deployed with the other FutureTrust services or as standalone service and which allows to manage Trust Service Status Lists for Trust Services and Identity Providers. The gTSL will allow to import the European "List of the Lists" (LOTL), which is a signed XML document according to [ETSI7] and all national Trust Service Status Lists (TSLs) referenced therein. This LOTL is currently published by the European Commission. This import includes a secure verification of the digital signatures involved. The gTSL will also allow to import Trusted Lists from other geographic regions, such as the Trust List of the Russian Federation[23] for example, and it is envisioned that the gTSL will generate a "virtual US-American Trust List" from the current set of available cross-certificates. gTSL will provide support for the traceable assessment of trust related aspects for potential trust anchors both with and without known trustworthiness and assurance levels[24] by providing claims or proofs of relevant information with respect to the trustworthiness of a trust service. This may give rise for a reputation based "web of trust" for trust services. It is expected that the corroboration of information from

[23] See http://e-trust.gosuslugi.ru/CA/DownloadTSL?schemaVersion=0.

[24] [EU1] implicitly defines the levels "qualified" and "non-qualified" for trust service providers and explicitly introduces in Article 8 the assurance levels "low", "significant" and "high" for electronic identification schemes.

relatively independent sources[25] will help to establish trustworthiness. Furthermore the gTSL is planned to provide a web interface as well as a SOAP or REST interface allowing for a small set of predefined queries, to allow the other FutureTrust services or other gTSL deployments to access the validated data. For implementation of the underlying gTSL model various options have already been identified. These include traditional models such as a Trusted Third Party model and a Trust List, as well as innovative models such as a semantic web ontology and a blockchain ledger.

2.4 Comprehensive Validation Service (ValS)

The major use case of ValS is the validation of Advanced Electronic Signatures (AdES) in standardized formats, such as CAdES, XAdES and PAdES for example. In order to support the various small legal and regulatory differences with respect to electronic signatures coming from different EU Member States or other global regions, the ValS will support practice oriented XML-based validation policies for electronic signatures, which consider previous work in this area, such as [ETSI4] and [ETSI6] and current standards, such as [ETSI1] and [ETSI8] for example. The ValS is envisioned to issue a verification report to the requestor of the service, which may be based on a revision of the OASIS DSS Signature Verification report [OAS4], which in particular considers the procedures defined in [ETSI1] and the XML-based validation policies mentioned above. This revised verification report may be brought back to standardization as a contribution to EN 319 102-2, which is planned[26] to be developed, but for which the standardization work has not yet started. Finally, it seems worth to be mentioned that the ValS is planned to be designed in an extensible manner, such that modules for other not (yet) standardized signatures or validation policies can be plugged into the ValS in a well-defined manner.

2.5 Scalable Preservation Service (PresS)

The PresS is used to preserve the integrity and conclusiveness of a signed document over its whole lifetime. For this purpose, the FutureTrust Preservation Service as outlined in Figure 3 will use the ValS and existing external time stamping services in order to produce Evidence Records according to [RFC1] and possibly [RFC2]. As depicted in Figure 3 the Preservation Service may support different input interfaces based on [OAS1] and [BSI1] for example and integrate various types of storage systems.

Unlike in [BSI2] the FutureTrust Preservation Service may however not use a rather inefficient XML-based Archive Information Package (AIP) structure, but possibly a zip-based container along the lines of the Associated Signature Container (ASiC) specification according to [ETSI2] as this would provide an easy to use and space efficient container format. An important goal of the envisioned Preservation Service is

[25] See [Sel16].
[26] See [ETSI5].

scalability, which may be realized by using efficient data structures, such as Merkle hash trees as standardized in [RFC1] for example. Using hash tree based signatures[27] may also provide additional security in the case that quantum computers have been built, because any digital signature that is in use today (based on the RSA assumption or on the discrete log assumption) can be forged in this case. However, message authentication codes (MACs), block-chain constructions and signature algorithms based on hash-trees seem to remain secure. Thus it is an interesting research question, whether fully operational and sufficiently performant preservation services can be built on MACs, block-chains or hash-trees alone.

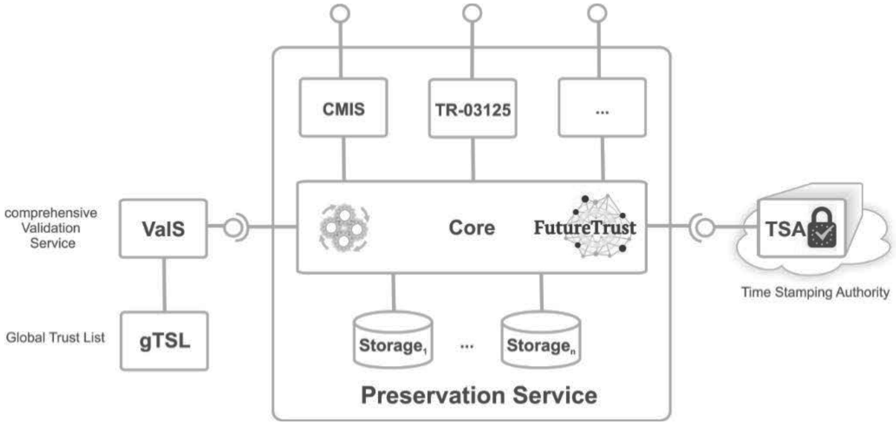


Figure 3: Outline of the Architecture of the Scalable Preservation Service

2.6 Identity Management Service (IdMS)

Many EU Member States and some non-European countries have established eID services, which produce slightly different authentication tokens. Within the EU, most[28] of these services produce SAML tokens (see [Zwa12]) and the eIDAS interoperability framework [eIDAS] is also based on [SAML]. In addition, industrial standardization activities have produced specifications like FIDO[29] or GSMA's MobileConnect[30] which have gained a broad customer base. The IdMS will be able to consume a broad variety of such authentication tokens (SAML, OpenID Connect, OAuth), work with a broad variety of mobile identification services (FIDO, GSMA MobileConnect, European Citizen cards) and transform them into a standardized, interoperable[31] and secure[32] format. The

[27] See [Buc09].

[28] The [Fra16] system seems to be an exception to this rule, as it produces and accepts identity tokens according to the [Ope15] specification.

[29] See [FID15].

[30] See [MOB] and [GSM15].

[31] Due to the fact that SAML is a very complex and highly extensible standard, the integration of different eID services considering all extensions points is a rather challenging task. In order to enable the communication between all eID services, their interoperability has to be thoroughly analysed.

choice of this standardized format will be based on industry best practices, and on the eIDAS interoperability framework [eIDAS]. Moreover, the IdMS is envisioned to be able to directly communicate with a selection of European and non-European eID services.

2.7 Mobile Signature Service (mSignS)

The mSignS will enable the remote creation of qualified electronic signatures and seals in a mobile environment[33]. For this purpose the mSignS will be operated in a secure environment and may contain an appropriate Hardware Security Module (HSM) which hosts the private keys of the signatories. While these keys are hosted at a central place, they are kept under the sole control of the Signatory as described in [CEN1]. In order to reach this seemingly contradictory requirement the FutureTrust project will in particular research means for securely sharing the private signing key between the mobile device of the Signatory and the HSM located at the mSignS or the along the lines of [Kut13].

[32] Based on [eIDAS] it is clear that SAML 2.0 will form the basis for eIDAS Interoperability Framework according to Article 12 of [EU1] and [EU2], but it is currently likely that the Assertions will be simple "Bearer Tokens", which is not optimal from a security point of view. Furthermore, the different authentication flows and optional message encryptions result in complex standard and thus expose conforming implementations to new attacks. In the last years, several papers (see e.g. [Som12]) showed how to login as an arbitrary use in SAML Single Sign-On scenarios or decrypt confidential SAML messages (see e.g. [Jag11]). Thus, existing eID services can be evaluated against known attacks and existing risks can be discovered. As a result, a metric to measure the security of eID services will be elaborated.

[33] See [Kub15] and [ETSI3] for more information on mobile signatures.

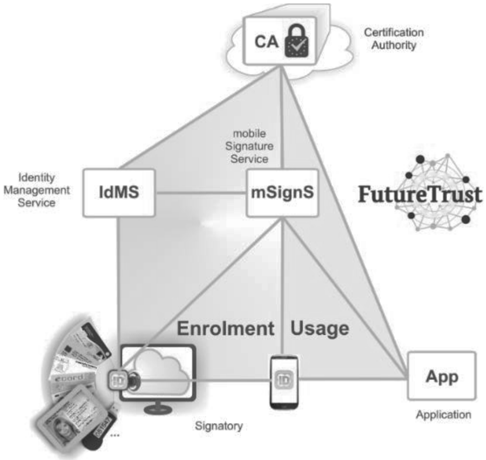


Figure 4: Enrolment and Usage Phase for Mobile Signing

As outlined in Figure 4, one may distinguish the enrolment phase and the usage phase. During enrolment, the Signatory uses his eID and the IdMS to perform an eID-based identification and registration at the mSignS or the Certification Authority (CA). The mSignS or the CA will create a key pair for the Signatory and requests or create a certificate. Within the enrolment phase, the mSignS or the CA will also provide appropriate credentials to the Signatory and her mobile device, which can later on be used to authenticate at the mSignS in order to trigger the signature creation within some application specific context. The OASIS DSS Extension for Local Signature Computation [OAS2] may be used as a protocol to expose the signing functionality of a local key under Signatory's sole control.

2.8 FutureTrust Pilot Applications

The FutureTrust consortium aims to demonstrate the project's contributions in a variety of demonstrators and pilot applications, which are planned to include a Governmental Service Portal, a Business Service Portal, an e-Apostille Validation System and a SEPA e-Mandate Service according to [EPC] for example. Furthermore the FutureTrust project is open for supporting further pilot applications related to innovative use cases for eID and electronic signature technology.

3 Summary and Invitation for Collaboration

The present paper provides an overview of the FutureTrust project, which will start on June 1st 2016 and which will be funded by the European Commission within the EU Framework Programme for Research and Innovation (Horizon 2020) under the Grant

Agreement No. 700542 with up to 6,3 Mio. .

As explained throughout the paper, the FutureTrust project will conduct basic research with respect to the foundations of trust and trustworthiness, actively support the standardisation process in relevant areas, and plans to provide innovative Open Source software components and trustworthy services which will enable ease the use of eID and electronic signature technology in real world applications by addressing the problems P1 to P7 introduced in Section 1.

Against this background the FutureTrust consortium invites interested parties, such as Trust Service Providers, vendors of eID and electronic signature technology, application providers and other research projects to benefit from this development and join the FutureTrust team as associated partner.

References

[EC1] 1999/93/EC. (1999). Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093.

[EU1] 2014/910/EU. (2014). Regulation (EU) No 910/2014 of the European Parliament and of the council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

[EU2] 2015/1501/EU. (2015). Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014. *of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance)* . http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0001.

[EU3] 2016/679/EU. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, . *and repealing Directive 95/46/EC and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)* . http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

[3xA16] 3xA Security AB . (2016). EU Trust Service status List (TSL) Analysis Tool. http://tlbrowser.tsl.website/tools/.

[EC2] 95/64/EC. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.

[BSI1] BSI TR-03125-E. (2015, January 31). Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI). *Preservation of Evidence of Cryptographically Signed Document - Annex E: Concretisation of the Interfaces on the Basis of the eCard-API-Framework* . https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/

TG03125/BSI_TR_03125_TR-ESOR-E_V1_2_EN.pdf?__blob=publicationFile&v=4: Technical Guideline 03125, Annex E, Version 1.2.

[BSI2] BSI TR-03125-F. (2015, January 31). Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI). *Preservation of Evidence of Cryptographically Signed Documents - Annex F: Formats* . https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03125/BSI_TR_03125_TR-ESOR-F_V1_2_EN.pdf?__blob=publicationFile&v=2: Technical Guideline 03125, Annex F, Version 1.2.

[Buc09] Buchmann, J., Dahmen, E., & Szydlo, M. (2009). Hash-based digital signature schemes. In *Post-Quantum Cryptography* (pp. 35-93). Springer.

[CEN1] CEN/TS 419 241. (2014). Security Requirements for Trustworthy Systems supporting Server Signing.

[DIR] Directory of Signature Creation Devices. (2016). *Open Signature Initiative*. Retrieved from http://opensignature.org/devices/

[eIDAS] eIDAS Spec. (2015, November 26). eIDAS Technical Subgroup. *eIDAS Technical Specifications v1.0* . https://joinup.ec.europa.eu/software/cefeid/document/eidas-technical-specifications-v10.

[EPC] EPC 208-08. (2013, April 9). European Payments Council. *EPC e-Mandates e-Operating Model - Detailed Specification* . Version 1.2: http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/epc-e-mandates-e-operating-model-detailed-specification/epc208-08-e-operating-model-detailed-specification-v12-approvedpdf/.

[ETSI1] ETSI EN 319 102-1. (2016, May). Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, Version 1.1.1. http://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf.

[ETSI2] ETSI EN 319 162-1. (2015, August). Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers. http://www.etsi.org/deliver/etsi_en/319100_319199/31916201/01.00.00_20/en_31916201v010000a.pdf.

[ETSI3] ETSI SR 019 020. (2016, February). The framework for standardisation of signatures: Standards for AdES digital signatures in mobile and distributed environments. *V1.1.1* . http://www.etsi.org/deliver/etsi_sr/019000_019099/019020/01.01.01_60/sr_019020v010101p.pdf.

[ETSI4] ETSI TR 102 038. (2002, April). TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies.

[ETSI5] ETSI TR 119 000. (2016, April). Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview. Version 1.2.1: http://www.etsi.org/deliver/etsi_tr/119000_119099/119000/01.02.01_60/tr_119000v010201p.pdf.

[ETSI6] ETSI TS 102 853. (2012, July). Electronic Signatures and Infrastructures (ESI); Signaturue verification procedures and policies. *V1.1.1* . http://www.etsi.org/deliver/etsi_ts/102800_102899/102853/01.01.01_60/ts_102853v010101p.pdf.

[ETSI7] ETSI TS 119 612. (2016, April). Electronic Signatures and Infrastructures (ESI); Trusted Lists. *Version 2.2.1* . http://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.02.01_60/ts_119612v020

201p.pdf.

[ETSI8] ETSI TS 199 172-1. (2015, July). Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents. http://www.etsi.org/deliver/etsi_ts/119100_119199/11917201/01.01.01_60/ts_11917201v010101p.pdf.

[EUTL] EU Trusted Lists of Certification Service Providers. (2016). *European Commision*. Retrieved from https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers

[FID15] FIDO. (2015). *FIDO Alliance*. Retrieved from https://fidoalliance.org/

[Fra16] FranceConnect. (2016). https://doc.integ01.dev-franceconnect.fr/.

[MOB] GSMA. (2015). *Introducing Mobile Connect – the new standard in digital authentication*. Retrieved from http://www.gsma.com/personaldata/mobile-connect

[GSM15] GSMA-CPAS5. (2015). CPAS 5 OpenID Connect - Mobile Connect Profile - Version 1.1. https://github.com/GSMA-OneAPI/Mobile-Connect/tree/master/specifications.

[Jag11] Jager, T., & Somorovsky, J. (2011). How to break xml encryption. *Proceedings of the 18th ACM conference on Computer and communications security* .

[Kub15] Kubach, M., Leitold, H., Roßnagel, H., Schunck, C. H., & Talamo, M. (2015). SSEDIC.2020 on Mobile eID. *to appear in proceedings of Open Identity Summit 2015.*

[Kut13] Kutylowski, M., & Kubiak, P. (2013, May 06). Mediated RSA cryptography specification for additive private key splitting (mRSAA). *IETF Internet Draft, draft-kutylowski-mrsa-algorithm-03* . http://tools.ietf.org/html/draft-kutylowski-mrsa-algorithm-03.

[OAS1] OASIS CMIS v1.1. (2013, May 23). Content Management Interoperability Services (CMIS). http://docs.oasis-open.org/cmis/CMIS/v1.1/CMIS-v1.1.html.

[OAS2] OASIS DSS LocSig. (2015, July 27). *DSS Extension for Local Signature Computation Version 1.0.* Retrieved from Committee Specification: http://docs.oasis-open.org/dss-x/localsig/v1.0/cs01/localsig-v1.0-cs01.pdf

[OAS3] OASIS DSS v1.0. (2010, November 12). *Profile for Comprehensive Multi-Signature Verification Reports Version 1.0.* Retrieved from http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0-profiles-vr-cs01.pdf

[OAS4] OASIS-DSS. (2007, April 11). *Digital Signature Service Core Protocols, Elements, and Bindings Version 1.0.* Retrieved from OASIS Standard: http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.html

[Ope15] OpenID Connect. (2015). OpenID Foundation. *Welcome to OpenID Connect* . http://openid.net/connect/.

[RFC1] RFC 4998. (2007, August). Gondrom, T.; Brandner, R.; Pordesch, U. *Evidence Record Syntax (ERS)* . https://tools.ietf.org/html/rfc4998.

[RFC2] RFC 6238. (2011, July). Jerman Blazic, A.; Saljic, A.; Gondrom, T. *Extensible Markup Language Evidence Record Syntax (XMLERS)* . https://tools.ietf.org/html/rfc6283.

[SAML] SAML 2.0. (2005, March 15). *OASIS Standard.* Retrieved from Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[SDDSS] SD-DSS. (2011, August 09). *Digital Signature Service | Joinup*. Retrieved from https://joinup.ec.europa.eu/asset/sd-dss/description

[Sel16] Sel, M. (2016). Improving interpretations of trust claims, published in the proceedings of the. *Trust Management X: 10th IFIP WG 11.11 International Conference, IFIPTM 2016* (pp. 164-173). Darmstadt, Germany: Springer.

[SkID] SkIDentity. (2016). Retrieved from https://www.skidentity.com/

[Som12] Somorovsky, J., Mayer, A., Schwenk, J., Kampmann, M., & Jensen, M. (2012). On breaking saml: Be whoever you want to be. *Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)* .

[STO2] STORK 2.0. (2014). Retrieved from https://www.eid-stork2.eu/

[STO] STORK. (2012). Retrieved from https://www.eid-stork.eu/

[Zwa12] Zwattendorfer, B., & Zefferer, T. T. (2012). The Prevalence of SAML within the European Union. *8th International Conference on Web Information Systems and Technologies (WEBIST)*, (pp. 571-576). http://www.webist.org/?y=2012.

One mobile ID to secure physical and digital Identity

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

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

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

1 Introduction

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

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

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

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

the SCRUM framework.

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

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

2 Related Work

2.1 Biometrics Authentication on mobile Devices

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

2.2 Identity Federation

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

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

2.3 Mobile ID Solutions

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

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

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

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

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

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

3 My Identity App – A smartphone-based mobile ID

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

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

The ecosystem consists of the following high-level components:

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

3.1 Security and Privacy by Process

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

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

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

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

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

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

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

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

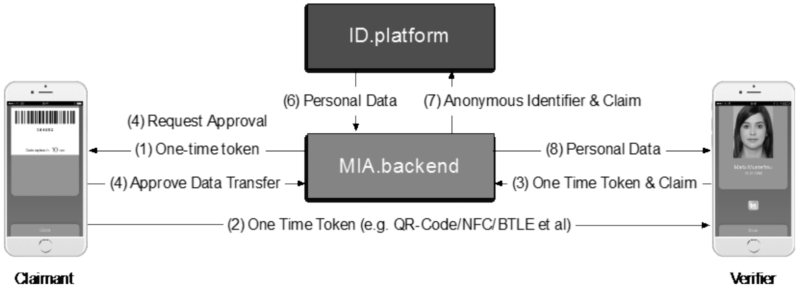

ID.platform
(6) Personal Data
(7) Anonymous Identifier & Claim
(4) Request Approval
(1) One-time token
MIA.backend
(8) Personal Data
(4) Approve Data Transfer
(3) One Time Token & Claim
(2) One Time Token (e.g. QR-Code/NFC/BTLE et al)
Claimant
Verifier

Fig. 1: General person-to-person workflow

3.2 Major Application Scenarios

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

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

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

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

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

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

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

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

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

3.3 Architectural Considerations and Integration Aspects

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

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

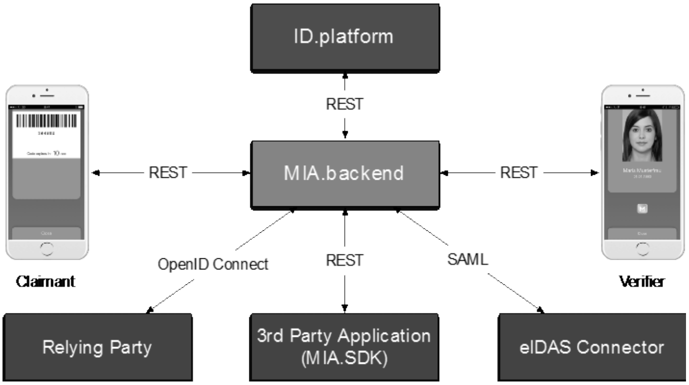


Fig. 2: Simplified architectural overview

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

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

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

3.4 Differentiation from other ID Solutions

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

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

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

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

4 Summary and Conclusion

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

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

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

Acknowledgements

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

References

[Eu14] European Union: REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Official Journal of the European Union/L 257, Pg. 73-114, 2014.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Towards a Decentralized Identity Management Ecosystem for Europe and Beyond

Bud P. Bruegger[1], Heiko Roßnagel[1]

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

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

1 Introduction

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

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

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

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

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

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

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

2 Related Work

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

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

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

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

3 Approach

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

Three major artefacts have been evaluated in FutureID: the reference architecture, the implementation, and the pilot applications. Wherever possible, feedback loops were created where the evaluation identified certain shortcomings that were fixed in an improved version of the artefact that was then again evaluated. In the case of the reference architecture, several rounds of the evolutionary loops were necessary to yield the present architecture that satisfies all major requirements. This work also underlines the interdisciplinary and participatory character of such an evaluation and improvement loop—no single person/expert can cover all the disciplines necessary to successfully design such a complex artefact. The separate evaluation of architecture, implementation, and pilots also illustrates how different aspects of a project are verified with different artefacts. For example, an architecture must enable a wide range of possible uses, deployment scenarios, and configurations of which only a small part can be actually implemented and demonstrated within the limits of a project. Pilot applications are very concrete on the other hand. Here, it is clear, for example, which stakeholders with which legal characteristics actually operate given software components. Only now, certain legal requirements can be evaluated. Thanks to this approach, FutureID managed to satisfy all major requirements from all disciplines and there were very strong reasons (e.g., a tradeoff between conflicting requirements from different disciplines) for the few cases where a requirement was not satisfied.

4 Results

4.1 The FutureID Architecture

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

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

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

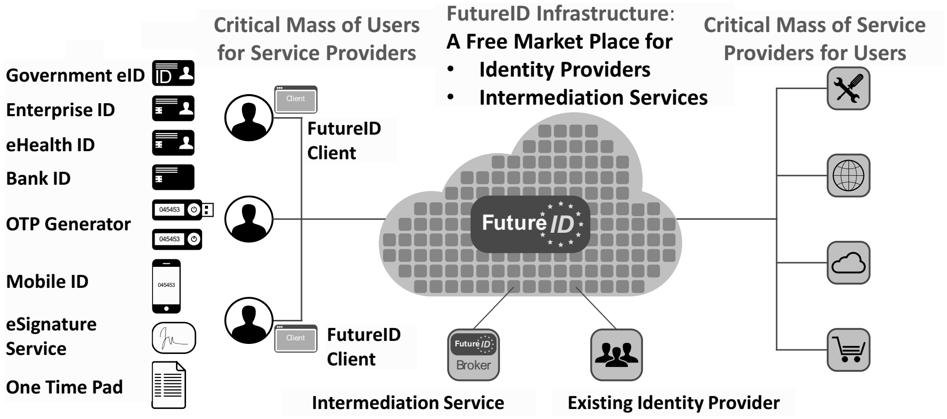


Figure 1: Intermediation to reach a critical mass of both users and services.

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

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

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

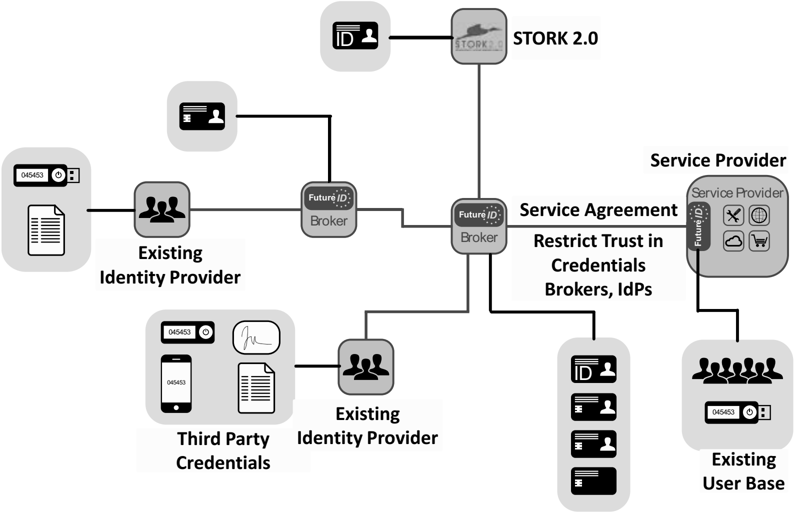


Figure 2: How a Service Provider reaches out to a massive potential user base.

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

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

4.2 Scalability

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

[3] Note that bearer assertions cannot usually reach the full potential of security [Bur13].

[4] Note that important privacy features of Attribute Based Credentials get lost when an intermediary is introduced.

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

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

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

4.3 Support for a Free Marketplace of Intermediation Services

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

[5] For example, SAML assertions

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

4.4 Other Contributions

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

FutureID has further developed a universal open source eID client that can be used as a multi-card eID middleware that offers complex authentication functions as required by the German nPA and for signatures. Already, a wide variety of eIDs and other smart cards are supported [Fut15]. Additional smart cards are easy to support through simply providing declarative and standards-compliant CardInfo files. Tools to support creation of such files are available. An add-on framework renders it possible to easily extend the functionality of the FutureID client, e.g., with additional protocols. The client exists both, as PC and mobile version and is easy to install through Java Web Start. Demonstrating its extensibility, the FutureID client has been used to secure authentication of patients and healthcare professionals in the epSOS e-health platform, as well as providing the first legal compliant, signature-based mechanism for patient consent. The FutureID client has been accepted by the eSENS large scale pilot as integral, officially supported part. To our knowledge, FutureID is the only FP7 project with contributions accepted by eSENS.

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

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

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

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

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

5 Future Work

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

6 Conclusions

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

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

7 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Architecture for Controlled Credential issuance Enhanced with Single Sign-On (ACCESSO)

Daniel Nemmert[1] Detlef Hühnlein[1] Tobias Wich[1] Tina Hühnlein[1]

Abstract: As more than half of the EU Member States already have rolled out electronic identity cards (eIDs) [Le13], it seems to be a rewarding approach to investigate whether and how eIDs may be used for the purpose of controlling the log-on process for operating systems and similar local access control facilities. While this paper shows that all currently rolled out eIDs may be used for such access control purposes, our investigation also reveals that for some types of eIDs it is significantly harder to support this kind of use case.

Keywords: electronic identity cards (eIDs), access control management, operating system log-on.

1 Introduction

Using two factor authentication for machine log-ins received a serious boost when Apple introduced a fingerprint reader on its mobile devices in 2013. Other manufacturers followed and provide similar biometric readers in their products. Looking at the desktop and laptop market, a quite different picture is shown as fingerprint readers are usually only added to expensive business models.

The other type of candidates for two-factor authentication are smart cards and hardware based authentication tokens in general. In the past this technology has mainly been available to enterprises with large scale deployments and their own Public-Key-Infrastructure (PKI). Nowadays many countries issue eID cards to their citizens leading to the broad availability of secure cryptographic hardware devices. However these cards are mostly intended for online eGovernment use and in some cases to perform digital signatures. Software to integrate these cards into the machine log-on procedure is usually not available or the documentation on how to configure these cards for this purpose is missing. Furthermore there are authentication tokens which are not capable of performing the necessary operations to simply hook into the available log-in frameworks, such as the German eID ("Personalausweis") or FIDO tokens (cf. [FI]) for example.

Information about procedures that can be used in the scope of an operating system log-in is mainly available in the form of standards (cf. RFC 4210 [Ad05], RFC 4556 [ZT06]) or open specifications (eg. Pluggable Authentication Module (PAM)[2]). The field of research concerning this topic seems mainly to be done by companies in internal projects or in the case of PAM in an open source development environment.

[1] {daniel.nemmert,detlef.huehnlein,tobias.wich,tina.huehnlein}@ecsec.de,ecsec GmbH, Sudetenstraße 16, 96247 Michelau

[2] `http://www.linux-pam.org`

This paper presents a universal Architecture for Controlled Credential issuance Enhanced with Single Sign On (ACCESSO), which abstracts the technical details of arbitrary authentication tokens in a way which allows to integrate them into major log-in frameworks, such as Microsoft's Winlogon [In15, Inf] or the Pluggable Authentication Module (PAM) architecture [Th97], which is supported by Linux and Mac OS X. The ACCESSO approach either directly uses the provided capabilities and X.509 certificates of the authentication tokens or generates the required X.509 certificates on the fly after an according authentication has been performed with some alternative authentication method.

2 Background

The ACCESSO proposal integrates eID technology into access control frameworks and hence, we will briefly provide the necessary background with respect to these topics here: In Section 2.1 the various widespread hardware tokens, especially eID cards and the authentication protocols they use, will be discussed. After that in Section 2.2 the architecture and extension capabilities of the major authentication frameworks are considered.

2.1 eID Cards and Authentication Tokens

With respect to currently rolled out eIDs in Europe (cf. FutureID D32.1 [Le13]) one may distinguish between X.509-based eIDs and non-X.509-based eIDs:

- *X.509-based eIDs*
  The majority of the currently deployed eIDs in Europe are equipped with an X.509 certificate, which can be used for authentication and signature purposes. Examples include Finland, Estonia, Sweden, Belgium, Portugal, Italy, Luxembourg and Spain. These type of eIDs may be used for plain challenge-response based authentication protocols in which the eID computes a digital signature over a challenge, which may be chosen at random or be derived from previous protocol messages as in the case of TLS (cf. RFC 5246 [DR08]) for example. While such eIDs may be utilized in a variety of applications, their drawback is that they are not optimal from a privacy point of view, because the legitimate use of the eID in the internet can trivially be misused to create user profiles.
- *non-X.509-based eIDs*
  On the other hand there are non-X.509-based eIDs, such as the German Identity Card (Personalausweis) for example, which uses the Extended Access Control (EAC) protocol as defined in BSI-TR-03110 [Fe15a] for authentication. Such eIDs have great advantages with respect to privacy, as the protocol ensures that only identified entities which have a valid authorization certificate can access the data stored on the card and it is not possible to create user profiles in the internet.
  Furthermore there may be entirely different means for identification and authentication as the eIDAS-regulation (cf. [20114] and [20115]) is fully technology neutral

and the only standardized interface for integrating such eIDs, which is likely to be endorsed by the European Commission, is the SAML-based interface defined in the eIDAS Technical Specifcation [eTS15].

2.2 Access Control Frameworks

Apart from some exotic systems, all current operating systems use a log-in framework to authenticate and authorize their users. In the Unix world the Pluggable Authentication Module (PAM) framework [Th97] is the framework of choice, whereas Microsoft uses the Winlogon System [In15, Inf] for this purpose. We briefly introduce PAM and then focus mostly on the architecture of the Winlogon Framework, because it seems to be more widespread and has a very solid integration of X.509 based signature cards in combination with the Kerberos-based Active Directory (AD) system.

2.2.1 Pluggable Authentication Module (PAM) Framework

PAM was originally proposed by Sun Microsystems in 1995 in the form of an Open Software Foundation RFC [SS95] and later became the Unix standard "X/Open Single Sign-on Service" (XSSO) [Th97]. The specification provides a coarse architecture and a set of C APIs to build a log-in framework as it can be seen in Fig. 1, which has been extracted from the XSSO specification [Th97]. Module implementors must only follow the specification and their modules can run on any system that uses PAM. A wide variety of authentication modules exist for PAM. The most important ones are the Kerberos, LDAP and PKCS#11 authentication plugin. But there are also modules for fingerprint readers, OTP tokens, Bluetooth devices and even Google Authenticator.

2.2.2 Microsoft's Winlogon Framework

Winlogon, in contrast to PAM, is not just a specification by Microsoft, but also an implementation with a fine grained architecture and utility functionality. It has been improved with every Windows version. The biggest change happened in the switch to Windows Vista, where the Graphical IdentificatioN and Authentication (GINA) module [Ing] was replaced by the Credential Providers API [Inf]. Credential Providers are represented by different log-on tiles on the desktop. Credential Providers do not enforce policies or grant access to the operating system, but they are instead used to collect and serialize various types of credentials.

While the high level view of the Winlogon architecture as shown in Fig. 2 seems to be similar to the PAM architecture depicted in Fig. 1, there are two major differences: First there are user interfaces (UI), which provide rich features to display forms to communicate with the user. The second significant difference is represented by the Local Security Authority (LSA). It is a component taking care of authenticating the user with a remote authentication protocol or against some local password database for example. This leads to a looser

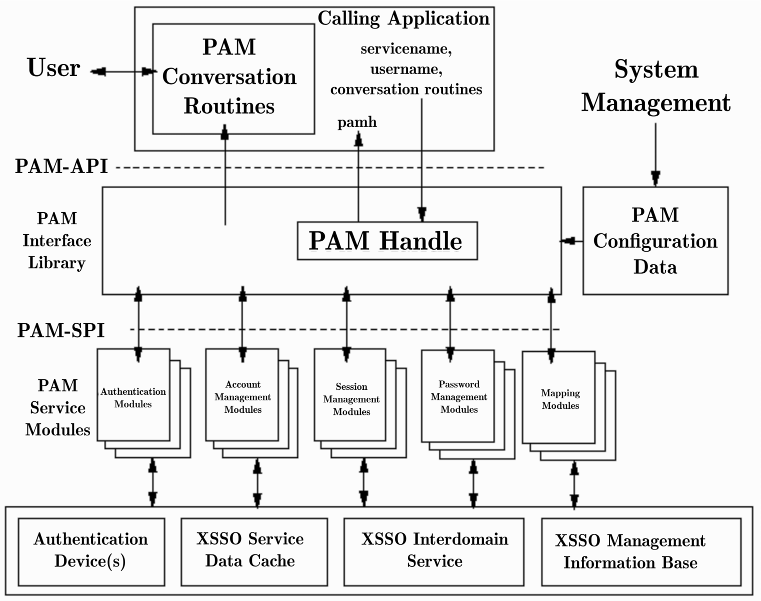


Fig. 1: PAM Framework (source: [Th97, Figure 4-1])

coupling between the authentication protocol such as Kerberos and the credential when compared to the PAM architecture. A high level overview of the Windows log-on process since Windows Vista is presented in [In14]. The Smart Card Infrastructure is outlined in [Ine].

3 Architecture for Controlled Credential issuance Enhanced with Single Sign On (ACCESSO)

In this paper we present a novel and unified system architecture for operating system log-in that supports arbitrary eID and authentication tokens called ACCESSO (Architecture for Controlled Credential issuance Enhanced with Single Sign On), which even allows to support the German eID for controlling access to computers running Windows, Linux or MacOS X for example.

3.1 Overview of ACCESSO

The ACCESSO architecture is depicted in Fig. 3 and comprises a Client, a Server and an Identity Management component:

The *ACCESSO Server* component is a regular Microsoft Domain Controller, which comprises the Active Directory Service (ADS) and a Key Distribution Center (KDC) [Inb], which supports the Kerberos protocol according to RFC 4120 [Ne05] together with the

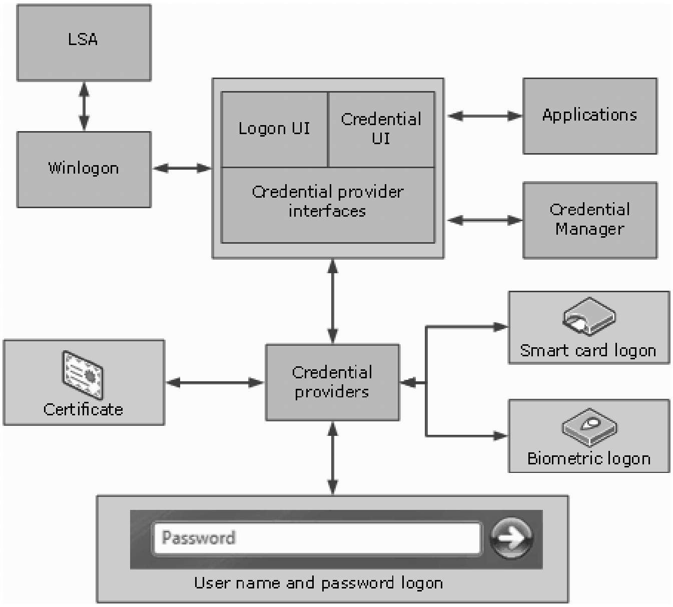


Fig. 2: Winlogon Framework Architecture (source: [In10])

PKINIT enhancements according to RFC 4556 [ZT06] as profiled in [Ind]. The KDC is started by its Local Security Authority (LSA) and is a part of the LSA's process. It is responsible for issuing Ticket-Granting Tickets (TGT) which are presented to the Ticket-Granting Service (TGS) of a domain to gain access to a system.

The *ACCESSO Identity Management* contains a variety of *Authentication Services* (AS) and a *Credential Producer* (CP), which upon request creates certificates and credentials, that are necessary for performing the log-in process. This component may be realized "on-premise" as additional server systems, or the necessary functionality could be obtained as a service from the SkIDentity Service which has received multiple German and European awards and is also patented[3].

The certificate authority used for the issuance of the required certificates has to be trustworthy enough to be suitable for usage in an operating system logon scenario. The validity period of the issued certificate is out of scope for this paper because it has to be defined on a case by case basis, since for a private user a much longer validity of the certificate would be feasible than for example for an institution that handles critical and classified information.

The *ACCESSO Client* contains various modules, which are introduced in the following:

- The *Logon* component represents the Winlogon and the PAM-Interface library on Windows and Unix systems respectively and initiates the Single Sign-On process. It

[3] cf. `https://skidentity.com`, [Hü15a] and [Hü15b] for example.

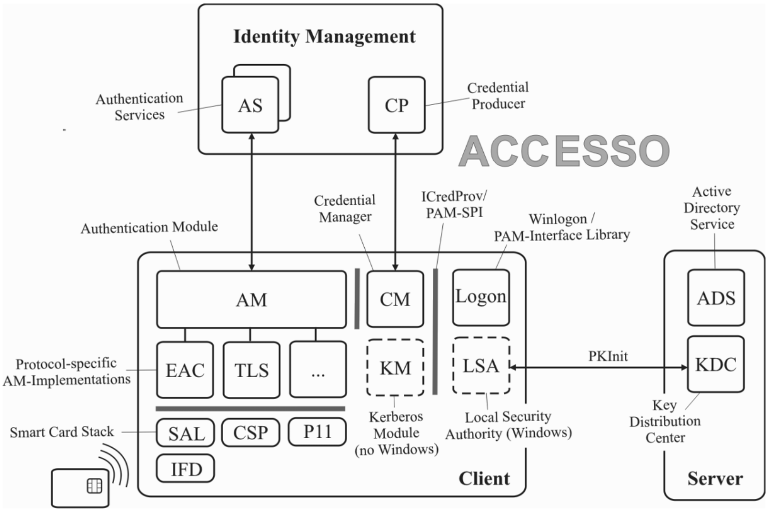


Fig. 3: Architecture for Controlled Credential issuance Enhanced with Single Sign-On (ACCESSO)

is also responsible for the communication with security enforcement points, like the Local Security Authority (LSA) in Windows operating systems.

- The *Credential Manager* (CM) is responsible for generating a key pair on demand and starting the authentication process. The CM also collects the created credential (e.g. a CloudID[4]) and serializes it before it is used in the access decision procedure.
- The *Authentication Module* (AM) provides several protocol-specific implementations that are dependent on which type of credential is being used. For X.509-based eIDs this component can be a TLS implementation. For the German eID an implementation of the EAC protocol is needed. To read information from smart cards, the Smart Card Stack provides components that enable reading of e.g. certificates from smart cards and possibly other types of authentication tokens. Possible modules in the Smart Card Stack include a PKCS#11 module, an Interface Device (IFD) for the German eID that implements an IFD-Interface specified in ISO/IEC 24727-4 [IS08b] and BSI TR-03112-6 [Fe12a] or a Service Access Layer (SAL) that provides an API for client-applications according to ISO/IEC 24727-3 [IS08a].
- The *Local Security Authority* (LSA) (cf. [Inc]) is part of the Windows log-on process and is responsible for authenticating users via an Authentication Package (AP) (cf. [Ina]) (typically Kerberos) and enforcing security and access decision from the AP. The Local Security Policy of a system is maintained through the LSA as well.
- In non-Windows systems there needs to be an additional *Kerberos Module* (KM), which would talk to the KDC in the ACCESSO Server.

[4] cf. `https://www.skidentity.de/en/system/cloud-identity`

3.2 The ACCESSO Protocol

The goal of ACCESSO is to make it possible that arbitrary eID cards and authentication tokens can be used for operating system logon. As some tokens (cf. Section 2.1) are not equipped with an X.509 certificate, the ACCESSO system creates the necessary certificate on the fly after an according authentication has taken place.

While it would seem to be straightforward to use the Certificate Management Protocol (CMP) specified in RFC 4210 [Ad05] for issuing the required credential, the required authentication is neither specified nor seriously considered in CMP and hence CMP does not seem to be a good choice, especially when incorporating complex protocols such as the Extended Access Control (EAC) protocol required for supporting the German eID card.

As only the certificate issuance is needed from the CMP protocol, an alternative solution would be to use authentication protocols capable of exchanging arbitrary data inside the protocol messages. An obvious choice in this regard would be SAML v2.0 [Ca05a], because of its extensibility features and the possibility to send arbitrary data in the authentication request, which is not always the case in other protocols. SAML also has good support in major identity management frameworks and services, such as SkIDentity for example.

In a classical Web SSO setting with SAML, a web browser provides the user agent part of the protocol, which communicates with the Service Provider (SP) and Identity Provider (IdP). However, since the Windows, Linux and Mac OS X log-ons are rather constrained environments, using a browser as the user agent is out of question. As a consequence the Web Browser SSO Profile is not applicable in this scenario. A possible solution would be the SAML 2.0 SSO Profile "Enhanced Client or Proxy" (ECP) [Sc13]. The profile was specifically designed for clients such as desktop applications and anything else which is not a web browser. The ECP application takes the role of the the user agent in the Web SSO SAML profile. A client application using the SAML ECP profile, may be capable of directly initiating an authentication protocol to be performed with the selected IdP as outlined in [Ja10]. As in the Web-SSO profile, there is no means of negotiating the authentication protocol or protocol endpoint, which may lead to complex and hard to maintain client configurations in case of dynamic IdP discovery and the support of multiple tokens is required.

A solution to the discovery issue is given in the "SAML Privacy-Enhancing Profile" [HTW14] that originated from the research project FutureID[5], which was funded by the European Commission in the 7th Framework Programme. This profile is based on the SAML Web Browser SSO profile [Ca05b] and the profile defined in the Technical Guideline TR-03124-1 [Fe15b] of the German Federal Office for Information Security. It allows users to know and choose the IdPs and their supported authentication protocols in advance, saving the user from contacting each possible IdP. Besides that this is primarily benefiting the privacy of the user, it also provides the missing details to use SAML ECP with arbitrary IdPs and credentials.

[5] cf. `http://futureid.eu`

3.3 Protocol Flow

The ACCESSO protocol is implemented in the communication between the CM and the CP and the authentication components (AS and AM). Fig 4 shows the communication between these components in the context of the complete log-on procedure. The following protocol flow corresponds to the flow in a Windows environment. The sequence diagram is meant to provide an overview of the procedure and omits or simplifies steps, which are not necessary for understanding the underlying idea.

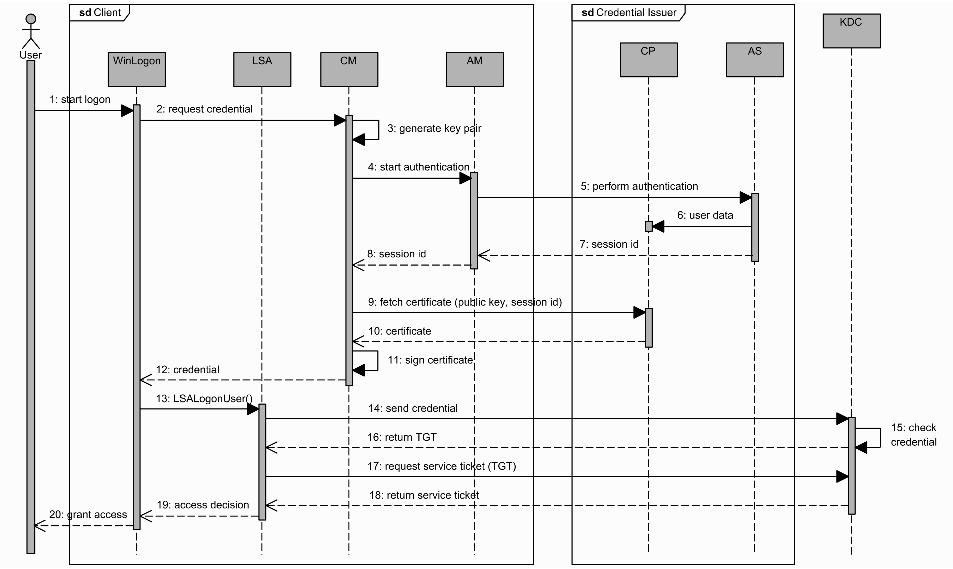


Fig. 4: ACCESSO Sequence Diagram

(1) The user starts the log-on process.

(2) The Winlogon process requests the user credential from the CM.

(3) The CM generates a public/private key pair, if required.

(4) The CM starts the authentication and sends the generated public key to the AM.

(5) In this step the authentication is performed by suitable communication between AM and AS.

(6) The AS sends the user data gathered during authentication, which may comprise an identifier or other identity attributes of the user, to the CP.

(7/8) Parallel to sending the user data to the CP, the AS sends the valid session id back to the CM via the AM.

(9/10) The CM uses the session id and probably additional holder-of-key data to fetch the certificate from the CP.

(11) The CM signs the credential with the generated private key.

(12) The CM serializes the credential according to the needs of the authorization package (in this case the KDC) and returns the created credential to the Winlogon process.

(13) The Winlogon process calls the LSA and provides the generated credential. The call LSALogonUser() starts the access decision procedure.

(14) The LSA sends the credential to the Authorization Package in use, in this case Kerberos.

(15) The KDC checks the credential against a database (typically an Active Directory) to find a valid user for it.

(16) If the credential is valid, the KDC returns a Ticket Granting Ticket (TGT) to the LSA.

(17) The LSA enforces the access decision and returns the decision to the Winlogon process.

(18) Winlogon informs the user about the access decision and grants or denies access.

4 Related Work

For the scope of this paper, the following topics provided relevant information.

The concept of **derived credentials** is not a new one. In october 2014 the National Institute of Standards and Technology (NIST) released Special Pubblication 800-157 [Naa] which contains guidelines for derived "Personal Identity Verification (PIV)" credentials.
One implementation performing the creation of derived credentials is SkIDentity[6]. The service uses the identity information provided by an electronic identity document (eID) to create a so-called *Cloud Identity* (CloudID) which theoretically enables the use of any electronic identity document for authentication. The created CloudID can even be transferred to a mobile phone for (pseudonymous) authentication purposes with a strong identity token.
In 2013 Schröder and Morgner explained the concept of eIDs with derived credentials [SM13] and the advantages over the classic username and password, which is still the most widespread log-in procedure today.

The Technical Guideline BSI-TR-03124-1 [Fe15b] defines how an eID-Client for the **German eID-Card** (defined in BSI-TR-03127 [Bu15]) interacts with an eID-Server in order to perform an authentication. Credentials such as SAML Tokens can then be retrieved from the eID-Server according to the Technical Guideline BSI-TR-03130 [Fe12b].

An example for an upcoming project in the field of derived credentials is **FIDELIO**[7] by the German Federal Office for Information Security which aims to link FIDO and the German eID-Card for online authentication. Results of this project will include the implementation

[6] https://www.skidentity.com

[7] https://www.evergabe-online.de/tenderdocuments.html?1&id=129326

of a FIDELIO-Authenticator-Client and FIDELIO-eService and the operation a FIDELIO-Server for test purposes.

Operating System Logon solutions are provided by various companies. SecureAuth offers a Windows Logon module with the SecureAuth Identity Provider[8]. Yubico offers the possibility to associate a YubiKey with a Microsoft Windows Account[9] for both enterprises and individuals. Enterprise users can use certain YubiKey versions like any other smart card supporting NIST SP 800-73 Personal Identity Verification Card (PIV) [Nab].

5 Conclusions and Outlook

The ACCESSO architecture and protocol outlined in the present paper makes it possible to use arbitrary authentication tokens, including the German eID card, FIDO tokens or OTP tokens for example, for secure operating system logon. This is achieved by generating the X.509 certificates necessary for the Windows logon on the fly. As the protocol may be based on existing SAML profiles, it should be easy to integrate into existing infrastructures based on this protocol.

Besides future research on the topic, further work needs to be spent on creating production ready implementations for the major operating systems. While our research investigated the feasibility of the ACCESSO approach for Microsoft Windows and the PAM implementation used in most Linux distributions, it is not said that other implementations such as the one in Apple's OSX allow these kind of extensions to the login framework.

References

[20114] Regulation (EU) No 910/2014 of the European Parliament and of the council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC), 2014. http://data.europa.eu/eli/reg/2014/910/oj.

[20115] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance)), 2015. http://data.europa.eu/eli/reg_impl/2015/1501/oj.

[Ad05] Adams, C.; Farrell, S.; Kause, T.; Mononen, T.: . Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP). Request For Comments – RFC 4210, 2005. http://www.ietf.org/rfc/rfc4210.txt.

[Bu15] Bundesamt für Sicherheit in der Informationstechnik: . Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel. Technische Richtlinie (BSI-TR-03127), Version 1.16, 14.10.2015, 2015. https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03127/tr-03127.html.

[8] https://www.secureauth.com/IdP.aspx

[9] https://www.yubico.com/why-yubico/for-individuals/computer-login/windows-login/

[Ca05a] Cantor, Scott; Kemp, John; Philpott, Rob; Maler, Eve: . Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, 15.03.2005, 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

[Ca05b] Cantor, Scott; Kemp, John; Philpott, Rob; Maler, Eve: . Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, 15.03.2005, 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.

[DR08] Dierks, T.; Rescorla, E.: . The Transport Layer Security (TLS) Protocol Version 1.2. Request For Comments – RFC 5246, August 2008. http://www.ietf.org/rfc/rfc5246.txt.

[eTS15] eIDAS Technical Subgroup: . eIDAS Technical Specifications v1.0, November 2015. https://joinup.ec.europa.eu/software/cefeid/document/eidas-technical-specifications-v10.

[Fe12a] Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik): . eCard-API-Framework – IFD-Interface. Technical Directive (BSI-TR-03112), Version 1.1.2, Part 6, 2012. http://docs.ecsec.de/BSI-TR-03112-6.

[Fe12b] Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik): . eID-Server. Technical Directive (BSI-TR-031030), Version 1.6, 20.04.2012, 2012. http://docs.ecsec.de/BSI-TR-03130.

[Fe15a] Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik): . Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token. Technical Directive (BSI-TR-03110), Version 2.20, Part 1-4, 2015. https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03110/index_htm.html.

[Fe15b] Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik): . eID-Client – Specifications. Technical Directive (BSI-TR-03124), Version 1.2, Part 1, 2015.

[FI] FIDO Alliance: . FIDO Alliance Specifications (UAF and U2F). https://fidoalliance.org/specifications/download/.

[HTW14] Horsch, Moritz; Tuengerthal, Max; Wich, Tobias: SAML Privacy-Enhancing Profile. In (Hühnlein, Detlef; Rossnagel, Heiko, eds): Proceedings of Open Identity Summit 2014. volume 237 of LNI. GI, pp. 11–22, 2014.

[Hü15a] Hühnlein, Detlef; Tuengerthal, Max; Wich, Tobias; Hühnlein, Tina; Biallowons, Benedikt: Innovative Building Blocks for Versatile Authentication within the SkIDentity Service. In (Hühnlein, Detlef; Rossnagel, Heiko; Kuhlisch, Raik; Ziesing, Jan, eds): Proceedings of Open Identity Summit 2015. volume 251 of LNI. GI, pp. 141–152, 2015. http://www.ecsec.de/pub/OID_2015_SkIDentity_Service.pdf.

[Hü15b] Hühnlein, Tina: . Method and device for authentification. European Patent, EP 2439900, 2015. https://register.epo.org/application?number=EP11184139&lng=en&tab=main.

[Ina] Inc., Microsoft: . Authentication Packages. https://msdn.microsoft.com/en-us/library/windows/desktop/aa374733%28v=vs.85%29.aspx.

[Inb] Inc., Microsoft: . Key Distribution Center. https://msdn.microsoft.com/de-de/library/windows/desktop/aa378170%28v=vs.85%29.aspx.

[Inc] Inc., Microsoft: . LSA Authentication. https://msdn.microsoft.com/en-us/library/windows/desktop/aa378326%28v=vs.85%29.aspx.

[Ind] Inc., Microsoft: . Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol. http://download.microsoft.com/download/9/5/E/95EF66AF-9026-4BB0-A41D-A4F81802D92C/[MS-PKCA].pdf.

[Ine] Inc., Microsoft: . Windows Vista Smart Card Infrastructure. https://msdn.microsoft.com/en-us/library/bb905527.aspx.

[Inf] Inc., Microsoft: . Winlogon and Credential Providers. https://msdn.microsoft.com/de-de/library/windows/desktop/bb648647%28v=vs.85%29.aspx.

[Ing] Inc., Microsoft: . Winlogon and GINA. https://msdn.microsoft.com/de-de/library/windows/desktop/aa380543%28v=vs.85%29.aspx.

[In10] Inc., Microsoft: . Windows Interactive Logon Architecture, February 2010. https://technet.microsoft.com/en-us/library/ff404303%28WS.10%29.aspx.

[In14] Inc., Microsoft: . Credentials Processes in Windows Authentication, May 2014. https://technet.microsoft.com/en-us/library/dn751047(v=ws.11).aspx.

[In15] Inc., Microsoft: . How Interactive Logon Works, March 2015. https://technet.microsoft.com/en-us/library/cc780332%28v=ws.10%29.aspx#w2k3tr_intlg_how_tpxs.

[IS08a] ISO/IEC: . Identification cards – Integrated circuit cards programming interfaces – Part 3: Application programming interface, ISO/IEC 24727-3. International Standard, 2008.

[IS08b] ISO/IEC: . Identification cards – Integrated circuit cards programming interfaces – Part 4: API Administration, ISO/IEC 24727-4. International Standard, 2008.

[Ja10] Jan Eichholz and Detlef Hühnlein and Gisela Meister and Johannes Schmölz: New Authentication concepts for electronic Identity Tokens. In: Proceedings of ISSE 2010. Vieweg, pp. 26–38, 2010. https://www.ecsec.de/pub/ISSE2010.pdf.

[Le13] Lehmann, Anja et al.: . Survey and Analysis of Existing eID and Credential Systems. FutureID Deliverable, D32.1, Version 1, March 2013. http://www.futureid.eu/data/deliverables/year1/Public/FutureID_D32.1_WP32_v1.0_Survey%20of%20existing%20eID%20and%20credential%20systems.pdf.

[Naa] National Institute of Standards and Technology: . Guidelines for Derived Personal Identity Verification (PIV) Credentials. NIST Special Publication 800-157. http://dx.doi.org/10.6028/NIST.SP.800-157.

[Nab] National Institute of Standards and Technology: . Interfaces for Personal Identity Verification – Part 1: PIV Card Application Namespace, Data Model and Representation. NIST Special Publication 800-73-4. http://dx.doi.org/10.6028/NIST.SP.800-73-4.

[Ne05] Neuman, C.; Yu, T.; Hartman, S.; Raeburn, K.: . The Kerberos Network Authentication Service (V5). Request For Comments – RFC 4120, July 2005. http://www.ietf.org/rfc/rfc4210.txt.

[Sc13] Scott Cantor et al.: . SAML V2.0 Enhanced Client or Proxy Profile Version 2.0. OASIS Committee Specification 01, 26.08.2013, 2013. docs.oasis-open.org/security/saml/Post2.0/saml-ecp/v2.0/cs01/saml-ecp-v2.0-cs01.html.

[SM13] Schröder, Martin; Morgner, Frank: . eID mit abgeleiteten Identitäten. Datenschutz und Datensicherheit (DUD), 2013. https://www.bundesdruckerei.de/sites/default/files/documents/2013/08/fachartikel_dud_abgeleitete_identitaeten.pdf.

[SS95] Samar, V.; Schemers, R.: . Unified Login with Pluggable Authentication Modules (PAM). Open Software Foundation Request for Comments 86.0, October 1995. http://www.kernel.org/pub/linux/libs/pam/pre/doc/rfc86.0.txt.gz.

[Th97] The Open Group: . X/Open Single Sign-on Service (XSSO) - Pluggable Authentication Modules. X/Open Document Number: P702, Preliminary Specification, 1997. http://www.opengroup.org/onlinepubs/008329799/toc.htm.

[ZT06] Zhu, L.; Tung, B.: . Public Key Cryptography for Initial Authentication in Kerberos (PKINIT). Request For Comments – RFC 4556, June 2006. http://www.ietf.org/rfc/rfc4559.txt.

Public Online Services at the Age of MyData: a New Approach to Personal Data Management in Finland

Teemu Rissanen[1]

Abstract: MyData is a framework and model for a human-centric approach for managing and processing personal information in the context of online services. The MyData approach is based on the right of individuals to access all data collected about them in public and commercial records. The core principle driving the MyData effort is that individuals should be in control of their own data. The MyData approach aims at strengthening digital human rights while opening new opportunities for businesses to develop innovative personal data based services built on mutual trust and respect of digital privacy rights in a positive way. The Finnish Trust Network (FTN) is a circle of trust composing of nationally notified Identity Providers (IDP) and notified identity service Brokers. It is a technical and legal framework under which different notified IDP's are mandated to provide strong authentication services for Finnish citizens and residents that can access public online services in Finland, in compliance with the provisions of the eIDAS regulation. As a whole, the FTN and MyData networks offer a new platform for reorganising public online services for the 21st century.

Keywords: eIDAS, eGovernment, OpenID Connect, MyData, open data, public online services, user centric data management, consent management, privacy protection, interoperability.

1 Introduction

When we talk about the knowledge or the information society, we can think of "information" as data about and related to a user, whereas "knowledge" as data that is inherent to a user. Therefore the transition from the information society to the knowledge society cannot be achieved unless information about the user becomes inherent to the user, i.e. as an integral part of how a user interacts online with the society and its services. We can call this a user-centric approach, by which we mean a paradigm shift from personal information that is managed in relation to a user, to personal information managed by a user, or with the consent of the user. It is a paradigm shift because it affects how online services should be delivered, designed and developed.

In this paper we present the MyData approach which offers an innovative and practical framework for delivering online services and managing personal data from a user-centric point of view. We will also introduce the Finnish Trust Network (FTN), which is a cloud-based mechanism for connecting large scale, consumer facing services with trusted identity and service providers. The Trust Network follows the requirements and objectives of the European eIDAS regulation for a network of trust service providers enabling Citizen-to-Business-to-Government secure and trusted

[1] Teemu Rissanen, CISM, EuroConseils SPRL, teemu.rissanen@simplysecure.be

electronic service provisioning. The Network is built upon strong privacy and security principles and enables a user-centric attribute consent model.

The MyData initiative is one of the Finnish Government's Spearhead projects as part of the Big Data initiative that is funded by the Ministry of Transport and Communications [HK15]. As a part of the Government's strategic planning with regards to the adoption of policies defining use of Big Data in public services and overall in the regulated society, MyData is seen as a key component in the development of next generation public online services. One of the aims of this policy work is to align it with the EU's forthcoming Digital Single Market initiative, which should address the issues of data ownership, access, interoperability and accessibility as barriers to free movement of data and services across the EU.

In the Finnish eGovernment architecture, the FTN forms the backbone for all trusted, notified and officially accepted ID's in Finland. The aim of the FTN is to offer a standard and interoperable framework for IDP's and Service Providers to offer identity and trust-providing and trust-consuming services for both public and private organisations, with support for cross-border services. In the eGovernment context, the MyData infrastructure is aimed at bridging data flow gaps that exist between public and private service domains, by inserting the citizen / user / consumer in the middle of the data flow puzzle.

We argue that together, the MyData infrastructure and the FTN circle of trust for public and private online services, form an innovative solution for delivering public online services and managing trust in an open multi-stakeholder environment. As both the MyData infrastructure and the FTN circle of trust are at a development stage and no public services that build on them is available yet, this paper aims at envisioning how the future of public online services could and should be delivered in a user-centric and identity-driven way.

2 The case for identity driven user-centricity in public online services

User-centricity has been a very important design concept in popular social media services, but public online services have not put serious design efforts to change their traditional service delivery models. Social media services have also successfully implemented user identity-driven solutions where user accounts form the key for service aggregation. These solutions are dominated by strong industry ecosystems such as Google, Apple or Facebook. Public online services have occasionally taken some advantages from service aggregators but their proprietary nature and lack of identity assurance frameworks limit their usability whit regards to public services. Identity-driven integration within public services has been limited in the use of unique identifiers which are used to connect different personal data sets stored in various databases. This model has different implementation models depending on national legislations on the use of unique identifiers.

The main driver for both identity-driven and user-centric online service models is the increasing economic value of personal data in the digital economy. The Boston Consulting Group [Va12] has calculated that the value created through digital identity could increase at a 22% annual growth rate and applying personal data can deliver a 330 billion annual economic benefit for organisations in Europe by 2020. According to the study, the consumer value of digital identity for consumers will be even bigger (670 billion) and the combined total digital identity value could amount to roughly 8% of the EU-27 GDP by 2020.

This value growth is not automatic though as the study also finds that two-thirds of potential value generation in 2020 (440 billion) could be at risk if stakeholders fail to establish a trusted flow of data. Another trust-based obstacle is related to personal data management. The study finds that most consumers don't know what happens to their data and only 30% have a relatively comprehensive understanding of which sectors are collecting and using their data.

Also usability and awareness are an important issue as the study finds that consumers who are able to manage and protect their privacy are up to 52% more willing to share information than those who aren‘t, but only just 10% of the study respondents had ever done six or more out of eight common privacy-protecting activities (e.g., private browsing, disabling cookies, opt-in/out). Privacy controls need to be easy to use and they should not become an obstacle for getting through online services. The study finds that control and convenience are both highly rated, which means that a truly effective privacy control mechanism should be machine-aided using policy enforcement practices that follow pre-set rules and allows low end-user involvement during normal service use. [Va12] The study gives a positive outlook on personal data sharing: when proper privacy controls and sufficient user benefits are met, most users are effectively willing to share their personal data with public- and private-sector organisations.

Another study done for Orange [Fu14] reaches similar conclusions by stating that while consumers may feel that they no longer govern their data held by organisations, they are increasingly savvy when it comes to the value that they assign to their personal data. The study finds that users not only appreciate that their data has a value to businesses, but that value is variable based on the type of information and the relationship with the organisation. The study states that 80% of respondents think that their personal data has a value to businesses, and it has a higher value when they fit the organisation's customer profile. In conclusion we can state that an important portion of online service users in Europe and in the world want to spend their new "currency" on deals that they like, i.e. consume more personalised online services as long as they are in control of the data, receive adequate benefits from sharing their data and can trust the security of the service.

3 MyData principles

The governing principle for MyData is to provide human centric control and privacy where individuals are empowered actors, not passive targets in the management of their personal lives both online and offline [HK15]. A study conducted for Orange [Fu14] finds that consumers in all parts of the world have a growing mistrust of organisations' ability to protect personal data, even though some services are faring better than others. European consumers feel that there is a vacuum when it comes to the presence of a trusted entity to advise them on how to protect their personal data. The study finds that European consumers struggle to have control over their personal data when organisations are becoming increasingly sophisticated in the ways in which they capture and use this data. With MyData, users have the right and practical means to manage their data and privacy.

The second MyData principle is that data should usable so that personal data is technically easy to access and use in machine readable open formats via secure, standardized APIs. MyData is a way to convert data from closed silos into an important, reusable resource. It can be used to create new services which help individuals manage their own data. The providers of these services can create new business models and economic growth to the society. The Orange study also supports this principle as it finds that consumers feel that, on balance, organisations benefit most from customer data sharing. [HK15]

The third MyData principle is about creating an open business environment where a shared MyData infrastructure enables decentralised management of personal data, improves interoperability and makes it easier for companies to comply with tightening data protection regulations. This environment should also allow individuals to change service providers without proprietary data lock-ins. [HK15]

4 The Finnish Trust Network

4.1 FTN organisation and objectives

The Finnish Trust Network (FTN) is a circle of trust composing of nationally notified Identity Providers (IDP) and notified Identity Service Brokers. The FTN is not a national identity scheme per se – it is a legal framework under which different notified IDP's are mandated to provide strong authentication services for citizens to access public services in Finland. The FTN is based on the revised law on Strong Electronic Authentication and Electronic Signatures [La09].

Technically the FTN is a cloud-based mechanism for connecting large scale, consumer facing services with trusted identity and service providers. The Trust Network delivers the following benefits:

- For citizens, the FTN delivers a familiar, fast and simple online service sign-on experience
- For online services, the FTN removes the barriers of security and complexity related to implementing strong authentication, which is based on mutually accepted levels of assurance.
- For identity providers that issue authentication credentials, the FTN provides new opportunities to leverage the success of their credentials platform and expand credential usage.

The Trust Network follows the requirements and objectives of the European eIDAS regulation for a network of trust service providers enabling Citizen-to-Business-to-Government secure and trusted electronic service provisioning. The Network is built upon strong privacy and security principles and enables a user-centric attribute consent model.

4.2 FTN members and legal framework

The FTN is a circle of trust whose members are either Identity Providers or service Brokers that notify their respective services in accordance with the provisions of the forthcoming regulation MPS72 [Fi16] and the law on strong authentication and electronic signature [La09]. The members will compose of a mix of Public and Private IDP's and identity service Brokers. The FTN IDP's include banks, mobile network operators and the Finnish Population Register Centre, which is the national CA that issues the Finnish eID. Identity Brokers can be private or public service providers, that enable the integration of Service Providers with Identity Providers and offer a technical platform for users to access public sector Service Providers. In most cases the IDP takes the role of an Identity Broker, but these roles can be independent from one another.

The Regulation MPS72 defines requirements, amongst others, for FTN IDP's and Brokers, and transfers enforcement obligations for Brokers towards Service Providers. Even though service providers are not directly subjected to the requirements of the regulation, the FTN Brokers are responsible for the service providers to comply with the regulation's secure data processing requirements.

The FTN conforms with the eIDAS technical specifications for cross-border authentication using national PEPS nodes with regards to exchanged attributes and attribute naming, which are kept identical. The security requirements are compliant with the eIDAS technical specifications: all tokens and assertions are encrypted and signed, at the transport level, TLS 1.2 is required. [Fi16]

The FTN providers need to comply with published technical interface standards as defined in the regulation MPS72. These specifications mainly describe the mandatory and optional data exchange protocols, attributes and minimum security requirements. The FTN providers can implement additional features and services or alternative protocols, provided that the interfaces are publicly available, open to implement and comply with the attribute and security requirements. This approach gives the industry the freedom to develop and deploy solutions that best fit the functional requirements. The regulator is confident that all FTN providers will mutually agree on the technical implementation details since there is no business incentive for individual IDP's or Brokers to deploy un-interoperable solutions since they would not be able to attract service providers to sign up and register as customers. The regulation references two alternative FTN service interface protocol specifications, which are published as implementation examples that define the minimum data sets for attribute exchange within the FTN and the minimum security requirements. The specific security implementation requirements are included as references to mandatory national security implementation standards. [Fi16]

The FTN SAML 2.0 interface specification is based on the currently implemented Finnish public sector SAML 2.0 profile, which in turn is based on the SAML 2.0 WebSSO profile. The specification complies with the eIDAS technical specifications for cross-border authentication using national PEPS nodes and it is very similar to the Swedish national eID SAML 2.0 profile.

The FTN OpenID Connect interface specification is based on OpenID Connect 1.0 specification and it follows the US Connect.gov draft specification with the aim of updating the specification in the future in order to comply with the OpenID Connect iGov profile specification, as this will be ready. It is well understood that security wise the OIDC protocol is not as mature as SAML2 and even though it supports strong encryption and electronic signing of Java Web Tokens, other security issues that are addressed in SAML2 by default, are open in the OIDC basic specification. The security requirements will eventually be revised by the regulator as regulation MPS72 updates. The two interface specifications are not published yet, but will be by September 2016.

4.3 Levels of Assurance within the FTN network and the MyData infrastructure

User authentication assurance levels are based on the eIDAS Level of Assurance (LOA) levels. The same assurance levels are implemented in order to simplify the normative referencing of standardised authentication assurance levels. For accessing Finnish public online services, only LOA levels “Substantial” and “High” are accepted. At the current moment all existing and previously notified national IDP’s offer only Substantial level authentication, but the National eID will seek for conformance with LOA level High. [Fi16] The benefit of aligning the FTN with eIDAS node specifications is that IDP’s would not need to implement different technologies or methods in a cross-border scenario. Also common language and shared standards limits the need to create and maintain proprietary or domain specific standards and practices.

In the cross-border authentication eIDAS Node context, the Finnish Population Register Centre (PRC) acts as the country Node [Fi16]. As it is also a member of the FTN, the relation with the FTN and the cross-border context is identical. Also mobile network providers will be participating in the trust network. The three main mobile operators Elisa, Sonera and DNA already provide mobile eID services that are usable in a federated mechanism. The FTN can have natural cross-border interactions, due to the cross-national nature of its IDP service providers: Sonera is part of Telia of Sweden, which is a major carrier and mobile operator in other Nordic and Baltic countries, and two of the three major banks that are currently acting as IDP’s on a national level (Nordea and Danske Bank) are active IDP providers in other Nordic countries as well. In this context it is foreseeable that a lot of cross-border trust service provisioning could take place in the Nordics, thanks to eIDAS.

As a private sector solution, the MyData infrastructure would require the use of identity services that conform to minimum national requirements and LOA level Low identity assurance. But as MyData also aims at becoming a trusted infrastructure to service citizens in relation to their own data stored and managed in public service records and systems, the need for a MyData / FTN interaction becomes apparent. How this would work in practice is that as some IDP’s are already members of both the FTN and the MyData Alliance networks, these IDP’s could provide trusted and notified identity services that bridge and link the different components that make up the fabric of online services in Finland; public and private.

The benefit in this approach is that it would combine the goals and benefits of both networks and enable increased added value for all parties involved. The added value for the public services comes from the innovative solutions for service delivery and provisioning for citizens and also intra-administration data exchange, based on the MyData model. An added benefit comes from increased security as the FTN would provide for a strong authentication mechanism that protects user credentials that are used for accessing the user’s MyData Account at the MyData Operator.

5 MyData architecture

In this section we provide an overview of the main features of the MyData Infrastructure and key elements for an MyData-FTN integration.

5.1 How MyData works

MyData is an infrastructure-level approach for ensuring data interoperability and portability. The open infrastructure makes it possible for individuals to change service providers without proprietary data lock-ins. MyData is sector independent and offers a consent-based data management and control solution for individuals to store all their data in centralised repositories in order to control the data flow. [HK15]

In practice the MyData approach works as follows: MyData Accounts hold the consents that determine how an Individual's data can flow from data sources to data users in an authorised system. For personal data management it is sufficient for the authorisation consents to be centralised in the MyData account. Data can flow directly between the source and the user.

With the MyData infrastructure data flows become manageable, comprehensive, and transparent, meaning that they include all privacy relevant transaction processes in a uniform way that follows predefined rules and policies, and which can be audited. Users can deactivate information flows and withdraw consent for all or specific services and applications from one single point. The MyData Account holds machine-readable consents that can be visualized, compared, and processed automatically. There is also a possibility to use pre-defined privacy and consent policy rules that respond to different profiles and contexts. [HK15]

5.2 The MyData services and authentication

The primary function of a MyData account is to enable consent management. The individual's data itself is not necessarily streamed through the servers where the MyData Account is hosted. In the MyData architecture, data flows from a data source to a service or application that uses the subsequent data and within the MyData infrastructure, the flow of consents or permissions is separate from the actual flow of data.

There are four defined roles within the MyData architecture include 1) Users, 2) MyData Operators, 3) data Sources that hold personal data, and 4) data Sinks that use and consume personal.

Core parts of the MyData authentication mechanism and the MyData APIs can be realised using the User-Managed Access (UMA) standard created by the Kantara Initiative. The UMA specification and its open-source implementations let individuals control authorisations to share their data and to manage how their data is shared between online services. Just like OpenID Connect, UMA is a profile of OAuth 2.0, which is a standard for controlling access to web API's. As OpenID Connect enriches the OAuth 2.0 data access protocol with Federated Identity and Web Single-Sign-On functionality, UMA enriches the OAuth 2.0 protocol with user-centric authorisation functionality. UMA bring two essential elements to the authorization workflow: asynchronous consent and centralized consent management, which are key for enabling the MyData model to work. [HK15]

5.3 Consent Based Approach for Personal Data Management

A legal framework for protecting personal data online is based on a specific, informed, unambiguous and freely given user consent. Processing of personal data is thus subject to the conscious choice to give consent for an external organisation to process data. Also this consent has to be withdrawable, changeable and readable by the involved trusted parties. Finally the consent should be stored appropriately for enabling validity checking by the parties using or providing personal data.

MyData is focused on consents because consents are a primary legislative framework that defines information processing from the human-centric perspective. The same consent management framework can also be used with minor modification for notifications and assignments. In additions the human and machine readable standardised consents unite technical data management systems, legislative frameworks, and the human perspective. [My16a]

5.4 MyData Service Linking

The MyData service end-user is also called a MyData Account Owner. To be able to manage access to their data, the Account Owner first has to attach the related service to the MyData Account. MyData Service Linking means the act of adding a service (a Source or a Sink) to a specific Account Owner's MyData Account. A successful Service Linking results in a Service Link Record stored in the MyData Account. A valid Service Link Record is required before any data processing consent authorisation can be issued or used within the MyData ecosystem.

Service Link removal process is initiated when either a) Account Owner wants to remove a service from MyData Account, b) service deregisters from the Operator, or c) Account Owner removes an account at the service and there is no need to keep the Service Link, in which case it's service's duty to remove the unnecessary Service Link. The main purpose of Service Linking is to create a Service Link Record as this record contains keys used to sign MyData Consent Records. Without a Service Link Record, MyData Authorisation is not possible.

Service Link Record can be in Active or Removed state. When a new Service Link Record is constructed, it is in Active state. When a Service Link is removed, the Service Link Record is set to Removed state. There can be only one Active Service Link Record between the Account Owner and a service. [My16b]

In the FTN context the Broker service would need to provide the relevant MyData interfaces so that the user can authorise provisioned services.

5.5 MyData Service Registry

The main feature of the Service Registry is to allow the registration and discovery of available services and to facilitate service developers and service providers to manage registrations and to discover available services. The Service Registry is a component that provides identities to all services registered at a given Operator. Each service has a comprehensive Service Description accessible through the Service Registry. A Service Description consists of multiple parts enabling different types of service discovery.

The MyData architecture comprises of two types of services:

1. Services providing data resources to others are called Source services (data providing service)
2. Services requiring data from other services are called Sink services (data consuming service)

The main difference between these service types is that the Sink services do not expose a service interface for data access whereas the Source services do. The Service Registry is part of the MyData Operator service and it maintains a database of all the accessible and registered services. The service registration phases are as follows:

1. A service provider registers services, receives a unique ID for the service and creates the

required service descriptions.

2. The Service Registry provides identities to all services registered to an Operator and provides access to the required Service Descriptions
3. A service instance is then set up, which implements the described service interfaces. After a successful Service Registration, a MyData Operator is then able to search for compatible services (Service Discovery).

Service Descriptions are defined for each service in the MyData architecture. The service end-users are provided with a Human Readable Description of the service and its purpose, and for computer services, several Technical Descriptions of the service are provided by the service registry. The machine-readable API description of the service interface is essential for service developers for enabling service integration. In addition to providing the identity and description of the different services, the Service Registry also manages the endpoints of the registered services using specific Service Access URI addresses. [My16c]

In the FTN context the Broker service would need to provide the relevant MyData interfaces so that different available services can be discovered and provisioned for the authorised user.

5.6 MyData Authorisation

In the MyData architecture, all processing of personal data requires a legal basis. The term personal data processing is used to describe all data collection, movement and processing. There can be several possible bases for processing, but all data processing that is based on the consents from the Account Owner, can always be changed or withdrawn at will by the user.

The consent mechanism is restricted to processing activities that can be legally subjected to user consent, as defined in the EU GDPR. From a public service provider point of view, consent is only one possible ground for processing personal data and it does not always constitute the most typical ground. The MyData architecture provides a tool for the Account Owners to control the processing of their personal data not only when consent based data processing is grounded, but also in other case by providing a unified vantage point for all types of personal data processing activities.

In the MyData Architecture, when an Account Owner issues a consent this is documented in a MyData Consent Record (CR). A Consent Record is a manifestation of legally valid Consent which enables dynamic changing or withdrawing the user's consent. Consent Records are stored in the MyData Account and at the related service. For authorising data processing within a service, the Account Owner creates a single Consent Record for the related service. For authorising data transfer from a specific Source to a specific Sink, the Account Owner creates a pair of Consent Records (one for the Source and one for the Sink). Then, the Source's Consent Record defines, what data can be provisioned to the specified Sink. The Sink's Consent Record defines how the data can be accessed and it can also include the permissions for data processing. On a more granular level, the consents are managed as Resource Sets, which define specific subsets of data that a particular Source service provisions or processes. [My16d]

In the FTN context the user could authorise and manage consents for the different public online services and hold all the consents in one single MyData Account. Currently these features are implemented in certain services such as the tax service, but the MyData approach could generalise authorisation and consents management to all available services.

5.7 MyData Connection

In the MyData architecture a Data Connection is an authorised transfer of data from a specific Source to a specific Sink. This authorisation is given by the Account Owner in the MyData Authorisation transaction. Multiple Data Connections from a Source to a Sink are allowed as long as the subsequent authorisation is not deactivated or withdrawn. For the Source service the user's authorisation consists of a Consent Receipt which describes what data can be provisioned to the requesting Sink service. For the Sink service, the authorisation consists of a Consent Receipt describing how data can be processed and a access token, which is used to authenticate as an authorised data requester towards the Source service. The token is a Proof-of-Possession / holder-of-key type token, which contains Sink services public key. The data request must be signed with the Operator's corresponding private key. The token is both generated and signed by the Operator. [My16e]

The Data Connection Transactions are the following:

- The MyData Operator delivers an access token to the Sink service
- The Sink service request an access token from the Operator
- The Sink service requests data from the Source service

The FTN requires authorisation and authentication of all data connections and transfers and as such, the MyData infrastructure would enable a user-controlled assurance mechanism for securing data transactions towards service providers, which are not supervised by the national regulator. This feature would benefit the service providers as they would be able to integrate within the MyData and FTN networks in a standardised and compliant way. The FTN Broker would need to assure that the access connection token scopes match the scopes that requested and also that the rules applying the various scopes are met. In the FTN the service Broker defines access token scopes on the behalf of the service provider that describe what personal data is requested and fetched from the IDP. In the MyData context this same mechanism is delegated to the MyData aware Broker.

6 Conclusions: online services and the MyData infrastructure

The FTN forms the backbone for all trusted, notified and officially accepted ID's in Finland. The aim of the FTN is to offer a standard and highly interoperable framework for IDP's and Service Providers to offer identity and trust providing and consuming services for both public and private uses, and also supporting cross-border services. The MyData infrastructure is aimed at bridging data flow gaps that exist between the public and private domains, by inserting the citizen / user / consumer in the middle of the data flow puzzle.

As a private sector solution, the MyData infrastructure would only require the use of identity services that conform to minimum national requirements and LOA level Low identity assurance. But as MyData also aims at becoming a trusted infrastructure to service citizens in relation to their own data stored and managed in public service records and systems, the need for a MyData / FTN interaction becomes apparent. How this would work in practice is that as some IDP's are already members of both the FTN and the MyData Alliance networks, these IDP's could provide trusted and notified identity services that bridge and link the different components that make up the fabric of online services in Finland; public and private.

The benefit in this approach is that it would combine the goals and benefits of both networks and enable increased added value for all parties involved. The added value for the public services comes from the innovative solutions for service delivery and provisioning for citizens and also intra-administration data exchange, based on the MyData model. For the MyData network the obvious added value is the possible inclusion of major personal data services from the public domain in the MyData infrastructure, hence strengthening its uptake as a new standard solution for user-centric data exchange.

For the MyData community, which comprises of major private, public and semi-public service providers and stakeholders, the added value comes from the possibility to engage with users and consumers in a more meaningful way as the infrastructure enables user-consent based data exchange between all parties involved. In the current silo and verticality bound data contexts, the inter-linking of the public-driven FTN and the private-driver MyData networks would create a totally new way for citizens to interact with all relevant parties that are currently in custody of the citizen's own data.

The possibilities to create and recreate public online services that are based on user-centricity are limitless and they should be regarded as a major innovation enabler for the public services globally. User centricity is seen as key when facing the challenges for citizens privacy, posed by over-exposure to digital services that fail to protect private data when it is linked and utilised and many separate contexts and systems. User centricity is also key for addressing the compliance challenges posed by the upcoming GDPR for the public and private bodies that manage private data in their systems and services. In both contexts the MyData approach offers an infrastructure solution that addresses the needs and requirements of all parties and domains.

The FTN IDP service providers can offer two types of services within the FTN/MyData networks: user identity federation for both FTN service providers and MyData Operators and strong end-user authentication for the MyData Operator. The MyData Operator may choose to opt for different LOA authentication levels, but depending on the MyData Source and Sink services higher LOA levels may be required. The MyData Source service defines the required authentication assurance level and it is up to the MyData aware FTN service Broker to assure that the access token scope rules are met when connecting between a FTN IDP and a MyData Source, through the MyData Account, which acts as the end-user control point. Based on the national legislation, at least a substantial assurance level authentication is required for accessing public sector Source and Sink services.

For the sake of user friendliness, commercial MyData Sink services may be satisfied if a user is authenticated at a Low level. This lower level security option should not endanger the integrity of the integrated FTN/MyData infrastructure since the MyData aware FTN Broker would not accept sending access token requests for FTN service providers when the required LOA minimum assurance level is not satisfied. The FTN service brokers, which connect IDP's with different service providers can specialise in different sectors of online service areas: some brokers would integrate only public sector domains whereas others would only integrate with commercial services, or MyData Operators. In order for service providers to not need to implement separate interfaces for the FTN and MyData Operators, the FTN brokers could provide unique integration points for the different interfaces.

The possibilities to create and recreate public online services that are based on user-centricity are limitless and they should be regarded as a major innovation enabler for the public services globally. User centricity is seen as key when facing the challenges for citizens' privacy, posed by over-exposure to digital services that fail to protect private data when it is linked and utilised and many separate contexts and systems. User centricity is also key for addressing the compliance challenges posed by the upcoming GDPR for the public and private bodies that manage private data in their systems and services. In both contexts the MyData approach offers an infrastructure solution that addresses the needs and requirements of all parties and domains.

References

[Fi16] Finnish Communications Regulatory Authority, Regulation MPS72. https://www.viestintavirasto.fi/en/steeringandsupervision/actsregulationsdecisions/regulations.html, https://www.viestintavirasto.fi/attachments/maaraykset/Luonnos_13.5.2016_MPS72_maarayksen_perustelut_ja_soveltaminen.pdf, Stand: 1.8.2016

[Fu14] The Future of Digital Trust: a European study on the nature of consumer trust and personal data, Orange, Loudhouse , 2014. www.orange.com/en/content/download/21358/412063/version/5/file/Orange+Future+of+Digital+Trust+Report.pdf, Stand: 1.8.2016

[HK15] Honko, H; Kuikkaniemi, K; Poikola, A: MyData - Nordic Model for human-centered personal data management and processing – Whitepaper-Ministry of Transport and Communicaitons, Helsinki 2015. http://urn.fi/URN:ISBN:978-952-243-455-5, Stand: 1.8.2016

[La09] Law on Strong Electronic Authentication and Electronic Signatures 2009/617, http://www.finlex.fi/fi/laki/ajantasa/2009/20090617, Stand: 1.8.2016

[My16a] MyData Architecture - Consent Based Approach for Personal Data Management, v1.1, http://hiit.github.io/mydata-stack, Stand: 1.8.2016

[My16b] MyData Service Linking Specification, v1.1, http://hiit.github.io/mydata-stack, Stand: 1.8.2016

[My16c] MyData Service Registry Specification, v1.1, http://hiit.github.io/mydata-stack, Stand: 1.8.2016

[My16d] MyData Authorisation Specification, v1.1, http://hiit.github.io/mydata-stack, Stand: 1.8.2016

[My16e] MyData Data Connection Specification, v1.1, http://hiit.github.io/mydata-stack, Stand: 1.8.2016

[Va12] The Value of Our Digital Economy, Liberty Global, Inc. with The Boston Consulting Group, Inc., 2012. www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf, Stand: 1.8.2016

An eID mechanism built along Privacy by Design principles using secure elements, pseudonyms and attributes

Denis Pinkas[1]

Abstract: This eID mechanism has been built taking into consideration Privacy by Design principles. It uses some of the basic principles of the FIDO model (Fast Identification On-line) adding certain constraints and extending the model to push user attributes. It allows a user to open an anonymous account on a server using a random pseudonym and then to push one or more attributes contained in an access token that has been obtained from an Attribute Issuer. In order to prevent the forwarding of an access token between collaborative users, a Secure Element must be used. That Secure Element shall conform to specific requirements, e.g. defined using a Protection Profile. This eID mechanism will be worldwide usable as soon as the providers of such Secure Elements publish information that can verify the genuineness of these secure elements.

Keywords : Privacy by Design, secure element, eID mechanism, authentication, Attribute Issuer, access token.

1 Introduction

Numerous eID mechanisms have been proposed up to now, but none of them has been built taking into consideration at the very beginning the privacy of individuals. In some cases, the motivation only came from the invention of a new cryptographic algorithm, for example, able to hide some of the attributes placed inside an access token that would contain all the attributes of a user.

In many cases, privacy considerations have been added afterwards while in other cases they have been simply ignored, as it is the case for the eIDAS Regulation [Re14].

The goal of this document is first to define a model and to identify requirements in order to define a world-wide scalable interoperability framework able to support the implementation of the principle of privacy by design in a secure manner and then to describe an eID mechanism that complies with these requirements.

This document uses principles established by FIDO [FIDO]. The principles and the concepts of FIDO are assumed to be understood and are not explained in detail.

[1] DP Security Consulting, 13 Rue Du Pave Des Gardes, 92370 Chaville, France, denis.ietf (at) free.fr

2. Architecture

The model has three components:

- The human user that is represented by a *User Agent*, a software and or hardware component running on a local device (e.g. on the user’s computer or the user's mobile phone).

- A *Service Provider* that protects the access to a service (or to a resource within a service). In the literature, a Service Provider is sometimes referred as a *Verifier* or as a server.

- An *Attribute Issuer* that delivers in an electronic form the users' attributes of any kind. In the literature, an Attribute Issuer is sometimes referred as an Attribute Provider.

Attributes are obtained by the User Agent from an Attribute Issuer. These attributes are placed inside an access token, i.e. a string of bytes cryptographically signed by an Attribute Issuer. The use of access tokens allows support for direct trust relationships eliminating the need to include nodes in the architecture. This is illustrated on Figure 1.

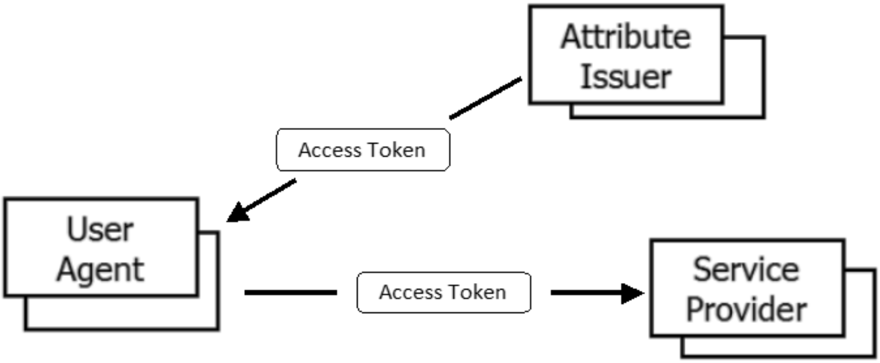


Figure 1 — The basic components of the basic model

The eID scheme is based on a push model, where user's attributes are pushed by the User Agent from an Attribute Issuer towards a Service Provider using an access token.

3. Privacy by Design (PbD) requirements

Most "Privacy by Design" principles are currently defined from the perspective of a single "data controller".

For example, the UK Data protection Act or the EU General Data Protection Regulation Principles relating to personal data processing. The point of view of the user is mainly ignored, as well as unauthorized collaborations between servers from a privacy perspective (or between users from a security perspective).

From a user perspective, it is necessary:

(a) to prevent the linkability of transactions of a user among distinct servers or even within a single server (Unlinkability),

(b) to restrict the amount of attributes being disclosed by a user to the minimum necessary to achieve a stated purpose (Data minimization),

(c) to enable users to give their consent for the communication of their attributes through an affirmative process (User Consent), and

(d) to prevent an Attribute Issuer knowing to which Service Provider an access token will be presented by the User Agent (Untraceability).

These four privacy properties will be used to construct the eID mechanism.

4. Security requirements

It is then necessary to make sure that the eID mechanism will also be secure.

Prevention of token forwarding

Generally, the access of a client to a server is conditioned by the presentation of certain "attributes" of the user.

There are cases where it is desirable to demonstrate to a server that a person is over 18 years, without the need to reveal his birth date nor any other attribute.

It is generally considered that there are two kinds of people: honest people who use a system that are located inside the system and attackers located outside of this system. While this vision is helpful, it is not sufficient. People who use a system that are located "inside the system" may also be considered as attackers in particular when they agree to work collaboratively to cheat a server.

As an example, a person over 18 that can legitimately obtain an access token demonstrating that he is over 18 could attempt to transfer that access token to a person that is under 18 so that second person could take advantage of this property long after the transfer: if someone is over 18 one day, he will necessarily remain over 18 the following days. Thus a server could remember that property and then not ask the person to present the same property again when subsequent accesses are performed by the same person.

The ABC4Trust project provides an interface able to support two solutions: "U Prove" from Microsoft and "Identity Mixer" (IdeMix) from IBM Zurich. As described in the publicly available documentation, despite the sophistication of the cryptographic algorithms that are being used, none of these two solutions is able to prevent the transfer of an attribute of a person that indeed possesses it to a person that does not possess it.

Whatever cryptography is being used, a solution that uses software only will be unable to prevent the transfer of an attribute of a person that possess it to a person that does not possess it. As soon as access tokens are being managed, Secure Elements meeting "some specific requirements" need to be involved in the process.

5. Construction of the eID mechanism

5.1. Taking into consideration PbD requirements

In order to prevent the linkability of transactions of a user among different servers, a different pseudonym will be used for every server. This eID mechanism is based on the concepts developed by FIDO [FIDO]. However one major difference with FIDO should be noted.

The FIDO Universal 2nd Factor (U2F) Overview [Un16] states on line 145:

> "Thus, the Key Handle is simply an identifier of a particular key on the U2F device".

In this eID mechanism, the key handle will be used as a pseudonym. A change in the semantics of the key handle is thus needed:

> The Key Handle shall be a random number sufficiently large (e.g. 16 bytes) generated by the U2F device, that will be used :
>
> - by the U2F device as an identifier of a particular key on the U2F device.
> - by the Service Provider as a pseudonym to identify the user.

As a result, a user can open a user account on a server using only one pseudonym. This account may be permanent or temporary. In both cases, it is thus possible to prevent the linkability of transactions of a user among distinct servers or even for the same server. As in FIDO, Secure Elements are used to store Key Handles (in this case, pseudonyms) and the associated private keys.

In order to minimize the amount of attributes being disclosed by a user to the minimum necessary to achieve a stated purpose, an access token will only contain the set of attributes that is needed. This may be done using conventional cryptography.

In order to enable users to agree to consent for the communication of their attributes through an affirmative process, the user will be able to select the attributes that he would like to be placed in an access token.

He will also be able to verify himself which attributes have effectively been placed in an access token by the Attribute Issuer before forwarding it to a Service Provider.

As a counter example, there exists a mechanism described in EN 419 212 [Ap15] that allows support for pseudonyms after 27 exchanges and identity attributes after 45 exchanges. However, since most of the exchanges are made using secure messaging, a User Agent will be unable to verify the content of the response obtained from the Attribute Issuer and hence the content of the access token.

The debugging of these exchanges is also a concern, since it cannot be done at the level of the User Agent.

In order to prevent an Attribute Issuer from knowing to which Service Provider an access token will be presented by the User Agent:

- there shall be no direct interaction between an Attribute Issuer and a Service Provider, and
- the access token shall not contain any data that would allow the Attribute Issuer to identify the Service Provider.

5.2. Taking into consideration security requirements

5.2.1 Prevention of token forwarding

It is necessary to prevent a legitimate user collaborating with another user to obtain an access token for himself but targeted to a user account (i.e. a pseudonym) belonging to an illegitimate user.

This will be done using the combination of several mechanisms:

1) pseudonyms are pseudo random numbers sufficiently large that can only be generated by secure elements. Since neither users, nor Services Providers will be able to choose their values, this means that their values will be unique.
2) key pairs associated with pseudonyms are randomly generated by secure elements. Private keys cannot be exported, nor imported.
3) access token requests can only be granted if generated by secure elements. An element of the access token request contains a field that designates the owner of the access token and the designated owner can only be a pseudonym that already exists within the secure element. That field will be duplicated into the

access token by the Attribute Issuer to designate the owner of the access token,

4) access tokens shall be presented to a Service Provider either after an authentication exchange using the private key relative to the pseudonym or as part of a data origin authentication message using the private key relative to the pseudonym.

In this way, a Secure Element will be unable to generate an access token request for a pseudonym that exists externally to the Secure Element, either contained within another access token or not (software implementation of FIDO). This means that an access token targeted to one pseudonym cannot be stolen by another user.

5.2.2 Verification that a Secure Element is being used

It is important to notice that only Attribute Issuers need to know that such Secure Elements are being used before accepting to issue an access token.

In other words, Service Providers do not need to check directly that a Secure Element is being used. They will know it indirectly: Attribute Issuers trusted by Service Providers shall not agree to issue access tokens unless they have verified that a Secure Element is being used by a User Agent to request an access token.

When Secure Elements (called "authenticators") are being used, FIDO (Fast Identification On-line) [Fa16] uses "attestation certificates". However, Secure Elements of the same model share the same attestation private key. This is necessary since attestation certificates may be checked by Service Providers. Otherwise a different private key assigned to each Secure Element would permit tracking the users. The drawback is that it is not possible to individually revoke a secure element.

In this eID scheme, a "conformance certificate" shall only be issued by the provider for a Secure Element when it meets specific requirements usually defined using a Protection Profile (PP). This does not also prevent issueing "attestation certificates" in order to remain FIDO compatible when no user attributes are being used, but "attestation certificates" are not used with this mechanism.

Another advantage of such an approach is to allow the use of individual "conformance certificates" that allow, when necessary, to revoke a given secure element.

The verification by an Attribute Issuer of the fact that a Secure Element is being used may be performed at the time of the enrollment of the user towards the Attribute Issuer or when requesting an access token from the Attribute Issuer.

Some messages generated by the Secure Element that will be forwarded to Attribute Issuers shall be signed or counter-signed using the private key initially stored by the device's provider. Obviously, to allow the verification of the digital signature of such messages, the conformance certificate shall be added to the signed or counter-signed message.

6. The eID mechanism at work

6.1. Basic scenario

All the exchanges between a User Agent and either Attribute Issuers or Service Providers are made either using HTTPS, SSH or a VPN. The User Agent connects to a Service Provider in order to register a user. To do this, it first connects to the Secure Element and issues a SERVICE_ENROLL command (1). It forwards the response obtained from the Secure Element to the Service Provider (2). If the response is accepted by the Service Provider an account is created by the Service Provider. The Service Provider then contains an account composed of that pseudonym and an associated public key while the Secure Element contains a pseudonym and an associated private key.

Subsequently, the User Agent connects to the Service Provider and indicates the kind of service the user wishes to perform.

The Service Provider indicates the attributes types needed for this service. The Service Provider may also provide a list of Attribute Issuers that it trusts, so that the user can make a choice among them.

The user decides whether he wishes or not to disclose these attributes types considering the requested service. He may also select one of the proposed Attributes issuers. If he accepts, he then needs to decide which Attribute Issuer to contact to get them.

If this has not already been done, the User Agent creates an account for the selected Attribute Issuer using an ATTRIBUTE_ISSUER_ENROLL command (3). It forwards the response obtained from the Secure Element to the Attribute Issuer (4).

One way or another the Attribute Issuer already knows one or more attributes of the user.

For example, Mr John Doe has opened a bank account on November 12, 2010 at a branch of the Bank of North Carolina in Raleigh. His identity is checked in the presence of the customer in line with regulatory "know-your-customer" requirements.

The exchanges are illustrated in Figure 2.

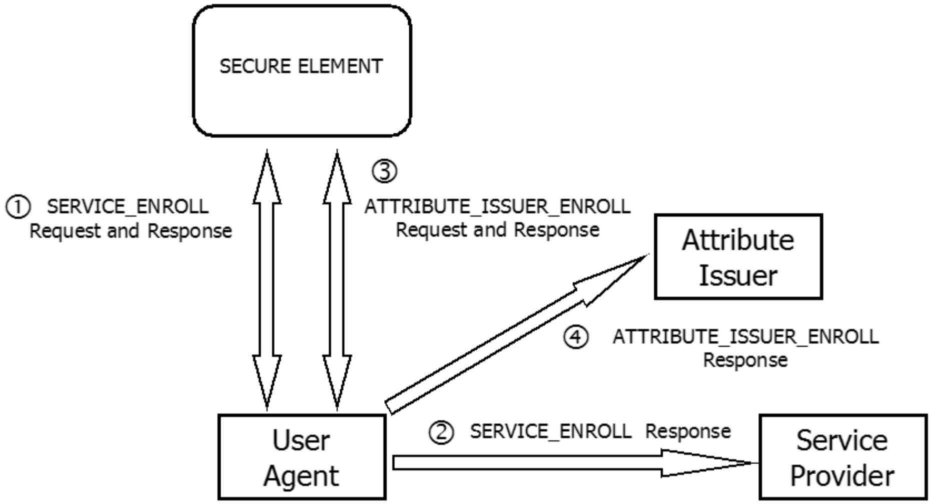

SECURE ELEMENT
① SERVICE_ENROLL Request and Response
③ ATTRIBUTE_ISSUER_ENROLL Request and Response
Attribute Issuer
④ ATTRIBUTE_ISSUER_ENROLL Response
User Agent
② SERVICE_ENROLL Response
Service Provider

Figure 2 — Enrollment towards a Service Provider and an Attribute Issuer

The user may then wish to ask a server, acting as an Attribute Issuer for the Bank of North Carolina, to generate an access token where the owner of the access token will be the pseudonym that has been used to open an account on the Service Provider. This will be done using several steps:

The User Agent connects to the Secure Element and issues a GET_ACCESS_TOKEN command (5). The response to this command, i.e. an APDU (Application data unit) is forwarded by the User Agent to the Attribute Issuer (6). The Attribute Issuer verifies that this APDU contains a digital signature for the other content of the APDU as well as the conformance certificate of the secure element. It validates the digital signature using a trusted root. If the validation is successful, it generates the requested access token (7).

The FIDO U2F Implementation Considerations [U216] states:

> "Keys generated during a U2F registration must not be used for any purpose other than U2F authentications".

In this eID mechanism, the keys generated during registration may also be used for other purposes. In particular, they are used to provide a data origin authentication service. A change for the use of these keys in the quoted document would be required.

The User Agent receives the access token signed by the Attribute Issuer, it verifies its digital signature and makes sure that the attributes that are contained in it match the attributes that were requested.

The exchanges are illustrated in Figure 3.

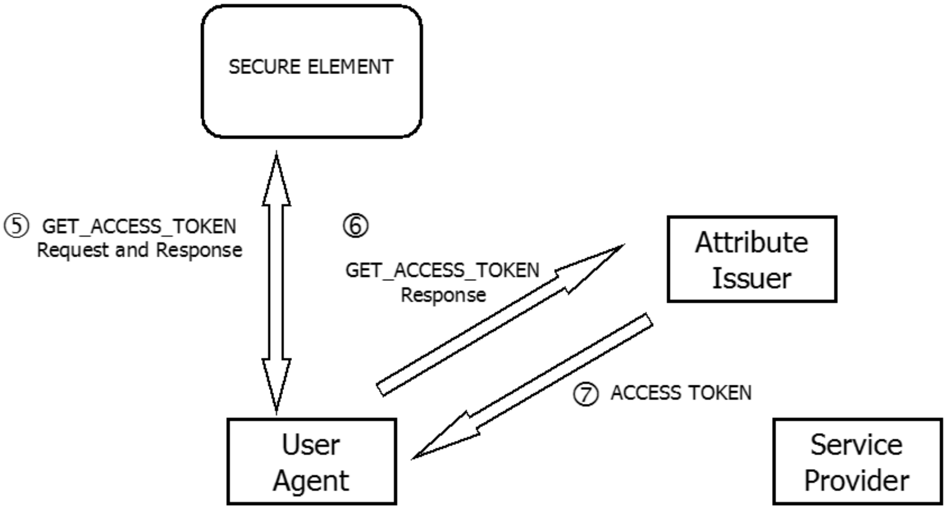


Figure 3 — The exchanges to get an access token

Once authenticated, the User Agent is able to generate a Query associated with the access token that has been received (8). This mandates the use of either HTTPS, SSH or a VPN. Alternatively, the User Agent may be willing to provide an end-to-end security in case some modification could be performed on the Service Provider side after a proxy. He can thus generate a SIGN_DATA command (8) to the Secure Element where the data contains:

(a) the access token that has just been received from the Attribute Issuer,

(b) the pseudonym that has been used to open an account on the Service Provider, and

(c) the query addressed to the Service Provider.

The response to this command, i.e. an APDU (Application Data Unit) is forwarded by the User Agent to the Service Provider (9) together with the Query and the access token. The Service Provider verifies that this APDU contains a digital signature for the Query and the access token using the public key associated with this account.

If the verification is successful and if the attributes contained in the access token matches with the expectations of the Service Provider, the Service Provider responds to the Query.

The exchanges are illustrated in Figure 4.

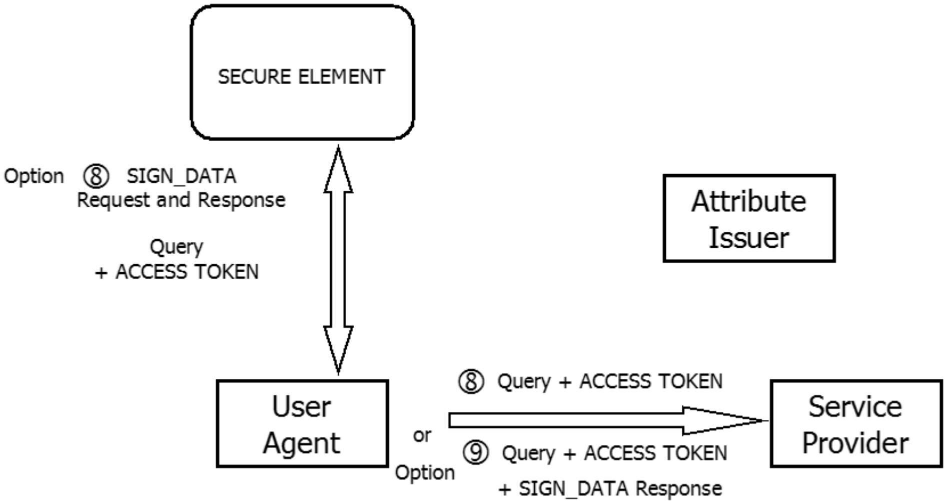


Figure 4 — The exchanges to push an access token

7. A continuous scale from anonymity to full identification

A user is able to use a full range of identification options starting from anonymity using pseudonyms to full identification using a set of attributes that will be sufficient to identify him among a set of users in a given context. He can also choose to only reveal that he is older that 18 or that he is living in a given state or/and a given town. This is achieved using "computed attributes".

8. Accumulation of attributes and Unlinkability

When the user is willing to use an existing account to access a given Service Provider, he can accumulate different attributes that will then be remembered by the Service Provider during some time period. The duration of the attributes may be controlled through information placed in the access token.

When it is desirable to prevent the linkability of transactions of a user even within a given service, once a set of transactions has been completed, the pseudonym that has been used can be deleted from the secure element. In this way, if another set of transactions is performed on the same Service Provider, a new account (and pseudonym) will automatically be created and the Service Provider will have no way of knowing that it comes from the same user.

9. The use of Secure Elements

Originally, a smart card with contacts was the favored implementation method for a secure element. Alternatives exist today, e.g. NFC (Near Field Contact) smart cards, embedded SE or SE Advanced Security SD card (SD card with an embedded SE chip).

Whatever type of Secure Element is chosen, a given user should have the ability to backup the data contained in his Secure Element in case he looses it. However, he shall not be able to use more that one Secure Element that contains that data active at any one time. The back up phase as well as the transfer of activity from one Secure Element to another Secure Element shall be controlled.

10. Interoperability

Interoperability between access tokens shall be facilitated using a limited number of formats. Access tokens may be formatted using SAML [Se16], JSON [Th16] or ASN 1 as in RFC 5755 [An16].

It will also be necessary to standardize APDUs. The SERVICE_ENROLL response shall be processable by Service Providers. The ATTRIBUTE_ISSUER_ENROLL and the GET_ACCESS_TOKEN responses shall be processable by Attributes Issuers. The SIGN_DATA response should be processable by both.

11. Conclusion

This eID scheme has been built from the very beginning along Privacy by Design principles. It is based upon a model that ends up with four components: User Agents, Service Providers, Attribute Issuers and Secure Elements taking into consideration first privacy requirements and then applying security requirements.

As with FIDO, this eID mechanism does not need the user to remember multiple identifiers and the associated authentication data. However, it extends the FIDO model in order to support the user's attributes. Changes in the FIDO specifications will be required.

This eID scheme mandates the use of Secure Elements in order to generate and store pseudonyms and associated private keys. Every Secure Element shall be manufactured in order to support a specific set of APDUs and once verified by an independent body, the provider will insert a private key and a conformance certificate inside each such manufactured secure element.

Secure elements manufactured to support the specific set of APDUs may be provided by any provider and distributed by anyone, e.g. sold in a supermarket. Hence, they do not originally contain any personal data. Obviously, these Secure Elements should be protected by a mechanism like a PIN or/and some biometric recognition.

This eID scheme does not mandate the deployment of national eID smart cards. It is not restricted to the EU, nor to relationships with government administrations. It is worldwide scalable for both the private and the public sector.

A patent application has been made on this scheme. The next phase will be to demonstrate the mechanism through a PoC (Proof of Concept).

In comparison, the GOV.UK Verify project [Go16] which is limited to accesses to government services mandates the use of a GOV.UK Verify Hub that acts as an orchestration point for authentication requests and responses. It is stateless, i.e. it doesn't store any part of the message exchange any longer than a session. However, how users make sure that messages exchanged with that central UK hub will not be intercepted and forwarded elsewhere?

With a similar approach, the EU eIDAS Regulation [Re14] mandates the use of cross-border nodes, where such nodes could act as Big Brother.

Given the impracticality/impossibility of the eIDAS Regulation to support interoperability for eID where roughly 756 translation protocols (27 x 28) would need to be developed (it has not even been demonstrated that this is feasible) and then maintained (the amount of money for it has not been estimated), this mechanism is a realistic, simple and tangible solution.

References

[Re14] Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation).

[Ap15] EN 419 212. Application Interface for Secure Elements used as Qualified electronic Signature (Seal-) Creation Devices.

[Fa16] Fast IDentification On-line. https://fidoalliance.org/specifications/download/

[Th16] The JavaScript Object Notation (JSON) Data Interchange Format. RFC 7159

[An16] An Internet Attribute Certificate Profile for Authorization. RFC 5755

[Se16] Security Assertion Markup Language (SAML) V2.0 http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

[Go16] GOV.UK Verify https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

[U216] U2F Implementation Considerations https://fidoalliance.org/specs/u2f-specs-master/fido-u2f-implementation-considerations.html

[Un16] Universal 2nd Factor (U2F) Overview. https://fidoalliance.org/specifications/overview/

Non-technical Challenges of Building Ecosystems for Trustable Smart Assistants in the Internet of Things: A Socioeconomic and Legal Perspective

Michael Kubach[1], Caterina Görwitz[1], and Gerrit Hornung[2]

Abstract: In this position paper, we present non-technical challenges that arise while building ecosystems for trustable smart assistants in the Internet of Things. Such non-technical challenges are often neglected in the development process of information systems, even though they are important elements for their success. Only if the assistants are technically effective and fit into the non-technical framework conditions of their application area (e.g. the market structure, stakeholder, liability, and data-protection requirements), they will be able to become successful innovations. We will support this argument in our position paper, focusing on the socioeconomic and legal perspective.

Keywords: internet of things, smart assistants, smart services, ecosystems, socioeconomic perspective, legal perspective, data protection, business models, stakeholders, research project

1 Introduction

The present development in the context of the Internet of Things enables a new kind of smart services and smart assistants that support every user individually depending on his or her needs. Nevertheless, there are still some challenges on the way that need to be overcome.

Many of the challenges found in building smart assistants are rather technical and refer to aspects like interoperability or IT security. However, smart assistants require the combination of various data from several sources and therefore the cooperation of various stakeholders. Moreover, people will only be willing to use the assistants in their daily lives if they trust them and if they comply with the rules that govern these lives. These are all non-technical aspects and in this position paper, we are going to put our focus on them, as practical experience from the history of information systems has shown that they have often been overlooked.[3] Examples to how problematic an insufficient consideration of these factors can be for the long term success of modern IT solutions can be illustrated with two relatively new German projects; DE-Mail and the new German elec-

[1] Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, vorname.nachnname@iao.fraunhofer.de

[2] Universität Kassel, Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht, Kurt-Schumacher-Str. 25, 34117 Kassel, gerrit.hornung@uni-kassel.de

[3] There is, however, related work from other research projects that we can build on. Such is the EU FP7 Project "SmartSociety" that has produced insights on ethical aspects for hybrid systems where people and machines tightly work together to build a smarter society (www.smart-society-project.eu).

tronic identity card (neuer Personalausweis or “nPA”). In spite of high technical effectiveness and security, both solutions fail to succeed in the market. Therefore, a prime aim of this paper will be to address particularly the socioeconomic and legal challenges in building ecosystems for trustable smart assistants in the Internet of Things. In addition to the latter, technical challenges will be thoroughly investigated in a new research project, which is briefly presented later in the paper. We expect that the discussion and feedback on our position paper can be of high value for the future course of this research project.

The remainder of this paper is structured as follows. In the second chapter, we clarify some basic terms in the relatively young field of trustable smart assistants and ecosystems in the Internet of Things. The third chapter then focuses on the socioeconomic challenges and issues that may emerge from smart assistants in the Internet of Things to a success on the market. The fourth chapter specifies legal issues that appear on different stages of the work of smart assistants, namely: personal data protection and processing, data collection, the principles of transparency and data minimization, and liability. Moreover, it draws links to the new EU General Data Protection Regulation. The fifth chapter then presents the ENTOURAGE research project – an open ecosystem for smart assistants – that will address the challenges stated in the previous chapters in the next three years of its development. Finally, the paper finishes with a short conclusion.

2 Ecosystems for Trustable Smart Assistants in the Internet of Things

2.1 Trustable Smart Assistants

Assistance systems store, process, and transmit information and support users in personal decisions in a variety of life situations. Nevertheless, these assistants cannot be reduced to technology alone. An essential factor is the interaction with the user and the reaction to a certain context. Therefore, in general, assistance systems are contextual and personalized [GM02].

In the last years, there has been an increasing interest in the development of intelligent personal assistants in research and practice. Some voice-controlled products such as Apple’s Siri, Google’s Now, Microsoft’s Cortana or Amazon Echo are already in the market. Some studies have been researching the trustworthiness and acceptance of such systems. Moorthy and Vu [MV14] have analyzed the acceptance of personal assistants that are integrated in smartphones. The results show that the willingness to deliver private information via the natural language interface depends on the particular location and context of the user. Glass et al. [GMW08] have identified some factors, which are important for the trust of users towards personal assistants. The systems should be designed transparent, so that it is evident for the user to understand which steps are carried out for what reasons. Moreover, the user should be able to find out the sources where the system finds the requested information. Finally, personal assistants should not be designed too autonomously, so that the users always have the power to change or adjust the functions and consequences induced.

Nevertheless, it should be noted that not only end-users are required to trust the assistants. Other stakeholders in the ecosystem (see next section) should also be able to trust in the fact that, for example, the data of their sensors are not misused and they are compensated appropriately for the services they provide. Moreover, if wrong decisions have been made, liability questions could become an issue. So far, these aspects of trust have hardly been considered in the literature.

2.2 Ecosystems for Smart Assistants

To date, existing smart assistants are limited to a large extent to the IoT platforms of their vendors or operators. A platform is considered to be a set of technological building blocks and complementary assets that companies, entrepreneurs and individuals can use and consume to develop complementary products, technologies and services [Mu13]. The restriction to single "platform-silos" significantly hinders the combination of application fields and cross-platform use of data and thus the achievement of the full potential of smart services.

This is why an open ecosystem for smart assistants is that valuable. Following Muegge [Mu13], the ecosystem-approach towards smart assistants is much broader than the platform-approach. It overcomes some of its limitations and further extends it towards the (economic) actors involved. In the networked ecosystem of interdependent and codependent actors with partially aligned incentives, a technology entrepreneur can achieve more, learn faster, and reach farther than otherwise possible, while sharing some of the risks and costs with others. The ecosystem is not defined and limited to one single (technological) platform, but rather through the outcome and incentives that are more or less shared among the different actors in the ecosystem.

By constructing such an ecosystem, it will become possible for the assistants to filter data from different sources, aggregate it, process it and make it easily accessible to the users. Additionally, user interfaces could be made available at higher levels, or even autonomous decisions within the framework of determined users' preferences taken. Therefore, such assistants as intelligent smart services in respective open ecosystems represent a key technology for the development of the potential of the Internet of Things.

3 Socioeconomic Challenges

The current separation of platforms for smart assistants follows economic interests. The manufacturers of smart end devices have invested resources for development and operation of these devices in order to finally obtain valuable sensor data. There is no functioning mechanism that allows for flexible integration of new actors and their information, services or devices into this system, and takes into consideration the particular economic interests.

A crucial challenge is to analyze how such an ecosystem can be offered and used in an economically viable form. Particularly in an open ecosystem, where different actors deliver and use data and offer services based on that data (in this case particularly to assistants), the consideration of incentive and pricing models is necessary. Otherwise, this exchange can hardly be reached. To achieve this, the economic framework conditions need to be appropriately analyzed and respective requirements for the components of the ecosystem need to be derived.

Powerful smart assistants in an ecosystem rely on an exchange of data and services between different actors. This exchange could be regarded as a type of a multi-sided market between data providers, operators of smart assistants, and end users. In addition, other actors like providers of specific services (e.g. big data analysts, platform operators, and vendors of technical devices) could also participate in this market. Analyzing the structure of this market and its participants will be the first step in developing appropriate framework conditions in the ecosystem such as a market place for data. No matter who exactly the participants in the ecosystem are, it is rather certain that the ecosystem will face a multi-sided market. This implies that the success of the ecosystem will depend on the successful coordination of the demand of the distinct actors who need each other in some way [Ev03]. Another aspect to consider is that the ecosystem is subject to network effects so that, for example, the attractiveness of the ecosystem increases for operators of smart assistants if more data providers are active. Furthermore, the ecosystem becomes more attractive for data providers and operators of smart assistants if more end users are able to use the smart assistants with their smartphones or from their cars. This can result in a positive feedback and thus in an exponential growth once a critical mass has been reached. However, this also works vice versa, resulting in a chicken-and-egg problem and negative feedback [MR99]. If there are no smart assistants in the ecosystem the incentives for data providers to offer their data in the format required for the ecosystem is presumably low. Therefore, when building the ecosystem the specific market-structure and respective strategies for entering the market as well as balancing the interests of its actors have to be considered.

As the previous section already indicated, identifying the incentive structures necessary for the acceptance of the ecosystem through its integral actors or stakeholders poses another important challenge. However, the analysis and the efficient management of multidiscipline requirements towards an ecosystem for smart assistants are not trivial. Therefore, currently discussed economic models and theories have to be evaluated for their applicability in the context of an ecosystem for smart assistants in the Internet of Things. One of these approaches is stakeholder theory with its practical application stakeholder analysis. Stakeholder analysis is an established socioeconomic method. It allows to specifically address the demands of the stakeholders of a certain organization, product, as well as technology and far exceeds a simple market analysis. In addition, it is used successfully in the area of information systems [Po99]. Thus, a stakeholder analysis of the ecosystem seems to be necessary.

When the integral stakeholder and incentive structures are identified, viable business models for these structures can be developed. Only solutions developed in that way have the potential to meet market needs and technical performance requirements and later become successful [Ac14]. However, the development of viable business models is not a trivial process but pivotal to the success of new technologies. This is also represented in the discussions on business model approaches in Business Economics, Information Systems, and specifically literature on the Internet of Things [Ka15], [Li11], [EHB11], [ZA10], [OPT05].

The pricing strategy or a pricing model that is used in the business model is the final socioeconomic challenge that we want to highlight here. As we have shown, reaching the critical mass of actors in the ecosystem is crucial due to the multi-sided market and its network effects. Finding a suitable pricing strategy for the various actors is one important element in reaching the critical mass and sustaining the ecosystem. For other application areas with multi-sided markets various pricing strategies have been discussed in the literature, the main strategies being of a “divide-and-conquer” nature. In these strategies the participation of some actors on one side of the market (divide) is subsidized through revenues generated from the other side (conquer) [CJ03]. Of course, this depends on the willingness to pay of the actors as well, which has already been analyzed for multi-sided markets [Ro14] but not for the context of ecosystems smart assistants. Overall, this shows that pricing strategies are another important research gap and challenge building ecosystems for smart assistants.

4 Legal Issues

Smart assistants are assistants that know as much as possible about their owner. It is thus necessary to collect and exchange an ample amount of data. This can be considered critical because detailed behavioral, motion and personality profiles can be derived while working with smart assistants [ST05] [Gi07] or the Internet of Things in general [HH15a]. However, not all data in smart environments will be personal data that relates to an identified or identifiable person. Many smart objects and cyber-physical systems will produce “technical” data, which at first glance may look anonymous. One big challenge of the never-ending storage of this data could however be the long-term perspective, as the growing information in data bases might, in the end, lead to identifiable persons [Ro13].

To determine whether data is personal, Art. 2 (a) of the current Data Protection Directive defines an identifiable person as "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”. In its core activity, a trustable smart assistant in the Internet of Things will process a plethora of data of this kind. This leads to the application of national data protection laws, as well as of the future General Data Protection Regulation (cf. below), because the latter will only slightly change the respective definition.

If the system is to process personal data, there has to be a proper legal basis for the processing, i.e. either legislation or an effective consent by the persons affected. Without such a legal basis, every collection and processing of personal data is illegal [SS14]. Hence there are two main options that allow data collection. On the one hand, data could be collected with the consent of the data subject according to Art. 7 (a) of the Data Protection Directive; on the other hand, a law that permits the collection is required [TF14]. For example, the collection could be used as a means for the performance of a contract according to Art. 7 (b) of the Data Protection Directive. These traditional mechanisms are highly debated nowadays, particularly as regards the question who may use personal data as a basis for new business models ("data ownership", cf. [HG15]).

If a legal basis has been found, the data controller must continue to comply with the principle of transparency. According to Art. 10 of the Data Protection Directive, the user of smart assistants must firstly be informed about the data controller, the purposes of the processing, and the recipients or categories of recipients to which these data are transmitted. This could be problematic if the data which is exchanged originate from different sources, as it may no longer be clear which controller currently stores the data and who is responsible for it. Moreover, the data collection and use should be as transparent as possible for the individuals concerned, especially when the data are transmitted and processed in "third countries" (i.e. outside the European Union and the European Economic Area). However, this transparency will be challenging due to the large number of participating data.

According to Art. 6 (1) (b) of the Data Protection Directive, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The original purposes may thus not be exceeded during the data processing. However, these purposes are hard to define in advance for smart assistants due to the increasing complexity of the surrounding ecosystem and the various targets of external stakeholders. Especially, when the purpose binding principle of Art. 6 (1) (b) of the Data Protection Directive is applied to very broad purposes it can lose its value [Ro13]. If the purpose of a smart assistant is defined as "to help the data subject in professional and personal settings in every respect, including situations and modes of assistance which are not yet clear", than literally every personal data may be regarded as being necessary to this end.

In addition, the principle of data minimization must be observed. Art. 6 (1) (c) of the Data Protection Directive indicates that as little personal information as possible should be collected. According to Art. 6 (1) (e) of the Data Protection Directive, this applies also to the duration of data retention, as the data has to be deleted or at least anonymized if the controller does not need it for the stated purpose anymore [Sc14]. This raises the question for how long the data may be stored, which becomes even more difficult to answer if smart assistants use data to build a network that consists of these data and grows with them.

Another important point in question is the processing of special categories of personal data. Regarding to Art. 8 (1) of the Data Protection Directive, these kinds of data refer to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union memberships, and the processing of data concerning health or sex life. As smart assistants will collect data of many areas of personal life, it is very likely that this will include sensitive data of this kind. If smart assistants, for example, permanently track the current location of the user, this may include a stay in hospital, leading to the information about medical treatment. Data protection law then demands higher requirements: while a simple consent for normal personal data has to be "unambiguously given" in general, the consent for sensitive data must be "explicit" regarding these data. Depending on the number of consents and the technical design, this could be very burdensome.

Continuing, the guarantee of data security is another challenge. The more data a controller stores, the greater the interest from others will be to obtain access to this information. Especially cross-platform applications are very crucial as they increase the vulnerability for external attacks, because IT architectures will be designed more standardized and uniformly. As data security is not only a legal requirement (cf. Art. 17 of the Data Protection Directive), but also a prerequisite for any trust of the user in smart assistants, it will be mandatory for data controllers to ensure a high, state-of-the-art standard.

Further the question of liability must be addressed if shortcomings arise after working with smart assistants. Here it must be clarified whether a device was malfunctioning due to an application of smart assistants or due to the device itself. It makes a difference whether devices can be connected externally, for example with a kind of API or if direct access to the software of the devices is required. In such cases, it could be hard to prove when and why defects occur, because the software of the device has to be inspected. This could mean that the Source Code of the software must be disclosed, at least to courts or for expert evidence.

As other technical innovations and data-based business models, smart assistance in the Internet of Things will meet the challenge of the new General Data Protection Regulation that will become effective in May 2018 [Wy16] after a long negotiation process [Ho13a]. This new framework tries to establish common data protection requirements and enforcement mechanisms within the European Union. It aims, inter alia, at strengthening data subjects, introducing effective sanctions, proposing new mechanisms such as privacy by design [Ho13b] and data protection seals [HH15b], and at enhancing the cooperation of the data protection officers in the Member States [Al16]. However, the Data Protection Regulation still leaves many decisions up to the Member States, which makes it hard to realize this unity [Ro15]. Moreover, problems about smart assistants, big data, or cloud computing are not mentioned at all [RNR15]. Thus, there is a great need for research on the specific requirements for these and other innovative technologies, because companies need to be prepared once the new rules become applicable in 2018.

It is very likely that neither law nor technology alone are able to solve the privacy and data protection issues of smart assistants. There is a great need for an "alliance" of the two [Ro01]. Legal requirements serve as criteria for the design of specific technical and organizational solutions, so that the latter can comply with the data protection law from the very outset of the process of research and development (for examples, see [Ro11]). While working with smart assistants, it is almost impossible to avoid personal data. Therefore, a safe processing of these data has to be guaranteed in order to avoid restricting the users in their rights and, at the same time, losing their trust in innovative technical solutions.

5 The Entourage Research-Project

The challenges described above will be addressed over the next three years in the new research project "ENTOURAGE – Smart Assistance – Enabling Trusted Ubiquitous Assistance"[4] that has attracted funding from the German Federal Ministry for Economic Affairs and Energy (BMWi) through its "Smart Service World" technology competition.

The interdisciplinary project started earlier this year and is one of 16 successful projects selected from among 130 entries. Together, the industrial and research-partners[5] are developing and testing an open ecosystem to support smart, secure, and reliable assistance systems in the Internet of Things. ENTOURAGE provides a hub for data and services, functioning as the link between IoT-platforms and services. It unites technical, organizational, and legal components, which lays the groundwork for innovative open assistance systems.

In ENTOURAGE an open ecosystem is being developed that is interoperable on many levels. The ecosystem allows a legally compliant and optimized access to the future field of assistance systems through the establishment of technical standards and collaboration models for system and server providers.

The open platform developed within the project ensures the flexible connectivity between assistance systems. To give special consideration to the user acceptance of the developed solutions, the combination of relevant information of different sources is complemented by the consideration of data protection and security issues (also from the legal perspective). This aspect is central to the project.

By analyzing the market potential and deriving business models for suppliers and users, the economic viability of ENTOURAGE is pursued. Especially in an open ecosystem where different actors deliver and process data and offer services (in this case particular-

[4] www.entourage-project.de

[5] The ENTOURAGE team brings together experts from Robert Bosch GmbH, Fraunhofer IAO, CONWEAVER GmbH, HaCon Ingenieurgesellschaft mbH, the Technische Universität Darmstadt, the Universität of Kassel and is coordinated by the ENX Association. Other associate partners include BITKOM, TeleTrust, T-Systems, the city of Cologne and the transit network of Berlin-Brandenburg.

ly smart assistants) based on that data, the consideration of incentive and pricing models is necessary as this exchange can hardly be achieved otherwise. However, as of now such incentive and pricing models do not exist and should be developed on the basis of profound scientific analyses.

Moreover, ENTOURAGE develops a security assistant which supports users in the areas of login details, data access and data usage. This way, the security assistant contributes significantly to the user acceptance as it helps to handle challenges of data protection and usability. It also supports legal compliance when solutions based on ENTOURAGE are applied.

To verify and demonstrate the potential of ENTOURAGE, three pilot scenarios are planned. They are complementary and integrated into one ecosystem. First is the scenario "Automobile platforms and sustainable mobility“. This scenario deals with the interaction of home, commercial, vehicle, and mobility platforms. It pursues the goal of an intelligent governance of the individual traffic at personal and system levels. The second scenario „Public transport and elastic infrastructures“ includes among other aspects travel planning, which takes into account real time information, appointments, choice of modes of transport, and navigation information exchanged between platforms (smartphone, car, house), as well as additional services such as recommendations on the nearest gas stations or gastronomic possibilities. In the third scenario „Smart Home and Digital Life Balance“ the question of how technical and planning components can help employees to keep a better life-work balance with the use of smart assistance is investigated.

6 Conclusion

In this position paper we have argued that while the Internet of Things enables innovative smart services and smart assistants that are much more powerful than before, there are still some challenges to be overcome to reach their full potential. As they are often neglected in the research and development of IT systems due to a focus on technical aspects, we have concentrated on non-technical challenges in this paper. Socioeconomic and legal aspects represent important framework conditions for the success of ecosystems for trustable smart assistants and therefore are discussed in greater detail. The main challenges for these ecosystems that have been identified and will be analyzed further in the ENTOURAGE-project and its pilot scenarios are summarized in table 1 (following page).

As this is a position paper, we were only able to present our understanding of the main terms and sketch out the basic challenges that we see from a socioeconomic and legal perspective for this relatively new area of research. As for a next step, a more thorough investigation of the issues presented will be performed in our new research project ENTOURAGE, which was presented in the last chapter. Feedback and discussion about the arguments presented in this paper will be highly valuable for our future research and the success of the project.

Main socioeconomic challenges	Main legal challenges
• Functioning mechanism allowing for flexible integration of new actors • Economic viability of the ecosystem • Incentive and pricing models • Multi-sided market between different actors in the ecosystem • Strategies for market entry considering network effects • Interests of various stakeholders • Business models in the ecosystem	• Privacy risks of personal profiles and sensitive data in the Internet of Things • Addressing the problem of de-anonymization in big data • Strategies for data minimization • Applying the new General Data Protection Regulation to specific technologies and business models • Liability for unreliable data in software ecosystems

Table 1: Summary of the main challenges that have to be analysed

References

[Ac14] Acatech: Smart Service Welt: Umsetzungsempfehlungen für das Zukunftsprojekt Internet-basierte Dienste für die Wirtschaft. Berlin, 2014.

[Al16] Albrecht, J. P.: Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung, Computer und Recht, pp. 88-98, 2016.

[CJ03] Caillaud, B.; Jullien, B.: Chicken & Egg: Competition among Intermediation Service Providers. The RAND Journal of Economics, 34(2), pp. 309-328, 2003.

[EHB11] Eppler, M. J.; Hoffmann, F.; Bresciani, S.: New Business Models Through Collaborative Idea Generation. International Journal of Innovation Management, 15(06), pp. 1323–1341, 2011.

[Ev03] Evans, D. S.: Some Empirical Aspects of Multi-sided Platform Industries. Review of Network Economics, 2(3), pp. 191–209, 2003.

[Gi07] Gitter, R.: Softwareagentensysteme im elektronischen Geschäftsverkehr: Rechtliche Rahmenbedingungen und Gestaltungsanforderungen an agentengestützte Assistenzsysteme, Baden-Baden: Nomos, 2007.

[GMW08] Glass, A.; McGuinness D. L.; Wolverton, M.: Toward establishing trust in adaptive agents. Proceedings of the 13th international conference on Intelligent user interfaces. ACM, 2008.

[GM02] Göker, A.; Myrhaug, H. I.: User context and personalisation. Workshop proceedings for the 6th European Conference on Case Based Reasoning, 2002.

[HG15] Hornung, G.; Goeble, T.: “Data Ownership“ im vernetzten Automobil. Die rechtliche Analyse des wirtschaftlichen Werts von Automobildaten und ihr Beitrag zum besseren Verständnis der Informationsordnung, Computer und Recht, pp. 265-273, 2015.

[HH15a] Hofmann, K.; Hornung, G.: Rechtliche Herausforderungen des Internets der Dinge. In: Sprenger, F.; Engemann, C. (Hrsg.): Internet der Dinge. Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt, Bielefeld: transcript, pp. 181-203, 2015.

[HH15b] Hornung, G.; Hartl, K.: Datenschutz durch Marktanreize – auch in Europa? Stand der Diskussion zu Datenschutzzertifizierung und -audit, Zeitschrift für Datenschutz, pp. 219-225, 2014.

[Ho13a] Hornung, G.: Die europäische Datenschutzreform – Stand, Kontroversen und weitere Entwicklung, in: Scholz, M.; Funk, A. (Hrsg.): DGRI-Jahrbuch 2012, Köln: Dr. Otto Schmidt, pp. 1-24, 2013.

[Ho13b] Hornung, G.: Regulating privacy enhancing technologies: seizing the opportunity of the future European Data Protection Framework, Innovation: The European Journal of Social Science Research, pp. 181-196, 2013, http://dx.doi.org/10.1080/13511610.2013.723381.

[Ka15] Kaufmann, T.: Geschäftsmodelle in Industrie 4.0 und dem Internet der Dinge. Springer, Wiesbaden, 2015.

[Li11] van Limburg, M.; van Gemert-Pijnen, J.; Nijland, N.; Ossebaard, H. C.; Hendrix, R.; Seydel, E. R.: Why business modeling is crucial in the development of eHealth technologies. Journal of Medical Internet Research, 13(4), e124, 2011.

[MR99] Mahler, A.; Rogers, E.: The diffusion of interactive communication innovations and the critical mass: The adoption of telecommunications services by German banks. Telecommunications Policy, 23(10/11), pp. 719–740, 1999.

[MV14] Moorthy, A. E.; Vu, K. L.: Voice activated personal assistant: Acceptability of use in the public space. Human Interface and the Management of Information. Information and Knowledge in Applications and Services. Springer International Publishing, pp. 324-334, 2014.

[Mu13] Muegge, S.: Platforms, Communities, and Business Ecosystems: Lessons Learned about Technology Entrepreneurship in an Interconnected. Technology Innovation Management Review, 3(2), pp. 5–15, 2013.

[OPT05] Osterwalder, A.; Pigneur, Y.; Tucci, C. L.: Clarifying business models: Origins, present, and future of the concept. Communications of the association for Information Systems, 16(1), pp. 1-25, 2005.

[Po99] Pouloudi, A.: Aspects of the stakeholder concept and their implications for information systems development. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences, pp. 1-17.

[Ro01] Roßnagel, A. (Hrsg.): Allianz von Medienrecht und Informationstechnik? Ordnung in digitalen Medien durch Gestaltung der Technik am Beispiel von Urheberschutz, Datenschutz, Jugendschutz und Vielfaltschutz, Baden-Baden: Nomos, 2001.

[Ro11] Roßnagel, A.: Das Gebot der Datenvermeidung und -sparsamkeit als Ansatz wirksamen technikbasierten Persönlichkeitsschutzes? In: Eifert, M.; Hoffmann-Riem, W. (Hrsg.): Innovation, Recht und öffentliche Kommunikation, Berlin: Duncker&Humblot, pp. 41-66, 2011.

[Ro13] Roßnagel, A.: Big Data – Small Privacy? Konzeptionelle Herausforderungen für das Datenschutzrecht. Zeitschrift für Datenschutz, pp. 562-567, 2013.

[Ro14] Roßnagel, H.; Zibuschka, J.; Hinz, O.; Muntermann, J.: Users' willingness to pay for web identity management systems. European Journal of Information Systems, 23(1), pp. 36–50, 2014.

[Ro15] Roßnagel, A.: Was bringt das neue europäische Datenschutzrecht für die Verbraucher – Die Datenschutzgrundverordnung steht vor ihrer Verabschiedung. Verbraucher und Recht, 10, pp. 361-362, 2015.

[RNR15] Roßnagel, A.; Nebel, M.; Richter P.: Was bleibt vom Europäischen Datenschutzrecht? - Überlegungen zum Ratsentwurf der DS-GVO. Zeitschrift für Datenschutz, pp. 455-460, 2015.

[Sc14] Scholz, P.: Kommentierung von § 3a, Rn. 17, in: Simitis, S. (Hrsg.): Bundesdatenschutzgesetz, 8. Auflage, Baden-Baden: Nomos, 2014.

[SS14] Scholz, P.; Sokol, B.: Kommentierung von § 4, Rn. 3, in: Simitis, S. (Hrsg.): Bundesdatenschutzgesetz, 8. Auflage, Baden-Baden: Nomos, 2014.

[SFG99] Sharp, H.; Finkelstein, A.; Galal, G.: Stakeholder identification in the requirements engineering process. In Proceedings of the Tenth International Workshop on Database and Expert Systems Applications, pp. 387–391, 1999.

[St05] Steidle, R.: Multimedia-Assistenten in Betrieb. Datenschutzrechtliche Anforderungen, rechtliche Regelungs- und technische Gestaltungsanforderungen für mobile Agentensysteme, Wiesbaden 2005.

[TF14] Thüsing, G.; Forst, G.: Beschäftigtendatenschutz und Compliance, 2. Aufl., § 17, Rn.15, 2014.

[Wy16] Wybitul, T.: Datenschutzgrundverordnung verabschiedet – die wichtigsten Folgen für die Praxis auf einen Blick. Zeitschrift für Datenschutz-Aktuell, EU, 8, 2016.

[ZA10] Zott, C.; Amit, R.: Business model design: an activity system perspective. Long range planning, 43(2), pp. 216–226, 2010.

Risk-centred role engineering in identity management audits – An approach for continuous improvement of the access control model and possible risk accumulations

Sebastian Kurowski[1]

Abstract: Success and costs of audits in identity management largely depend on the structure of the underlying access control model. Auditing access rights includes the determination of actuality and adequacy of provided access rights. In order to ease audit and administration of access rights, role mining approaches have provided several solutions for identifying a minimal set of roles based upon either existing usage data, or business data. However, these approaches have focused on homogeneous, static environments. When facing dynamic, heterogeneous environments, such as infrastructure administration or smart systems, the accompanied noise of access rights provisioning hinder the determination of adequacy and actuality of access rights. With application of static approaches, accumulation of access risks at users may arise due to inadequate access rights, or aggregation of access roles. These issues are however mostly neglected by current approaches. Within this contribution we propose a method based upon the design structure matrix approach, which enables the identification of role aggregations, and examination of access risk accumulation within aggregated roles, and their assigned users throughout continuous audits of the access control model.

Keywords: identity management, access control, role engineering, design structure matrix, smart systems, cloud computing, RBAC, role mining

1 Introduction

Within the identity data lifecycle [MR08] auditing of identity data, including access rights enables identification of old, or falsely provided access rights. If this process is carried out regularly, it enables the identification of mistakes and, thus mitigation of potential access risks, due to the provisioning of too many privileges, or privileges which are no longer required. The success and costs of such audits are largely depending on the underlying access control model. For instance, [OL10] find that audit and policy maintenance costs are nearly doubled when using a classical access control list (ACL) paradigm over role-based access control (RBAC), stating that employing roles makes "it easier to accomplish [the policy review and attestation process]". Yet, the same study finds that half of all companies still used ACL as a secondary access control alternative in a hybrid solution along with RBAC, in 62% of all cases for their directory services [OL10]. Also multiple issues, especially with hierarchical RBAC have been known

[1] University of Stuttgart, Competence Team Identity Management, Allmandring 35, 70565 Stuttgart, sebastian.kurowski@iat.uni-stuttgart.de

resulting out of the complexity of the reality projected by the access control model. For instance, across multiple circles-of-trust, the application of hierarchical RBAC may lead to unintended privilege escalations for some roles [JGZ11]. However, these issues do not arise out of formal issues with RBAC itself, but out of the aggregating characteristics of these models. The classic role of access control, as regulating interactions between subjects and objects leads to the technologies itself having to deal with potentially endless possibilities in the respective real world scenario. As Luhmann states "technologies [are usually] conceived as relations between cause and effect, confirmed by scientific knowledge or practical experience" [Lu90]. Yet, technology and as such also access control is more an encapsulating of causal dependencies between subjects and objects, which itself may be numerous and even potentially infinite in their variations. This mismatch yields dire consequences in the application of technology: "Paradoxically, we lose control of causalities, as they become too complex" [Lu90].

Paradigms such as RBAC, which aim at decreasing administrative complexity, by encapsulating causality between multiple subjects and objects, rather than encapsulating the causality of existence of one object (as in the case of ACL), transform this paradox to the following: While on the one hand RBAC results in significantly lower audit and administrative efforts, imperfections of the access control model may lead to conflicts with the reality it is applied to. This paradox may especially become visible, when dealing with environments characterized by highly heterogeneous and dynamic workflows, and objects, e.g. in privileged identity management for cloud based platform- and infrastructure-as-a-service environments. In current research this paradox has mostly been accounted for as noise, which results in an open research issue [Fr09] [KSS03] [Mo09] [VAG07] [ZRE03].

The noise created by applying of role mining approaches in dynamic and heterogeneous workflows (e.g. privileged identity management), further translates to noise in access risk distribution at the subjects. Aggregation of subject – object relationships, as in RBAC in such scenarios may lead to subjects inadequately gaining access rights and thus access risks to objects. Additionally, hierarchical role mining may lead to access risk accumulation, which, especially in heterogeneous environments with dynamic component introduction and access rights modifications, may be hard to examine.

In this contribution we therefore propose an approach for risk centred role mining by using the user assignment matrix UA, which can be obtained from the identity directory. In order to account for the noise, associated with the underlying access control model in dynamic environments, we transfer an approach from process and engineering planning [YB03]. This approach tries to determine the best order in inter-dependent engineering processes. By transferring the approach we are able to determine both, intra-dependent clusters of subject-object associations (e.g. possible candidates for role aggregations), along with their inter-dependencies upon other roles. Therefore, we aim to use it both for simplifying the access control models in order to ease the administration, and for identifying possible risk accumulations which may arise as a consequence of aggregating roles.

In the following we provide an overview on current role mining approaches (Section 2). Our used scenario along with our assumptions of access control administration in dynamic environments is introduced within Section 3. This scenario includes a definition of the risk consolidation problem which may arise within aggregated role systems (e.g. hierarchical RBAC). Finally, our approach is presented within Section 4, along with its application for clustering of possible role aggregations, and analysis of intra- and inter-dependencies of the role clusters (Section 5). The presented approach is implemented within an Excel spreadsheet, and will be provided to organizations for usage within this year. As our approach only requires access to data acquirable from the directory services, easier integration into existing identity and access management (IAM) audit commodities and tools is expected. It is therefore intended for use in the audit phase of the identity lifecycle [MR08].

2 State-of-the-Art

By using the Scopus[2] literature database, we found a total of 132 publications[3] regarding role mining and access control. Hereby the first publications are dated back to 2002. Since 2008 the academic interest in the topic has increased to about 15 publications, and since then shows only a small decline in interest, except for the years 2011, and 2014. However, this indicates that the topic of Role Mining has so far not been highlighted in academic research on access control. Interestingly, the decrease in interest aligns well, with the overall decrease in academic interest regarding Role-Based Access Control (RBAC)[4], and the slight decrease in academic interest regarding Access Control itself[5]. The reasons for this decrease in interest may not be subject to this paper. However, it is worthwhile noting that the decrease of interest in Role Mining might well be rooted within the mentioned paradox resulting out of causal encapsulation within role-based policies and the collision of the necessarily imperfect model with the real-world scenarios they are applied in. The contribution of Vaidya et. al. [VAG07] define various role mining problems, including the problem of finding a minimized set of roles which is consistent with user-permission assignments of the scenario, while the amount of roles is smaller than a defined threshold (DECISION RMP), consistent to a certain threshold with user-permission assignments of the scenario, while the amount is smaller than a defined threshold (δ-DECISION RMP), and consistent to a certain threshold, without any upper boundary on the amount of roles (DECISION MinNoise RMP). Hereby, the

[2] http://www.scopus.com: The search using the literature database was conducted in April 2016.

[3] The used search term was: TITLE-ABS-KEY (role mining) AND (LIMIT-TO (EXACTKEYWORD , "Access control"))

[4] The search term TITLE-ABS-KEY (rbac) AND (LIMIT-TO (EXACTKEYWORD , "Access control")) provides a sum of 1656 publications. However, analysis shows, that the amount of publications have decreased by nearly 50% in 2015 (104 publications), compared to the peak-of-interest in 2008 (189 publications).

[5] The search term TITLE-ABS-KEY (access control) AND (LIMIT-TO (SUBJAREA , "COMP")) provides a sum of 53148 publications. However, the amount of publications has slightly decreased from its peak-of-interest in 2008 (4711 publications), to 3996 publications in 2015.

DECISION RMP is of little interest for our contribution, as it mostly applies to static environments. In dynamic environments a perfect consistency with the user-permission assignments is very likely to be impossible [VAG07]. All problems are shown to be NP complete [VAG07]. One possible problem solving proposition is found in the application of the minimum tiling problem [GGM04]. But, since this problem aims at finding the minimum set of tiles consistent with the original Boolean dataset of user and role assignments, it is not applicable to hierarchical RBAC. Furthermore, the MinNoise RMP, which aims at finding an imperfect set of roles, and thus is more likely to be applicable in dynamic scenarios [VAG07], is shown to be transferrable to the NP-hard discrete basis problem, considering segmentation of Boolean matrices [Mi08]. The NP-completeness and even NP-hard character of non-hierarchical Role Mining Problemes indicate the appropriateness for meta-heuristic, over exact searching algorithms. Furthermore, it favours user-centric, organizational approaches, where Role Mining is considered within a process during regular audit. Kuhlmann et. al. [KSS03] present a Role Mining approach, which enables a bottom-up approach by mining data from different Access Control Systems. The approach being presented mines access control data, and therefore presents a similar approach to this contribution. Their approach uses the IBM Intelligent Miner for Data, for segmentation and mining of User-Role assignments. However, the approach in [KSS03] considers flat RBAC, whereas this contribution aims at administration and continuous improvement of hierarchical RBAC. Finally, [Fr09] provide a probabilistic approach for role mining, and demonstrate this approach on large enterprises. Their approach is able to extract understandable roles, showing that most relevant information for mining business roles arises out of the organization unit, rather than the job description itself. By applying an objective function, which penalizes the assignment of roles to a user which does not share the same business information as other users assigned to that role, business information can be incorporated into the role mining process. However, the application of this approach for our scenario is highly unlikely. The proposed introduction of business information requires the set of information implying authorization rights to be at least partially disjunctive. However, in our scenario this is not necessarily the case.

Our considerations show, that the NP-completeness of the Role Mining problem [VAG07], requires further consideration of non-exact search and organizational integration of such techniques. Approaches, such as [Fr09] or [KSS03] are merely applicable for hierarchical RBAC. However, hierarchical roles may provide the necessary decrease in complexity, in order to administer highly dynamic scenarios.

3 Scenario

Our scenario considers hierarchical RBAC in a dynamic, and heterogeneous environment, such as in privileged access of IT service operations. If we consider, for instance cloud service providers, multiple different systems, such as VM Hypervisors, Logging components, Privileged Identity and Access Management (IAM), firewalls, VPN gateways, FTP servers, Fileshares, and Workflow engines are possible objects, accessed by privileged users. Classically, privileged IAM focuses on accountability of actions [Ja11], rather than minimization of provided accesses. However, as the infrastructural, and thus the amount of involved administrators increases, formalization of workflows and responsibilities may yield groups, which are neither disjunctive nor equal in terms of access rights. This means, that while e.g. administrative teams for managing the security infrastructure, and administrative teams for managing the VM hypervisors may exist, both may be required to access similar systems, e.g. the logging system.

In such a scenario, we use the definition of the hierarchical RBAC, as in [Sa96]. Hereby we omit the concepts of sessions and separation of duties (SOD). We argue, that sessions can be omitted for the sake of simplicity, as we do not aim on optimizing the currently used roles, but ease administration of assigned roles for the respective subject. The concept of SOD is omitted since it does not fully extend to the issue of risk consolidation, requiring duties to be formalized and thus disjunctive in nature. However, this is very likely not the case in our scenario. Therefore we yield the following definition of the RBAC [Sa96]:

- Users, Roles, and Permissions: U,R, and P
- A many-to-many permission to role assignment relation: $PA \subseteq P \times R$
- A many-to-many user to role assignment relation: $UA \subseteq U \times R$
- A partial order on R called the role hierarchy or role dominance relation : $RH \subseteq R \times R$

In our scenario we aim at improving the role structure throughout regular audit. Improving the role structure includes both minimization of the roles involved within the role structure [KSS03] [VAG07], and providing understandable roles, which match with the semantics of the regarded scenario [Fr09].

3.1 Role Structure Optimization and the risk accumulation problem

Additionally, improving the role structure requires consideration of possible access risks. We consider the access risks which occur with each permission as:

- A many-to-many permission to access risk relation: $AR \subseteq P \times Ri$

Especially, in our privileged access scenario, not all possible access risks combinations may be determinable, nor formalized. This is especially the case, if access risks materialize according to the accumulation principle which involves the combination of different lower risks leading to a high access risks, rather than the maximum principle which allows the formal application of the highest risk. If we denote access risks as a binary matrix, whereas a 1 indicates, that the access risks should be strictly separated, we are still only able to depict access risk accumulations between two risks. Accumulations between three risks, would require an additional matrix, for up to four possible access risks two additional matrices, and so on. The possible solution space therefore grows rapidly, and may quickly become hard to administer.

As the problem of finding a minimal set of roles itself is NP-complete [VAG07], and the access risks being many to many regarding the respective permission, which itself are in a many-to-many relation with the respective roles, the issue of detecting access risk accumulations on a full role list is hardly expectable.

Additionally, access risks accumulate at the user itself, due to multiple access rights assignment to the same set of users. This means, that information on the user, the roles, and the assignment is required to identify accumulated access risks.

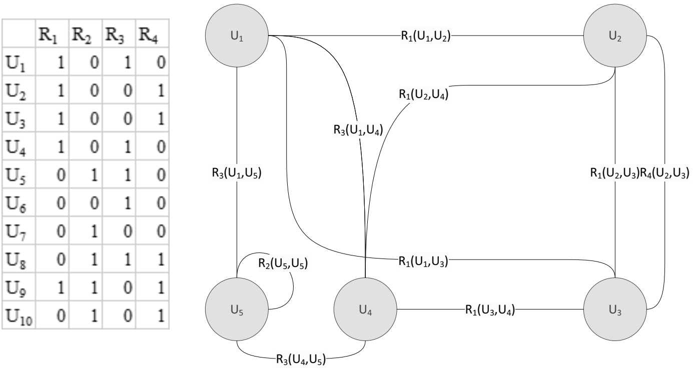
Following the definition by [Sa96], hierarchical RBAC enables easier maintenance by providing a superset of permissions. This means, that roles accumulate the permissions along their hierarchy. For the detection of accumulated access risks, this means that only a subset of all roles, a subset of permissions, and thus a subset of access risks must be determined, enabling the accumulation of access risks to become manageable.

Current approaches for mining RBAC roles however, either neglect the mining of hierarchical RBAC, such as [Fr09] [KSS03] [VAG07], or abstract information on the user by edge minimization between user and role nodes, such as [ZRE03].

Our approach therefore uses a different graph construction approach as [ZRE03], by providing a Graph with only one type of nodes (the users), wherein each role assignment becomes an edge. This graph is being clustered and analysed using the design structure matrix method, enabling detection of interdependencies between clusters and in clusters.

4 Approach for risk centred role mining

In our scenario, business data such as the organisational unit is very likely to not provide sufficient mutual information on roles, as in [Fr09] [KSS03]. Therefore we largely focus on role mining approaches, which use the UA as a source for role mining, such as [VAG07] [ZRE03]. Both approaches consider the UA as input, and either aim at clustering the UA [VAG07], or try to minimize the edges in a graph built from different types of nodes (roles, and users) [ZRE03]. One key issue with these approaches for risk centred mining of hierarchical roles, is that neither provides sufficient information on possible risk consolidations, and conflicts with user-role assignments of the mined roles.



	R_1	R_2	R_3	R_4
U_1	1	0	1	0
U_2	1	0	0	1
U_3	1	0	0	1
U_4	1	0	1	0
U_5	0	1	1	0
U_6	0	0	1	0
U_7	0	1	0	0
U_8	0	1	1	1
U_9	1	1	0	1
U_{10}	0	1	0	1

Figure 1 Overview on the graph based approach. The edges depict the mutual group assignments of roles (Right). The corresponding UA is shown on the left

By using graph optimization as in [ZRE03], the followed approach of minimizing the edges [Mo09] most likely aggregates user assignments, and does not allow further follow up on possible risk consolidations at users due to a role aggregation. The same holds for [VAG07], where the NP-completeness of the underlying non negative matrix factorization issue [Va09] results in various possible solutions, and may thus make it impossible to follow-up on risk and access rights consolidations occurring out of role aggregation.

We therefore follow a slightly different, yet graph-based approach, in order to enable the evaluation of access risk consolidations in our current role structure, and in the aggregated role structure. This means, that we do neither aggregate roles, users, nor assignments in our analysis. This is achieved by defining the UA as a Graph, in which each user is depicted as a node, and each mutual role assignment between users results in an edge. Figure 1 visualizes this approach. The matrix indicated on the left, shows an example UA, which corresponds to a binary matrix, indicating 1, if a role is assigned to a user, and 0 otherwise.

Based on the UA, we extract the corresponding graph of mutual role assignments, by creating an edge for each shared role. In our example, shown in Figure 1, this means that role R1 results in 8 edges (4 edges between U1, U2, U3, and U4, 3 edges between U2, U3, and U4, and 1 edge between U3, and U4). The present data now enables us to follow three different strategies: (1) clustering of the resulting incidence matrix of the graph I(G); (2) clustering of the resulting adjacency matrix of the graph, and (3) clustering of the adjacency matrix of the line graph. As we want to preserve information on possible role assignments, and possible risk consolidations, Strategy (2) would only provide information on which users share mutual roles, lacking information on which roles are shared mutually by which users, and thus not enabling further risk analysis. Strategies (1) and (3) preserve the required information. However, since each edge can be assigned to up to two user nodes, and one role, strategy (3) promises the most efficient handling of our issue.

Therefore, we obtain the line graph in the next step, indicating which edges correspond together, and thus which roles are assigned mutually at which users. The line graph can be obtained by:

$$Adj(G)^L = I(G)' * I(G) - 2 * I_{|V|}$$

Where $Adj(G)^L$ indicates the adjacency matrix of the line graph, I(G) the incidence matrix of the graph, and $I_{|V|}$ indicates the identity matrix in the size of the resulting number of edges in our graph.

5 Clustering of mutual roles and analysis

As $Adj(G)^L$ is a symmetric matrix, indicating mutual roles, and in a broader term interactions between roles, we can apply the methodologies around design structure matrices [YB03], This approach is mostly used within process and product planning, and knowledge management, and is applied in scenarios where multiple interactions between components occur. Hereby the resulting interaction matrices, which indicate whether two components interact, are being clustered, and analysed. Clustering hereby takes both internal and external dependencies into account. As our approach seeks to find mutually shared roles and risk consolidations, using an approach that identifies both internal and external dependencies throughout the mining of hierarchical RBAC roles seems reasonable.

We therefore follow this approach, by clustering $Adj(G)^L$, using the algorithm described in Section 5.1, followed by an analysis of the resulting internal, and external dependencies of the resulting role clusters (see Section 5.2).

5.1 Clustering of the Role Assignment Adjacencies

For clustering of the role assignment adjacencies in $Adj(G)^L$, we follow the algorithm proposed by [Id95] along with the refinements by [Th01]. The following pseudo-code describes the process of clustering within the role assignment adjacencies:

```
Clusters[] <- Initialize each element in role assignment
adjacencies as own Cluster;
Do While (iteration < abortIteration)
                 And (deltaCosts < abortDelta)
   clusterCurrent <- Pick a cluster from Clusters[]
   u.a.r.;
   totalCosts <- Calculate Costs according to equation
 2, 3 and 4;
   highestBiddingCluster <- calculate Bids from all
   Clusters in Clusters[] according to equation 1 to
```

```
        clusterCurrent and pick the highestBiddingCluster;
        If (highestBid = random_Bet)
                       highestBiddingCluster <- Pick second
                       highest Bidding Cluster;
        fi
        clusterJoined <- Join clusterCurrent and
        highestBiddingCluster;
        newCosts <- Calculate Costs;
        r <- Pick integer r u.a.r.;
        If (newCosts < totalCosts) Or (r < acceptThreshold)
                   Clusters[] <- Remove clusterCurrent and
                   highestBiddingCluster and Add
                   clusterJoined;
        Else
                   Clusters[] <- Restore old Cluster List;
        fi
        iteration <- iteration + 1;
    Od
```

The algorithm by [Ja11] [Th01] requires two basic input parameters. random_Bet specifies a random guess by the user, and enables the algorithm to take the second best option in search for an optimum, rather than following the best option as in greedy strategies. The second algorithm, with the same intention, enables the algorithm to randomly accept solutions which result in a worse solution than the one of the previous iteration. As such, the algorithm roughly follows the path of simulated annealing [Hw88], which partially accepts worse solutions, rather than following a greedy strategy by only accepting the best solution during an iteration. As the role mining problem, and the problem of finding clusters in non-binary matrices are both NP-complete [VAG07] [Va09], reliance on local optima in finding optimal solutions will most likely result in the algorithm becoming stuck in a local optima. Therefore, following the approach of simulated annealing within the clustering, as done by [Id95] [Th01] provides a promising approach.

For determining the elements which should be joined towards a new cluster, the algorithm is using bids. These bids of a cluster j to a cluster k, depend on the internal dependencies of the newly joined cluster (j,k) and punish the size of the bidding cluster j. The bids are defined in [Th01] as:

$$\mathrm{ClusterBid}_{j,k} = \frac{\mathrm{DSM}_{j,k}^{\mathrm{powDep}}}{\mathrm{ClusterSize}_{j}^{\mathrm{powBid}}}$$

Equation 1 Function for determining the bid of a cluster j to a cluster k

Where the bid is considered as a bid from cluster j to cluster k. DSM depicts the internal dependency of the newly arranged cluster. In our case, DSM is the sum of adjacencies within the cluster in $\mathrm{Adj}(G)^{L}$. ClusterSize indicates the size of the bidding cluster j. Both the internal dependency DSM and the size of the bidding cluster are additionally adjusted by using the input variables powDep, and powBid. powDep determines the weight of the internal dependency of the newly arranged cluster over the bidding cluster's size. powBid on the other hand emphasizes the role of the bidding clusters size. If larger cluster should be obtained, this value should be lower than the input value powDep, and vice versa.

The target function of the clustering algorithm aims at minimizing the overall costs. These are defined as:

$$TotalCosts = \sum IntraClusterCost + \sum ExtraClusterCost$$

Equation 2 Function for determining the overall costs

The IntraClusterCost hereby indicate the cost function within each cluster, which considers both the internal dependencies DSM of the cluster, and the cluster size (ClusterSize).

$$IntraClusterCost_j = DSM_j * ClusterSize^{powCC}$$

Equation 3 Function for determining the internal costs of a cluster j

Hereby the size of each cluster is being punished by using the exponent powCC, which is being defined by the user. In order to calculate the Extra Cluster Costs, the algorithm originally determines the dependencies between each cluster [Id95]. However, as the DSM value in our case is being defined, as the sum of adjacencies, and as our goal is to minimize the adjacencies outside of our clusters, we define the Extra Cluster Costs as:

$$ExtraClusterCost_j = DSM_{i,j} * DSMSize^{powCC}$$

Equation 4 Function for determining the external costs of a cluster j

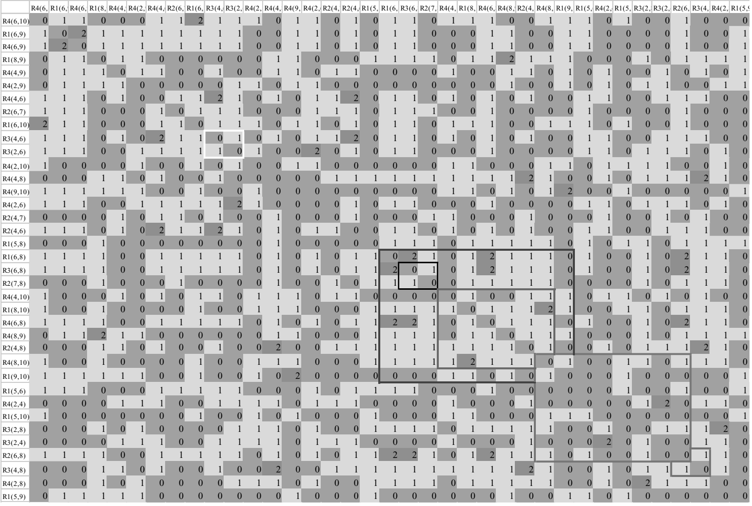
Where $DSM_{i,j}$ defines the dependability of all elements outside of the cluster, but within the rows i, or the columns j of the cluster. DSMSize considers the amount of external elements which depend upon the cluster j. These elements reside within the rows i, or the colums j of the cluster. As with the IntraClusterCosts the weight of the amount of external dependencies is emphasized by the value powCC.

This cluster algorithm can be executed for a maximum amount of iterations, or until the cost function converges.

5.2 Analysing the Clustered Role Assignment Adjacencies

After clustering of the role assignment adjacencies a matrix, such as in Figure 2 is obtained. The clusters are indicated within the squares, showing which user role assignment could be aggregated, and which risk accumulations should be further examined. If a dependency is indicated with the value 0 no association between the role assignments is given (meaning, that these roles are not associated with the same subjects). A value of 1 indicates, that one of the roles is assigned to both subjects (e.g. in Figure 2, role R1 is associated both with subjects 6, and 9. Subject 6 is additionally associated with role R4). Finally, a value of 2 indicates that both roles are assigned with both subjects are associated with both roles (e.g. in Figure 2, subjects 6 and 8 are both associated with roles R1 and R3). The algorithm flips rows and columns according to the algorithm introduced in Section 5.2, and tries to establish clusters along the diagonal line of the adjacency matrix.

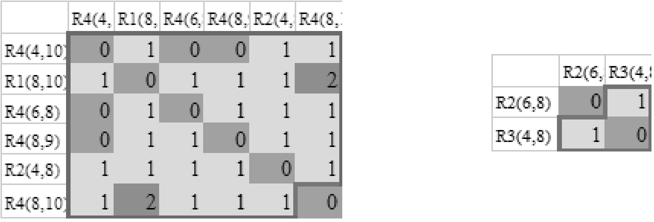
For further analysis of the obtained role assignment adjacencies, we must consider both the internal structure of the cluster, and the external structure of the elements within the rows and columns, but outside of the cluster. In this section, we will therefore discuss different observations that can occur within the clustered role adjacency matrix, and their implications.



	R4(6,	R1(6,	R4(6,	R1(8,	R4(4,	R4(2,	R4(4,	R2(6,	R1(6,	R3(4,	R3(2,	R4(2,	R4(4,	R4(9,	R4(2,	R2(4,	R2(4,	R1(5,	R1(6,	R3(6,	R2(7,	R4(4,	R1(8,	R4(6,	R4(8,	R2(4,	R4(8,	R1(9,	R1(5,	R4(2,	R1(5,	R3(2,	R3(2,	R2(6,	R3(4,	R4(2,	R1(5,9
R4(6,10)	0	1	1	0	0	0	1	1	2	1	1	1	0	1	1	0	1	0	1	1	0	1	1	1	0	0	1	1	1	0	1	0	0	1	0	0	0
R1(6,9)	1	0	2	1	1	1	1	1	1	1	1	0	0	1	1	0	1	0	1	1	0	0	0	1	1	0	0	1	1	0	0	0	0	1	0	0	1
R4(6,9)	1	2	0	1	1	1	1	1	1	1	1	0	0	1	1	0	1	0	1	1	0	0	0	1	1	0	0	1	1	0	0	0	0	1	0	0	1
R1(8,9)	0	1	1	0	1	1	0	0	0	0	0	0	1	1	0	0	0	1	1	1	1	0	1	1	2	1	1	1	0	0	0	1	0	1	1	1	1
R4(4,9)	0	1	1	1	0	1	1	0	0	1	0	0	1	1	0	1	1	0	0	0	0	1	0	0	1	1	0	1	0	1	0	0	1	0	1	0	1
R4(2,9)	0	1	1	1	1	0	0	0	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	1	0	1	0	1	1	0	0	1	1
R4(4,6)	1	1	1	0	1	0	0	1	1	2	1	0	1	0	1	1	2	0	1	1	0	1	0	1	0	1	0	0	1	1	0	0	1	1	1	0	0
R2(6,7)	1	1	1	0	0	0	1	0	1	1	1	0	0	0	1	1	1	0	1	1	1	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0
R1(6,10)	2	1	1	0	0	0	1	1	0	1	1	1	0	1	1	0	1	0	1	1	0	1	1	1	0	0	1	1	1	0	1	0	0	1	0	0	0
R3(4,6)	1	1	1	0	1	0	2	1	1	0	1	0	1	0	1	1	2	0	1	1	0	1	0	1	0	1	0	0	1	1	0	0	1	1	1	0	0
R3(2,6)	1	1	1	0	0	1	1	1	1	1	0	1	0	0	2	0	1	0	1	1	0	0	0	1	0	0	0	0	1	1	0	1	1	1	0	1	0
R4(2,10)	1	0	0	0	0	1	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	1	1	0	1	1	1	1	0	0	1	0
R4(4,8)	0	0	0	1	1	0	1	0	0	1	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	2	1	0	0	1	0	1	1	1	2	1	0
R4(9,10)	1	1	1	1	1	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	1	1	0	1	0	1	2	0	0	1	0	0	0	0	0	1
R4(2,6)	1	1	1	0	0	1	1	1	1	1	2	1	0	0	0	0	1	0	1	1	0	0	0	1	0	0	0	0	1	1	0	1	1	1	0	1	0
R2(4,7)	0	0	0	0	1	0	1	1	0	1	0	0	1	0	0	0	1	0	0	0	1	1	0	0	0	1	0	0	0	1	0	0	1	0	1	0	0
R2(4,6)	1	1	1	0	1	0	2	1	1	2	1	0	1	0	1	1	0	0	1	1	0	1	0	1	0	1	0	0	1	1	0	0	1	1	1	0	0
R1(5,8)	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1	1	0	1	1	1	1	1	0	1	0	1	1	0	1	1	1	1
R1(6,8)	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	0	1	1	0	2	1	0	1	2	1	1	1	0	1	0	0	1	0	2	1	1	0
R3(6,8)	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	0	1	1	2	0	1	0	1	2	1	1	1	0	1	0	0	1	0	2	1	1	0
R2(7,8)	0	0	0	1	0	0	0	1	0	0	0	0	1	0	0	1	0	1	1	1	0	0	1	1	1	1	1	0	0	0	0	1	0	1	1	1	0
R4(4,10)	1	0	0	0	1	0	1	0	1	1	0	1	1	1	0	1	1	0	0	0	0	0	1	0	0	1	1	1	0	1	1	0	1	0	1	0	0
R1(8,10)	1	0	0	1	0	0	0	0	1	0	0	1	1	1	0	0	0	1	1	1	1	1	0	1	1	1	2	1	0	0	1	1	0	1	1	1	0
R4(6,8)	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	0	1	1	2	2	1	0	1	0	1	1	1	0	1	0	0	1	0	2	1	1	0
R4(8,9)	0	1	1	2	1	1	0	0	0	0	0	0	1	1	0	0	0	1	1	1	1	0	1	1	0	1	1	1	0	0	0	1	0	1	1	1	1
R2(4,8)	0	0	0	1	1	0	1	0	0	1	0	0	2	0	0	1	1	1	1	1	1	1	1	1	1	0	1	0	0	1	0	1	1	1	2	1	0
R4(8,10)	1	0	0	1	0	0	0	0	1	0	0	1	1	1	0	0	0	1	1	1	1	1	2	1	1	1	0	1	0	0	1	1	0	1	1	1	0
R1(9,10)	1	1	1	1	1	1	0	0	1	0	0	1	0	2	0	0	0	0	0	0	0	1	1	0	1	0	1	0	0	0	1	0	0	0	0	0	1
R1(5,6)	1	1	1	0	0	0	1	1	1	1	1	0	0	0	1	0	1	1	1	1	0	0	0	1	0	0	0	0	0	0	1	0	0	1	0	0	1
R4(2,4)	0	0	0	0	1	1	1	0	0	1	1	1	1	0	1	1	1	0	0	0	0	1	0	0	0	1	0	0	0	0	0	1	2	0	1	1	0
R1(5,10)	1	0	0	0	0	0	0	0	1	0	0	1	0	1	0	0	0	1	0	0	0	1	1	0	0	0	1	1	1	0	0	0	0	0	0	0	1
R3(2,8)	0	0	0	1	0	1	0	0	0	0	1	1	1	0	1	0	0	1	1	1	1	0	1	1	1	1	1	0	0	1	0	0	1	1	1	2	0
R3(2,4)	0	0	0	0	1	1	1	0	0	1	1	1	1	0	1	1	1	0	0	0	0	1	0	0	0	1	0	0	0	2	0	1	0	0	1	1	0
R2(6,8)	1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	0	1	1	2	2	1	0	1	2	1	1	1	0	1	0	0	1	0	0	1	1	0
R3(4,8)	0	0	0	1	1	0	1	0	0	1	0	0	2	0	0	1	1	1	1	1	1	1	1	1	1	2	1	0	0	1	0	1	1	1	0	1	0
R4(2,8)	0	0	0	1	0	1	0	0	0	0	1	1	1	0	1	0	0	1	1	1	1	0	1	1	1	1	1	0	0	1	0	2	1	1	1	0	0
R1(5,9)	0	1	1	1	1	1	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0	1	1	0	1	0	0	0	0	0	0

Figure 2 Example for Role Assignment Adjacencies after Clustering. Clusters are indicated in squares. The clustering used the values (powDep = 1; powBid = 1; powCC = 2), maximum Iterations were 1500, and convergence criteria was set to 0.5.

5.3 Internal structure of the clusters

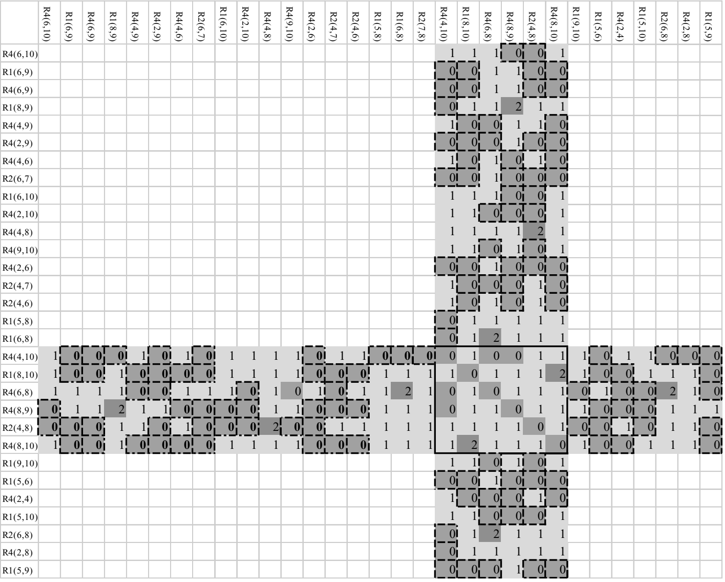


	R4(4,	R1(8,	R4(6,	R4(8,	R2(4,	R4(8,
R4(4,10	0	1	0	0	1	1
R1(8,10	1	0	1	1	1	2
R4(6,8)	0	1	0	1	1	1
R4(8,9)	0	1	1	0	1	1
R2(4,8)	1	1	1	1	0	1
R4(8,10	1	2	1	1	1	0

	R2(6,	R3(4,
R2(6,8)	0	1
R3(4,8)	1	0

Figure 3 Examples of the internal cluster dependencies. The left shows a cluster with incomplete dependencies, indicating that users may gain additional access rights, and thus risks if the role is aggregated. The right shows a cluster with full internal dependency, indicating that all user assignments within this cluster would be achieved by aggregating the roles (in this case role R2, and R3).

The internal structure of the clusters provides insights into how many user assignments are actually affected by a possible role aggregation. Additionally, it may provide insights into which roles are currently assigned together, at which users. Figure 3 shows two possible cases of internal dependencies. The left case shows a cluster with incomplete internal dependency. Here the roles R1, R2, and R4 are being proposed for aggregation. However, since (except for the diagonal line), 0-elements are within the cluster, we can conclude that the aggregation of roles will result in users gaining additional access rights, and thus access risks.



	R4(6,10)	R1(6,9)	R4(6,9)	R1(8,9)	R4(4,9)	R4(2,9)	R4(4,6)	R2(6,7)	R1(6,10)	R4(2,10)	R4(4,8)	R4(9,10)	R4(2,6)	R2(4,7)	R2(4,6)	R1(5,8)	R1(6,8)	R2(7,8)	R4(4,10)	R1(8,10)	R4(6,8)	R4(8,9)	R2(4,8)	R4(8,10)	R1(9,10)	R1(5,6)	R4(2,4)	R1(5,10)	R2(6,8)	R4(2,8)	R1(5,9)
R4(6,10)																			1	1	1	0	0	1							
R1(6,9)																			0	0	1	1	0	0							
R4(6,9)																			0	0	1	1	0	0							
R1(8,9)																			0	1	1	2	1	1							
R4(4,9)																			1	0	0	1	1	0							
R4(2,9)																			0	0	0	1	0	0							
R4(4,6)																			1	0	1	0	1	0							
R2(6,7)																			0	0	1	0	0	0							
R1(6,10)																			1	1	1	0	0	1							
R4(2,10)																			1	1	0	0	0	1							
R4(4,8)																			1	1	1	1	2	1							
R4(9,10)																			1	1	0	1	0	1							
R4(2,6)																			0	0	1	0	0	0							
R2(4,7)																			1	0	0	0	1	0							
R2(4,6)																			1	0	1	0	1	0							
R1(5,8)																			0	1	1	1	1	1							
R1(6,8)																			0	1	2	1	1	1							
R4(4,10)	1	0	0	0	1	0	1	0	1	1	1	1	0	1	1	0	0	0	0	1	0	0	1	1	1	0	1	1	0	0	0
R1(8,10)	1	0	0	1	0	0	0	0	1	1	1	1	0	0	0	1	1	1	1	0	1	1	1	2	1	0	0	1	1	1	0
R4(6,8)	1	1	1	1	0	0	1	1	1	0	1	0	1	0	1	1	2	1	0	1	0	1	1	1	0	1	0	0	2	1	0
R4(8,9)	0	1	1	2	1	1	0	0	0	0	1	1	0	0	0	1	1	1	0	1	1	0	1	1	1	0	0	0	1	1	1
R2(4,8)	0	0	0	1	1	0	1	0	0	0	2	0	0	1	1	1	1	1	1	1	1	1	0	1	0	0	1	0	1	1	0
R4(8,10)	1	0	0	1	0	0	0	0	1	1	1	1	0	0	0	1	1	1	1	2	1	1	1	0	1	0	0	1	1	1	0
R1(9,10)																			1	1	0	1	0	1							
R1(5,6)																			0	0	1	0	0	0							
R4(2,4)																			1	0	0	0	1	0							
R1(5,10)																			1	1	0	0	0	1							
R2(6,8)																			0	1	2	1	1	1							
R4(2,8)																			0	1	1	1	1	1							
R1(5,9)																			0	0	0	1	0	0							

Figure 4 Cluster with incomplete dependency outside the cluster, indicating the increase of access

rights for users (marked with dashed lines) in the case of role aggregation

On the contrary, the right side of Figure 3 shows an example for a cluster with full internal dependency, in this case with the roles R2, and R3. This means that if the roles R2, and R3 would be aggregated no additional access rights, compared to the status quo would be provided to the users within this cluster.

5.4 Dependency outside the role cluster

The dependency outside the role cluster provides additional insights into possible access rights, and thus access risk increases in the case of a role aggregation.

	R4(6,10)	R1(6,9)	R4(6,9)	R1(8,9)	R4(4,9)	R4(2,9)	R4(4,6)	R2(6,7)	R1(6,10)	R4(2,10)	R4(4,8)	R4(9,10)	R4(2,6)	R2(4,7)	R2(4,6)	R1(5,8)	R1(6,8)	R2(7,8)	R4(4,10)	R1(8,10)	R4(6,8)	R4(8,9)	R2(4,8)	R4(8,10)	R1(9,10)	R1(5,6)	R4(2,4)	R1(5,10)	R2(6,8)	R4(2,8)	R1(5,9)
R4(6,10)																			1	1	1	1	1	1							
R1(6,9)																			1	1	1	1	1	1							
R4(6,9)																			1	1	1	1	1	1							
R1(8,9)																			1	1	1	2	1	1							
R4(4,9)																			1	1	1	1	1	1							
R4(2,9)																			1	1	1	1	1	1							
R4(4,6)																			1	1	1	1	1	1							
R2(6,7)																			1	1	1	1	1	1							
R1(6,10)																			1	1	1	1	1	1							
R4(2,10)																			1	1	1	1	1	1							
R4(4,8)																			1	1	1	1	2	1							
R4(9,10)																			1	1	1	1	1	1							
R4(2,6)																			1	1	1	1	1	1							
R2(4,7)																			1	1	1	1	1	1							
R2(4,6)																			1	1	1	1	1	1							
R1(5,8)																			1	1	1	1	1	1							
R1(6,8)																			1	1	2	1	1	1							
R2(7,8)																			1	1	1	1	1	1							
R4(4,10)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1
R1(8,10)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	2	1	1	1	1	1	1	1
R4(6,8)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	0	1	1	1	1	1	1	1	2	1	1
R4(8,9)	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1
R2(4,8)	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1
R4(8,10)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	0	1	1	1	1	1	1	1
R1(9,10)																			1	1	1	1	1	1							
R1(5,6)																			1	1	1	1	1	1							
R4(2,4)																			1	1	1	1	1	1							
R1(5,10)																			1	1	1	1	1	1							
R2(6,8)																			1	1	2	1	1	1							
R4(2,8)																			1	1	1	1	1	1							
R1(5,9)																			1	1	1	1	1	1							

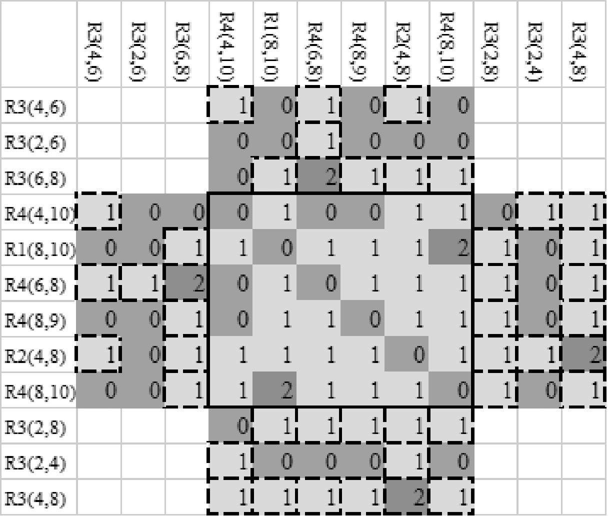
Figure 5 Example of a cluster within the role assignment adjacency matrix that indicates full dependency outside the cluster

By masking the edges, which are not element of a role, whose edges are within the cluster, we can highlight the accumulation of access rights outside the cluster (see Figure 4). Hereby, each 0-element indicates that a user does not participate in a role assignment that is proposed as aggregated by the cluster. These elements have been highlighted with dashed lines for better visibility.

Aggregation of the roles in the cluster could in this case lead to users gaining additional access rights. Therefore, it should be examined, why these users do not participate in the role assignments of the cluster, and whether the risk of providing the additional access rights within the cluster is feasible.

Another example is given in Figure 5. Here all assignments of the same roles, as in the cluster, are fully given. All affected users have been assigned to the same set of roles, which is indicated by the 1-elements outside of the cluster, but within the cluster rows and columns. This indicates that the access risks of the roles participating in the cluster must be examined. If the examination concludes that the combination of access risks is feasible, then aggregation of the roles enables easier maintenance of the role structure. Therefore these roles should be aggregated into a single role.

In the next step, the role assignments of roles participating in the cluster, which are outside the cluster, are being masked.



	R3(4,6)	R3(2,6)	R3(6,8)	R4(4,10)	R1(8,10)	R4(6,8)	R4(8,9)	R2(4,8)	R4(8,10)	R3(2,8)	R3(2,4)	R3(4,8)
R3(4,6)				1	0	1	0	1	0			
R3(2,6)				0	0	1	0	0	0			
R3(6,8)				0	1	2	1	1	1			
R4(4,10)	1	0	0	0	1	0	0	1	1	0	1	1
R1(8,10)	0	0	1	1	0	1	1	1	2	1	0	1
R4(6,8)	1	1	2	0	1	0	1	1	1	1	0	1
R4(8,9)	0	0	1	0	1	1	0	1	1	1	0	1
R2(4,8)	1	0	1	1	1	1	1	0	1	1	1	2
R4(8,10)	0	0	1	1	2	1	1	1	0	1	0	1
R3(2,8)				0	1	1	1	1	1			
R3(2,4)				1	0	0	0	1	0			
R3(4,8)				1	1	1	1	2	1			

Figure 6 Dependency of roles not participating in the cluster on the role cluster

This leads to a matrix indicating the role assignments participating in the cluster. Additionally we can see the role assignment of users, who would be affected by the cluster, whereas the role is not included in the cluster. This way, we can see which access risks accumulate at the user in the case of role aggregation within the cluster. Figure 6 provides an example for such an overview. When examining the dependencies with roles not affected by the cluster, the elements of the adjacency matrix, which are not set to zero are of most interest for us. These elements have been highlighted with a dashed bordering. In this case we can see, that from those users that have been assigned to the roles R4, R1, and R2 which are contained in the cluster, some have been assigned additional roles. For instance, some users that have obtained one of the roles R1, R4, or R2 have also obtained R3.

This means, that in order to successfully aggregate the roles, we must in this case not only consider the access risk accumulation occurring out of the set R1, R2, and R4, but also the access risk accumulation occurring out of the set R1, R2, R3, and R4. Furthermore, the access risk of the combinations (R1, R3), (R2, R3), and (R4,R3) should be examined if the role is not further aggregated.

6 Conclusion

Improving the role hierarchy and operative structure of RBAC is important to allow feasible administration of the access control data infrastructure [Fr09] [KSS03] [Mo09] [ZRE03]. However, as we have showed simply finding a minimal set of descriptive roles [VAG07] is merely enough, when it comes to dynamic and heterogeneous environments, such as infrastructure administration, smart systems. We have showed that entangling possible access risks within the role mining process is complex, due to the lack of formalization of access risks, and their combinations. While e.g. the maximum principle allows to use the highest risk, risk accumulations which may result in a more severe access risk than its' risk components, cannot be faced within classic role mining. We have therefore proposed to introduce a role mining approach within regular audits of the identity data infrastructure, and provided an approach which can be used to find role aggregations, while enabling examination of access risks. Hereby all access risks associated with the objects can be examined regarding their possible accumulation at subjects. The introduction of approaches surrounding design structure matrices seems feasible and provides a promising approach for identifying access risks. The ability to identify aggregation of subjects and objects within dynamic environments promises application during audit in dynamic environments. Further application of this approach for document exchanges in engineering will be considered within future research.

A central issue with such approaches however, as with most role mining approaches, remains the amount of noise incorporated within the UA. If the UA contains short-term role assignment, adjustment of the role structure within regular audits may cause to role data infrastructure to become instable between audits. In this case, the resulting structure may undergo several unnecessary adjustments, increasing workload for the administrators, while diverging from the regular work of the users. A technological solution could for instance incorporate the usage statistics. However, in most identity data infrastructure, such statistic is merely available for separate roles, but rather for the whole user (e.g. last account activity, or last log on). Therefore a solution of this issue may be found within case studies of concrete role data infrastructure within the given environments.

Still, the approach enables administrators to deal with issues of access risk consolidation, and to examine a role aggregation on a per user basis, without being required to examine the whole UA itself.

Acknowledgement

The research leading to these results was supported by the "German Ministry of research and Education (BMBF)" as part of the VERTRAG research project.

References

[Fr09] Frank, M.; Steich A. P.; Basin D.; Buhmann J. M.: A probabilistic approach to hybrid role mining. In: Proceedings of the 16th ACM conference on Computer and communications security. pp. 101–111 ACM (2009).

[GGM04] Geerts, F.; Goethals, B.; Mielkäinen T.: Tiling databases. In: Discovery science. pp. 278–289 Springer (2004).

[Hw88] Hwang, C.-R.: Simulated annealing: theory and applications. Acta Appl. Math. 12, 1, 108–111 (1988).

[Id95] Idicula, J.: Planning for concurrent engineering. Gintic Inst. Singap. (1995).

[Ja11] Jahchan, G.J.: Privileged User Management. In: Information Security Management Handbook. (2011).

[JGZ11] Jianyong, C.; Guiha, W; Zhen, J.: Secure interoperation of identity managements among different circles of trust. Comput. Stand. Interfaces. 33, 6, 533–540 (2011).

[KSS03] Kuhlmann, M.; Shohat, D.; Schimpf, G.: Role mining-revealing business roles for security administration using data mining technology. In: Proceedings of the eighth ACM symposium on Access control models and technologies. pp. 179–186 ACM (2003).

[Lu90] Luhmann, N.: Technology, environment and social risk: a systems perspective. Organ. Environ. 4, 3, 223–231 (1990).

[MR08] Meints, M., Royer, D.: Der Lebenszyklus von Identitäten. Datenschutz Datensicherheit DuD. 32, 3, 201 (2008).

[Mi08] Miettinen, P. et al.: The discrete basis problem. Knowl. Data Eng. IEEE Trans. On. 20, 10, 1348–1362 (2008).

[Mo09] Molloy, I. et al.: Evaluating Role Mining Algorithms. In: Proceedings of the 14th ACM Symposium on Access Control Models and Technologies. pp. 95–104 ACM, New York, NY, USA (2009).

[OL10] O'Connor, R.C., Loomis, R.J.: 2010 Economic Analysis of Role-Based Access Control. NIST, Gaithersburg, MD, USA (2010).

[Sa96] Sandhu, R.S.; Coyne, E. J.; Feinstein, H. L.; Youman, C. E.: Role Based Access Control Models. IEEE Comput. 29, 2, 38–47 (1996).

[Th01] Thebeau, R.E.: Knowledge management of system interfaces and interactions from product development processes. Massachusetts Institute of Technology (2001).

[VAG07] Vaidya, J.; Atluri, V.; Guo, Q.: The role mining problem: finding a minimal descriptive set of roles. In: Proceedings of the 12th ACM symposium on Access control models and technologies. pp. 175–184 ACM (2007).

[Va09] Vavasis, S.A.: On the complexity of nonnegative matrix factorization. SIAM J. Optim. 20, 3, 1364–1377 (2009).

[YB03] Yassine, A., Braha, D.: Complex Concurrent Engineering and the Design Structure

Matrix Method. Concurr. Eng. Res. Appl. 11, 3, 165–176 (2003).

[ZRE03] Zhang, D.; Ramamohanarao, K.; Ebringer, T.: Role engineering using graph optimisation. In: Proceedings of the 12th ACM symposium on Access control models and technologies. ACM (2007).

Password Policy Markup Language

Moritz Horsch, Mario Schlipf, Stefen Haas, Johannes Braun, Johannes Buchmann[1]

Abstract: Password-based authentication is the most widely used authentication scheme for granting access to user accounts on the Internet. Despite this, there exists no standard implementation of passwords by services. They have different password requirements as well as interfaces and procedures for login, password change, and password reset. This situation is very challenging for users and often leads to the choice of weak passwords and prevents security-conscious behavior. Furthermore, it prevents the development of applications that provide a fully-fledged assistance for users in securely generating and managing passwords. In this paper, we present a solution that bridges the gap between the different password implementations on the service-side and applications assisting users with their passwords on the client-side. First, we introduce the Password Policy Markup Language (PPML). It enables a uniformly specified Password Policy Description (PPD) for a services. A PPD describes the password requirements as well as password interfaces and procedures of a service and can be processed by applications. It enables applications to automatically (1) generate passwords in accordance with the password requirements of a service, (2) perform logins, (3) change passwords, and (4) reset passwords. Second, we present a prototypical password manager which uses PPDs and is capable of generating and completely managing passwords on behalf of users.

Keywords: Passwords, Password Generation, Password Management

1 Introduction

Passwords are the dominating authentication means for granting access to user accounts on the Internet. The concept of password-based authentication is well-established and well-known by users. It is platform independent and can be used across many applications. From the perspective of services, password-based authentication can be implemented with little effort and has a negligible cost per user [Bo12b]. The key challenge for users is the creation of secure passwords and their proper management. Users must create strong and individual passwords for each of their accounts and need to memorize them for later use. Moreover, passwords should be changed on a regular basis. The possible oblivion of passwords require that users keep the recovery email address or phone number of the user accounts up-to-date. Doing all these tasks for the huge amount of passwords that users have today is practically impossible. This causes that users choose weak passwords and do not change them. However, this is crucial because passwords are the sole barrier that protects the multitude of personal data such as email and photos stored in the user accounts.

For several of these tasks, users can fall back on password generators and managers. They allow creating strong passwords and their secure storage and thus eliminate the burden of memorizing passwords. However, their assistance is nonsatisfying, because they still

[1] Technische Universität Darmstadt, Hochschulstraße 10, 64289 Darmstadt, {horsch | mschlipf | shaas | jbraun | buchmann}@cdc.informatik.tu-darmstadt.de

require a lot of manual user interactions. Users need to adapt generated passwords and the assistance for login and password change is error-prone or limited to a few services. The key problem is that password-based authentication is not standardized and services implement passwords in different ways. They have different password requirements as well as interfaces and procedures for login, password reset, and password change.

We address the issues induced by the different password implementations by services with the definition of the Password Policy Markup Language (PPML). PPML allows a structured description of password requirements as well as password interfaces and procedures of a service. Based on such a well-defined Password Policy Description (PPD), password creation and management can be automated and performed by applications without manual user interaction. More precise, optimal passwords are generated in accordance with the respective requirements and passwords can be changed or reset on behalf of users. This facilities a secure and ubiquitous user-side password management.

This paper is organized as follows. After a short presentation of related work in Section 2, we provide our main contributions:

First, in Section 3, we analyze the *password life cycle* and identify the different challenges for users. The password life cycle is described based on the work done in [SB14, Ch14]. It illustrates the different stages of a password and related tasks for users. The cycle starts with the generation of a password, continues with its management, and ends when the password cannot be used anymore. For each of the identified challenges we describe existing approaches and point out their drawbacks. We show, that many password related problems are unsolved so far.

Second, in Section 4, we specify PPML and the syntax of PPDs in detail and show how PPDs solve the identified open problems. We present how password requirements as well as password procedures and interfaces of a service are described in a PPD. We explain how the necessary information to enable an automatic password management are specified in a PPD. Moreover, we provide an exemplary PPD as well as PPDs for 5 existing services.

Third, Section 5 presents the implementation of our solution. First, we present a central service for making PPDs available to applications. Second, we provide a password manager that is capable of automatically creating passwords in accordance with service's password requirements and changing them, based on the information provided by the PPDs.

Finally, Section 6 concludes the paper and presents future work.

2 Related Work

There are multiple studies such as [Fu11, Fu07, WW15, FH10] which analyze password policies of services. All point out the enormous diversity of password requirements and password management implemented by the services. Shay et al. [SBB07] present a language and simulation model for password policies. Their language is based on the generic authentication policy language AuthSL [Sq07], but it is not capable of expressing password requirements of real services. The simulation model is later enhanced by technical and human factors [SB09], but it still focuses on simulating policies instead of expressing policies of existing services. Stobert and Biddle [SB14] conducted a series of interviews to analyze how users cope with the challenge of creating and managing passwords. Based on the answers of the participants they identify a password life cycle which follows the password behavior of the users. Choong [Ch14] develop a cognitive-behavioral framework which presents the cognitive process and user behavior of managing passwords in order to provide guidance on future research directions. Stajano et al. [St14] propose semantic annotations for password-related HTML forms to improve the effectiveness of password managers. They introduce a set of class names which should be used by web developers for the `class` attribute of HTML elements. Password managers can detect these class names and interpret the meaning of the HTML form. Whereas this approach requires that every service updates its website, our approach is completely independent from the services.

3 Password Life Cycle

In this section, we describe the password life cycle and show the numerous challenging duties and tasks of users with regard to passwords.

The password life cycle is a progression of stages through which each password passes (cf. Figure 1). The circles depict the states of a password from the perspective of a user. The arrows represent tasks for the user. The dashed arrow illustrates the possible oblivion or expiration of a password. The cycle begins with the creation of a password. This task is repeated until the password fulfils the individual password requirements of a service. Then the user needs to assign the password to a service and memorize it. For each login or password change the password must be recalled by the user. The change of a password leads back to the creation and finally to the memorization of the new password. In case that the user forgets the password or it expires he or she cannot use it anymore. The user can reset the password which requires the creation and memorization of a new password.

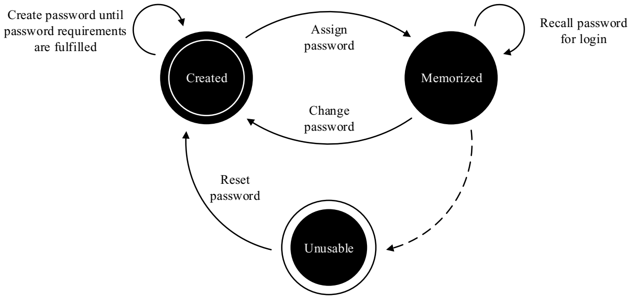

Create password until password requirements are fulfilled
Created
Assign password
Change password
Memorized
Recall password for login
Reset password
Unusable

Figure 1: Password Life Cycle.

We use the term *password creation* to refer to the part of the password life cycle which addresses the creation of a password. And we use the term *password management* to refer to the part of assigning, memorizing, recalling, changing, and resetting a password.

In the following, we take a closer look at the different stages and transactions of the cycle. We show how users cope with the various tasks in practice and point out security and usability problems. Moreover, we analyze existing proposals to mitigate these problems. We show that password generators and managers are the best approaches today. However, they are not solving the problems in a satisfactory manner, because they still require that users need to do many tasks manually. For an overview of approaches to replace passwords we refer to Bonneau et al. [Bo12b].

3.1 Password Creation

The creation of passwords that resist brute-force [Ke12, We09], dictionary [Bo12a, We10], and social engineering [Ca13] attacks is difficult. Users tend to choose passwords that are simple and easy to remember, but at high risk of compromise [ASL97, BK95, DMR10, FH07, ZH99]. However, strong passwords are essential for the user accounts' security.

Services implement password requirements and password meters to enforce or rather encourage users to select strong passwords. Password requirements are fixed rules with respect to the password length and the allowed and/or required characters. They do not cover the issue of common passwords like *123456*, where the password on the one hand might fulfill the requirements, while on the other hand is easy to guess.

Password meters assess the strength of passwords. They provide dynamic feedback to users by labeling passwords as weak, medium, or strong. On the one hand studies have shown that password meters lead towards more secure passwords [Ur12, Eg13]. On the other hand, in practice they are highly inconsistent in assessing the password strength. Even obviously weak passwords like *password1* are rated as strong which makes users believe that they have chosen a strong password, but actually they have not [dCdCM14].

In the past it was generally acknowledged that users should create passwords based on mnemonic phrases (so called passphrases), because they are easy to remember but hard to guess by current cracking tools [Ya04]. However, the recently published tool Phraser [SS16] uses common sentences to crack passphrases consisting of up to 20 characters.

Another approach are password generators. They create random and strong passwords based on predefined password generation rules. These rules can be modified with respect to the length and the allowed character sets for the generated passwords. However, in practice such passwords are often rejected by services because they do not comply with the various password requirements of services. For instance, the generated passwords are too short, too long, or do not contain a special character. One possible solution would be that all services agree on a single set of requirements [Al12, St14]. Yet, this seams unrealistic with respect to the multitude of existing different password implementations and security needs. Also, a common set of generation rules that fit to the password requirements of all services is not realizable due to the enormous diversity of requirements. Wang et al. [WW15] mention that such a set does not even exist for a set of 50 services. Currently, the only solution for users is to look up the password requirements of each service manually and configure the password generator accordingly. This is error-prone, very inconvenient for users, and not infrequently prevents users from employing password generators at all.

3.2 Password Memorization

Memorizing strong and individual passwords for many user accounts is practically impossible. Users are reusing passwords to cope with this issue. However, this bears the risk that adversaries get access to multiple accounts by just obtaining a single password. To prevent this, users must use individual passwords for their accounts. One possible solution for the problem of memorizing numerous passwords is to store them. This also solves the problem of memorizing which password is assigned to which service as well as recalling passwords even if they are rarely used. However, storing passwords demands an protection mechanism (usually another password) to protect them from unauthorized access. Moreover, the stored passwords need to be available on all devices of the users, so that they are able to access their accounts at anytime and from anywhere. This becomes even more challenging in case that the passwords are changed on a regular basis.

In comparison to diaries or text files, password managers are the best solution for storing passwords. They securely store them in a database and protect them by a *master password*. Furthermore, the database can be stored online in order to share it between arbitrary devices. Password managers can also automatically fill out login forms to make the use of passwords for users very convenient. However, this requires complex heuristics to detect login forms. Such heuristics are error-prone and can even be exploited by adversaries to extract passwords from the password manager without any user interaction [Si14].

3.3 Password Change

Regularly changing passwords of all user accounts is a very time-consuming task. Therefore, users barely change their passwords [Ha15, THB15], even after security breaches or exceptional events like the Heartbleed bug [Co14, Da14, Pe14]. However, changing passwords is crucial to invalidate former possibly compromised passwords.

The password managers LastPass [La16] and Dashlane [Da16] provide means for changing passwords automatically. However, both support only popular services and do not allow to add further services. LastPass is implemented as a browser extension and performs the password change in a browser tab. This is error-prone, because any interaction or close of the tab causes a failure of the password change. Furthermore, this solution makes it practically impossible to change a huge number of passwords at the same time. In comparison, Dashlane sends the user's username as well as his or her old and new password to a Dashlane server, which performs the password change on behalf of the user. As a consequence, the company behind Dashlane gets to know the passwords of the users!

3.4 Password Reset

Memorized or stored passwords might be forgotten or lost. Users need to answer security questions or need to prove access to a recovery phone number or email address to get access to their accounts again. However, memorizing and keeping all recovery information up-to-date is practically impossible. Today, there exists no solution for this problem.

4 Password Policy Markup Language

In Section 3, it was shown that password generators and managers are the best approach for users to obtain and use secure passwords, but they still require many manual user interactions. Users need to adapt generated passwords and the assistance in automatic login and password change are error-prone or limited to a few services. The root of these problems are the different password implementations of services, which prevent a fully automated generation and management of passwords.

In this Section we present the Password Policy Markup Language (PPML) which solves this problem. PPML enables the definition of Password Policy Descriptions (PPDs) for Internet services. A PPD is a standardized description of the password requirements as well as the password interfaces and procedures of a service. The objective of a PPD is twofold. First, it provides all required information to enable applications to completely automate the password life cycle. More precise, a PPD facilitates applications to (1) generate passwords in accordance with the password requirements of a service, (2) perform logins, (3) change passwords, and (4) reset passwords on behalf of users. Second, in case that an automatic password management is not possible for a service (e.g. in case that users need to enter a CAPTCHA to change a password), a PPD provides all information to assist users in accessing and performing the password interfaces and procedures manually. In detail, a PPD provides the URLs to the password interfaces so that users can directly access them out of an application instead of finding them for each service by hand.

We conducted an analysis of password requirements as well as password procedures and interfaces of 200 representative services[1] in order to develop a comprehensive and representative specification for PPDs. Based on the results, we identified common patterns and created a universal description scheme for password requirements, password management procedures, and technologies of password interfaces. Finally, we transformed this common description into a XML Schema. XML is well-specified and supported by many programming languages, which enables an easy integration of PPDs in password generators, password managers, and other applications.

A PPD is presented by a XML element `<ppd>`, which has two attributes to identify and manage PPDs. The attribute `url` specifies for which URL (i.e. service) the PPD is valid. The attribute `version` defines a version number of a PPD. It allows applications to differentiate between different versions and to update a PPD in a reliable manner.

We describe in Section 4.1 how to express the password requirements and in Section 4.2 the password management of a service. An exemplary PPD can be found in Listing 1.

[1] The Alexa Top 500 US list [Al15] reduced by websites with pornographic and illegal content, non-english websites, and websites that do not have or allow the creation of user accounts (e.g. banking websites).

4.1 Password Requirements

A PPD allows specifying the following password requirements (see also [Ho16]).

- *Character Sets.* The `<characterSets>` element defines a list of allowed character sets. Each set is described by a `<characterSet>` element and defines a name (e.g. numbers) and the list of characters (e.g. 0..9).
- *Properties.* The `<properties>` element defines further restrictions for the password as a whole and the character sets. It contains information about the password length and its expiration. Character set restrictions are defined by a `<characterSettings>` element. A PPD allows the definition of minimum and maximum occurrences of characters, position restrictions for characters, and choices of character sets.

4.2 Password Management

In addition to the password requirements, a `<ppd>` element contains a `<service>` element that describes the password management of a service. It provides information about the registration, login, password change, and password reset which are represented by a `<register>`, `<login>`, `<passwordChange>`, and `<passwordReset>` element, respectively. All elements contain a `<url>` element which is described in the following:

- *Location of Password Interfaces.* The `<url>` contains the location of the HTML form for the registration, login, password change, and password reset at the service's website. This information is intended to directly guide users to these password interfaces to access them manually. The information for accessing these interfaces automatically are part of the `<routines>` element (see below).

In addition, the `<login>`, `<passwordChange>`, and `<passwordReset>` elements contain a `<maxTries>` and `<routines>` element which are described in the following:

- *Retry Counter for Passwords.* The `<maxTries>` element specifies the number of attempts to enter a password. In case of the login it defines the number of possible login attempts. In case of a password change it defines how often users can enter an incorrect old password. And in case of a password reset it defines how often users can answer security questions (or enter recovery information) before an account gets completely disabled. Similar to the `<url>` element, the `<maxTries>` element is intended for an manual interaction with the service's password interfaces.
- *Password Procedures.* The `<routines>` element describes the procedure for the login, password change, and password reset at a service. A routine is a set of instructions telling applications what actions need to be performed and how the execution of these actions can be verified. For example, a login routine describes how to log in to a user account and how to verify that the login was successful. We provide more technical information about routines in the following.

Listing 1: Exemplary PPD. It provides information about the password requirements as well as routines to perform an automatic login and password change at the service.

```
<ppd url="https://www.example.com" version="1.0">
  <characterSets>
    <characterSet name="Letters">
      <characters>abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ</characters>
    </characterSet>
    <characterSet name="Numbers">
      <characters>0123456789</characters>
    </characterSet>
  </characterSets>
  <properties>
    <characterSettings>
      <characterSet name="Numbers">
        <minOccurs>1</minOccurs>
      </characterSet>
      <positionRestriction characterSet="Letters">
        <positions>1</positions>
      </positionRestriction>
    </characterSettings>
    <minLength>10</minLength>
    <maxLength>20</maxLength>
  </properties>
  <service>
    <register>
      <url>https://www.example.com/register</url>
    </register>
    <login>
      <url>http://www.example.com/login</url>
      <maxTries>3</maxTries>
      <routines>
        <htmlLoginRoutine>
          <get>
            <url>https://www.example.com/login/</url>
            <assert>
              <url><prefix>https://www.example.com/login/</prefix></url>
            </assert>
          </get>
          <form>
            <selector>#main form[action^="https://www.example.com/login/"]</selector>
            <element>
              <selector>#username</selector><value>{{username}}</value>
            </element>
            <element>
              <selector>#password</selector><value>{{password}}</value>
            </element>
            <assert>
              <select><selector>#userMenu</selector></select>
            </assert>
          </form>
        </htmlLoginRoutine>
      </routines>
    </login>
    <passwordChange>
      <routines>
        <htmlPasswordChangeRoutine login="htmlLoginRoutine">
          <get>
            <url>https://www.example.com/account/</url>
            <assert>
              <url><prefix>https://www.example.com/account/</prefix></url>
            </assert>
          </get>
          <form>
            <selector>#main form[action^="https://www.example.com/account/"]</selector>
            <element>
              <selector>#password</selector><value>{{password}}</value>
            </element>
            <element>
              <selector>#newPassword</selector><value>{{newPassword}}</value>
            </element>
            <element>
              <selector>#confirmNewPassword</selector><value>{{newPassword}}</value>
            </element>
            <assert>
              <select><selector>div.success</selector></select>
            </assert>
          </form>
        </htmlPasswordChangeRoutine>
      </routines>
    </passwordChange>
    <passwordReset>
      <url>https://www.example.com/account/recovery</url>
    </passwordReset>
  </service>
</ppd>
```

Due to the different technologies that services use for their password interfaces, we defined four different types of routines: HTTP, HTML, JavaScript, and Extended JavaScript. They are represented by the elements <*LoginRoutine>, <*PasswordChangeRoutine>, and <*PasswordResetRoutine> element where '*' indicates the technology (http, html, js, or extentedJS. For instance, <httpLoginRoutine>).

The basis for all these routines are HTTP POST and GET commands which are used to interact with the service's password interfaces and to perform a login, password change, or password reset. A POST or GET command is defined by a <post> or <get> element, respectively. Both contain an element <url> which defines the target URL of the command. Furthermore, both include an <assert> element which is used to define a list of assertions that need to be verified in order to check whether the POST or GET command was performed successfully or not. We provide more information about the assertions later. The <post> element additionally contains a list of <data> elements representing the data which is sent to the service within the POST command (e.g. the username and password within a login routine). In the following, we describe the routines in detail:

- *HTTP.* A HTTP-based routine contains a list of <post> and <get> elements. Such a routine is used in case that the password interfaces of a service can be accessed by using plain HTTP GET or POST commands.
- *HTML.* A HTML-based routine extends the HTTP routine by a <form> element. The element consists of a list of <selector> elements which define identifiers to select HTML input fields and enter values in a HTML form (cf. Listing 1). HTML-based routine must be in case that HTML forms contains hidden input field with random values such as a session identifier.
- *JavaScript.* A JavaScript-based routine provides the same functionality like HTML routines. The elements of the type js only indicate that applications need to support JavaScript in order to access the password interfaces of the service. This is necessary when services use JavaScript to manipulate the input of a HTML form before submitting it. For instance, services hash the password by JavaScript on the client-side before sending it to their servers.
- *Extended JavaScript.* This type of routine extends the HTTP routine and additionally defines a <javascript> element which contains plain JavaScript. In case that the aforementioned technologies are insufficient, developers can use this type to implement the procedure using the complete functionality of JavaScript. Applications need to browse the password interface and execute the JavaScript in order to perform the routine.

Listing 1 shows an example for a HTML-based login and password change routine. Please note that the <htmlPasswordChangeRoutine> has an attribute login which refers to the login routine. This allows to reuse existing routines and makes the creation of PPDs easier and more efficient.

It is essential that applications can verify the correct execution of a routine, e.g., verify that a login was successful. To this end, a routine contains one or more assertions that applications need to verify. PPML defines the following types of assertions:

- *Existence of a Cookie.* A certain cookie is set after performing a routine.
- *Non-existence of a Cookie.* A certain cookie is not set after performing a routine.
- *Content.* The content of the response from the service contains a particular content. For instance, the text ”the password is wrong”.
- *Location.* The response redirects to a certain URL.

The routines of PPML are a powerful tool to describe password interfaces and procedures. They are highly flexible and support the wide range of different technologies and methods of password implementations used by services. In the next Section we provide more information of putting PPDs into practice.

5 Prototype

In the previous section we explained the syntax of PPDs in detail. We now show how to employ PPDs in practice and how to enable their broad application. We developed the PPD Distribution Service (PPDDS) which makes PPDs available to applications. Applications can query the PPDDS using the service’s URL to search for a corresponding PPD. Furthermore, we developed a password manager and created PPDs for 5 services to demonstrate the feasibility of our solution. The key component of our Java-based password manager is the *Routine Engine*. It is capable of executing routines defined by a PPD and performs logins, password changes, and password resets. We use the Web Engine of JavaFX to interact with the services’ password interface, which allows us to support all types of technologies of routines.

6 Conclusion and Future Work

In this paper, we presented the Password Policy Markup Language which closes the gap between the different implementations of password-based authentication on the service-side and applications managing passwords on the user-side. PPML facilitates a fully-fledged assistance along the complete password life cycle. Furthermore, it eliminates the need for error-prone heuristics to find password forms. Our password manager shows the practicality of our solution and provides an open and easily extendable basis for further research and development. To support further services users just need to create the corresponding PPDs for the services. The development of tools that assist in a fast and convenient creation of PPDs is part of future work.

References

[Al12] AlFayyadh, Bander; Thorsheim, Per; Jsang, Audun; Klevjer, Henning: Improving Usability of Password Management with Standardized Password Policies. In: The Seventh Conference on Network and Information Systems Security. pp. 38–45, May 2012.

[Al15] Alexa Internet: , The top 500 sites on the web, 2015. http://www.alexa.com/topsites.

[ASL97] Adams, Anne; Sasse, Martina Angela; Lunt, Peter: Making Passwords Secure and Usable. In (Thimbleby, Harold W.; O'Conaill, Brid; Thomas, Peter, eds): People and Computers XII, Proceedings of HCI '97. Springer, pp. 1–19, 1997.

[BK95] Bishop, Matt; Klein, Daniel V.: Improving system security via proactive password checking. Computers & Security, 14(3):233–249, 1995.

[Bo12a] Bonneau, Joseph: The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In: IEEE Symposium on Security and Privacy, SP 2012, 21-23 May 2012, San Francisco, California, USA. IEEE Computer Society, pp. 538–552, 2012.

[Bo12b] Bonneau, Joseph; Herley, Cormac; van Oorschot, Paul C.; Stajano, Frank: The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In: IEEE Symposium on Security and Privacy, SP 2012, San Francisco, California, USA. IEEE Computer Society, pp. 553–567, 2012.

[Ca13] Castelluccia, Claude; Abdelberi, Chaabane; Dürmuth, Markus; Perito, Daniele: When Privacy meets Security: Leveraging personal information for password cracking. CoRR, abs/1304.6584, 2013.

[Ch14] Choong, Yee-Yin: A Cognitive-Behavioral Framework of User Password Management Lifecycle. In (Tryfonas, Theo; Askoxylakis, Ioannis G., eds): Human Aspects of Information Security, Privacy, and Trust - Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings. volume 8533 of Lecture Notes in Computer Science. Springer, pp. 127–137, 2014.

[Co14] Codenomicon: , The Heartbleed Bug, 2014. http://heartbleed.com.

[Da14] Daniel Humphries: , 67 Percent of Internet Users Haven't Changed Passwords After Heartbleed, 2014. http://intelligent-defense.softwareadvice.com/67-percent-havent-changed-passwords-after-heartbleed-0414/.

[Da16] Dashlane, Inc: Best Password Manager, Free Form Filler, Secure Digital Wallet. 2016. https://www.dashlane.com.

[dCdCM14] de Carné de Carnavalet, Xavier; Mannan, Mohammad: From Very Weak to Very Strong: Analyzing Password-Strength Meters. In: 21st Annual Network and Distributed System Security Symposium, NDSS 2014, San Diego, California, USA, February 23-26, 2014. The Internet Society, 2014.

[DMR10] Dell'Amico, Matteo; Michiardi, Pietro; Roudier, Yves: Password Strength: An Empirical Analysis. In: INFOCOM 2010. 29th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 15-19 March 2010, San Diego, CA, USA. IEEE, pp. 983–991, 2010.

[Eg13] Egelman, Serge; Sotirakopoulos, Andreas; Muslukhov, Ildar; Beznosov, Konstantin; Herley, Cormac: Does my password go up to eleven?: the impact of password meters on password selection. In (Mackay, Wendy E.; Brewster, Stephen A.; Bødker, Susanne, eds): 2013 ACM SIGCHI Conference on Human Factors in Computing Systems, CHI '13, Paris, France, April 27 - May 2, 2013. ACM, pp. 2379–2388, 2013.

[FH07] Florêncio, Dinei A. F.; Herley, Cormac: A large-scale study of web password habits. In (Williamson, Carey L.; Zurko, Mary Ellen; Patel-Schneider, Peter F.; Shenoy, Prashant J., eds): Proceedings of the 16th International Conference on World Wide Web, WWW 2007, Banff, Alberta, Canada, May 8-12, 2007. ACM, pp. 657–666, 2007.

[FH10] Florêncio, Dinei A. F.; Herley, Cormac: Where do security policies come from? In (Cranor, Lorrie Faith, ed.): Proceedings of the Sixth Symposium on Usable Privacy and Security, SOUPS 2010, Redmond, Washington, USA, July 14-16, 2010. volume 485 of ACM International Conference Proceeding Series. ACM, 2010.

[Fu07] Furnell, Steven: An assessment of website password practices. Computers and Security, 26(7-8):445–451, 2007.

[Fu11] Furnell, Steven: Assessing password guidance and enforcement on leading websites. Computer Fraud & Security, 2011(12):10–18, 2011.

[Ha15] Harris Interactive; Various sources (Dashlane): , Which of the following online security precautions did you take within the past 30 days?, March 2015. `http://www.statista.com/statistics/418676/us-online-security-precuations/`.

[Ho16] Horsch, Moritz; Schlipf, Mario; Braun, Johannes; Buchmann, Johannes A.: Password Requirements Markup Language. In (Liu, Joseph K.; Steinfeld, Ron, eds): Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part I. volume 9722 of Lecture Notes in Computer Science. Springer, pp. 426–439, 2016.

[Ke12] Kelley, Patrick Gage; Komanduri, Saranga; Mazurek, Michelle L.; Shay, Richard; Vidas, Timothy; Bauer, Lujo; Christin, Nicolas; Cranor, Lorrie Faith; Lopez, Julio: Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms. In: IEEE Symposium on Security and Privacy, SP 2012, 21-23 May 2012, San Francisco, California, USA. IEEE Computer Society, pp. 523–537, 2012.

[La16] LastPass Corporate: LastPass - The Last Password You Have to Remember. 2016. `https://lastpass.com`.

[Pe14] Pew Research Center: , Heartbleed's Impact, 2014. `http://www.pewinternet.org/2014/04/30/heartbleeds-impact/`.

[SB09] Shay, Richard; Bertino, Elisa: A comprehensive simulation tool for the analysis of password policies. Int. J. Inf. Sec., 8(4):275–289, 2009.

[SB14] Stobert, Elizabeth; Biddle, Robert: The Password Life Cycle: User Behaviour in Managing Passwords. In (Cranor, Lorrie Faith; Bauer, Lujo; Biddle, Robert, eds): Tenth Symposium on Usable Privacy and Security, SOUPS 2014, Menlo Park, CA, USA, July 9-11, 2014. USENIX Association, pp. 243–255, 2014.

[SBB07] Shay, Richard; Bhargav-Spantzel, Abhilasha; Bertino, Elisa: Password policy simulation and analysis. In (Goto, Atsuhiro, ed.): Proceedings of the 2007 Workshop on Digital Identity Management, Fairfax, VA, USA, November 2, 2007. ACM, pp. 1–10, 2007.

[Si14] Silver, David; Jana, Suman; Boneh, Dan; Chen, Eric Yawei; Jackson, Collin: Password Managers: Attacks and Defenses. In (Fu, Kevin; Jung, Jaeyeon, eds): Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, August 20-22, 2014. USENIX Association, pp. 449–464, 2014.

[Sq07] Squicciarini, Anna Cinzia; Bhargav-Spantzel, Abhilasha; Bertino, Elisa; Czeksis, Alexei B.: Auth-SL - A System for the Specification and Enforcement of Quality-Based Authentication Policies. In: ICICS. volume 4861 of Lecture Notes in Computer Science. Springer, pp. 386–397, 2007.

[SS16] Sparell, Peder; Simovits, Mikael: Linguistic Cracking of Passphrases Using Markov Chains. IACR Cryptology ePrint Archive, 2016:246, 2016.

[St14] Stajano, Frank; Spencer, Max; Jenkinson, Graeme; Stafford-Fraser, Quentin: Password-Manager Friendly (PMF): Semantic Annotations to Improve the Effectiveness of Password Managers. In: PASSWORDS. volume 9393 of Lecture Notes in Computer Science. Springer, pp. 61–73, 2014.

[THB15] Taneski, Viktor; Hericko, Marjan; Brumen, Bostjan: Impact of security education on password change. In: MIPRO. IEEE, pp. 1350–1355, 2015.

[Ur12] Ur, Blase; Kelley, Patrick Gage; Komanduri, Saranga; Lee, Joel; Maass, Michael; Mazurek, Michelle L.; Passaro, Timothy; Shay, Richard; Vidas, Timothy; Bauer, Lujo; Christin, Nicolas; Cranor, Lorrie Faith: How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In: Proceedings of the 21th USENIX Security Symposium, Bellevue, WA, USA. USENIX Association, pp. 65–80, 2012.

[We09] Weir, Matt; Aggarwal, Sudhir; de Medeiros, Breno; Glodek, Bill: Password Cracking Using Probabilistic Context-Free Grammars. In: IEEE Symposium on Security and Privacy. IEEE Computer Society, pp. 391–405, 2009.

[We10] Weir, Matt; Aggarwal, Sudhir; Collins, Michael P.; Stern, Henry: Testing metrics for password creation policies by attacking large sets of revealed passwords. In: Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA. ACM, pp. 162–175, 2010.

[WW15] Wang, Ding; Wang, Ping: The Emperor's New Password Creation Policies: An Evaluation of Leading Web Services and the Effect of Role in Resisting Against Online Guessing. In: Computer Security - ESORICS 2015 - 20th European Symposium on Research in Computer Security, Vienna, Austria. volume 9327 of Lecture Notes in Computer Science. Springer, pp. 456–477, 2015.

[Ya04] Yan, Jeff Jianxin; Blackwell, Alan F.; Anderson, Ross J.; Grant, Alasdair: Password Memorability and Security: Empirical Results. IEEE Security and Privacy, 2(5):25–31, 2004.

[ZH99] Zviran, Moshe; Haga, William J.: Password Security: An Empirical Study. J. of Management Information Systems, 15(4):161–186, 1999.

Open Identity Summit 2016

Further Conference Contributions

Ethical Data Handling – beyond risk and compliance.

Robin Wilton[1]

Abstract: We can all think of instances where we find that data about us has been used in a way that we find surprising, unwelcome, or even harmful. The more our lives are conducted on, or through, online services, the more potential there is for this to happen, and the greater our dependence on the behaviour of other entities over whom we may have little or no control. In that context, how can we optimise the outcomes for ourselves, as individuals, citizens and consumers?

Keywords: Ethics, Data Protection, Privacy, Personal Data, Risk, Compliance

1 Summary

Everything we do online is mediated through at least one third party, and there is usually also a power imbalance between us and the online service providers on whom we rely more and more in our digital lives. As a result, data about us (and data that affects us) is held by many third parties whose interests do not wholly coincide with our own.

In some cases, those entities have a business model predicated on the collection and monetisation of personal data – whether or not that is our primary expectation in signing up for their services. Simply withdrawing from digital life is not an option: even passively-collected data can have far-reaching impacts on our lives, and we cannot realistically avoid its collection.

It is tempting to assume that technology can fix this problem for us („is there an app for that?") - but experience should tell us that a point solution based on some technical widget will not work.

In this talk, I will suggest that the problems arising from over-collection of personal data are systemic ones, and that therefore no single point solution is likely to succeed. Rather, what is needed is a set of point solutions – the actions of multiple stakeholders, aimed at producing changes at multiple points in the system.

Key amongst these is a shift, in data controllers, from a mentality based on risk and compliance, to a culture of ethical treatment of personal data. I will look at the phases through which technical innovations usually pass, and identify the points at which systemic changes can be applied to improve the over-all outcomes for data subjects.

I will also give examples of the kinds of practical resource that the Internet Society and its partners are identifying and collecting, in order to inform and influence the relevant

[1] Internet Society, 1775 Wiehle Avenue, Suite 201, Reston, VA 20190-5108 U.S.A, wilton@isoc.org

stakeholders.

An Interdisciplinary Approach to Develop a Secure, Usable and Economically successful software

Janina Hofer[1], Rachelle Sellung[1]

Abstract: Some argue that software developers of security solutions often neglect the importance of incorporating usability and socio-economic aspects and focus more on security and privacy aspects. However, it can be observed that many solutions are not accepted by both the users and the market, even though they are technically sophisticated. This work-in-progress paper proposes an interdisciplinary approach and a prospective supportive tool that guides the developer through the process, which is referred to as the *Wizard*. It consists of selected, carefully analyzed and edited methods and standards from the fields of (a) Usability and User Experience, (b) Socio-economics, and (c) IT-Security and other disciplines. The Wizard proactively recommends various methods according to the status of the development and assists in their selection and application.

Keywords: Usable Security, Viable Security, Socio-Economic Security, Assistant Tool, Wizard

1 Introduction

A common problem observed in developing secure solutions for software often relies on focusing too much on security and privacy requirements and not enough on other disciplines. While security and privacy solutions are important, it is also essential to not neglect user and market needs. However, typically solutions that are easy to use and meet the user demands can successfully exist on the market [ZR11a] [ZR11b] [Gr04]. To our knowledge, there exists no reliable and holistic model that supports software developers in both secure and demand-actuated in and for practice [RZ10]. To close this gap, the research project CUES[2][3] develops an integrated guidance tool, the *Wizard*. The solution is not anticipated to propagate security at all costs; however, its aim is to enable a reliable security that considers user and market preference, which is then able to be integrated into existing business processes. Applying the *Wizard* during the software development process will help developers to ensure that the developed solution is not only sophisticated IT-security, but has a wide acceptance of all important stakeholders, is economically successful, and has viable user benefits and is user friendly. The overall goal of the *Wizard* is to assist developers, who are typically already experts in the IT security field, build on their foundation with assistance to integrate other disciplines in order to establish a secure but also market friendly software.

[1] Fraunhofer-Gesellschaft, Arbeits- und Organisationswissenschaften, Identitätsmanagement,
Nobelstraße 12, 70569, Stuttgart, janina.hofer@iao.fraunhofer.de; rachelle.sellung@iao.fraunhofer.de

[2] CUES: Interdisciplinary software development approach and tool. www.cues-projekt.de

[3] We thank and acknowledge the Baden-Württemberg Stiftung [Ba16] for financing the CUES project.

2 Interdisciplinary Applications and Importance

The *Wizard* is a tool that will contribute to improving the software development process. The tool will aid developers by providing helpful suggestions during the development process; such as, instating what new measures could be done in other disciplines that could improve the overall success of the product of the developer. By including more disciplines in the development process, the *Wizard* will make the whole development process better-rounded. Further this helps address a common technical bias that is found, which often leads to drawbacks or blind spots that could have been avoided had the development process inquired more disciplines [ZR11a] [ZR12] [RZ10]. For instance, the costs and benefits of security solutions estimated are not often distributed fairly, leading to a lack of incentive for users to adopt the technology. In addition, vendors or developers of security technology often fail to consider the users' willingness to pay when creating their price models, which results in overprizing and eventually a lack of market success [Gr04]. In addition, these technologies often fail to address user requirements like usability and accessibility by individuals and organizations [ZR11b]. This section will dive deeper into how adding disciplines of usability, socio-economic, and security could add great value to the development process by using the *Wizard*.

2.1 Usability and User Experience

Improving the usability and user experience of software can drastically improve the overall perception of the end product. There are many possible constraints at hand; such as, having too little time, an insufficient budget, or the lack of knowledge about existing methods and approaches. Further, these constraints could lead to the aspects that are not considered in software development, but are important in the overall outcome of success. To ensure and measure the ease of use and usability of software, there are a number of established standards that exist, for instance the ISO 9241. Further, the 9241-210 (Human-centered design for interactive systems) [In15] is relevant, which describes the approach and processes. Heuristics, checklists, and guidelines of usability experts [Ni93] [Sc92] are lightweight tools that can be integrated at various points in the development process. User Experience claims a holistic view on the human-computer interface. In this consideration, user needs play a particularly important role, among them the need for security [FP14]. The *Wizard* is responsible for informing the developers of existing usability approaches, methods and standards, to provide prepared methods in accordance with the conditions of development and to assist in their selection and application.

2.2 Socio-economic aspects

Including a socio-economic perspective in the process helps developers avoid making poor decisions that could hinder market success. It is often assumed that those technologies will bring market success, based on their technological sophistication and the elegance of their design. The resulting business models are usually poorly designed and fail to address important success factors appropriately [ZR11b]. Some methods or theories that could be suggested in the development process would be; Stakeholder Theory [Fr84], Diffusion of Innovations [Ro03], Transaction Costs Economics [Wi81], or Willingness to Pay models [Ro14]. For instance, a common happenstance in the IT-security field is to rely on general assumptions on human behavior to guide the direction of development and to design the end product. This is the case, if a developer designs according to a general assumption of what he/she perceives stakeholders would want instead of what they actually want. A suggestion to hold a Stakeholder analysis in the earlier stages of development would assist the developer in creating a product tailored to this analysis of what is desired from the final product, rather than just by assumption. Further, it would be beneficial to suggest developers to consider an evaluation of the final product to reconsider important parts and if they truly met the goals set. Including the socio-economic discipline is necessary to help developers become aware of the importance of recognizing the needs of the market and the end user.

2.3 IT-Security aspects

While there is an ample amount of literature on the security and privacy aspects of secure solutions for software, this paper's scope relies on other important disciplines needed for the success of software. Further, the purpose of including a stronger security disciplinary influence in the development process is to better analyze security problems that often arise or get over looked [ZR11a] [Zr11b]. However, the *Wizard* serves as a tool to assist developers whom are already expected to be experts in the IT-Security field. Their own knowledge base serves as a foundation of the IT-Security perspective. The goal is for the *Wizard* to help developers decide during the process, how to incorporate other disciplines but to remain at an acceptable security standard. Further, it is to help developers to compromise between having a very secure and privacy friendly tool and to still being user friendly and market ready.

3 Real world application

The *Wizard* can be applied in a variety of areas. Within the project, CUES, the *Wizard* is applied on a pilot basis in two selected application scenarios. These scenarios are in the areas of Smart Home and Industry 4.0. Both domains are characterized by an extremely complex structure and communication of different devices and applications and are therefore very suitable for pilot applications. For each pilot application, industry experts are consulted in order to formulate valid requirements, define a realistic application scenario according to the need within this area and to evaluate the result against meaningful measurements. For each domain, the pilot application will be conducted based on two focus groups [Zi97] [KC15], each of which consists of software developers. Both groups will be asked to develop the same security solution, one group along the traditional software development process whereas the other group develops the application based on the *Wizard's* suggestions. Following, the resulting product of each group will be evaluated both argumentatively and empirically. Further, there will be a comparison between the two resulting artefacts. Choosing this in the real world embedded evaluation approach, both the *Wizard* itself, as well as, the developed products can be evaluated by means of an improved usability, effective improvement of the security mechanism, and market success. Moreover, this form of analysis allows for making general and cross-industry statements regarding the effective benefit of the *Wizard*.

4 Approach

Many relevant pieces of knowledge from the fields of IT-Security, Socio-economics, and Usability (including: UX, User Experience Design, and UID, User Interface Design) will be collected in a *toolbox* and analyzed to determine their relevance for software development. To be more concrete, the overall collection of various models, practice approaches, patterns, methods for analyses, implementation and evaluation, as well as, guidelines and checklists will be integrated in an interdisciplinary manner. However, simply providing a potpourri of well researched knowledge would probably not lead to developing better software regarding its security, usability, and market acceptance. In order to help better apply and implement the collected methods properly, they will be further developed, graphically edited, and integrated into a process-accompanying *Wizard*. One of the *Wizard's* many purposes is to be a guide that supports the developer during the various phases of software development. Utilizing a collection of interdisciplinary knowledge-based approaches, allows the *Wizard* to provide context-based recommendations regarding different tools and methods that offers assistance in the developer's selection and application. This allows for context-based recommendations for various methods and tools according to what development phase the developer is in. As a basis for this structure, the general conditions of the development process need to be established; such as, the budget, number of developers, and the time frame.

5 Mutual benefit

By combining Usability, Socio-economic and IT-Security aspects, the *Wizard* assists developers in implementing successful security solutions. As the *Wizard* will be integrated into the actual applied development process, the developer will not be inconvenienced, but will rather benefit from assets of this supportive tool. On the one hand, it raises awareness towards topics that go beyond software development itself and on the other hand it leads to an optimized product. Referring to the other end of the software development chain, we will find the client, who buys and eventually sells the product to their customers. In our scenario, they represent the end-users of the software that is developed. Depending on the type of order, the client and the end-user are the same person. Although the user has no direct or deeper insight of the actual process of development of the product they use (at least they shouldn't) it indirectly affects them. Both the client and the end-user will most likely recognize the difference in the final product when the software developer had a wider scope in mind while implementing the software, which positively affects both the marketing of the product and the satisfaction during usage. If a developer implements software with the assistance of the *Wizard*, it will both support them in their individual tasks and ultimately create added value for the client and their users. The Figure 1 below gives a visual representation of the mutual benefits gained while utilizing the *Wizard*.

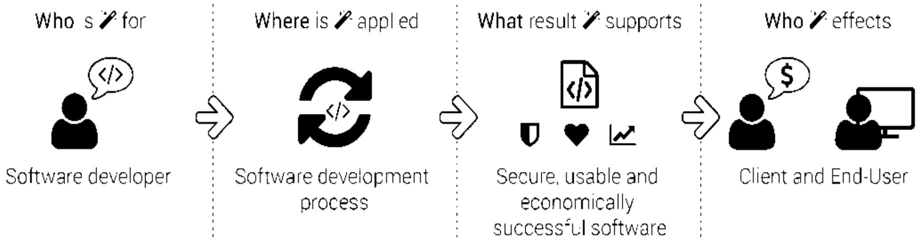


Fig. 1: Mutual Benefits from the *Wizard*

6 Conclusion

Developing secure and usable software that is accepted by various stakeholders and is economically successful is a challenge. Addressing this challenge, the proposed interdisciplinary approach and the *Wizard* tool supports software developers in taking usability and socio-economic aspects into account during the development process. The *Wizard* will guide developers through the process and assists in selection and application of various IT-Security, Usability and socio-economic methods. Following this approach, secure, usable, and economically successful software can be developed. This work-in-progress paper highlights the strengths, goals, and drive of the results that are to be achieved in the CUES project by the end of 2017.

7 References

[Ba16] Baden-Württemberg Stiftung, [Online]. Available: http://www.bwstiftung.de/.

[FP14] N. Fronemann und M. Peissner, „User experience concept exploration: user needs as a source for innovation," pp. 727-736, 2014.

[Fr84] R. E. Freeman, Strategic Management: A Stakeholder Approach, Cambridge: Ballinger Publishing Co, 1984.

[Gr04] S. J. Greenwald, K. G. Olthoff, V. Raskin und W. Ruch, „The user non-acceptance paradigm: INFOSEC's dirty little secret," Proceedings of the 2004 workshop on New secuirty paradigms, pp. 35-42, 2004.

[In15] International Organization for Standardization, 2015. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:52075:en. [Zugriff am 14 04 2016].

[KC15] R. A. Krueger und M. A. Casey, Focus Groups: A Practical Guide for Applied Research (5th edition), Thousand Oaks: Sage Publications, Inc. , 2015.

[Ni93] J. Nielsen, Usability Engineering, Boston: Academic Press, 1993.

[Ni97] J. Nielsen, „The use and misuse of focus groups," in IEEE Software, 1997

[Ro03] E. M. Rogers, Diffusion of Innovations, 5th edition Hrsg., New York: Free Press, 2003.

[RZ10] H. Roßnagel und J. Zibuschka, „Tragfähige IT-Sicherheitslösungen," igma. Zeitschrift für Datenrecht und Informationssicherheit, Bd. 10, Nr. 2, pp. 68-72, 2010.

[Ro14] H. Roßnagel, J. Zibuschka, O. Hinz und J. Muntermann, „Users' Willingness to Pay for Web Identity Management Systems," European Journal of Information Systems, Bd. 23, pp. 36-50, 2014.

[Sc92] B. Schneidermann, Designing the User Interface - Strategies for Effective Human-Computer, Addison-Wesley Publishing Company, 1992.

[Wi81] O. E. Williamson, „The Economics of Organization: The Transaction Cost Approach," The American Journal of Sociology, Bd. 3, Nr. 87, pp. 548-577, 11 1981.

[ZR11a] J. Zibuschka und H. Roßnagel, „A Structured Approach to the Design of Viable Security Systems, Proceedings of the Information Security Solutions Europe (ISSE)," Proceedings of the Information Security Solutions Europe (ISSE), 2011.

[ZR11b] J. Zibuschka und H. Roßnagel, A framework for Designing Viable Security Solutions, Shanghai, 2011.

[ZR12] J. Zibuschka und H. Roßnagel, „On Some Conjectures in IT Security: The Case for Viable Security Solutions.," Sicherheit 2012: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 6. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft, pp. 25-33, 7-9 März 2012.

Challenging eID & eIDAS at University Management

Hermann Strack[1] and Sandro Wefel[2]

Abstract: Based on national eID solutions for university scenarios, in this paper eIDAS extensions will be discussed, with benefits and Challenges (from eID to eIDAS)

Keywords: eID, eIDAS, electronic signature, legally binding, university management

1 Introduction

The use of security functions like qualified signatures and the eID of the German national identity card (eID/nPA or GeID/PA [Be08]) offered new possibilities for the electronization of processes with legally binding in university management. We report about some of these innovations within the projects "eCampus/Scampii" resp. "eID at universities", based on national signature and eID frameworks in Germany. At this background we will outline some proposals for eIDAS [In15] based extensions for secured university management.

2 eID and signatures for University Management (D)

The eID online function of the national identity card in Germany offers a strong two factor and doubled end-to-end authentication between the identity card at the card reader and the eID server/service, with privacy enhancements (non traceable by eavesdroppers; eID data flow from the card to the eID service requires a pin authentication; the amount of eID data within the request from eID service will be mandatory filtered by the card item field profile, which is defined within the eID service certificate specific for the eID application provider; this eID certificate will be authorized by a federal administration office - the so called Bundesverwaltungsamt BVA - accordingly to privacy concerns of the eID application and application users). Furthermore, there will be offered additional optional functionality, organizational framework and legally bindings for special security contexts:

a) eID-Forms-Sign: In the case, that the eID application provider will be a public administration office, the eID based access to the application web site of the provider

[1] Hochschule Harz, Fachbereich Automatisierung und Informatik / netlab, Friedrichstr. 57-59, D-38855 Wernigerode, hstrack@hs-harz.de

[2] Martin-Luther-Universität Halle-Wittenberg, Institut für Informatik, Von-Seckendorff-Platz 1, D-06120 Halle (Saale), sandro.wefel@informatik.uni-halle.de

and the filling of contents to the application web forms of this office by the eID card owner allows an analogous legally binding of the contents like in the paper world case, with handwritten signature.

b) Defined by law, the user has the duty to apply for a German eID card at age of sixteen or if his former ID card would get invalid, by default the eID online function will be activated (the cancellation by user is on own choice). The eID card and user data management will be performed by special public administration offices, only.

c) eID-Card-Sign: optionally, the user could request at a qualified CA the activation of a qualified signature certificate (public key pair) on his eID card, usable for qualified signatures with fully legally binding.

At university management level there will be some principal benefits in case of using the eID for electronic processes:

A) A **strong eID based two factor authentication** for university electronic services / processes, without formerly physical presence of the user at the university

B) eID-Forms-Sign: fully legally bindings for **eID based electronic forms fillings**

C) **Mobile eID extensions**: mobile devices with NFC extended length interface could be used for eID/PA authentication directly (without an reader device), the SkiDentity platform [Hu15] offers to use security smart cards as a trust anchor (e.g. PA).

2.1 Intra domain eID applications

eID based applications within an university domain context will be presented at this section: eTestate, MyCredentials, eForms, eDiploma, eAccess.

eTestate: this was the first eID based application at Hs Harz to enable eID based registration application & login for lab exercises for students in a fully electronically manner with strong two factor eID authentication & qualified signatures, based on the eCampus architecture, see [SB13, St13, Pu12, St15] and Fig. 1.

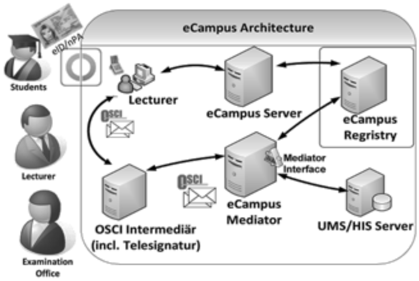
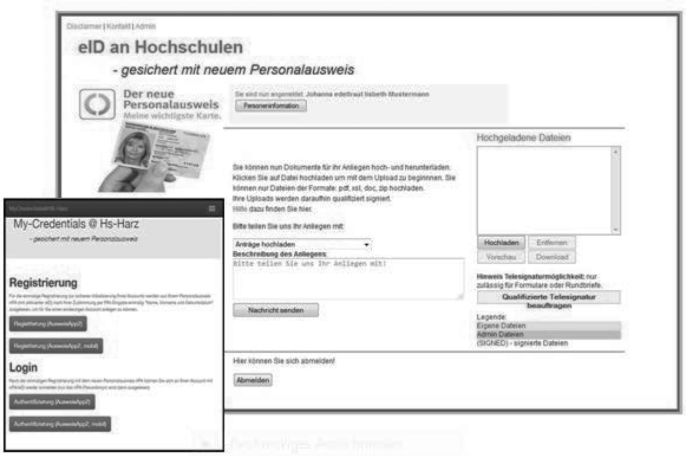


Fig. 1: The eCampus security shell architecture, integrating GeID, OSCI, QES standards

My-Credential: in case of loss of university credentials (like passwords or PKI certificates), the current policy at universities often requires the physical presence & authentication of the credential owner at the computer center of the university to apply for new credentials. By using the eID function of the German ID Card, we enabled now a remotely usable new eID based platform solution "myCredentials" to apply for new credentials by customers, which are pre-registered by eID at the platform (Fig. 2). The applied new credentials will be uploaded by the administrator in an encrypted manner to the web site of the customer (e.g. via AES based ZIP archive encryption), a decryption enabling PIN will be transferred over a separate channel, e.g. via SMS to the smartphone of the customer. Therefore, a strong protection for a confidential credential exchange (e.g. passwords, secret keys) will be established. In the future, this scheme could be extended also to exchange other confidential documents in an effectively managed and analogously end-to-end secured manner by eID (using pre-encrypted key and document exchanges by eID), usable for multiple parties/customers (pre-registered by eID at the platform), without the need for additional PKI schemes/keys, This could be an interesting add-on feature for so called "interoperable Bürgerkonten" (interoperable public administration accounts for citizens), which are planned in Germany [BMI15, Ma16, Me16, BIT16].


Disclaimer | Kontakt | Admin
Der neue Personalausweis
Meine wichtigste Karte.
Personeninformation
Hochgeladene Dateien
Hochladen
Entfernen
Vorschau
Download
Qualifizierte Telesignatur beauftragen
Nachricht senden
Abmelden
Registrierung (AusweisApp2)
Registrierung (AusweisApp2, mobil)
Authentifizierung (AusweisApp2)
Authentifizierung (AusweisApp2, mobil)

eID an Hochschulen

- gesichert mit neuem Personalausweis

Sie sind nun angemeldet: Johanna edeltraut lisbeth Mustermann

Sie können nun Dokumente für Ihr Anliegen hoch- und herunterladen. Klicken Sie auf Datei hochladen um mit dem Upload zu beginnen. Sie können nur Dateien der Formate: pdf, xsl, doc, zip hochladen. Ihre Uploads werden daraufhin qualifiziert signiert. Hilfe dazu finden Sie hier.

Bitte teilen Sie uns Ihr Anliegen mit:

Anträge hochladen

Beschreibung des Anliegens:

Bitte teilen Sie uns Ihr Anliegen mit!

Hinweis Telesignaturmöglichkeit: nur zulässig für Formulare oder Rundbriefe.

Legende:
Eigene Dateien
Admin Dateien
(SIGNED) - signierte Dateien

Hier können Sie sich abmelden!

My-Credentials @ Hs-Harz

- gesichert mit neuem Personalausweis

Registrierung

[illegible]

Login

[illegible]

Fig. 2: My-Credentials- & eForms-Platform - Security via eID/PA-Access/Upload

eForms: eID based Registration and Login by a eID extended web site will be offered to visitors or partners of the university, additionally an upload feature with combined remote qualified signing of the uploaded contents is available (as tele signature), with legally binding. This platform could also be used for application and matriculation of student applicants. If electronic certificates for higher education entry qualifications (qualified signed by schools) are allowed by law, then the whole process of matriculation could be implemented electronically.

eDiploma: As a variation of the visitor web site with eID the eDiploma application will be configured. By using his eID, the graduated student could download here his (by university) qualified signed electronic diploma certificate (as an electronic copy to the paper based certificate). Additionally, the graduated student will have by access control rights the ability to delegate temporary read access rights to other parties (e.g. to a potential employer, to whom the graduated student made an application). To improve privacy and traceability of the diploma certificate data, the owner could produce a self-signed temporary watermark overlay - with specifically produced watermark [Di00] for the granted accessor of the original diploma certificate data, signed by the university.

eAccess: WLAN and other network based services requires reliable authentication mechanism. Furthermore, authorization and accounting mechanism are needed in multi user environments with varied type of users, e.g. for university management. Therefore AAA[3] systems like RADIUS[4] are used.

To combine the advantage of reliable and strong eID authentication and fast certificate based challenge-response mechanism we use the eID function for the first authentication. A secret token is generated during the authentication process and stored on the device of the authenticated user, e.g. the laptop or smartphone. The token allows the challenge-response authentication for a limited time. After expiration a reauthentication process with eID is required. As an example of the practical application we use the authentication for WLAN access. eID authentication allows foreign users the self-registration process to get a WLAN account and an user specific token which can be used for future authentication. Additionally, in future the level of eID based authentication could be differentiated and marked by remotely signed eID specific attributes (e.g. SAML), which were added within the authentication process.

2.2 Cross domain eID applications

The federal administration office assigns eID certificate to access the information of identity cards in the domain of the specific eID application provider. An eID certificate assigned to one university offers access for more than one application but limited to the domain of the certificate owner. The limit prohibits a cross domain usage between universities. But access from domains of other universities are required for joint eID based services. An example for cross domain authentication and authorization service is eduroam (education roaming). Eduroam offers secure network access, especially to WLAN, for matriculated student ore researchers of foreign European universities and colleges when visiting an institution other than their own [Ed16]. The authentication process is delegated by the RADIUS protocol to the home institution of the user, which needs to be a part of the inherent domain hierarchy. As authentication factor a username

[3] AAA: Authentication, Authorization, Accounting

[4] RADIUS: Remote Authentication Dial-In User Service

password combination is used. To allow the authentication with eID cards we need cross domain access to the eID function.

To overcome the problem of the domain limitation, we use eID delegation with an eID proxy system analogous to the eduroam authentication. Fig. 3 shows the system and the eID extended communications (projects "eCampus/Scampii"[5] and "eID at Universities").

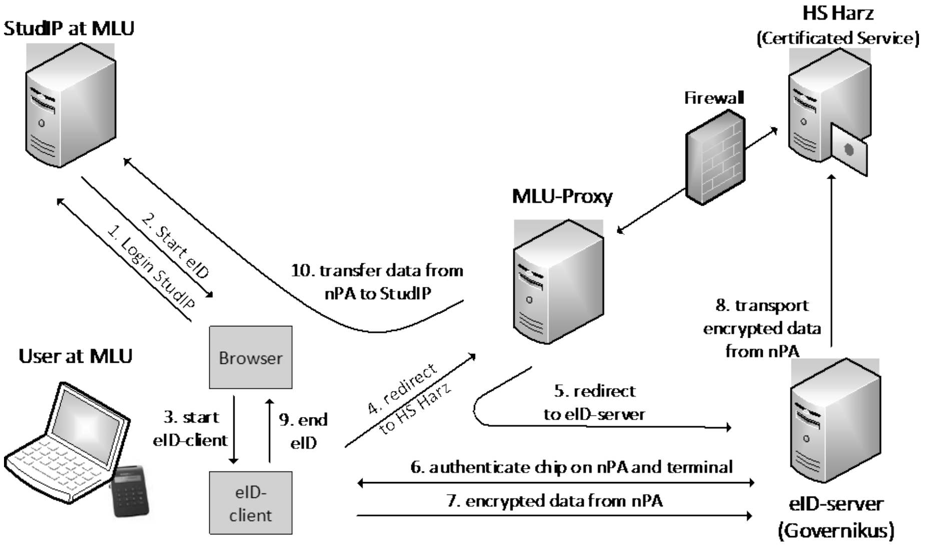


Fig. 3: eID proxy system for cross domain university access

3 University Services & eIDAS - Challenges & Benefits

The new eID solutions based on the nation German ID Card would enable strong two factor authentications (at level "high") with legally bindings for German users and also for such foreign users, which are originated from countries outside the European Union. Now, to cover also the users from the other EU member states an eIDAS based eID extension of national eID services at the same security & trust level would be obligatorily needed [Me16]. New EU Project proposals (CEF Telecom Program[6]were made for such architectures and solutions, based on former EU projects [Le15]. There is no such duty for integration of other eID solutions of EU member states at lower levels. An eID based extension of local eduroam authentications in a member state with an eID

[5] Supported by European Fund for Regional Development ERDF (EFRE FKZ: 11.03-08-03)

[6] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom

(SAML) attribute could be considered to close this gap for university authentications, more trustworthy. Furthermore, a standard solution would be needed for handling the eID authentication data from other EU member state for university processes.

An extension of the national solution with legally binding for eID based form fillings e.g. for matriculation would require to integrate eIDAS solutions from other EU member states, which are accredited for strong personal authentication (level "high"). For electronic university documents with legally bindings, a decision would be needed, if qualified eIDAS signatures or seals are adequate, or both of them. E.g. at paper level, nowadays, diploma certificates are signed manually by two professoral roles of the faculty. A problem could occur, if the eID solution of the other member state would not meet the level "high". In this case, as an alternative, an upload solution for qualified signed documents could be offered.

4 Summary

Electronic eID solutions for Universities based on eIDAS could improve and standardize aspects of the electronic processing at universities in a dramatically way (incl. privacy and legally bindings), especially at the Bologna Process background. In Germany, a special need for changes of administrative regulations or laws at university level could occur. For electronic university documents/forms with legally bindings, future decisions are required, if qualified eIDAS signature or seals are needed, or both of them. The integration of different eID trust levels could generate a problem at some university processes, because of document/forms with legally bindings - therefore, alternative solutions could use qualified signatures/seals The use of eIDAS eID, signatures or seals would require long term storage solutions embedded in an electronic document management environment, accordingly. Different trust levels at eIDAS eID based access solutions may require signed eID (SAML) attributes.

References

[Be08] Bender J.; Kügler D.; Margraf M.; Naumann I.: Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. DUD, 3/2008.

[SB12] Strack H.; Brehm N.; et al.: eCampus – Services & Infrastrukturen für elektronische Campusverwaltung mit verbesserter Sicherheit auf Basis von eGov.-Standards/ Komponenten. eGovernment Review, 2012.

[St13] Strack H.; et.al.: Hochschule Harz - eID-Anwendungskonzept (eTestate"). BMI E-Government-Inititative eID/PA (BMI ed.), http://www.personalausweisportal.de, 2013.

[Pu12] European Commission (ed.): Public Services Online, Centric eGovernment performance in Europe – eGovernment Benchmark 2012. Hs Harz, pp. 47, 2012.

[SH12] Strack H..: Authentication and security integration for eCampus services at the University of Applied Sciences Harz using the German Electronic Identity Card/eID and eGovernment Standards. Open Identity Summit, Kloster Banz 2013, GI Lecture Notes in

Informatics (LNI), 2013.

[BMI15] Bundesministerium des Inneren (BMI): Studie zu interoperablen Identitätsmanagement für Bürgerkonten. http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/Steuerungsprojekte/eID/Studie_Identitaetsmanagement_BK.pdf?__blob=publicationFile&v=2, Berlin, 2015.

[Hu15] Hühnlein D.: SkIDentity macht den Personalausweis mobil - Vertrauenswürdige Identitäten nun auch für mobile Endgeräte (2015). https://www.skidentity.de

[Le15] Leitold H., Lioy A., Ribeiro C.: Stork 2.0: Breaking New Grounds on EID and Mandates. https://www.eid-stork2.eu, 2015.

[St15] Strack H.: eID/nPA und E-Government-Standards für das elektronische Hochschulmanagement. BSI-CAST-Workshop"Die elektronische Identität des Personalausweises", , FHG-SIT, Darmstadt, 23.9.2015.

[Ro16] Roßnagel, A.: Vertrauensdienste-Gesetz. CAST-Forum, FHG-SIT, Darmstadt, 28.1.2016

[Ma16] Maas, S.: (BMWI): Stand der Anpassung des nationalen Rechts an die eIDAS-Verordnung, BMWi-Workshop "elektronisches Siegel", Berlin, 7.3.2016.

[Me16] Meister, G.: (G&D): BMWi-Workshop 'elektronisches Siegel'". Berlin, 7.3.2016.

[In15] EU: eIDAS – Interoperability Architecture. https://joinup.ec.europa.eu/sites/default/files/eidas_interoperability_architecture_v1.00.pdf, 6.11.2015.

[BIT16] BMI-IT4 (ed.): Die grenzüberschreitende gegenseitige Anerkennung elektronischer Identifizierungsmittel im E-Government nach Umsetzung der eIDAS-Verordnung - Umsetzungsbedarf und Auswirkungen für elektronische Verfahren der deutschen Verwaltung. Berlin, 25.4.2016.

[Ed16] eduroam Governance and Infrastructure. https://www.eduroam.org, 1.8.2016.

[Di00] Dittmann, J.: Digitale Wasserzeichen. Springer-Verlag, Berlin, 2000.

What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation

Niko Tsakalakis,[1] Sophie Stalla-Bourdillon[2] and Kieron O'Hara[3]

Abstract:

Pseudonymisation is gaining traction among modern electronic identification systems as a privacy enhancing technique that can significantly reduce risks of personal data misuse. The recently agreed General Data Protection Regulation (the GDPR) encourages the use of pseudonymisation to comply with its requirement of privacy-by-design. Art. 5 of the European Regulation on electronic identification and trust services (eIDAS) on data processing and protection simply allows the use of pseudonyms in electronic transactions although the facilitation of the implementation of the principle of privacy by design is clearly among the aims listed by Art. 12 of eIDAS. This paper examines the concept of pseudonymisation under eIDAS and the GDPR and suggests that the two Regulations employ two very different, if not incompatible, notions of pseudonymisation. It concludes that a common terminology and approach would be preferable in order to ensure consistency and legal certainty.

Keywords: eIDAS, GDPR, pseudonymisation, e-ID, electronic identity, eIDM

1 Introduction

This paper focuses on pseudonymisation, a concept that was only recently formally introduced in the EU policy landscape. In particular it attempts to derive the effects of the introduction of pseudonyms (or pseudonymous credentials) as part of the Regulation on electronic identification and trust services (eIDAS). It examines how eIDAS conceives pseudonymisation and explains how this interpretation would translate in practical uses in the context of a pan-European interoperability framework. It then assesses this approach in the light of the newly adopted data protection rules, i.e. the final version of the General Data Protection Regulation (the GDPR). The GDPR, as adopted on the 27th of April 2016, introduces a new category of data, between personal and data that has undergone anonymisation, that allows flexible processing of the data beyond the initial collection purposes. Finally it concludes with some useful insights about the intersection of the two Regulations and possible inconsistencies. The paper is organised as follows: Sect. 2 offers an overview of eIDAS Regulation and its requirements in sect. 2.1. Sect. 2.2 examines how eIDAS conceives pseudonymisation and a parallel is drawn with the definition and approach of the GDPR in sect. 3. Sect. 3 combines both eIDAS and the GDPR to assess their compatibility.

[1] http://orcid.org/0000-0003-2654-0825, University of Southampton, Web Science Doctoral Training Centre, Building 32, Highfield Campus, Southampton SO17 1BJ, UK, N.Tsakalakis@southampton.ac.uk

[2] University of Southampton, Institute for Law and the Web, Faculty of Business and Law, Highfield Campus, Southampton SO17 1BJ, UK, S.Stalla-Bourdillon@soton.ac.uk

[3] University of Southampton, Web and Internet Science Group, Electronics and Computer Science, Highfield Campus, Southampton SO17 1BJ, UK, kmo@ecs.soton.ac.uk

Finally sect. 4 offers arguments for the need to redress how pseudonymisation is currently defined essentially in the GDPR and how privacy by design is promoted in eIDAS.

2 eIDAS Regulation

In 2012 the Commission decided that a revision to the eSignatures Directive[4] was necessary. The proposed draft was adopted by the Parliament and the Council in 2014.[5] eIDAS' aim is to create a uniform legal framework under which the various national electronic identification schemes and trust services will be able to interoperate in cross-border transactions. In line with most recent policy initiatives, eIDAS follows a technology-agnostic approach in regulating the interoperability framework. The Regulation sets out the goals of the policy but does not define any system specifications. According to eIDAS member states that wish to operate cross-border authentication should notify their national eID Management systems (eIDM) to a designated body. Voluntary notification applications are accepted since September 2015 and by 2018 all member states are required to start accepting identifications from notified schemes.[6]

2.1 eIDAS minimum requirements

As already mentioned, the Regulation and implementing acts try to keep requirements to a minimum.[7] eIDAS defines three Levels of Assurance that define a risk based identification, requiring higher levels of identification certainty depending on the importance of the transaction about to be performed. The levels are named 'Low', 'Substantial' and 'High' and their requirements are defined through an implementing act.[8] A specific mention is made to data protection, as all components of the framework are required to fully comply with the Data Protection Directive (DPD),[9] which was in effect when the Regulation was published.[10] All services also need to be built around 'Privacy-by-design' principles.[11] Though not legally binding, the recitals advise that services follow the data minimisation principle and request and process only data strictly necessary for each transaction.[12] The goal of the framework is identification 'uniquely representing' a natural or legal person.[13]

[4] Council Directive 1999/93/EC [1999] OJ L013/0012

[5] Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73

[6] eIDAS n 5 arts 6, 7 and 9

[7] Specific technologies are acceptable only when absolutely essential for the security of the system or the users. Note that the first drafts of the Regulation were even stricter, prohibiting member states to operate any scheme that would require extra hardware or software to be implemented by other member states. This wording was toned down in the final text after objections: *See* [CS14]. However, the implementing acts point towards specific implementations, creating therefore de facto standards.

[8] Commission Implementing Regulation (EU) 2015/1502 [2015] OJ L235/7 ANNEX 2 pp 7-20

[9] Directive 95/46/EC [1995] OJ L281/0031

[10] eIDAS n 5 art 12(3d)

[11] eIDAS n 5 art 12(3c)

[12] eIDAS n 5 recital 11

[13] eIDAS n 5 art 3(1)

Implementating Regulation 2015/1501 clarifies this further by providing a minimum dataset (MDS) that should be transmitted at every identification.[14] The MDS defines four compulsory and four optional identifiers that need to be included (table 1). Note that the presence of a unique identifier is mandatory. The format of the identifier is up to the Member States, but it should be as persistent in time as possible. This decision of the regulating committee, that points to centralised architectures with unique links to users, which have lately been substituted with more privacy-preserving methods, was questioned for designing a framework that offers less privacy than what is currently technically possible [MG13].

	mandatory	optional
attributes	current family name(s)	first and family name(s) at birth
	current first name(s)	place of birth
	date of birth	current address
	unique identifier	gender

Tab. 1: Minimum dataset for a natural person

2.2 Pseudonyms under eIDAS

Art. 5(2) of eIDAS allows the use of pseudonyms for electronic transactions including electronic identification:

> Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited

Pseudonyms are artificial identifiers constructed to replace some information in a dataset in order to make attribution of a record to a person harder. Pseudonyms are not included in the definitions of eIDAS and the only other mentions in the Regulation are in relation to qualified certificates. At first instance inclusion of pseudonyms in art 5(2) could appear like an attempt to encourage the use of privacy-enhancing technologies in national eID systems (eIDM). Pseudonyms offer better privacy protection [PH10, Br14, Ve15] and have been used by national eIDM already to enhance user privacy. In Austria, eIDs use a Unique Identifier (UID) that derives from the Central Residents Register. The architecture resembles in some respects Estonia's, which also uses central Resident Numbers. In contrast to Estonia though, where Residents Numbers are publicly available information, in Austria it is prohibited by law to share this number with the services.[15] Instead the system employs Sector-specific PINs (ssPin) – pseudonyms constructed partly from citizen number and partly from the services requiring them [Rö08]. This way every department receives different credentials for the same user and the eID is cross-sector unlinkable which does not allow to trace the transactions of a user across the system, i.e. the eIDM does not allow the tracing of

[14] Commission Implementing Regulation (EU) 2015/1501 [2015] OJ L235/1 ANNEX 1 pp 1-6

[15] Art. 6, Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz-E-GovG) [2008] BGBl. I Nr. 7/2008, in combination with Bundesgesetz über das polizeiliche Meldewesen (Meldegesetz 1991 – MeldeG) [1992] BGBl. Nr. 9/1992

a user's transactions across services. Pseudonyms are employed by the German nPA as well. The German system revolves around the eID card, the nPA, since there is no Identity Provider present. Instead the user is in charge of their eID and where it will be disclosed. Pseudonymisation is built directly into the system: every time a nPA is used to a service a specific pseudonym is created that is unique to this particular use [Po12]. Pseudonymisation as a requirement is actually found in various pieces of German legislation.[16]

It seems, thus, that inclusion of pseudonyms by eIDAS would afford similar data protection of the personal data exchanged as in the national systems mentioned above. This expectation might seem reasonable also by the fact that pseudonyms are mentioned immediately after the requirement in art 5(1) for all services to comply with the DPD. At the time of publication of eIDAS the DPD was still the prevalent data protection instrument. Although the DPD did not specifically acknowledge the usefulness of pseudonyms in data protection, the GDPR that will soon replace it does.

3 Combining eIDAS and the GDPR

Recently the Council, Commission and Parliament agreed on the final text of the GDPR.[17] The GDPR is set to replace the existing DPD on 25th of May 2018. As this is a Regulation, it will have direct effect within all Member States.

The GDPR includes for the first time a definition for pseudonymisation: Art 4(5) defines 'pseudonymisation' as *"the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information"*. These additional sources need to be kept separately by the data controller, who should have taken all appropriate technical and organisational measures to ensure non-attribution.[18] Pseudonymised data are not exempt from the GDPR. Although recital 28 accepts that pseudonymisation can reduce risks of personal data breaches, according to recital 26 pseudonymised data should still be considered to include information relating to identifiable natural persons.[19]

Unfortunately the GDPR's definition of pseudonymisation seems to be too strict to be practically attainable. And, even though 'pseudonymisation' is expressly defined, not once a reference to what a pseudonym is given. An illustrative example of the difficulty to meet the GDPR's definition of pseudonymisation is to be found in eIDAS Minimum Data Set.

[16] For example, *see* the 'telemedia act' that mandates users use and pay for services pseudonymously: Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179). *See* also the Constitutional Court decision that bans the use of any UID in Germany: Volkszählung Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983, BVerfGE 65, 1, 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden [in German].

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

[18] Another innovation of the GDPR is the introduction of privacy-by-design and data-protection-by-design as the appropriate minimum technical requirements to ensure data protection: n 17 art 25

[19] The GDPR proposes a risk-based analysis to mitigate risk of re-identification, so that data controllers judge how 'reasonably likely' it is for attempts to use indirect identifiers to re-identify the dataset to come into fruition, but it has been criticised as too subjective [Es16].

As aforementioned, in order for any dataset to be considered pseudonymised by the GDPR any attribution of information to identifiable persons should be excluded. This is perhaps possible in systems that allow for selective disclosure. Selective disclosure allows the system to transmit only those attributes of the eID that are absolutely necessary for the needs of each service [PH10], i.e. if a service needs only to know if a user is a citizen or not, the system can reply with only a pseudonym for the particular user and a Yes/No answer to their citizen status. This is a function that can be observed in modern privacy-preserving systems, such as in the German nPA [Fe11]. The nPA could potentially transmit completely pseudonymous datasets (by the GDPR's definition) when, apart from the pseudonym, no other information could potentially identify a person. For example, if a service only requires a user to be over a certain age, the system will send only a pseudonym for this use (see sect. 2.2) and a calculation of the user's age based on their date of birth. [20] In this case the chance of re-identifying the person based on indirect identifiers is minimal – and therefore the test of 'reasonably likely' of the GDPR can be satisfied while the data are in transit.[21] On the other hand, in a dataset where the pseudonym is accompanied by a date of birth, address and gender the possibility of re-identification is significantly higher.[22]

Evidently the MDS would fail this test: As required by Implementing Regulation 2015/1501, it is mandatory for the MDS to *always* include all of the identifiers needed to uniquely single out a person. And even though the Regulation introduces the possibility of pseudonyms, no other mention of them exists in either the rest of the main text or the implementing acts. It seems, therefore, that pseudonyms were never conceived as a privacy-enhancing tool,[23] meaning that the interoperability framework will likely offer less privacy protection than the individual national systems are capable of.

Omission of pseudonyms as privacy-preserving features begs the question why the definition was included in eIDAS in the first place. A practical application of pseudonyms under the current regime can be seen when considering eIDAS' requirement for a UID. The framework needed to be able to accommodate all available national architectures. Detailing the differences in eIDM architecture is beyond the scope of this paper, but implementation varies from systems with central governmental databases that use the Central Residents Register number as a UID, like Estonia's [Ma10], to systems employing a varying UID like Austria [Rö08] and systems designed specifically to disallow the existence of such UID, like Germany's nPA [Po12] and UK's Verify [BD11].

As a result, requiring a mandatory UID at the national level would have prohibited some member states from notifying their schemes. It seems that the use of a pseudonym can rectify this issue. This has already been the accepted solution in the design of the nPA

[20] The German system is capable of performing calculations based on the date of birth. Every identifier of an eID resides inside the eID card of the user and the system reads and transmits only the necessary information for each use [Po12].

[21] The GDPR employs a risk-based approach to data protection (n 19 above). Organisations are encouraged to implement organisational and technical measures suitable for the activities they engage in, following a risk assessment. See n 17 arts. 30-34 and rec. 26.

[22] According to [Sw00] these three indirect identifiers are enough to identify 87% of the American population.

[23] See, for example, [ZS13] where the authors explain how pseudonyms and selective disclosure can enhance system privacy.

interoperability functionality [BS15] and it has been proposed as a necessary architectural amendment of UK's Verify [Ts16]. Such a view seems compatible with art 87 of the GDPR that implicitly states that member states are free to determine any identifier in place of a national identification number.[24]

4 Conclusion

According to the above it seems that eIDAS and the GDPR do not have the same approach to pseudonymisation. The GDPR promotes pseudonymisation as a useful compliance tool to mitigate personal data risks and effect data minimisation and data-protection-by-default [Es15]. Yet, its proposed definition appears over-restrictive [SK16] and will create confusion between pseudonymous datasets (that still fall within the scope of the GDPR) and anonymous datasets (that are exempted). On the other hand, eIDAS regards pseudonyms only as a means to construct (perhaps safer) unique identifiers, failing to incorporate pseudonyms in a way that would allow the system to enjoy selective disclosure functionality – a fact that was highlighted during the drafting phase of eIDAS by the Article 29 Working Party [Ar15].

In an effort to give an incentive to data controllers to pseudonymise datasets the GDPR seems to facilitate the further processing of pseudonymised datasets. Art 5 of the GDPR provides a waiver of the requirement for a legal basis to process data where, in conjunction with art 6(4), datasets that have been pseudonymised can be further processed if the controller deems the processing 'compatible' with the initial purpose(s). This could potentially be troublesome (assuming the definition of the GDPR is met), as many services connected to a national eID scheme collect a wealth of personal data, e.g. tax offices or healthcare providers, and eIDAS does not allow the use of a plurality of pseudonyms according to the service used each time.

Finally, in a recent communication about the future of online platforms, the Commission expresses the opinion that online platforms should be encouraged to start accepting eIDs notified under eIDAS as a means to authenticate their users [Eu16].[25] The possibility of applying a system that was designed to offer officially approved national identities to private service providers could be problematic. By not allowing for selective disclosure, eIDAS limits pseudonymisation in identifications to serve as a replacement for UID. If, by the GDPR, pseudonymisation is regarded as a key means of ensuring privacy- and data-protection- by default, eIDAS has missed a chance to further data privacy of citizens, which should be worrying if eIDAS is used in commercial online platforms. At the same time, the Commission and its policy making bodies should work on how to make its definition of pseudonymisation less obscure before it can fully live up to its envisaged potential as a means of compliance with data protection obligations.

[24] "Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application": n 17 art 87

[25] "In order to empower consumers and to safeguard principles of competition, consumer protection and data protection, the Commission will promote interoperability actions to encourage on-line platforms to recognise other elD means, in particular those notified under eIDAS Regulation, that offer the same reassurance as their own."Please note that this is a leaked draft; the official document has not been released at the time of writing.

Acknowledgements
This research was funded by the Research Councils UK Digital Economy Programme, Web Science Doctoral Training Centre, University of Southampton, EP/L016117/1, partly supported by the SOCIAM Project, funded by the UK Engineering and Physical Sciences Research Council under grant number EP/J017728/2, and was partly funded the European Union’s Horizon 2020 research and innovation programme under grant agreement No 700542. This paper reflects only the authors’ views; the Commission is not responsible for any use that may be made of the information it contains.

Literature

[Ar15] Article 29 Data Protection Working Party: Letter of the WP29 to eIDAS. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150622_letter_of_the_art_29_wp_to_eidas.pdf [Accessed 02 May 2016], 22 June 2015.

[BD11] Beynon-Davies, P.: The UK national identity card. J Inf technol, 1(1):12–21, 2011.

[Br14] Bringer, J.; Chabanne, H.; Lescuyer, R.; Patey, A.: Efficient and Strongly Secure Dynamic Domain–Specific Pseudonymous Signatures for ID Documents. In (Christin, Nicolas; Safavi-Naini, Reihaneh, Eds.): Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3–7, 2014, Revised Selected Papers. Springer Berlin Heidelberg, Berlin, Heidelberg, S. 255–272, 2014.

[BS15] BSI: TR-03110 eIDAS Token Specification. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-2-V2_2.pdf?__blob=publicationFile&v=1 [Accessed on 05 January 2016], 2015.

[CS14] Cuijpers, C.; Schroers, J.: eIDAS as guideline for the development of a pan European eID framework in FutureID. In (Hühnlein, Detlef, Ed.): Open Identity Summit 2014, Jgg. 237. Bonner Köllen Verlag, S. 23–38, 2014.

[Es15] Esayas, S. Y.: The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the ‘all or nothing’ approach. European Journal of Law and Technology, 6(2), 2015.

[Es16] Eskens, S. J.: Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should It? Master thesis, University of Amsterdam. Available from: http://ssrn.com/abstract=2752010 [Accessed 02 May 2016] 2016.

[Eu16] European Commission: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Online Platforms and the Digital Single Market, Opportunities and Challenges for Europe, COM (2016) DRAFT. Available from: http://www.politico.eu/wp-content/uploads/2016/04/Platforms-Communication.pdf [Accessed 06 May 2016], 25 May 2016.

[Fe11] Federal Office for Information Security: Technical Guideline TR-03127: Architecture electronic Identity Card and electronic Resident Permit. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03127/BSI-TR-03127_en.pdf [Accessed 10 January 2016], 2011.

[Ma10] Martens, T.: Electronic identity management in Estonia between market and state governance. Identity in the Information Society, 3(1):213–233, 2010.

[MG13] Massacci, F.; Gadyatskaya, O.: How to get better EID and Trust Services by leveraging eIDAS legislation on EU funded research results. White Paper. Available from: http://www.cspforum.eu/Seccord_eidas_whitepaper_2013.pdf []Accessed 09 January 2016], 27 July 2015 2013.

[PH10] Pfitzmann, A.; Hansen, M.: Anonymity, Unlinkability, Unobservability, Pseudonymity and Identity Management – A Consolidated Proposal for Terminology. Available from: http://www.maroki.de/pub/dphistory/Anon_Terminology_v0.34.pdf [Accessed 23 January 2016], 12 June 2015 2010.

[Po12] Poller, A.; Waldmann, U.; Vowe, S.; Turpe, S.: Electronic Identity Cards for User Authentication – Promise and Practice. 10(1):46–54, 2012. IEEE Security & Privacy.

[Rö08] Rössler, T.: Giving an interoperable e–ID solution: Using foreign e–IDs in Austrian e–Government. Computer Law & Security Review, 24(5):447–453, 2008.

[SK16] Stalla-Bourdillon, S.; Knight, A.: Anonymous data v. Personal data – A false debate: An EU perspective on anonymisation, pseudonymisation and personal data. Wis. Int'l L.J., 2016 [forthcoming].

[Sw00] Sweeney, L.: Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy [Working paper]. Available from: http://dataprivacylab.org/projects/identifiability/ [Accessed 02 May 2016], 2000.

[Ts16] Tsakalakis, N.; O'Hara K.; Stalla-Bourdillon, S.: Identity assurance in the UK: technical implementations and legal implications under the eIDAS regulation. WebSci'16, Hannover, DE, May 22–25 2016. Available from: http://eprints.soton.ac.uk/393204/ [Accessed 05 May 2016], 2016.

[Ve15] Verheul, E. R.: Privacy protection in electronic education based on polymorphic pseudonymization. Report 2015/1228. Available from: http://eprint.iacr.org/2015/1228 [Accessed 04 May 2016], 2015.

[ZS13] Zwingelberg, H.; Schallaböck, J.: H2.4 The Proposal for a Regulation on Electronic Identification and Trust Services under a Privacy and ABC4Trust Perspective. Available from: https://abc4trust.eu/index.php/pub/deliverables/176-h2-4 [Accessed 14 February 2016], 03 August 2015 2013.

Identity Mining Vs Identity Discovering: a new approach based on data mining in the context of Big Data

Constantina Caruso[1], Andrea Dimitri[2], and Massimo Mecella[3]

Abstract: The economy of an advanced country is, every day more, based on complex information systems and interconnected networks that made its cyberspace. Security in this cyberspace is an essential requirement. In Italy a national lab for Italian government has been constituted. In this framework identity and identity management systems has been studied. The depicted scenario defines new open questions and new challenges. In this paper we propose to deal with identity management in complex systems using analytical tools coming from anomaly detection for big data.

Keywords: identity management, big data, data mining, analytics, identity management system.

1 The context

The economy of an advanced country is, every day more, based on complex information systems and interconnected networks that made its cyberspace. Security in this cyberspace is an essential requirement.

To effectively face this new challenge, professors and researchers from 34 Italian universities have joined their efforts to constitute the Italian Cyber Security National Lab. In October 2015 a white book ("Il futuro della cyber security in Italia", [CD15]) established targets and future goals of this institution.

In this research container, the Universities of Roma Tor Vergata and La Sapienza, with the University of Bari Aldo Moro have been nominated responsible for the area Intelligence – Big Data Analytics.

In this organizational framework the data mining activity has been oriented to the particular task of identity discovering in complex systems for managing and adding security in Identity Management Systems; because of the new huge contexts (mobile, IoT, cloud computing), which stress the traditional activities of Identity Management Systems, experience and tools coming from Big Data Analytics have been considered.

Identity discovering in complex systems can enhance their security because, analyzing

[1] University of Bari,Aldo Moro, Piazza Umberto I, 1, 70121 Bari, Italy, costantina.caruso@uniba.it
[2] University of Rome Tor Vergata, Via Orazio Raimondo 18, 00173 Rome, Italy, andrea.dimitri@uniroma2.it
[3] University of Rome La Sapienzia, Piazzale Aldo Moro, 5, 00185 Rome, Italy, mecella@dis.uniroma1.it

the logs associated to the identity activities, we can compare discovered identities and previous known, formal identities of a complex service system thus obtaining factual information about novel or anomalous behaviour [SK15].Threats description

The progresses of technology in media and end devices and the necessity of complex resources sharing modified the architecture of the Organizations that cooperate to provide services. A lot of organizations, either public or private, without common hierarchic relationships, cooperate to administer an area and/or to provide services [SI01]. We refer to these organizations with the expression "Complex Systems".

One of the emerging tendencies is to build and develop distributed systems which have mobile and dynamic service endpoints (smart phones are typical examples) and, at the same time, computational, storage and networking resources are centralized (cloud storage, cloud networking, cloud computing) [DA05][DT07].

In this complex and explicitly not hierarchical structure, every elementary organization possesses its security system but this does not guarantee that the resulting complex system is secured [RA08].

2 Digital identity management in complex systems

A digital identity is a set of attributes owned by an entity used by computer systems to represent an agent (person, organization, application, or device) [RA08] [BG02]. Its management is typically delegated to Identity and Access Management (IAM) which enables the right individuals to access the right resources at the right times and for the right reasons.

Classical IAM methods are generally designed to use tables-based architectures for storing entities attributes and involve four basic functions: creation, management and deletion of identities, the access function i.e. the control that data used by an entity to access to services are right; the service function which delivers personalized, role-based, online, on-demand, multimedia content to entity w.r.t. its authorizations; the "identity federation" function: the system that relies on federated identity must authenticate an entity without knowing its password.

Many large organizations have IAM infrastructure for user provisioning, Single Sign On (SSO) and identity governance but to track all the aspects of user activity is very difficult. In a recent research survey, security professionals identified "user behaviour activity monitoring" as the weakest area of security monitoring.

Classical approaches are inadequate in a business and technical landscape dramatically modified by described complex systems: what do you do when you are asked to build an identity and access management system that can handle up to billions of identities that have to be stored, managed and controlled in real-time?

Big Data refers to large-scale information management and analysis technologies that exceed the capability of traditional data processing technologies. Big Data is differentiated from traditional technologies in three ways: the amount of data (volume), the rate of data generation and transmission (velocity), and the types of structured and unstructured data (variety) [SY14][IE14].

In the majority of cases, Big Data security analytics is applied to security data such as network packets, meta data, emails, transaction systems to help teams to detect malware, phishing sites and online frauds because it can help enterprises to address unprecedented information risk arising from two conditions:

1. dissolving organizations network boundaries; corporate applications and data are increasingly accessed through cloud services and mobile device, introducing new threat vectors and making the systems become more vulnerable to data misuse and theft [CH13];

2. more sophisticated cyber attackers which bypass traditional defences, static threat detection measures and signature-based tools.

Security data encompasses any type of information that could contribute for a complete control of the organization and its risks.

A more agile approach based on dynamic risk assessments, the analysis of vast volumes of data and real-time security operations is essential to provide meaningful security. The Security for Business Innovation Council [SB16] advises organizations to move to an intelligence-driven security model.

We must face the differentiation of login and user authentication functions and the exponential growth of logging data ought to billions of digital identities (machine-to-human and machine-to-machine).

An authentication process verifies the identity claimed by or for a system entity. User authentication methods use three approaches: “something you know”, “something you have” and “something you are” [RA08].

The “something you know” verification is typically the use of a password to access on-line services. This method is the weakest because people often use weak passwords which are simple to find. Despite its weakness, the one-factor authentication is still used but it is not sufficient for organizations which need to differentiate their services and, as a consequence, the typologies of access points and login functions.

“Something-you-have” methods identify the entity by means of an object, physical or virtual, it owns: bank token, Kerberos ticket, ATM card, credit card, smart card are use cases of these methods. “Something-you-are” methods use user's biometric measures and are really strong authentication methods but they are very expensive.

A valid alternative to the three more classical methods seems to be the entity authentication based on “something you do”. There are very recent but promising studies which uses Big Data in identification methods for network traffic [SY14], for recognizing fake identities in social media networks [SK15] [WE15] to identify social predators, all by using behaviour characteristics of users. To identify right or fake behaviours implies recognizing anomalies of the analyzing contest; in [IE14] a call detail record based anomaly detection method is presented; it analyzes the users' calling activities and detects the abnormal behaviour of user movements in a real cellular network. A major problem that many network/IT system administrators face is to detect a defect in user activity from a pool with many users and millions of transactions; the proposed approach reduces the cost of data processing compared to traditional data warehouse technologies. Event correlation is important when identifying anomalies and workflows: in [KM15] and in [RB15] and in Hadoop[AH16], cluster is used to study a scalable security event aggregator for situational awareness. The project Eagle [GS15] proposes a highly scalable system, based on Hadoop[AH16], capable of monitoring multiple eBay clusters in real-time. When a user performs any operation in the cluster, Eagle matches current user action against his prior activity pattern and raises an alarm if it suspects anomalous action.

Big Data technologies can reduce overall attack surface of IAMs addressing these issues:
1.clean up the access list by quickly identifying rogue accounts or users who haven't accessed applications for a prolonged period;
2. manage correctly separation of duties (SODs); IAM security analytics can clearly show business process relationships and find conflicts related to compliance and risk; this can help business managers to establish and manage correctly SODs;
3. to manage privileged users; analytics can be used to identify the privileged accounts and create a security system which alerts when anomalous behaviour is identified;
4. to secure IAM by discovering anomalous workflows activated by malicious entities (human or software);
5. to secure honest users by quickly identify fake identities.

3 The Big Data Analytics approach to anomaly detection in IAM: the Lab approach

Many large Organizations are already using security analytics tools to streamline processes and improve IAM oversight efficiency. From a security perspective, this can help enterprises reduce their overall attack surface and lower IT risk. Big data means the collection of hard amount of data to analyze them in a unique framework. Big data means, also, correlation of data coming from heterogeneous sources, meaning structured data versus unstructured data. This approach requires new technologies and new mathematical tools.

Many challenges are to be considered to plan a big data strategy [BC12][LA14]:

- interdisciplinary: manipulation of big data have to put together data mining, machine learning, information retrieval, natural language processing , statistics, applied mathematics, other than a strict interlacement with domain experts;

- quantity vs quality of data: the common vision deriving from big data privileges the quantitative. The step over is to develop statistical algorithms based on quality-aware methodologies;
- just in time predictions: a security system is to be able to notice a bug contextually and before it becomes a real threat. To prevent a bug means to evaluate stability and robustness of the workflow associated to that service;
- low user/organization impact: when importing a new technology in a context when an old one is already running, the impact has to be evaluated carefully; if the new technology has a strong impact in the old one, the switch-off could be not easy (often impossible);
- high security: classical security is highly related to cryptography; in this context the SSL (secure socket layer) protocol is a tunnel where clear data are redirected without considering their structure. This will be only partially feasible in the context of big data.

Atomic activities of the previous goals, planned in the context of the lab, are:

- analysis of algorithms of data analysis, statistical data analysis and learning and development of new algorithms and mathematical tools;
- entropy analysis and analysis of transaction entropy; entropy and conditioned entropy are the basis for the building of an index of forecast for the future state of a variable;
- anomaly detection systems and anomaly management;
- new algorithms for the manipulation of huge quantities of data;
- cryptographic systems for big data; in particular, we concentrate our research activities on the development of algorithms and protocols based on homomorphic encryption.

References

[SI01] Simon, H.A. (2001). Complex systems: The interplay of organizations and markets in contemporary society. Comp. & Math. Org. Th.y, Aug. 7(2), 79-85.

[SK15] K.D.B.H. Subasinghe, S.R.Kodithuwakku. “A Big Data Analytic Identity Management Expert System for Social Media Networks”, 2015 IEEE Int. WIE Conference on Electrical and Computer Engineering (WIECON-ECE).

[CH13] Chibber, A (2013)."Security analysis of cloud computing” Int. J.of Advanced Research in Engineering and Applied Sciences 2(3): 2278-6252.

[RB15] H. Reguieg, B. Benatallah, Hamid R., Motahari Nezhad, F. Toumani. “Event Correlation Analytics: Scaling Process Mining Using MapReduce-Aware Event Correlation Discovery Techniques”. IEEE Trans. on Services Computing. 2015.

[DA05] Dimitri A., Arcieri F. A prevention strategy for security: a bayesian approach to anomaly detection. IFIP Int. Fed. for Inf. Proc.. Sprinter Boston 2005.

[DT07] Dimitri A., Talamo M. A Meta Analysis Framework based on Hierarchical Mixture Model. Adv. and App. in Statistics. Volume 7, Issue 3, (Dec. 2007).

[BC12] R. Baldoni, G. Chockler: Collaborative Financial Infrastructure Protection - Tools, Abstractions, and Middleware. Springer 2012.

[LA14] G. Lodi, L. Aniello, G. A. Di Luna, R. Baldoni: An event-based platform for collaborative threats detection and monitoring. Inf. Syst. 39: 175-195,2014.

[MT15] A. Moroni, M. Talamo, and A. Dimitri. 2015. Adoption factors of NFC Mobile Proximity Payments in Italy. In Proc. of the 17th Int. C. on H-C Inter. with Mobile Devices and Services (MobileHCI '15). ACM, NY, USA, 393-399.

[CD15] C. Caruso, A. Dimitri, M. Mecella, M. Talamo Intelligence e Big Data Analytics, Il Futuro della Cyber Security in Italia, 2015, pagg. 50-53. CINI-Laboratorio Nazionale di Cyber Security.

[RA08] Ross J.Anderson, 2008. Security Engineering: a guide to building dependable distributed systems (2 edition), Wiley Publishing.

[BG02] Francesco Bergadano, Daniele Gunetti, and Claudia Picardi.“User authentication through keystroke dynamics”. ACM Transactions on Information and Systems Security. 5, 4 (November 2002), 367-397.

[SY14] Sung-Ho Yoon, Jun-Sang Park and Myung-Sup Kim. “Behaviour Signature for Big Data Traffic Identification”. 2014 Int. Conf. on Big Data and Smart Comp.

[IE14] Ilyas Alper Karatepe, Engin Zeydan. “Anomaly detection in cellular network datausing Big Data analytics”. European Wireless 2014.

[KM15] Jinoh Kim, Ilhwan Moon, Kyungil Lee, Sang C. Suh, Ikkyun Kim. “A scalable security event aggregator for situational awareness”. 2015 IEEE First Int. Conf. on Big Data Computing Service and Applications.

[GS15] Chaitali Gupta, Ranjan Sinha, Yong Zhang. “Eagle: User Profile-based Anomaly Detection for Securing Hadoop Clusters”. 2015 IEEE Int. Conf. on Big Data.

[WE15] Estée van der Walt, J.H.P. Eloff. “A Big Data Science experiment – Identity Deception Detection”. 2015 Int. Conf. on Computational Science and Computational Intelligence.

[AS16] Apache Spark, a general engine for large-scale data processing, http://spark.apache.org, 2016.

[AH16] Apache Hadoop, an open-source software project for reliable, scalable, distributed computing; http://hadoop.apache.org/, 2016.

Aligning ABAC Policies with Information Security Policies using Controlled Vocabulary

Raik Kuhlisch[1] and Sören Bittins[2]

Abstract: Attribute-based Access Control (ABAC) policies are based on mutually processable policy attributes. Assigned permissions in such policies need to be reflected or combined with organisational constraints. Best practice in information security dictates having the operational need to access a particular information artifact independent from the function of the specific application systems. Consequently, any policy regulating the behaviour towards information access must adhere to a minimum degree of mutual semantic expressiveness to be combined and processed with the matching ABAC policy. We show how to detect policy attribute conflicts between ABAC policies and information access policies by means of controlled vocabulary and Semantic Web technologies.

Keywords: policy conflict, access control, attribute-based access control (ABAC), information security, XACML

1 Introduction

An access control model defines how to evaluate authorisation decision or how to decide resource access requests in distributed computing environments. A security context anchors a user's roles and potential approvals to access protected resources [Be06, p. 18]. The paradigm of Attribute-based Access Control (ABAC) contributes to the appraisal and decision of requests by injecting additional attributes from all relevant information systems such as subject, object or environment conditions into the decision process. Consequently, a security context becomes more complex compared to other paradigms such as the user-centric Role-based Access Control (RBAC) [FK92] especially regarding the semantical expressivness, computability, and interoperability when policies of higher granularity must be evaluated for deciding on the legitimacy of a resource access request.

From the information security management point of view (e.g. ISO 27001 [In14]), information access is defined in or derived from an overarching information security policy [Ku13]. The specific access-regulating rules are implemented in more precise policies that capture the specifics of application systems and access contexts. Therefore, ABAC policy attributes need to be correlated with attributes from a variety of information security policies. Due to the use of atomic values in ABAC policies, interoperability issues may arise. This paper proposes a policy system that separates information access from access control rules in accordance with an information security management. Without proper means to relate ABAC policy attributes with other policies, inconsistencies or conflicts could occur.

[1] The University of Rostock, Faculty of Computer Science and Electrical Engineering,
Albert-Einstein-Str. 22, 18059 Rostock, Germany, raik.kuhlisch@uni-rostock.de

[2] Fraunhofer FOKUS, ESPRI – Collaborative Safety and Security
Kaiserin-Augusta-Allee 31, 10589 Berlin, Germany, soeren.bittins@fokus.fraunhofer.de

An integrated policy organisation mechanism is presented that addresses ABAC policy conflict identification through controlled vocabularies in conjunction with a conflict detection algorithm, includes a security policy poly-hierarchy with fitting-in ABAC policies.

Organisation. This paper is structured as follows: Section 2 discusses relevant previous work. Section 3 introduces background on policy-based information management and Semantic Web technology-based vocabulary management. The proposed ABAC policy conflict detection is outlined in Section 4, while Section 5 motivates a policy system that supports a policy alignment. Section 6 concludes and addresses future research.

2 Related Work

ABAC policies can be represented as eXtensible Access Control Markup Language (XACML) [Mo05] policies. Dersingh et al. [DLJ08] use knowledge representation and retrieval techniques to enhance XACML with context attributes. They extended the XACML framework with an ontology administration point that holds inferred knowledge about domain information associated with subjects, resources, actions, or environments. This work is aimed at a refinement of policies with semantic context attributes. However, their focus is rather on the evaluation of context-aware authorisation decisions than on policy conflict handling.

Conflict detection with ABAC policy has been investigated comprehensively. Zoo and Zhang [ZZ14] propose a conflict detection algorithm based on a binary sort tree. It fits into the XACML framework. Additional policies are registered through a policy administration point, a core component of the XACML framework. The detection algorithm is limited to XACML policies and does not take other kinds of security policies into account.

Shu, Yang and Arenas [SYA09] put forward conflict detection and handling among ABAC policy rules. Their notion of semantically-equivalent policies allows for matching policies with similar tuples (subject, object, action). However, an assumption is that these policies rely on fully comparable attribute predicates. This is true if policies share a common set of policy attribute values. External policy attributes cannot be readily compared.

We represent XACML policies in Semantic Web technologies in order to infer conflicts with other policies and propose to align ABAC policies with information security policies.

3 Preliminaries

3.1 Information Security Management Compliant Policy Hierarchy

Access control must ensure that access is constrained (e.g. through classification) to the minimal meaningful amount of permissions required to fulfill a legitimate operation in order to implement restricting security principles such as ”need-to-know”. Additionally, any permissions assigned to users must not be processed separately but assessed by all relevant decision workflows and must be computable by process-specific policies. They may be derived from security requirements as well, for instance, in [Sa15] a method engineering approach is shown that elicits permission sets from business processes. Nevertheless, authors should consider the following when authoring access control policies [Ca09]:

- What tasks support a dedicated information/software system?
- Who is allowed to perform these tasks?
- What kind of data an information/software system processes?
- What operations are defined on this data?

These questions define a specific application purpose and context. Additional transaction rules provide a context to requests for information resources and is more specific to a purpose of use. They describe a certain type of information that is processed in particular situations and implement the concept of functional roles where tasks have been assigned on the basis of existing expertise and routine organization of work. One means to develop access policies in a formal manner is to apply information security management, outlining a comprehensive handling of information disclosure according to an operational need. The most prominent framework is ISO/IEC 27001 [In15]. National equivalents exist (e.g. in Germany with the BSI Standard 100-1 [Bu08]). However, the most important thing is to apply a top-down approach (i.e. to break data activities into system specific permissions).

An adequate information security management system/approach should at least include information security objectives, measures, and controls. Access Control is just one measure in order to manage information security. However, the remainder of this document puts a strong focus on it—paper-based information processing is not examined.

We adapted the policy concepts from [So98, p. 222] as follows:

- An *information security policy* describes fundamental objectives for the protection of information in an organisation. It applies to all electronic and paper-based information processing methods. In order to achieve the fundamental objectives general principles and responsibilities are described.
- The part of an *information security policy* that describes legitimate accesses to protected information is defined as an *information access policy*. This policy defines the legitimate use of information (i.e. regulates the processing of information through purpose of use restrictions and who may access protected data under what circumstances) in terms of compliance, regulatory mandates as well as what data is protected (e.g. record types). Finally, it states employee's characteristics within an organization or organisational unit. It describes the constraints on the processing of data or might determine the purposes for which and the manner in which any data are to be processed.
- A *resource behaviour policy* controls resource access by taking into account the organisation of work and regulating the use of subsystems of an entire information/-software system. It holds a list of software services that realise a clear purpose of use. These services are implemented by automated subsystems of an information system (including belonging hardware, system software, communication equipment and the application system itself). The *resource behaviour policy* concludes with access types defined on the software services.
- A more detailed *ABAC policy* picks up access rights through permissions that are assigned to registered subjects. It may contain actions in the sense of a MUST or MUST NOT (i.e. obligations) or actions that are explicitly forbidden with authorized actions (refrain actions).

3.2 Policy and Policy Attribute Representation

A fundamental prerequisite for identifying policy conflicts among different types of policies is to rely on formal attribute relations. We formalize those relations through controlled vocabularies (also known as code systems or terminologies). One standard is the Common Terminology Services 2 (CTS2) by the Object Management Group (OMG) [Ob15] for defining structural and functional profiles over the entire lifecycle of concepts (i.e. codes).

We represent policy attributes through code systems and manage services, resources, actions etc. by a terminology server. In [Bi13] an implementation is described that runs a CTS2 instance with Semantic Web technologies. So-called Resource Description Framework (RDF) [Ha04] signatures with additional RDF Schema [BG14] axiomatic triples define structural constraints of a domain model with Frame Logic semantics [KLW95]. This ontological approach fits to well-established *denyAll* default behaviors in access control policies and provides means to reason about processing purposes. That means, we adapt the implementation from [Bi13] in order to provide a policy representation with ontologies. This requires the definition of policy signatures in RDF. The UML-like diagram in Figure 1 shows a rough outline of defined RDF classes and properties that represent policy types (multiplicity is derived from the Extended Backus-Naur Form notation). For the sake of clarity, no ABAC policy is shown. String patterns denote the use of code systems.

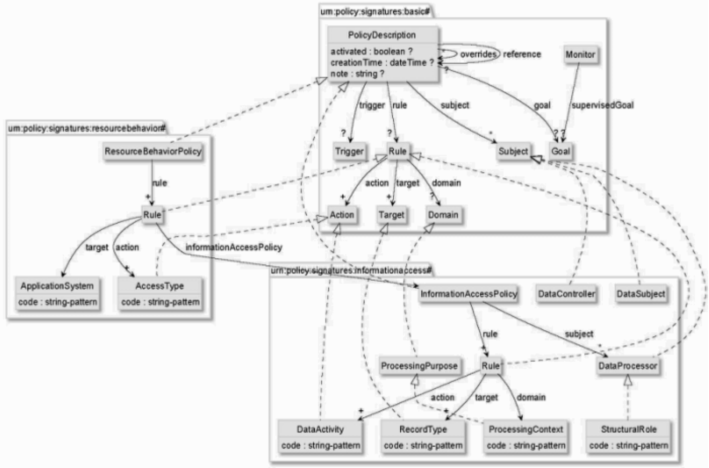


Fig. 1: Policy information model with relations

If all policies are stored within the same triple store, codes or attribute values can easily be referenced with CTS2 class concepts. However, a small list of acceptable codes might be represented as well with regular expressions (notion of facets in Frame Logic semantics). A disadvantage is the tight binding between policy and attribute values which makes a code system modification more difficult (forces an update of a policy signature). The following snippet in RDF Turtle syntax [Be14] shows the application of ”inline codes”.

```
@prefix:      <urn:policy:signatures:informationaccess#> .
@prefix sig:  <urn:negros:signatures#> .
```

```
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .

:StructuralRole
  a rdfs:Class ;
  rdfs:comment """Competence of an employee within an
        organisation or organisation unit. """@en ;
  rdfs:subClassOf :DataProcessor ;
  sig:propertyConstraint [
    sig:onProperty prop:code ;
    sig:range xsd:string;
    sig:min 1 ;
    sig:max 1 ;
    sig:facet '(ApplicationAdministrator)|(OfficeClerkOrAssistant)' ;
  ] .
```

List. 1: RDF signature for structural role values

A a shared triple store utilizing CTS2 terminology layer benefits from:

- strict separation of policy structure and policy attribute maintenance,
- support for any designations of policy attribute values,
- support for domain-specific attribute value bags through value list semantics.

3.3 ABAC Policy Model

An ABAC policy regulates access requests by subjects onto information objects through permissions in an information system. Usually, access control policies express authorisation rules with a quadruple (subjects, objects, actions, authorisation decisions). Other notions of access control policies include obligations and refrain actions. The single difference is the modality of the policy, i.e. which basic statement the policy defines (grant or deny). However, an authorisation decision can rely on non-matching policies as well which should usually cause a deny decision.

ABAC policies can be represented with industry standards such as the declarative XACML [Mo05] that supports Next Generation Access Control [Am13] being capable of handling different policies defined by distributed systems. XACML also supports authorisation statements and obligations but has poor semantic expressiveness due to its binding to XML. Thus, we defined a policy model with corresponding XACML equivalences using the RDF signature means of [Bi13]. This enables us to reason about XACML policies and to relate them with *resource behaviour policies* and *information access policies*.

The conversion of a XACML policy from XML to RDF/XML [Be04] is accomplished with a simple eXtensible Stylesheet Language (XSL) transformation [Ka07]. Although the binding of XACML to XML assumes a tree structure and a graph-based set of RDF triples supports multiple parent elements that may result in not generating a tree sturcture, the proposed conversion is not affected by this limitation.

The use of coded attribute values is originally not supported by XACML. However, the standard provides extensions to register own data types via the xs:Any element. For instance, useful data types for interoperability scenarios in healthcare environments are defined in [HL15b]. A coded value for a XACML resource match can be expressed as follows [HL15a]:

```
<ResourceMatch MatchId="urn:hl7-org:v3:function:CV-equal">
  <AttributeValue DataType="urn:hl7-org:v3#CV">
    <hl7:CodedValue code="B05"
             codeSystem="urn:oid:1.2.276.0.76.5.413"/>
  </AttributeValue>
  <ResourceAttributeDesignator
   AttributeId="urn:ihe:iti:xds-b:2007:folder:code"
   DataType="urn:hl7-org:v3#CV"/>
</ResourceMatch>
```

List. 2: Coded XACML resource attribute

The attribute value is now associated with a code system that is managed by a terminology service. However, the use of a particular coded value might conflict with rules of a Resource Behaviour Policy or Information Access Policy. Relations to policies of different types are achieved by class-based inheritance (cf. Fig. 1), which is a basic policy schema defining common policy classes as foundation for more specific policy types. For instance, the `urn:oasis:names:tc:xacml:2.0:policy:schema:os#Action` class is a subclass of the `urn:policy:signatures:basic#Action` class or the `urn:oasis:names:tc:xacml:2.0:policy:schema:os#Subject` is a `urn:policy:signatures:informationaccess#DataProcessor` class, too.

4 ABAC Policy Conflict Detection

Policy conflicts are manifold and basic model is defined by Moffett and Sloman [MS94] and distinguish conflicts between conflict of modalities and conflict of goals. Modality conflicts are defined by inconsistencies between the policy modes (e.g., one policy grants and another one denies access). Goal conflicts may occur when subjects and objects are overlapping in different combinations. Other policy conflicts have a semantical origin, such asdDomain or data conflicts as described in [Ku13]. These conflicts are detectable through of SPARQL queries [PS08] against a policy store (i.e. we do not rely on a rule system). However, semantic conflicts are more difficult to detect because their artifacts need to be mapped, resolved, and correlated by the policy system first.

4.1 Domain Conflict Detection

Formally subsumption relations between the policy attribute values must be defined from different policy types, so that $CodedValue_{PolicyTypeA} \sqsubseteq CodedValue_{PolicyTypeB}$ applies. This does not imply that the code values are organized hierarchically in the same code system but that one code value involves another causing domain conflicts when semantically similar policy attributes are not disjoint. For instance, the following instance is a valid definition of subsumption relations across multiple policy types (cf. Fig. 2). The code value `EXECUTE` of an action type in a *resource behaviour policy* means that it is a valid application with a registered `USE` data activity in an *information access policy*.

To capture codes without a subset of another code, this SPARQL query may be executed:

```
PREFIX conf: <urn:policy:signatures:conflicts#> .
PREFIX prop: <urn:policy:signatures:properties#> .
SELECT ?g1 ?g2 ? superior ? subordinate
  WHERE {
    ?x conf:superior [
      prop:code ?superior
    ].
    ?x conf:subordinate [
      prop:code ?subordinate
    ].
    GRAPH ?g1 {
      ?y prop:action [
        prop:code ?superior
      ].
    }
    GRAPH ?g2 {
      ?z prop:action [
    }
  }
```

List. 3: SPARQL query to detect missing subsumption relations

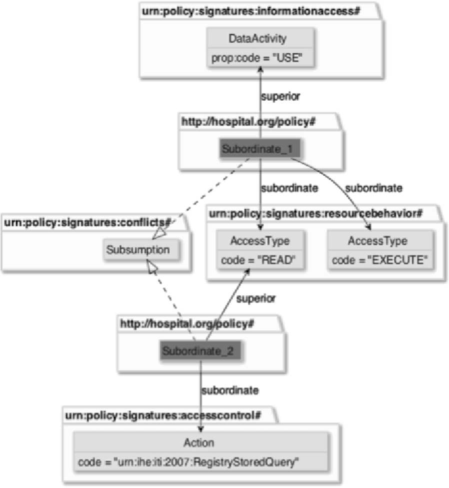

urn:policy:signatures:informationaccess#
DataActivity
prop:code = "USE"
superior
http://hospital.org/policy#
Subordinate_1
subordinate
subordinate
urn:policy:signatures:conflicts#
Subsumption
urn:policy:signatures:resourcebehavior#
AccessType
code = "READ"
AccessType
code = "EXECUTE"
superior
http://hospital.org/policy#
Subordinate_2
subordinate
urn:policy:signatures:accesscontrol#
Action
code = "urn:ihe:iti:2007:RegistryStoredQuery"

Fig. 2: UML-like policy object model for code-based subsumptions

4.2 Data Conflict Detection

Data conflicts can be either mitigated by a terminology CTS2 service or avoided entirely. Policy attributes with stored code systems or value sets can be linked via the CTS2 Map Services with related codes, in order to organise semantically connatural attributes. Thus, different designators and different scales of a coded value may be used for expressing policies. The challenge is to link the policy model with different identifiers of a coded value. To do so, each SPARQL query has to be checked: All literals with the predicate `prop:code` need to be enlarged by all available designators (SPARQL keyword `OPTIONAL`).

5 Implementation

In general, policy conflict handling may happen statically (”what if . . . ?” analysis) or dynamically during the runtime. The latter can be addressed by setting of priorities or introducing a meta policy (e.g. XACML policy rule combining algorithm). However, this primarily applies to scenarios that implement access control means in order to evaluate an authorisation decision. We focus on solving potential conflicts in policies in order to establish a valid sample space for the specific query dimensions. That is why we rely on a static approach since an automated handling of conflicts (e.g. heuristics) is impractical due to the complex relations between policy attributes based on code systems. Therefore, our conflict resolution policy sets an interventional correction mechanism for the author based on the ”security is a process” principle and is aimed at addressing most issues early through providing guidance for authoring policies.

We implemented a prototype policy management system in Java holding all applicable policies. A policy registration is accompanied by a systemic check against the policy store (RDF store). All services are facilitated with the SPARQL 1.1 Graph Store HTTP Protocol [Og13] and the SPARQL 1.1 Protocol [W313] as Figure 3 shows.

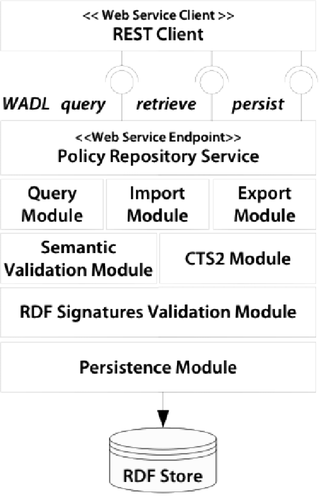
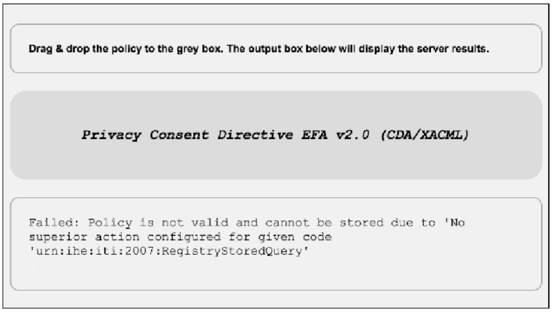


Fig. 3: Architecture policy management


Drag & drop the policy to the grey box. The output box below will display the server results.

Privacy Consent Directive EFA v2.0 (CDA/XACML)

```
Failed: Policy is not valid and cannot be stored due to 'No
superior action configured for given code
'urn:ihe:iti:2007:RegistryStoredQuery'
```

Fig. 4: Policy client interface

The *RDF Semantic Validation Module* checks for inconsistencies at a policy persist operation. It furthermore holds standard *information access policies* as well as *resource behaviour policies* that outline general security properties. Moreover, our prototype consists of a Web-based policy client (cf. Fig. 4) that accepts a patient privacy consent and an enclosed XACML policy. This policy is submitted to a `PERSIST` operation and validated. The sample output in Figure 4 indicates that the XACML action in the given context is not configured and thus not allowed to be used to avoid assigning inflated access rights.

6 Conclusions and Ongoing Work

ABAC policies should be aligned with resource behaviour and information access policies. This ensures that information security constraints are applied to access control policies. These policies may be represented through Semantic Web technologies. The presented approach does not suggest an extension of the XACML language but an in-band conversion of XACML policies to RDF in order to detect conflicts with other policy types. Although our prototype performs acceptably, more significant performance tests with more policy statements need to be executed as an acceptable response time is a prerequisite for a run-time policy decision. One facilitator could be the policy store acting as a policy decision point.

Next, we need to resolve potential conflicts between rule combination algorithms from XACML policies with *information access/resource behaviour policies*. The binary search techniques proposed by Shu et al. [SYA09] may be a good start for that. Finally, to provide a relevant contribution to the field of secure policies in eHealth domains, we will show through an exemplary patient privacy consent that inherently features a multi-dimensional policy (document/resource, external constraints, informational, and data), to be validated against and integrated with access control policies.

References

[Am13] American National Standards Institute: Next Generation Access Control – Functional Architecture (NGAC-FA). Technical Report INCITS 499-2013, ANSI, New York, NY, USA, March 2013.

[Be04] Beckett, Dave: RDF 1.1 XML Syntax. W3C Recommendation, W3C, February 2004. http://www.w3.org/TR/2014/REC-rdf-syntax-grammar-20140225/.

[Be06] Benantar, Messaoud: Access Control Systems: Security, Identity Management and Trust Models. Springer Science+Business Media, 2006.

[Be14] Beckett, Dave; Berners-Lee, Tim; Prud'hommeaux, Eric; Carothers, Gavin: RDF 1.1 Turtle: Terse RDF Triple Language. W3C Recommendation, W3C, February 2014. http://www.w3.org/TR/2014/REC-rdf-syntax-grammar-20140225/.

[BG14] Brickley, Dan; Guha, R. V.: RDF Schema 1.1. W3C Recommendation, World Wide Web Consortium (W3C), February 2014. http://www.w3.org/TR/2014/REC-rdf-schema-20140225/.

[Bi13] Billig, Andreas: Utilizing Semantic Technologies for a CTS2 Store. Fraunhofer FOKUS, CC E-HEALTH, June 2013. Retrieved 2016-08-01, from http://semantik.fokus.fraunhofer.de/WebCts2LE/main3/cts4omg.pdf.

[Bu08] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS). Technical report, Bundesamt für Sicherheit in der Informationstechnik, 2008. Version 1.5.

[Ca09] Caumanns, Jörg; Kuhlisch, Raik; Pfaff, Oliver; Rode, Olaf: IHE IT-Infrastructure White Paper: Access Control. September 2009. Retrieved 2016-08-13, from http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_WhitePaper_AccessControl_2009-09-28.pdf.

[DLJ08] Dersingh, Anand; Liscano, Ramiro; Jost, Allan: Context-aware access control using semantic policies. Ubiquitous Computing And Communication Journal (UBICC) Special Issue on Autonomic Computing Systems and Applications, 3:19–32, 2008.

[FK92] Ferraiolo, David F.; Kuhn, D. Richard: Role-based Access Controls. In: Proceedings, 15th National Computer Security Conference. Baltimore MD, pp. 554–563, 1992.

[Ha04] Hayes, Patrick: RDF Semantics. W3C Recommendation, W3C, February 2004. http://www.w3.org/TR/2004/REC-rdf-mt-20040210/.

[HL15a] HL7 Germany: Example: EFA Digital Consent Document. Wiki Portal for the Interoperability Forum, December 2015. Retrieved 2016-08-01, from http://wiki.hl7.de/index.php?title=Example:_EFA_Digital_Consent_Document.

[HL15b] HL7 Germany: IHE-XACML Binding: Custom Data Types (and related Comparison Functions) used for the bindings. Wiki Portal for the Interoperability Forum, March 2015. Retrieved 2016-08-01, from https://wiki.hl7.de/index.php?title=ihecb:IHE-XACML_Binding#Custom_Data_Types.

[In14] International Organization for Standardization: Information Technology – Security Techniques – Information Security Management Systems – Requirements. Technical Report ISO/IEC 27001:2013 + Cor. 1:2014, International Organization for Standardization, September 2014.

[In15] International Organization for Standardization: Information Technology – Security Techniques – Information Security Management Systems – Requirements. Technical Report ISO/IEC 27001:2013/Cor 2:2015, International Organization for Standardization, July 2015.

[Ka07] Kay, Michael: XSL Transformations (XSLT) Version 2.0. W3C Recommendation, W3C, January 2007. http://www.w3.org/TR/2007/REC-xslt20-20070123/.

[KLW95] Kifer, Michael; Lausen, Georg; Wu, James: Logical Foundations of Object-Oriented and Frame-Based Languages. Journal of ACM, 42:741–843, May 1995.

[Ku13] Kuhlisch, Raik: A Description Model for Policy Conflicts for Managing Access to Health Information. In (Lantow, Birger; Sandkuhl, Kurt; Seigerroth, Ulf, eds): Proceedings, 6th International Workshop on Information Logistics, Knowledge Supply and Ontologies in Information Systems (ILOG). volume 1028 of CEUR Workshop Proceedings, M. Jeusfeld c/o Redaktion Sun SITE, Informatik V, RWTH Aachen, Aachen, pp. 44–55, 2013.

[Mo05] Moses, Tim: eXtensible Access Control Markup Language (XACML) Version 2.0. Technical Report oasis-access_control-xacml-2.0-core-spec-os, OASIS, February 2005.

[MS94] Moffett, Jonathan D.; Sloman, Morris S.: Policy Conflict Analysis in Distributed System Management. Journal of Organizational Computing, 4(1):1–22, 1994.

[Ob15] Object Management Group: Common Terminology Services 2, Version 1.2. Technical Report formal/2015-04-01, OMG, April 2015. http://www.omg.org/spec/CTS2/1.2/.

[Og13] Ogbuji, Chimezie: SPARQL 1.1 Graph Store HTTP Protocol. W3C Recommendation, W3C, March 2013. http://www.w3.org/TR/2013/REC-sparql11-http-rdf-update-20130321/.

[PS08] Prud'hommeaux, Eric; Seaborne, Andy: SPARQL Query Language for RDF. W3C Recommendation, W3C, January 2008. http://www.w3.org/TR/2008/REC-rdf-sparql-query-20080115/.

[Sa15] Sandkuhl, Kurt; Matulevicius, Raimundas; Ahmed, Naved; Kirikova, Marite: Refining Security Requirement Elicitation from Business Processes Using Method Engineering. In: BIR 2015. volume 1420, pp. 98–109, 2015.

[So98] Solms, Rossouw von: Information Security Management (2): Guidelines to the Management of Information Technology Security (GMITS). Information Management & Computer Security, 6(5):221–223, 1998.

[SYA09] Shu, Cheng-chun; Yang, Erica Y.; Arenas, Alvaro E.: Detecting Conflicts in ABAC Policies with Rule-Reduction and Binary-Search Techniques. IEEE, pp. 182–185, July 2009.

[W313] W3C SPARQL Working Group: SPARQL 1.1 Overview. W3Crecommendation, W3C, March 2013. http://www.w3.org/TR/2013/REC-sparql11-overview-20130321/.

[ZZ14] Zou, Jiashun; Zhang, Yongsheng: Research of Policy Conflict Detection and Resolution in ABAC. Journal of Computational Information Systems, 10(12):5237–5244, 2014.

GI-Edition Lecture Notes in Informatics

P-1 Gregor Engels, Andreas Oberweis, Albert Zündorf (Hrsg.): Modellierung 2001.

P-2 Mikhail Godlevsky, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications, ISTA'2001.

P-3 Ana M. Moreno, Reind P. van de Riet (Hrsg.): Applications of Natural Lan-guage to Information Systems, NLDB'2001.

P-4 H. Wörn, J. Mühling, C. Vahl, H.-P. Meinzer (Hrsg.): Rechner- und sensorgestützte Chirurgie; Workshop des SFB 414.

P-5 Andy Schürr (Hg.): OMER – Object-Oriented Modeling of Embedded Real-Time Systems.

P-6 Hans-Jürgen Appelrath, Rolf Beyer, Uwe Marquardt, Heinrich C. Mayr, Claudia Steinberger (Hrsg.): Unternehmen Hochschule, UH'2001.

P-7 Andy Evans, Robert France, Ana Moreira, Bernhard Rumpe (Hrsg.): Practical UML-Based Rigorous Development Methods – Countering or Integrating the extremists, pUML'2001.

P-8 Reinhard Keil-Slawik, Johannes Magenheim (Hrsg.): Informatikunterricht und Medienbildung, INFOS'2001.

P-9 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Innovative Anwendungen in Kommunikationsnetzen, 15. DFN Arbeitstagung.

P-10 Mirjam Minor, Steffen Staab (Hrsg.): 1st German Workshop on Experience Management: Sharing Experiences about the Sharing Experience.

P-11 Michael Weber, Frank Kargl (Hrsg.): Mobile Ad-Hoc Netzwerke, WMAN 2002.

P-12 Martin Glinz, Günther Müller-Luschnat (Hrsg.): Modellierung 2002.

P-13 Jan von Knop, Peter Schirmbacher and Viljan Mahni_ (Hrsg.): The Changing Universities – The Role of Technology.

P-14 Robert Tolksdorf, Rainer Eckstein (Hrsg.): XML-Technologien für das Semantic Web – XSW 2002.

P-15 Hans-Bernd Bludau, Andreas Koop (Hrsg.): Mobile Computing in Medicine.

P-16 J. Felix Hampe, Gerhard Schwabe (Hrsg.): Mobile and Collaborative Business 2002.

P-17 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Zukunft der Netze –Die Verletzbarkeit meistern, 16. DFN Arbeitstagung.

P-18 Elmar J. Sinz, Markus Plaha (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2002.

P-19 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3. Okt. 2002 in Dortmund.

P-20 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3. Okt. 2002 in Dortmund (Ergänzungsband).

P-21 Jörg Desel, Mathias Weske (Hrsg.): Promise 2002: Prozessorientierte Methoden und Werkzeuge für die Entwicklung von Informationssystemen.

P-22 Sigrid Schubert, Johannes Magenheim, Peter Hubwieser, Torsten Brinda (Hrsg.): Forschungsbeiträge zur "Didaktik der Informatik" – Theorie, Praxis, Evaluation.

P-23 Thorsten Spitta, Jens Borchers, Harry M. Sneed (Hrsg.): Software Management 2002 – Fortschritt durch Beständigkeit

P-24 Rainer Eckstein, Robert Tolksdorf (Hrsg.): XMIDX 2003 – XML-Technologien für Middleware – Middleware für XML-Anwendungen

P-25 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Commerce – Anwendungen und Perspektiven – 3. Workshop Mobile Commerce, Universität Augsburg, 04.02.2003

P-26 Gerhard Weikum, Harald Schöning, Erhard Rahm (Hrsg.): BTW 2003: Datenbanksysteme für Business, Technologie und Web

P-27 Michael Kroll, Hans-Gerd Lipinski, Kay Melzer (Hrsg.): Mobiles Computing in der Medizin

P-28 Ulrich Reimer, Andreas Abecker, Steffen Staab, Gerd Stumme (Hrsg.): WM 2003: Professionelles Wissensmanagement – Er-fahrungen und Visionen

P-29 Antje Düsterhöft, Bernhard Thalheim (Eds.): NLDB'2003: Natural Language Processing and Information Systems

P-30 Mikhail Godlevsky, Stephen Liddle, Heinrich C. Mayr (Eds.): Information Systems Technology and its Applications

P-31 Arslan Brömme, Christoph Busch (Eds.): BIOSIG 2003: Biometrics and Electronic Signatures

P-32 Peter Hubwieser (Hrsg.): Informatische Fachkonzepte im Unterricht – INFOS 2003

P-33 Andreas Geyer-Schulz, Alfred Taudes (Hrsg.): Informationswirtschaft: Ein Sektor mit Zukunft

P-34 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 1)

P-35 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 2)

P-36 Rüdiger Grimm, Hubert B. Keller, Kai Rannenberg (Hrsg.): Informatik 2003 – Mit Sicherheit Informatik

P-37 Arndt Bode, Jörg Desel, Sabine Rathmayer, Martin Wessner (Hrsg.): DeLFI 2003: e-Learning Fachtagung Informatik

P-38 E.J. Sinz, M. Plaha, P. Neckel (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2003

P-39 Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.): IT-Incident Management & IT-Forensics – IMF 2003

P-40 Michael Rebstock (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2004

P-41 Uwe Brinkschulte, Jürgen Becker, Dietmar Fey, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle, Thomas Runkler (Edts.): ARCS 2004 – Organic and Pervasive Computing

P-42 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Economy – Transaktionen und Prozesse, Anwendungen und Dienste

P-43 Birgitta König-Ries, Michael Klein, Philipp Obreiter (Hrsg.): Persistance, Scalability, Transactions – Database Mechanisms for Mobile Applications

P-44 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): Security, E-Learning. E-Services

P-45 Bernhard Rumpe, Wofgang Hesse (Hrsg.): Modellierung 2004

P-46 Ulrich Flegel, Michael Meier (Hrsg.): Detection of Intrusions of Malware & Vulnerability Assessment

P-47 Alexander Prosser, Robert Krimmer (Hrsg.): Electronic Voting in Europe – Technology, Law, Politics and Society

P-48 Anatoly Doroshenko, Terry Halpin, Stephen W. Liddle, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications

P-49 G. Schiefer, P. Wagner, M. Morgenstern, U. Rickert (Hrsg.): Integration und Datensicherheit – Anforderungen, Konflikte und Perspektiven

P-50 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 1) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-51 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 2) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-52 Gregor Engels, Silke Seehusen (Hrsg.): DELFI 2004 – Tagungsband der 2. e-Learning Fachtagung Informatik

P-53 Robert Giegerich, Jens Stoye (Hrsg.): German Conference on Bioinformatics – GCB 2004

P-54 Jens Borchers, Ralf Kneuper (Hrsg.): Softwaremanagement 2004 – Outsourcing und Integration

P-55 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): E-Science und Grid Ad-hoc-Netze Medienintegration

P-56 Fernand Feltz, Andreas Oberweis, Benoit Otjacques (Hrsg.): EMISA 2004 – Informationssysteme im E-Business und E-Government

P-57 Klaus Turowski (Hrsg.): Architekturen, Komponenten, Anwendungen

P-58 Sami Beydeda, Volker Gruhn, Johannes Mayer, Ralf Reussner, Franz Schweiggert (Hrsg.): Testing of Component-Based Systems and Software Quality

P-59 J. Felix Hampe, Franz Lehner, Key Pousttchi, Kai Ranneberg, Klaus Turowski (Hrsg.): Mobile Business – Processes, Platforms, Payments

P-60 Steffen Friedrich (Hrsg.): Unterrichtskonzepte für informatische Bildung

P-61 Paul Müller, Reinhard Gotzhein, Jens B. Schmitt (Hrsg.): Kommunikation in verteilten Systemen

P-62 Federrath, Hannes (Hrsg.): „Sicherheit 2005“ – Sicherheit – Schutz und Zuverlässigkeit

P-63 Roland Kaschek, Heinrich C. Mayr, Stephen Liddle (Hrsg.): Information Systems – Technology and ist Applications

P-64 Peter Liggesmeyer, Klaus Pohl, Michael Goedicke (Hrsg.): Software Engineering 2005

P-65 Gottfried Vossen, Frank Leymann, Peter Lockemann, Wolffried Stucky (Hrsg.): Datenbanksysteme in Business, Technologie und Web

P-66 Jörg M. Haake, Ulrike Lucke, Djamshid Tavangarian (Hrsg.): DeLFI 2005: 3. deutsche e-Learning Fachtagung Informatik

P-67 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 1)

P-68 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 2)

P-69 Robert Hirschfeld, Ryszard Kowalcyk, Andreas Polze, Matthias Weske (Hrsg.): NODe 2005, GSEM 2005

P-70 Klaus Turowski, Johannes-Maria Zaha (Hrsg.): Component-oriented Enterprise Application (COAE 2005)

P-71 Andrew Torda, Stefan Kurz, Matthias Rarey (Hrsg.): German Conference on Bioinformatics 2005

P-72 Klaus P. Jantke, Klaus-Peter Fähnrich, Wolfgang S. Wittig (Hrsg.): Marktplatz Internet: Von e-Learning bis e-Payment

P-73 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): "Heute schon das Morgen sehen“

P-74 Christopher Wolf, Stefan Lucks, Po-Wah Yau (Hrsg.): WEWoRC 2005 – Western European Workshop on Research in Cryptology

P-75 Jörg Desel, Ulrich Frank (Hrsg.): Enterprise Modelling and Information Systems Architecture

P-76 Thomas Kirste, Birgitta König-Riess, Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Informationssysteme – Potentiale, Hindernisse, Einsatz

P-77 Jana Dittmann (Hrsg.): SICHERHEIT 2006

P-78 K.-O. Wenkel, P. Wagner, M. Morgenstern, K. Luzi, P. Eisermann (Hrsg.): Land- und Ernährungswirtschaft im Wandel

P-79 Bettina Biel, Matthias Book, Volker Gruhn (Hrsg.): Softwareengineering 2006

P-80 Mareike Schoop, Christian Huemer, Michael Rebstock, Martin Bichler (Hrsg.): Service-Oriented Electronic Commerce

P-81 Wolfgang Karl, Jürgen Becker, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle (Hrsg.): ARCS´06

P-82 Heinrich C. Mayr, Ruth Breu (Hrsg.): Modellierung 2006

P-83 Daniel Huson, Oliver Kohlbacher, Andrei Lupas, Kay Nieselt and Andreas Zell (eds.): German Conference on Bioinformatics

P-84 Dimitris Karagiannis, Heinrich C. Mayr, (Hrsg.): Information Systems Technology and its Applications

P-85 Witold Abramowicz, Heinrich C. Mayr, (Hrsg.): Business Information Systems

P-86 Robert Krimmer (Ed.): Electronic Voting 2006

P-87 Max Mühlhäuser, Guido Rößling, Ralf Steinmetz (Hrsg.): DELFI 2006: 4. e-Learning Fachtagung Informatik

P-88 Robert Hirschfeld, Andreas Polze, Ryszard Kowalczyk (Hrsg.): NODe 2006, GSEM 2006

P-90 Joachim Schelp, Robert Winter, Ulrich Frank, Bodo Rieger, Klaus Turowski (Hrsg.): Integration, Informationslogistik und Architektur

P-91 Henrik Stormer, Andreas Meier, Michael Schumacher (Eds.): European Conference on eHealth 2006

P-92 Fernand Feltz, Benoît Otjacques, Andreas Oberweis, Nicolas Poussing (Eds.): AIM 2006

P-93 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 1

P-94 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 2

P-95 Matthias Weske, Markus Nüttgens (Eds.): EMISA 2005: Methoden, Konzepte und Technologien für die Entwicklung von dienstbasierten Informationssystemen

P-96 Saartje Brockmans, Jürgen Jung, York Sure (Eds.): Meta-Modelling and Ontologies

P-97 Oliver Göbel, Dirk Schadt, Sandra Frings, Hardo Hase, Detlef Günther, Jens Nedon (Eds.): IT-Incident Mangament & IT-Forensics – IMF 2006

P-98 Hans Brandt-Pook, Werner Simonsmeier und Thorsten Spitta (Hrsg.): Beratung in der Softwareentwicklung – Modelle, Methoden, Best Practices

P-99 Andreas Schwill, Carsten Schulte, Marco Thomas (Hrsg.): Didaktik der Informatik

P-100 Peter Forbrig, Günter Siegel, Markus Schneider (Hrsg.): HDI 2006: Hochschuldidaktik der Informatik

P-101 Stefan Böttinger, Ludwig Theuvsen, Susanne Rank, Marlies Morgenstern (Hrsg.): Agrarinformatik im Spannungsfeld zwischen Regionalisierung und globalen Wertschöpfungsketten

P-102 Otto Spaniol (Eds.): Mobile Services and Personalized Environments

P-103 Alfons Kemper, Harald Schöning, Thomas Rose, Matthias Jarke, Thomas Seidl, Christoph Quix, Christoph Brochhaus (Hrsg.): Datenbanksysteme in Business, Technologie und Web (BTW 2007)

P-104 Birgitta König-Ries, Franz Lehner, Rainer Malaka, Can Türker (Hrsg.)
MMS 2007: Mobilität und mobile Informationssysteme

P-105 Wolf-Gideon Bleek, Jörg Raasch, Heinz Züllighoven (Hrsg.)
Software Engineering 2007

P-106 Wolf-Gideon Bleek, Henning Schwentner, Heinz Züllighoven (Hrsg.)
Software Engineering 2007 – Beiträge zu den Workshops

P-107 Heinrich C. Mayr, Dimitris Karagiannis (eds.)
Information Systems
Technology and its Applications

P-108 Arslan Brömme, Christoph Busch, Detlef Hühnlein (eds.)
BIOSIG 2007:
Biometrics and
Electronic Signatures

P-109 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.)
INFORMATIK 2007
Informatik trifft Logistik
Band 1

P-110 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.)
INFORMATIK 2007
Informatik trifft Logistik
Band 2

P-111 Christian Eibl, Johannes Magenheim, Sigrid Schubert, Martin Wessner (Hrsg.)
DeLFI 2007:
5. e-Learning Fachtagung
Informatik

P-112 Sigrid Schubert (Hrsg.)
Didaktik der Informatik in
Theorie und Praxis

P-113 Sören Auer, Christian Bizer, Claudia Müller, Anna V. Zhdanova (Eds.)
The Social Semantic Web 2007
Proceedings of the 1st Conference on Social Semantic Web (CSSW)

P-114 Sandra Frings, Oliver Göbel, Detlef Günther, Hardo G. Hase, Jens Nedon, Dirk Schadt, Arslan Brömme (Eds.)
IMF2007 IT-incident
management & IT-forensics
Proceedings of the 3rd International Conference on IT-Incident Management & IT-Forensics

P-115 Claudia Falter, Alexander Schliep, Joachim Selbig, Martin Vingron and Dirk Walther (Eds.)
German conference on bioinformatics
GCB 2007

P-116 Witold Abramowicz, Leszek Maciszek (Eds.)
Business Process and Services Computing
1st International Working Conference on Business Process and Services Computing
BPSC 2007

P-117 Ryszard Kowalczyk (Ed.)
Grid service engineering and manegement
The 4th International Conference on Grid Service Engineering and Management
GSEM 2007

P-118 Andreas Hein, Wilfried Thoben, Hans-Jürgen Appelrath, Peter Jensch (Eds.)
European Conference on ehealth 2007

P-119 Manfred Reichert, Stefan Strecker, Klaus Turowski (Eds.)
Enterprise Modelling and Information Systems Architectures
Concepts and Applications

P-120 Adam Pawlak, Kurt Sandkuhl, Wojciech Cholewa, Leandro Soares Indrusiak (Eds.)
Coordination of Collaborative Engineering - State of the Art and Future Challenges

P-121 Korbinian Herrmann, Bernd Bruegge (Hrsg.)
Software Engineering 2008
Fachtagung des GI-Fachbereichs Softwaretechnik

P-122 Walid Maalej, Bernd Bruegge (Hrsg.)
Software Engineering 2008 - Workshopband
Fachtagung des GI-Fachbereichs Softwaretechnik

P-123 Michael H. Breitner, Martin Breunig, Elgar Fleisch, Ley Pousttchi, Klaus Turowski (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Technologien, Prozesse, Marktfähigkeit
Proceedings zur 3. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2008)

P-124 Wolfgang E. Nagel, Rolf Hoffmann, Andreas Koch (Eds.)
9th Workshop on Parallel Systems and Algorithms (PASA)
Workshop of the GI/ITG Speciel Interest Groups PARS and PARVA

P-125 Rolf A.E. Müller, Hans-H. Sundermeier, Ludwig Theuvsen, Stephanie Schütze, Marlies Morgenstern (Hrsg.)
Unternehmens-IT: Führungsinstrument oder Verwaltungsbürde
Referate der 28. GIL Jahrestagung

P-126 Rainer Gimnich, Uwe Kaiser, Jochen Quante, Andreas Winter (Hrsg.)
10th Workshop Software Reengineering (WSR 2008)

P-127 Thomas Kühne, Wolfgang Reisig, Friedrich Steimann (Hrsg.)
Modellierung 2008

P-128 Ammar Alkassar, Jörg Siekmann (Hrsg.)
Sicherheit 2008
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)
2.-4. April 2008
Saarbrücken, Germany

P-129 Wolfgang Hesse, Andreas Oberweis (Eds.)
Sigsand-Europe 2008
Proceedings of the Third AIS SIGSAND European Symposium on Analysis, Design, Use and Societal Impact of Information Systems

P-130 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
1. DFN-Forum Kommunikations-technologien Beiträge der Fachtagung

P-131 Robert Krimmer, Rüdiger Grimm (Eds.)
3rd International Conference on Electronic Voting 2008
Co-organized by Council of Europe, Gesellschaft für Informatik and E-Voting. CC

P-132 Silke Seehusen, Ulrike Lucke, Stefan Fischer (Hrsg.)
DeLFI 2008:
Die 6. e-Learning Fachtagung Informatik

P-133 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 1

P-134 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 2

P-135 Torsten Brinda, Michael Fothe, Peter Hubwieser, Kirsten Schlüter (Hrsg.)
Didaktik der Informatik –
Aktuelle Forschungsergebnisse

P-136 Andreas Beyer, Michael Schroeder (Eds.)
German Conference on Bioinformatics
GCB 2008

P-137 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2008: Biometrics and Electronic Signatures

P-138 Barbara Dinter, Robert Winter, Peter Chamoni, Norbert Gronau, Klaus Turowski (Hrsg.)
Synergien durch Integration und Informationslogistik
Proceedings zur DW2008

P-139 Georg Herzwurm, Martin Mikusz (Hrsg.)
Industrialisierung des Software-Managements
Fachtagung des GI-Fachausschusses Management der Anwendungsentwicklung und -wartung im Fachbereich Wirtschaftsinformatik

P-140 Oliver Göbel, Sandra Frings, Detlef Günther, Jens Nedon, Dirk Schadt (Eds.)
IMF 2008 - IT Incident Management & IT Forensics

P-141 Peter Loos, Markus Nüttgens, Klaus Turowski, Dirk Werth (Hrsg.)
Modellierung betrieblicher Informations-systeme (MobIS 2008)
Modellierung zwischen SOA und Compliance Management

P-142 R. Bill, P. Korduan, L. Theuvsen, M. Morgenstern (Hrsg.)
Anforderungen an die Agrarinformatik durch Globalisierung und Klimaveränderung

P-143 Peter Liggesmeyer, Gregor Engels, Jürgen Münch, Jörg Dörr, Norman Riegel (Hrsg.)
Software Engineering 2009
Fachtagung des GI-Fachbereichs Softwaretechnik

P-144 Johann-Christoph Freytag, Thomas Ruf,
Wolfgang Lehner, Gottfried Vossen
(Hrsg.)
Datenbanksysteme in Business,
Technologie und Web (BTW)

P-145 Knut Hinkelmann, Holger Wache (Eds.)
WM2009: 5th Conference on Professional
Knowledge Management

P-146 Markus Bick, Martin Breunig,
Hagen Höpfner (Hrsg.)
Mobile und Ubiquitäre
Informationssysteme – Entwicklung,
Implementierung und Anwendung
4. Konferenz Mobile und Ubiquitäre
Informationssysteme (MMS 2009)

P-147 Witold Abramowicz, Leszek Maciaszek,
Ryszard Kowalczyk, Andreas Speck (Eds.)
Business Process, Services Computing
and Intelligent Service Management
BPSC 2009 · ISM 2009 · YRW-MBP
2009

P-148 Christian Erfurth, Gerald Eichler,
Volkmar Schau (Eds.)
9th International Conference on Innovative
Internet Community Systems
I^{2}CS 2009

P-149 Paul Müller, Bernhard Neumair,
Gabi Dreo Rodosek (Hrsg.)
2. DFN-Forum
Kommunikationstechnologien
Beiträge der Fachtagung

P-150 Jürgen Münch, Peter Liggesmeyer (Hrsg.)
Software Engineering
2009 - Workshopband

P-151 Armin Heinzl, Peter Dadam, Stefan Kirn,
Peter Lockemann (Eds.)
PRIMIUM
Process Innovation for
Enterprise Software

P-152 Jan Mendling, Stefanie Rinderle-Ma,
Werner Esswein (Eds.)
Enterprise Modelling and Information
Systems Architectures
Proceedings of the 3rd Int‘l Workshop
EMISA 2009

P-153 Andreas Schwill,
Nicolas Apostolopoulos (Hrsg.)
Lernen im Digitalen Zeitalter
DeLFI 2009 – Die 7. E-Learning
Fachtagung Informatik

P-154 Stefan Fischer, Erik Maehle
Rüdiger Reischuk (Hrsg.)
INFORMATIK 2009
Im Focus das Leben

P-155 Arslan Brömme, Christoph Busch,
Detlef Hühnlein (Eds.)
BIOSIG 2009:
Biometrics and Electronic Signatures
Proceedings of the Special Interest Group
on Biometrics and Electronic Signatures

P-156 Bernhard Koerber (Hrsg.)
Zukunft braucht Herkunft
25 Jahre »INFOS – Informatik und
Schule«

P-157 Ivo Grosse, Steffen Neumann,
Stefan Posch, Falk Schreiber,
Peter Stadler (Eds.)
German Conference on Bioinformatics
2009

P-158 W. Claupein, L. Theuvsen, A. Kämpf,
M. Morgenstern (Hrsg.)
Precision Agriculture
Reloaded – Informationsgestützte
Landwirtschaft

P-159 Gregor Engels, Markus Luckey,
Wilhelm Schäfer (Hrsg.)
Software Engineering 2010

P-160 Gregor Engels, Markus Luckey,
Alexander Pretschner, Ralf Reussner
(Hrsg.)
Software Engineering 2010 –
Workshopband
(inkl. Doktorandensymposium)

P-161 Gregor Engels, Dimitris Karagiannis
Heinrich C. Mayr (Hrsg.)
Modellierung 2010

P-162 Maria A. Wimmer, Uwe Brinkhoff,
Siegfried Kaiser, Dagmar Lück-
Schneider, Erich Schweighofer,
Andreas Wiebe (Hrsg.)
Vernetzte IT für einen effektiven Staat
Gemeinsame Fachtagung
Verwaltungsinformatik (FTVI) und
Fachtagung Rechtsinformatik (FTRI) 2010

P-163 Markus Bick, Stefan Eulgem,
Elgar Fleisch, J. Felix Hampe,
Birgitta König-Ries, Franz Lehner,
Key Pousttchi, Kai Rannenberg (Hrsg.)
Mobile und Ubiquitäre
Informationssysteme
Technologien, Anwendungen und
Dienste zur Unterstützung von mobiler
Kollaboration

P-164 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2010: Biometrics and Electronic
Signatures Proceedings of the Special
Interest Group on Biometrics and
Electronic Signatures

P-165 Gerald Eichler, Peter Kropf,
Ulrike Lechner, Phayung Meesad,
Herwig Unger (Eds.)
10th International Conference on
Innovative Internet Community Systems
(I^{2}CS) – Jubilee Edition 2010 –

P-166 Paul Müller, Bernhard Neumair,
Gabi Dreo Rodosek (Hrsg.)
3. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

P-167 Robert Krimmer, Rüdiger Grimm (Eds.)
4th International Conference on
Electronic Voting 2010
co-organized by the Council of Europe,
Gesellschaft für Informatik and
E-Voting.CC

P-168 Ira Diethelm, Christina Dörge,
Claudia Hildebrandt,
Carsten Schulte (Hrsg.)
Didaktik der Informatik
Möglichkeiten empirischer
Forschungsmethoden und Perspektiven
der Fachdidaktik

P-169 Michael Kerres, Nadine Ojstersek
Ulrik Schroeder, Ulrich Hoppe (Hrsg.)
DeLFI 2010 - 8. Tagung
der Fachgruppe E-Learning
der Gesellschaft für Informatik e.V.

P-170 Felix C. Freiling (Hrsg.)
Sicherheit 2010
Sicherheit, Schutz und Zuverlässigkeit

P-171 Werner Esswein, Klaus Turowski,
Martin Juhrisch (Hrsg.)
Modellierung betrieblicher
Informationssysteme (MobIS 2010)
Modellgestütztes Management

P-172 Stefan Klink, Agnes Koschmider
Marco Mevius, Andreas Oberweis (Hrsg.)
EMISA 2010
Einflussfaktoren auf die Entwicklung
flexibler, integrierter Informationssysteme
Beiträge des Workshops
der GI-Fachgruppe EMISA
(Entwicklungsmethoden für Informationssysteme und deren Anwendung)

P-173 Dietmar Schomburg,
Andreas Grote (Eds.)
German Conference on Bioinformatics
2010

P-174 Arslan Brömme, Torsten Eymann,
Detlef Hühnlein, Heiko Roßnagel,
Paul Schmücker (Hrsg.)
perspeGKtive 2010
Workshop „Innovative und sichere
Informationstechnologie für das
Gesundheitswesen von morgen“

P-175 Klaus-Peter Fähnrich,
Bogdan Franczyk (Hrsg.)
INFORMATIK 2010
Service Science – Neue Perspektiven für
die Informatik
Band 1

P-176 Klaus-Peter Fähnrich,
Bogdan Franczyk (Hrsg.)
INFORMATIK 2010
Service Science – Neue Perspektiven für
die Informatik
Band 2

P-177 Witold Abramowicz, Rainer Alt,
Klaus-Peter Fähnrich, Bogdan Franczyk,
Leszek A. Maciaszek (Eds.)
INFORMATIK 2010
Business Process and Service Science –
Proceedings of ISSS and BPSC

P-178 Wolfram Pietsch, Benedikt Krams (Hrsg.)
Vom Projekt zum Produkt
Fachtagung des GI-
Fachausschusses Management der
Anwendungsentwicklung und -wartung
im Fachbereich Wirtschafts-informatik
(WI-MAW), Aachen, 2010

P-179 Stefan Gruner, Bernhard Rumpe (Eds.)
FM+AM`2010
Second International Workshop on
Formal Methods and Agile Methods

P-180 Theo Härder, Wolfgang Lehner,
Bernhard Mitschang, Harald Schöning,
Holger Schwarz (Hrsg.)
Datenbanksysteme für Business,
Technologie und Web (BTW)
14. Fachtagung des GI-Fachbereichs
„Datenbanken und Informationssysteme“
(DBIS)

P-181 Michael Clasen, Otto Schätzel,
Brigitte Theuvsen (Hrsg.)
Qualität und Effizienz durch
informationsgestützte Landwirtschaft,
Fokus: Moderne Weinwirtschaft

P-182 Ronald Maier (Hrsg.)
6th Conference on Professional
Knowledge Management
From Knowledge to Action

P-183 Ralf Reussner, Matthias Grund, Andreas
Oberweis, Walter Tichy (Hrsg.)
Software Engineering 2011
Fachtagung des GI-Fachbereichs
Softwaretechnik

P-184 Ralf Reussner, Alexander Pretschner,
Stefan Jähnichen (Hrsg.)
Software Engineering 2011
Workshopband
(inkl. Doktorandensymposium)

P-185 Hagen Höpfner, Günther Specht,
Thomas Ritz, Christian Bunse (Hrsg.)
MMS 2011: Mobile und ubiquitäre
Informationssysteme Proceedings zur
6. Konferenz Mobile und Ubiquitäre
Informationssysteme (MMS 2011)

P-186 Gerald Eichler, Axel Küpper,
Volkmar Schau, Hacène Fouchal,
Herwig Unger (Eds.)
11th International Conference on
Innovative Internet Community Systems
(I^{2}CS)

P-187 Paul Müller, Bernhard Neumair,
Gabi Dreo Rodosek (Hrsg.)
4. DFN-Forum Kommunikationstechnologien, Beiträge der Fachtagung
20. Juni bis 21. Juni 2011 Bonn

P-188 Holger Rohland, Andrea Kienle,
Steffen Friedrich (Hrsg.)
DeLFI 2011 – Die 9. e-Learning
Fachtagung Informatik
der Gesellschaft für Informatik e.V.
5.–8. September 2011, Dresden

P-189 Thomas, Marco (Hrsg.)
Informatik in Bildung und Beruf
INFOS 2011
14. GI-Fachtagung Informatik und Schule

P-190 Markus Nüttgens, Oliver Thomas,
Barbara Weber (Eds.)
Enterprise Modelling and Information
Systems Architectures (EMISA 2011)

P-191 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2011
International Conference of the
Biometrics Special Interest Group

P-192 Hans-Ulrich Heiß, Peter Pepper, Holger
Schlingloff, Jörg Schneider (Hrsg.)
INFORMATIK 2011
Informatik schafft Communities

P-193 Wolfgang Lehner, Gunther Piller (Hrsg.)
IMDM 2011

P-194 M. Clasen, G. Fröhlich, H. Bernhardt,
K. Hildebrand, B. Theuvsen (Hrsg.)
Informationstechnologie für eine
nachhaltige Landbewirtschaftung
Fokus Forstwirtschaft

P-195 Neeraj Suri, Michael Waidner (Hrsg.)
Sicherheit 2012
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 6. Jahrestagung des
Fachbereichs Sicherheit der
Gesellschaft für Informatik e.V. (GI)

P-196 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2012
Proceedings of the 11th International
Conference of the Biometrics Special
Interest Group

P-197 Jörn von Lucke, Christian P. Geiger,
Siegfried Kaiser, Erich Schweighofer,
Maria A. Wimmer (Hrsg.)
Auf dem Weg zu einer offenen, smarten
und vernetzten Verwaltungskultur
Gemeinsame Fachtagung
Verwaltungsinformatik (FTVI) und
Fachtagung Rechtsinformatik (FTRI)
2012

P-198 Stefan Jähnichen, Axel Küpper,
Sahin Albayrak (Hrsg.)
Software Engineering 2012
Fachtagung des GI-Fachbereichs
Softwaretechnik

P-199 Stefan Jähnichen, Bernhard Rumpe,
Holger Schlingloff (Hrsg.)
Software Engineering 2012
Workshopband

P-200 Gero Mühl, Jan Richling, Andreas
Herkersdorf (Hrsg.)
ARCS 2012 Workshops

P-201 Elmar J. Sinz Andy Schürr (Hrsg.)
Modellierung 2012

P-202 Andrea Back, Markus Bick,
Martin Breunig, Key Pousttchi,
Frédéric Thiesse (Hrsg.)
MMS 2012:Mobile und Ubiquitäre
Informationssysteme

P-203 Paul Müller, Bernhard Neumair,
Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)
5. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

P-204 Gerald Eichler, Leendert W. M.
Wienhofen, Anders Kofod-Petersen,
Herwig Unger (Eds.)
12th International Conference on
Innovative Internet Community Systems
(I2CS 2012)

P-205 Manuel J. Kripp, Melanie Volkamer,
Rüdiger Grimm (Eds.)
5th International Conference on Electronic
Voting 2012 (EVOTE2012)
Co-organized by the Council of Europe,
Gesellschaft für Informatik and E-Voting.CC

P-206 Stefanie Rinderle-Ma,
Mathias Weske (Hrsg.)
EMISA 2012
Der Mensch im Zentrum der Modellierung

P-207 Jörg Desel, Jörg M. Haake,
Christian Spannagel (Hrsg.)
DeLFI 2012: Die 10. e-Learning
Fachtagung Informatik der Gesellschaft
für Informatik e.V.
24.–26. September 2012

P-208 Ursula Goltz, Marcus Magnor,
Hans-Jürgen Appelrath, Herbert Matthies,
Wolf-Tilo Balke, Lars Wolf (Hrsg.)
INFORMATIK 2012

P-209 Hans Brandt-Pook, André Fleer, Thorsten
Spitta, Malte Wattenberg (Hrsg.)
Nachhaltiges Software Management

P-210 Erhard Plödereder, Peter Dencker,
Herbert Klenk, Hubert B. Keller,
Silke Spitzer (Hrsg.)
Automotive – Safety & Security 2012
Sicherheit und Zuverlässigkeit für
automobile Informationstechnik

P-211 M. Clasen, K. C. Kersebaum, A.
Meyer-Aurich, B. Theuvsen (Hrsg.)
Massendatenmanagement in der
Agrar- und Ernährungswirtschaft
Erhebung - Verarbeitung - Nutzung
Referate der 33. GIL-Jahrestagung
20. – 21. Februar 2013, Potsdam

P-212 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2013
Proceedings of the 12th International
Conference of the Biometrics
Special Interest Group
04.–06. September 2013
Darmstadt, Germany

P-213 Stefan Kowalewski,
Bernhard Rumpe (Hrsg.)
Software Engineering 2013
Fachtagung des GI-Fachbereichs
Softwaretechnik

P-214 Volker Markl, Gunter Saake, Kai-Uwe
Sattler, Gregor Hackenbroich, Bernhard Mit
schang, Theo Härder, Veit Köppen (Hrsg.)
Datenbanksysteme für Business,
Technologie und Web (BTW) 2013
13. – 15. März 2013, Magdeburg

P-215 Stefan Wagner, Horst Lichter (Hrsg.)
Software Engineering 2013
Workshopband
(inkl. Doktorandensymposium)
26. Februar – 1. März 2013, Aachen

P-216 Gunter Saake, Andreas Henrich,
Wolfgang Lehner, Thomas Neumann,
Veit Köppen (Hrsg.)
Datenbanksysteme für Business,
Technologie und Web (BTW) 2013 –
Workshopband
11. – 12. März 2013, Magdeburg

P-217 Paul Müller, Bernhard Neumair, Helmut
Reiser, Gabi Dreo Rodosek (Hrsg.)
6. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung
03.–04. Juni 2013, Erlangen

P-218 Andreas Breiter, Christoph Rensing (Hrsg.)
DeLFI 2013: Die 11 e-Learning
Fachtagung Informatik der Gesellschaft
für Informatik e.V. (GI)
8. – 11. September 2013, Bremen

P-219 Norbert Breier, Peer Stechert,
Thomas Wilke (Hrsg.)
Informatik erweitert Horizonte
INFOS 2013
15. GI-Fachtagung Informatik und Schule
26. – 28. September 2013

P-220 Matthias Horbach (Hrsg.)
INFORMATIK 2013
Informatik angepasst an Mensch,
Organisation und Umwelt
16. – 20. September 2013, Koblenz

P-221 Maria A. Wimmer, Marijn Janssen,
Ann Macintosh, Hans Jochen Scholl,
Efthimios Tambouris (Eds.)
Electronic Government and
Electronic Participation
Joint Proceedings of Ongoing Research of
IFIP EGOV and IFIP ePart 2013
16. – 19. September 2013, Koblenz

P-222 Reinhard Jung, Manfred Reichert (Eds.)
Enterprise Modelling
and Information Systems Architectures
(EMISA 2013)
St. Gallen, Switzerland
September 5. – 6. 2013

P-223 Detlef Hühnlein, Heiko Roßnagel (Hrsg.)
Open Identity Summit 2013
10. – 11. September 2013
Kloster Banz, Germany

P-224 Eckhart Hanser, Martin Mikusz, Masud
Fazal-Baqaie (Hrsg.)
Vorgehensmodelle 2013
Vorgehensmodelle – Anspruch und
Wirklichkeit
20. Tagung der Fachgruppe
Vorgehensmodelle im Fachgebiet
Wirtschaftsinformatik (WI-VM) der
Gesellschaft für Informatik e.V.
Lörrach, 2013

P-225 Hans-Georg Fill, Dimitris Karagiannis,
Ulrich Reimer (Hrsg.)
Modellierung 2014
19. – 21. März 2014, Wien

P-226 M. Clasen, M. Hamer, S. Lehnert,
B. Petersen, B. Theuvsen (Hrsg.)
IT-Standards in der Agrar- und
Ernährungswirtschaft Fokus: Risiko- und
Krisenmanagement
Referate der 34. GIL-Jahrestagung
24. – 25. Februar 2014, Bonn

P-227 Wilhelm Hasselbring,
Nils Christian Ehmke (Hrsg.)
Software Engineering 2014
Fachtagung des GI-Fachbereichs
Softwaretechnik
25. – 28. Februar 2014
Kiel, Deutschland

P-228 Stefan Katzenbeisser, Volkmar Lotz,
Edgar Weippl (Hrsg.)
Sicherheit 2014
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 7. Jahrestagung des
Fachbereichs Sicherheit der
Gesellschaft für Informatik e.V. (GI)
19. – 21. März 2014, Wien

P-229 Dagmar Lück-Schneider, Thomas
Gordon, Siegfried Kaiser, Jörn von
Lucke,Erich Schweighofer, Maria
A.Wimmer, Martin G. Löhe (Hrsg.)
Gemeinsam Electronic Government
ziel(gruppen)gerecht gestalten und
organisieren
Gemeinsame Fachtagung
Verwaltungsinformatik (FTVI) und
Fachtagung Rechtsinformatik (FTRI)
2014, 20.-21. März 2014 in Berlin

P-230 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2014
Proceedings of the 13th International
Conference of the Biometrics Special
Interest Group
10. – 12. September 2014 in
Darmstadt, Germany

P-231 Paul Müller, Bernhard Neumair,
Helmut Reiser, Gabi Dreo Rodosek
(Hrsg.)
7. DFN-Forum
Kommunikationstechnologien
16. – 17. Juni 2014
Fulda

P-232 E. Plödereder, L. Grunske, E. Schneider,
D. Ull (Hrsg.)
INFORMATIK 2014
Big Data – Komplexität meistern
22. – 26. September 2014
Stuttgart

P-233 Stephan Trahasch, Rolf Plötzner, Gerhard
Schneider, Claudia Gayer, Daniel Sassiat,
Nicole Wöhrle (Hrsg.)
DeLFI 2014 – Die 12. e-Learning
Fachtagung Informatik
der Gesellschaft für Informatik e.V.
15. – 17. September 2014
Freiburg

P-234 Fernand Feltz, Bela Mutschler, Benoît
Otjacques (Eds.)
Enterprise Modelling and Information
Systems Architectures
(EMISA 2014)
Luxembourg, September 25-26, 2014

P-235 Robert Giegerich,
Ralf Hofestädt,
Tim W. Nattkemper (Eds.)
German Conference on
Bioinformatics 2014
September 28 – October 1
Bielefeld, Germany

P-236 Martin Engstler, Eckhart Hanser,
Martin Mikusz, Georg Herzwurm (Hrsg.)
Projektmanagement und
Vorgehensmodelle 2014
Soziale Aspekte und Standardisierung
Gemeinsame Tagung der Fachgruppen
Projektmanagement (WI-PM) und
Vorgehensmodelle (WI-VM) im
Fachgebiet Wirtschaftsinformatik der
Gesellschaft für Informatik e.V., Stuttgart
2014

P-237 Detlef Hühnlein, Heiko Roßnagel (Hrsg.)
Open Identity Summit 2014
4.–6. November 2014
Stuttgart, Germany

P-238 Arno Ruckelshausen, Hans-Peter
Schwarz, Brigitte Theuvsen (Hrsg.)
Informatik in der Land-, Forst- und
Ernährungswirtschaft
Referate der 35. GIL-Jahrestagung
23. – 24. Februar 2015, Geisenheim

P-239 Uwe Aßmann, Birgit Demuth, Thorsten
Spitta, Georg Püschel, Ronny Kaiser
(Hrsg.)
Software Engineering & Management
2015
17.-20. März 2015, Dresden

P-240 Herbert Klenk, Hubert B. Keller, Erhard
Plödereder, Peter Dencker (Hrsg.)
Automotive – Safety & Security 2015
Sicherheit und Zuverlässigkeit für
automobile Informationstechnik
21.–22. April 2015, Stuttgart

P-241 Thomas Seidl, Norbert Ritter,
Harald Schöning, Kai-Uwe Sattler,
Theo Härder, Steffen Friedrich,
Wolfram Wingerath (Hrsg.)
Datenbanksysteme für Business,
Technologie und Web (BTW 2015)
04. – 06. März 2015, Hamburg

P-242 Norbert Ritter, Andreas Henrich,
Wolfgang Lehner, Andreas Thor,
Steffen Friedrich, Wolfram Wingerath
(Hrsg.)
Datenbanksysteme für Business,
Technologie und Web (BTW 2015) –
Workshopband
02. – 03. März 2015, Hamburg

P-243 Paul Müller, Bernhard Neumair, Helmut
Reiser, Gabi Dreo Rodosek (Hrsg.)
8. DFN-Forum
Kommunikationstechnologien
06.–09. Juni 2015, Lübeck

P-244 Alfred Zimmermann,
Alexander Rossmann (Eds.)
Digital Enterprise Computing
(DEC 2015)
Böblingen, Germany June 25-26, 2015

P-245 Arslan Brömme, Christoph Busch ,
Christian Rathgeb, Andreas Uhl (Eds.)
BIOSIG 2015
Proceedings of the 14th International
Conference of the Biometrics Special
Interest Group
09.–11. September 2015
Darmstadt, Germany

P-246 Douglas W. Cunningham, Petra Hofstedt,
Klaus Meer, Ingo Schmitt (Hrsg.)
INFORMATIK 2015
28.9.-2.10. 2015, Cottbus

P-247 Hans Pongratz, Reinhard Keil (Hrsg.)
DeLFI 2015 – Die 13. E-Learning
Fachtagung Informatik der Gesellschaft
für Informatik e.V. (GI)
1.–4. September 2015
München

P-248 Jens Kolb, Henrik Leopold, Jan Mendling
(Eds.)
Enterprise Modelling and Information
Systems Architectures
Proceedings of the 6th Int. Workshop on
Enterprise Modelling and Information
Systems Architectures, Innsbruck, Austria
September 3-4, 2015

P-249 Jens Gallenbacher (Hrsg.)
Informatik
allgemeinbildend begreifen
INFOS 2015 16. GI-Fachtagung
Informatik und Schule
20.–23. September 2015

P-250 Martin Engstler, Masud Fazal-Baqaie,
Eckhart Hanser, Martin Mikusz,
Alexander Volland (Hrsg.)
Projektmanagement und
Vorgehensmodelle 2015
Hybride Projektstrukturen erfolgreich
umsetzen
Gemeinsame Tagung der Fachgruppen
Projektmanagement (WI-PM) und
Vorgehensmodelle (WI-VM) im
Fachgebiet Wirtschaftsinformatik
der Gesellschaft für Informatik e.V.,
Elmshorn 2015

P-251 Detlef Hühnlein, Heiko Roßnagel,
Raik Kuhlisch, Jan Ziesing (Eds.)
Open Identity Summit 2015
10.–11. November 2015
Berlin, Germany

P-252 Jens Knoop, Uwe Zdun (Hrsg.)
Software Engineering 2016
Fachtagung des GI-Fachbereichs
Softwaretechnik
23.–26. Februar 2016, Wien

P-253 A. Ruckelshausen, A. Meyer-Aurich,
T. Rath, G. Recke, B. Theuvsen (Hrsg.)
Informatik in der Land-, Forst- und
Ernährungswirtschaft
Fokus: Intelligente Systeme – Stand der
Technik und neue Möglichkeiten
Referate der 36. GIL-Jahrestagung
22.-23. Februar 2016, Osnabrück

P-254 Andreas Oberweis, Ralf Reussner (Hrsg.)
Modellierung 2016
2.–4. März 2016, Karlsruhe

P-255 Stefanie Betz, Ulrich Reimer (Hrsg.)
Modellierung 2016 Workshopband
2.–4. März 2016, Karlsruhe

P-256 Michael Meier, Delphine Reinhardt,
Steffen Wendzel (Hrsg.)
Sicherheit 2016
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 8. Jahrestagung des
Fachbereichs Sicherheit der
Gesellschaft für Informatik e.V. (GI)
5.–7. April 2016, Bonn

P-257 Paul Müller, Bernhard Neumair, Helmut
Reiser, Gabi Dreo Rodosek (Hrsg.)
9. DFN-Forum
Kommunikationstechnologien
31. Mai – 01. Juni 2016, Rostock

P-258 Dieter Hertweck, Christian Decker (Eds.)
Digital Enterprise Computing (DEC 2016)
14.–15. Juni 2016, Böblingen

P-259 Heinrich C. Mayr, Martin Pinzger (Hrsg.)
INFORMATIK 2016
26.–30. September 2016, Klagenfurt

P-260 Arslan Brömme, Christoph Busch,
Christian Rathgeb, Andreas Uhl (Eds.)
BIOSIG 2016
Proceedings of the 15th International
Conference of the Biometrics Special
Interest Group
21.–23. September 2016, Darmstadt

P-261 Detlef Rätz, Michael Breidung, Dagmar
Lück-Schneider, Siegfried Kaiser, Erich
Schweighofer (Hrsg.)
Digitale Transformation: Methoden,
Kompetenzen und Technologien für die
Verwaltung
Gemeinsame Fachtagung
Verwaltungsinformatik (FTVI) und
Fachtagung Rechtsinformatik (FTRI) 2016
22.–23. September 2016, Dresden

P-262 Ulrike Lucke, Andreas Schwill,
Raphael Zender (Hrsg.)
DeLFI 2016 – Die 14. E-Learning
Fachtagung Informatik
der Gesellschaft für Informatik e.V. (GI)
11.–14. September 2016, Potsdam

P-263 Martin Engstler, Masud Fazal-Baqaie,
Eckhart Hanser, Oliver Linssen, Martin
Mikusz, Alexander Volland (Hrsg.)
Projektmanagement und
Vorgehensmodelle 2016
Arbeiten in hybriden Projekten: Das
Sowohl-als-auch von Stabilität und
Dynamik
Gemeinsame Tagung der Fachgruppen
Projektmanagement (WI-PM) und
Vorgehensmodelle (WI-VM) im
Fachgebiet Wirtschaftsinformatik
der Gesellschaft für Informatik e.V.,
Paderborn 2016

P-264 Detlef Hühnlein, Heiko Roßnagel,
Christian H. Schunck, Maurizio Talamo
(Eds.)
Open Identity Summit 2016
der Gesellschaft für Informatik e.V. (GI)
13.–14. October 2016, Rome, Italy

The titles can be purchased at:

Köllen Druck + Verlag GmbH
Ernst-Robert-Curtius-Str. 14 · D-53117 Bonn
Fax: +49 (0)228/9898222
E-Mail: druckverlag@koellen.de