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 978-3-88579-645-9

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 in the area of electronic identification and trustworthy end-to-end encryption for example. 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 2015" is to link practical experiences and requirements with academic innovations. Focus areas of this event are research and applications in the area of Identity Management, Trust Services, Open Source, end-to-end encryption and Cloud Computing.

D. Hühnlein, H. Roßnagel, R. Kuhlisch, J. Ziesing (Eds.): Open Identity Summit 2015

251

GI-Edition

Lecture Notes in Informatics

Detlef Hühnlein, Heiko Roßnagel, Raik Kuhlisch, Jan Ziesing (Eds.)

Open Identity Summit 2015

10.–11. November 2015
Berlin, Germany

Proceedings

Detlef Hühnlein, Heiko Roßnagel,
Raik Kuhlisch, Jan Ziesing (Eds.)

Open Identity Summit 2015

10. - 11.11.2015
Berlin, Germany

Gesellschaft für Informatik e.V. (GI)

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

Volume P-251

ISBN 978-3-88579-645-9
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
Raik Kuhlisch | Jan Ziesing
Fraunhofer Institute for Open Communication Systems FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin, Germany
{raik.kuhlisch|jan.ziesing}@fokus.fraunhofer.de

printed by Köllen Druck+Verlag GmbH, Bonn

Preface

Welcome to the "Open Identity Summit 2015" (OID2015), 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 European Association for eIdentity and Security (EEMA), the SSEDIC.2020 project, the TeleTrusT – IT Security Association Germany, the SkIDentity project, which aims at providing trustworthy identities for the cloud, and last but not least the Trusted Cloud program supported by the German government.

The international program committee performed a strong review process according to the LNI guidelines. At least five reviews per paper and 37 percent accepted papers of the 19 submitted papers as full scientific papers guarantee the high quality of presentations. These proceedings cover the topics Mobile eID, Authentication, Cloud and Data Management, Open Source, and Identity 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.

Berlin, November 2015

Detlef Hühnlein
ecsec GmbH

Heiko Roßnagel
Fraunhofer IAO

Raik Kuhlisch
Fraunhofer FOKUS

Jan Ziesing
Fraunhofer FOKUS

Conference Chairs

Jörg Caumanns, Fraunhofer Institute for Open Communication Systems FOKUS
Detlef Hühnlein, ecsec GmbH
Heiko Roßnagel, Fraunhofer Institute for Industrial Engineering IAO

International Program Committee

Bud Bruegger, Germany
Christoph Busch, Germany
Jörg Caumanns, Germany
Roger Dean, United Kingdom
Jos Dumortier, Belgium
Igor Furgel, Germany
Robert Garskamp, Netherlands
Thomas Gross, United Kingdom
Marit Hansen, Germany
Olaf Herden, Germany
Jaap-Henk Hoepman, Netherlands
Gerrit Hornung, Germany
Moritz Horsch, Germany
Detlef Hühnlein, Germany
Tina Hühnlein, Germany
Klaus Junker-Schilling, Germany
Jan Jürjens, Germany
Ulrike Korte, Germany
Michael Kubach, Germany
Raik Kuhlisch, Germany
Andreas Kühne, Germany
Kai Rannenberg, Germany
Herbert Leitold, Austria
Peter Lipp, Austria
Luigi Lo Iacono, Germany
Milan Markovoic Serbia
David Naccache, France
Alexander Nouak, Germany
Sebastian Pape, Germany
Sachar Paulus, Germany
René Peinl, Germany
Henrich C. Pöhls, Germany
Heiko Roßnagel, Germany
Aleksandr Sazonov, Russia
Jörg Schwenk, Germany
Jon Shamah, United Kingdom
Max Tuengerthal, Germany
Tobias Wich, Germany
Alex Wiesmaier, Germany
Jan Zibuschka, Germany
Jan Ziesing, Germany
Frank Zimmermann, Germany

Invited Speakers

Alexander Sazonov, Russia
Robert Bielecki, Luxembourg

Hosts and Partners

SSEDIC (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 SSEDIC.

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.

CRYPTO – Applied Cryptology (http://fg-krypto.gi.de/)
The special interest group "Applied Cryptology" (CRYPTO) within GI e.V. connects users and researchers in the area of cryptology, whereas the scope of activities comprises the design, analysis, implementation and practical application of cryptographic systems.

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.

European Association for eIdentity and Security (EEMA) – (http://www.eema.org/)
For 25 years, EEMA has been Europe’s leading independent, non-profit e-Identity & Security association, working with its European members, governmental bodies, standards organisations and interoperability initiatives throughout Europe to further e-Business and legislation.

SkIDentity Project (http://www.skidentity.de/)
The SkIDentity Project aims at facilitating the use of electronic identity cards (eID) within existing and emerging cloud computing infrastructures in order to provide trustworthy identities for the cloud.

TeleTrusT – IT Security Association Germany (http://www.teletrust.de/)
TeleTrusT is a widespread competence network for IT security comprising members from industry, administration, research as well as national and international partner organizations with similar objectives.

Trusted Cloud Program (http://www.trusted-cloud.de/)
The Trusted Cloud Program is an initiative of the German Federal Ministry of Economics and Technology in which 38 companies and 26 academic institutions are collaborating in 14 projects in order to develop innovative, secure and legally valid technologies for trustworthy Cloud Computing.

Cooperation

Co-locating with

Information Security Solutions Europe (ISSE)
http://www.isse.eu.com/

Supported by

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

Table of Contents

Open Identity Summit 2015 – Regular Research Papers

Open Identity Summit 2015 – Further Conference Contributions

Open Identity Summit 2015

Regular Research Papers

Detlef Hühnlein et al. (Eds.): Open Identity Summit 2015,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2015 15

Identity Management and Cloud Computing in the Automotive Industry: First Empirical Results from a Quantitative Survey

Nicolas Fähnrich[1] Michael Kubach[1]

Abstract: The automotive industry forms a complex network of original equipment manufacturers and suppliers that requires a high level of cooperation in development projects. Therefore, an efficient identity management system is needed to control access to exchanged data and collaboratively used IT-solutions supporting the development process. One of the main requirements for this system is the reliable authentication of engineers of various companies with different credentials. The SkIDentity-Project, which aims at building trusted identities for the cloud, addresses this scenario. In this context, we carried out a quantitative survey to investigate the diffusion and adoption of cloud computing and identity management technologies. First results are presented in this paper and show that although cloud computing is used by approximately half of the companies in the sample, we noticed that with an increasing number of involved parties, the trust in this technology drops significantly. Regarding identity management systems, we found a similar effect. Company-wide identity management systems are used by the majority of the companies but cross-company solutions are not adopted to this extent. Further scrutiny identified a lack of motivation as one of the main reasons for the low diffusion of this technology.

Keywords: Identity Management, IdM, Cloud Computing, Empirical Study, Automotive Industry

1 Introduction

Reliable and secure authentication mechanisms are critical for trustworthy cloud computing that is regarded as to bring significant advantages in various for for the IT-infrastructure of companies in the automotive industry [Ac14]. To ensure a broad user acceptance, the interfaces and authentication processes have to be as user-friendly as possible [Se13]. Systems need to not only be accepted but to be frequently used in order to have the potential to achieve sustainably safer cloud computing systems. Accordingly, there is not only a technological challenge, but the overarching goal to create a high security solution, which respects the needs of all stakeholders with good usability.

One approach to address the challenge of using a federated identity management-approach is being developed in the SkIDentity project [Sk14]. Federated identity management (FidM) enables distributed identity management (IdM) in administratively idendepentend organizations. The mother-organization or a designated third party (Identiy Provider) is responsible for the digital identity of the user in the federation. The SkIDentity project covers technical and organizational aspects, as well as, the legal requirements. Its architecture

[1] Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, firstname.lastname@iao.fraunhofer.de

enables the user to use credentials for strong authentication according to her (or her organization's) choice in various applications. This simplifies the identity management in an environment like the engineering collaboration in the automotive industry. There are different engineers from various parent companies, who work on shared applications and exchange data, while the identity management infrastructure of their parent companies are significantly different.

The goal of the SkIDentity project is to develop a technology that is actually used and therefore provides viable security. As argued by Roßnagel and Zibuschka, the successful adoption of an identity management technology requires the consideration of the interests of all relevant stakeholders for the technology[ZR12]. The survey that forms the basis of this paper is part of the project's stakeholder analysis assesses, the stakeholder requirements and the current situation of cloud computing and identity management in the automotive industry.

In this article we analyze the diffusion of identity management technologies and cloud computing in the automotive industry as there is no current data on these issues available. The structure of this work continues as follows. Section two outlines the scenario in the automotive industry. In section three, we present related articles. Subsequently, in section four we present the study design and results of our empirical analysis, followed by the conclusion in section five.

2 Scenario: Automotive Industry

Globally, the number of car makers (original equipment manufacturers OEM) is fairly low. Since most of them are highly internationalized and target the world-market, the competition is intense. Competitive advantages are often achieved by a fast adoption of new technologies and a short time to market. Within the last two decades, this led to a fundamental change in the development and production processes. Increasingly, these processes are being outsourced to suppliers not only for simple components, but for complex interconnected systems [WRZ14], [Vo04]. Suppliers are categorized as Tier1 to TierN-suppliers accordingly to their position in the supply chain. Tier1-suppliers on the one side interact directly with the OEMs and on the other side with Tier2-suppliers. Tier2-suppliers then receive and develop parts and components from Tier3-suppliers. This extended workbench requires an intensive collaboration between the engineers at OEMs and suppliers in multi-user applications that are hosted locally at one partner or in the future in the cloud [VS02]. The fact that OEMs and TierN-suppliers each cooperate with several, often competing partners makes an effective access control inevitable in order to protect the intellectual capital of each partner.

With an increasing number of employees, the identity management (IdM) of even a single organization can be challenging. When several companies (OEMs, Tier1-, Tier2-, TierN-suppliers) are involved, the realization of a trusted authentication of all participating engineers becomes much more complex. Engineers from different organizations often join and leave projects, their identities have to be kept up-to-date, and credentials have to be rolled

out and collected. Particularly, the different authentication methods and security policies of each organization are a major obstacle. This shows the challenge for identity management in development projects of the automotive industry that can be addressed with the SkIDentity-technology as illustrated in [KÖF14]. However, for the further development of this technology for the automotive scenario a deeper analysis of the state-of-the-art and the requirements are needed.

3 Related Work

In order to identify relevant existing literature in this context, a search in online databases like Google Scholar and Scopus was performed. Our emphasis was on identifying articles with large empirical studies regarding identity management and cloud computing in general.

The search results on cloud computing were significantly larger and included several comparable investigations. In the work of Optiz et al., the technology acceptance of cloud computing was analyzed with empirical data from 100 CIOs and IT managers from stock indexed companies [Op12]. The authors identified the perceived usefulness and perceived ease of use as the critical factors for the technology acceptance. These two factors are in turn influenced by other aspects. Another approach to investigate the adoption of cloud computing was carried out by Chinyao et al. in 2011. In this work an empirical based analysis of 111 companies in Taiwan was used to derive relevant factors [LCW11]. These include top management support, relative advantage, firm size, competitive pressure, and trading partner pressure. As already stated by Fähnrich and Kubach in 2014, the number of publications regarding economic aspects of identity management technologies is fairly low [FK14]. In the work of Kubach et al. the service providers' requirements for eID solutions were investigated using an empirical approach [KRS13]. The findings showed that the surveyed service providers from the leisure sector don't plan to change their authentication methods in the near future. However, there is some interest in certain eID solutions. Furthermore, financial aspects for the users' adoption of identity management solutions were examined in the work of Roßnagel et al. [Ro14]. The findings were obtained by the conduction of a choice-based conjoint analysis and indicate that users prefer simple solutions with an intermediary that manages their data.

4 Empirical Analysis

The basic data and the design of the survey are presented below. In a subsequent section selected results of the study will be shown to give a first insight into the empirical findings of the study.

4.1 Study Design

We chose the method of a quantitative survey sent out in summer 2014 to collect data regarding the identity management and cloud computing technologies used in the auto-

motive industry. The aim of this study is an empirical analysis on the present demand for these technologies and based on these findings a prediction of the future development. These results will be used for the further development of the SkIDentity technology.

The automotive industry, including its OEMs and suppliers, is the target group of this survey. We chose this industry branch due to the complex development processes that involve a high number of companies in a large network. Another reason is the high demand for protection of the intellectual capital of every company. A global revenue of 127 billion US-Dollars in 2014 [Mc15], a high competitive pressure, and a global supplier network indicate that the use of efficient and secure IdM and cloud computing solutions are the most critical in this branch. Moreover, the SkIDentity-project has already developed a technology demonstrator showing that it's technology is basically suited for the industry [KÖF14].

To maximize the response rate, the survey was designed to take no longer than 15 minutes and sent out by e-mail including a link to an online survey. The survey was designed according to the recommendations of [Di07] and similar literature. With 73 usable questionnaires, we achieved an acceptable response rate of 8.4 %. For statistic analysis, SPSS was used.

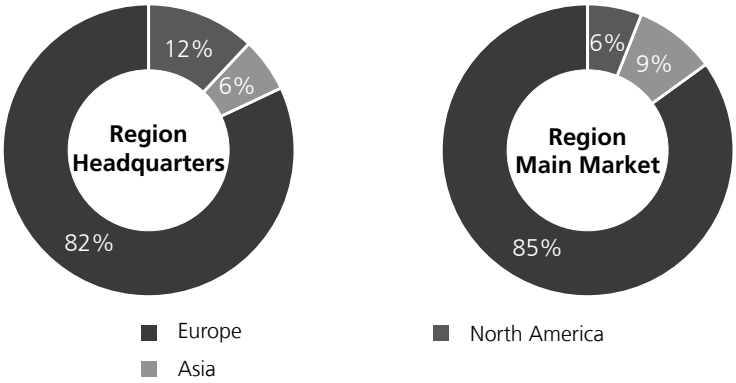

Fig. 1: Headquarters and main markets of sample companies

As shown in figure 1, the majority (82 %) of the surveyed companies are located in Europe. A further 12 % of the companies are located in North America and 6 % in Asia. When comparing this percentage distribution with the respective main markets of the companies, a similar picture as shown in Figure 1 emerges. It becomes apparent that with 85 %, Europe is the main market for most companies. Compared to the location of the company headquarters, Asia is the second largest target market. The results show an international sample with a regional (European) focus. We assessed the size of the sample-companies based on the number of employees and the recorded sales in the last financial year.

As shown in Figure 2, the focus is on companies with less than 5,000 employees and the largest fraction is located between 100 and 499 employees. By comparing this distribution with the turnover shown in Figure 3, clear parallels can be recognized.

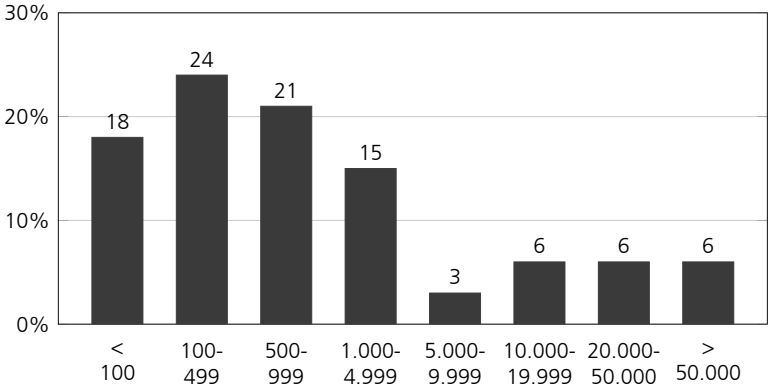

Fig. 2: Size distribution (number of employees) of sample campanies

The small percentages of companies with more than 10,000 employees match the distribution of large sales over 500 million euros. To sum up, we have a wide distribution from small to large companies in our sample.

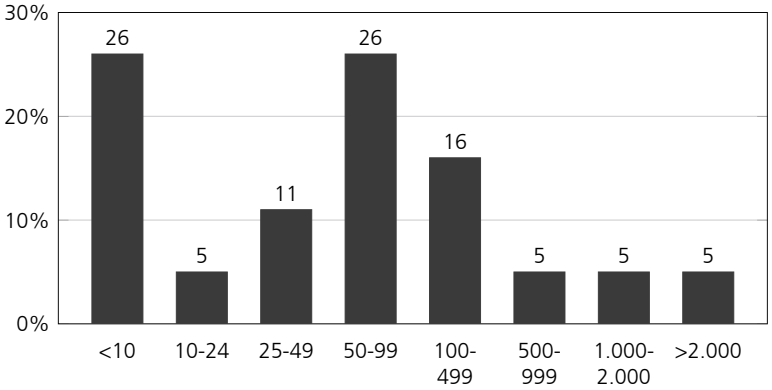

Fig. 3: Size distribution (sales last financial year in million euro)

Figure 4 shows the position in the value chain of the companies in the sample. With 32 %, car manufacturers take the largest share of the surveyed companies, followed by large suppliers with 30 %. Thus, the focus of the survey is on the strong positions of the value chain while other positions are included as well.

The distribution of the functional area of the respondents shows that the IT sector with 78 % is most strongly represented and indicates that the respondents have sufficient technical expertise to ensure a representative questionnaire response. As 60 % of the respondents employ a managerial position or higher it can also expected thay they have the overview and experience to give informed answers.

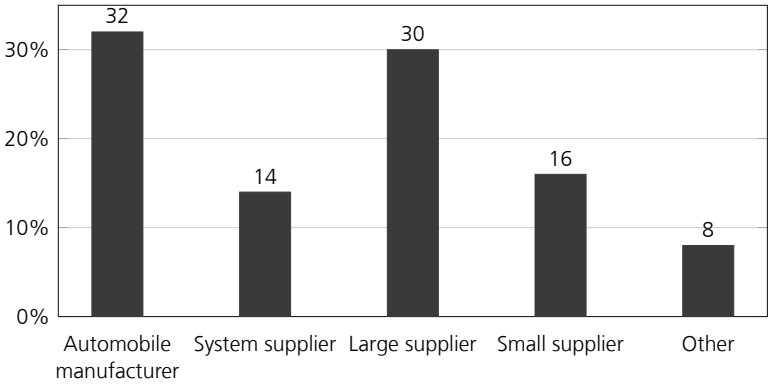

Fig. 4: Value chain position distribution in the sample

4.2 Study Results

Next, the current and anticipated diffusion of cloud computing and identity management technologies in our sample is presented. Further, a deeper analysis of the background circumstances is performed to gain insights regarding the acceptance of these technologies. A primary aim of this analysis is the identification of obstacles that inhibit the diffusion process. The method of frequency statistics is used to capture the current diffusion state. Further investigations are based on Likert-type scales that are evaluated using analysis of means.

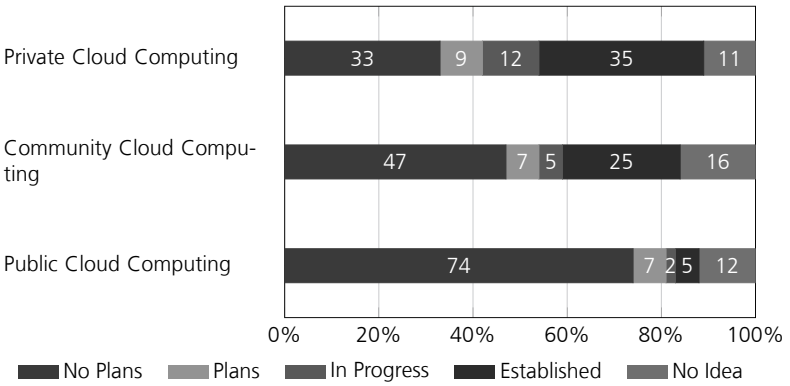

Fig. 5: Diffusion of cloud computing

As shown in Figure 5, cloud computing is categorized into three different types. A cloud solution for a single organization that is either hosted internally or provided by a third party for one single organization is referred to as private cloud computing. The restriction of use to a specifically defined user group like (a part of) the automotive industry is referred to as community cloud computing. The third type is a cloud service that is operated by a service provider and is not limited to a specific user group. Regarding private cloud computing, 33 % of the companies stated that there are no plans on establishing cloud

computing technologies. On the other hand, 35 % of the companies are currently using cloud based solutions and further 21 % are planning to do so or are in the implementation phase. The cumulative comparison between companies that are interested in cloud solutions and companies that are not planning to adapt this technology yields a ratio of 56 % to 33 %. This indicates a high acceptance of private cloud computing solutions among the surveyed companies. However, when it comes to community or public cloud computing technologies, a clear drop in the acceptance is recognizable. The share of companies that are not interested in community cloud computing solutions rises to 47 % and in the case of public cloud computing to 74 %. This result might reflect deficiencies in the trustworthiness and the loss of control as main causes for the low level of acceptance regarding cloud solutions that operate across companies.

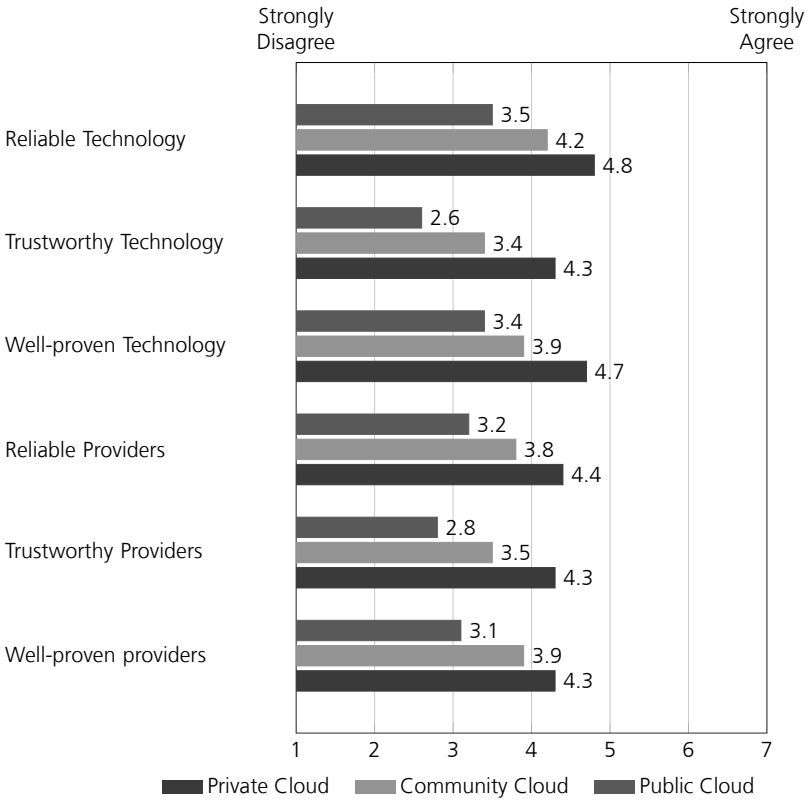

Fig. 6: Perceptions of cloud computing

A further investigation, which is shown in Figure 6, supports this hypothesis. In these items, we asked for the perception of reliability, trustworthiness and whether the re-spondents regard cloud computing as well-proven using a Likert-type scale. A distinction was made between the service itself and the participating providers. High values are never achieved, which shows that cloud computing faces general problems in perception for all three dimensions. As already shown in figure 5, achieved scores decrease in all categories with an increasing number of participating companies in a cloud solution. With all categories

taken into account, a maximum value of 4.8 and a minimum value of 2.6 is reached, which equals a mean value of 3.8. Private clouds manages at least to pass the neutral value of 4. But even these values are not markedly positive. Community clouds as a technology also manage to surpass the value of 4 for reliability, but this is the only item for this technology. Generally, one can conclude that the perception of cloud computing in terms of reliability, being well-proven or trustworthy is rather low. Only for private clouds, this looks a bit more positive. As the differences between the technology itself and the providers are rather low this seems to be a problem of the whole concept cloud computing rather than of the technology or the providers.

Looking at the use of company-wide IdM technologies in Figure 7, we notice a wide dissemination of 83 %, with only 10 % of the companies in the sample stating that there is no demand. This shows that IdM is a widely established security technology. A differentiation of access rights between internal and external access is also widely common in our sample, since 78 % of the companies are allocating customized access rights for connections outside their corporate network. Regarding the cooperation with other companies, 50 % of the surveyed companies state that they are using their IdM system to grant access to internal data and further 13 % state the demand for this handling. This supports the scenario as depicted in chapter 2. Thus, our findings show that IdM solutions are widespread and that the internal IdM is used for external employees as well.

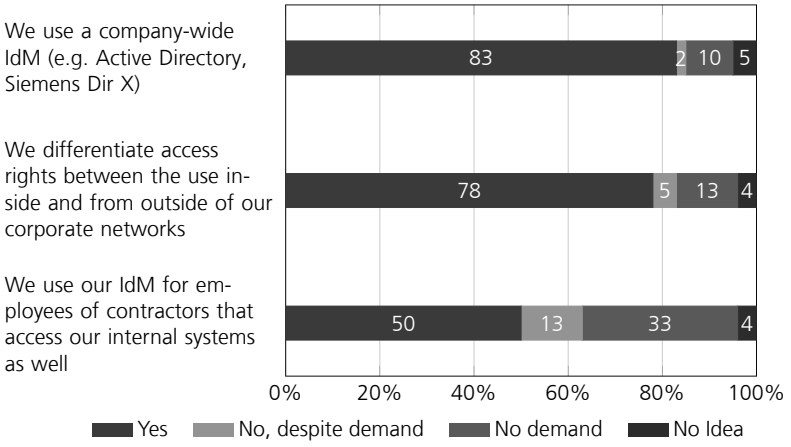

Fig. 7: Use of identity management technologies

Next, we wanted to asses the current state and the future development (plans for the next two years) of authentication methods in the automotive industry. The results are shown in Figure 8. An authentication based on a public-key-infrastructure is the most common method that is either already established or planned. The second most common method is the use of a one time password generator. When cumulating the categories established and plans, both methods reach a value of more than 40 %. The other alternatives achieve significantly lower percentages. The use of biometric data to authenticate a user reaches a cumulated value of 18 %, followed by mobile telephone methods like SMS-TAN with 15 %.

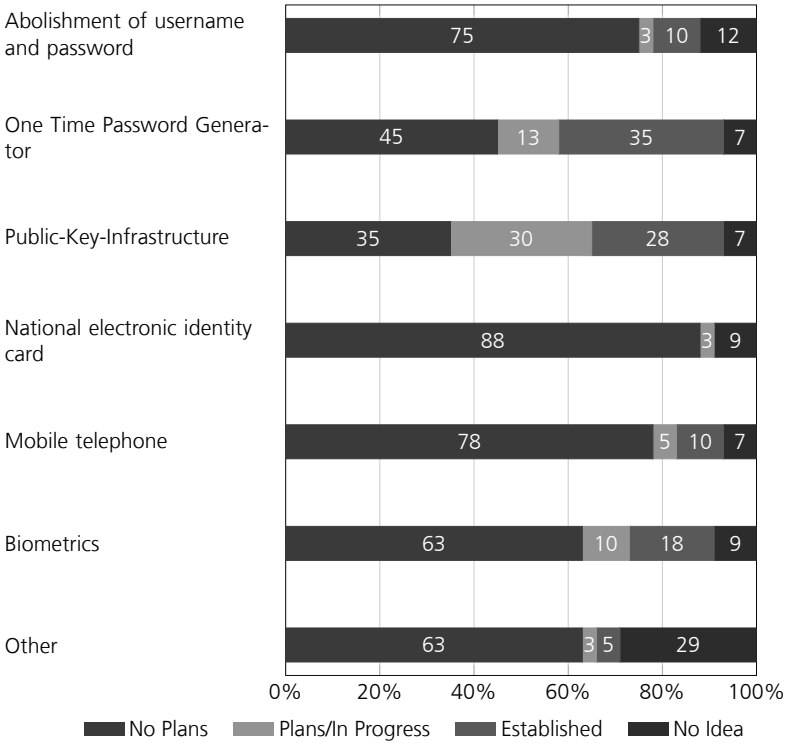

Fig. 8: Status and future (next two years) of authentication methods

Particularly noticeable is the low acceptance of national electronic identity cards like the German neuer Personalausweis as authentication method. None of the surveyed companies are using this authentication method and only 3 % are planning to establish it. Furthermore, only 10 % of the surveyed companies already abolished the classical username and password authentication method and 3 % are planning to do so. 75 % state that there are no plans on abolishing this authentication method. This shows how big the importance of this method still is, although it has been known for a long time that it brings many well known security flaws compared to other strong authentication methods.

Next, we have examined the distribution and acceptance of cross-company IdM solutions as this is the focus of the SkIDentity-project. As shown in Figure 9, about one third of the companies in the sample are already using a cross-company IdM. Futhermore, 18 % are stating the demand for a federated system. Combining these two groups, we see that almost half of the companies are interested in a cross-company IdM compared to 43 % that state no demand. However, turning to the handling of authentication data with other companies we see that only 10 % of the companies are sharing their IdM data with other companies and 65 % are stating no demand. This implies that the willingness to share authentication data is fairly low, which can likely be affiliated to trust issues as shown

earlier regarding cloud computing technologies in general. This, of course, makes it quite difficult to establish a federated identity management.

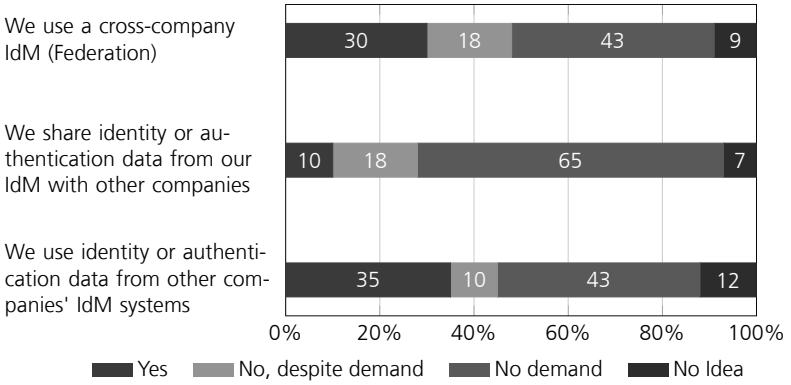

Fig. 9: Cross-company IdM

On the other hand, 35 % of the surveyed companies are using authentication data from other companies' IdM systems and another 10 % are stating the demand for this shared usage model. This imbalance between the willingness to share identity data and the demand for accessing other companies' IdM systems clearly shows the existence of unexploited potential for adapting cross-company IdM solutions. Again, this could reflect trust issues.

A further investigation of the motivating factors for the implementation of cross-company IdM is presented below.

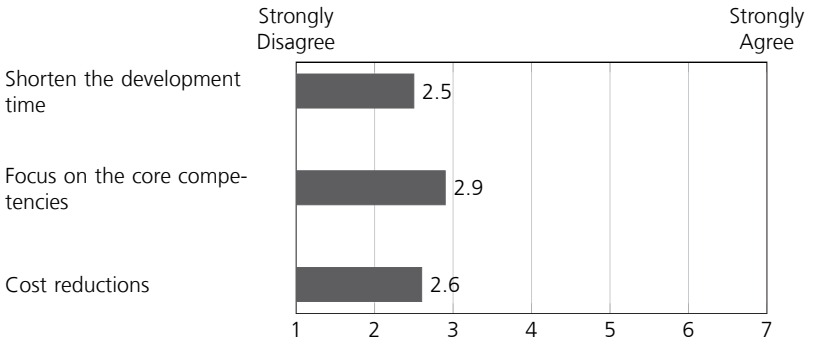

Fig. 10: Motivating factors for the implementation of cross-company IdM

As shown in Figure 10, all factors considered are rated below the value 3 on the scale, indicating that they don't seem that relevant for the integration. Probably other factors that were not listed were more relevant for implementing a cross-company IdM. From the factors that were listed in the survey, an increased focus in the companies' core competencies is the highest rated factor, followed by cost reductions and a shortening of the development time that are both rated at a comparable value. Here further research into these factors, possibly in qualitative form, is clearly recommended.

In order to obtain a complete picture of all relevant factors, we asked for the main barriers against the use of cross-company IdM. The results presented in Figure 11 allow for some differentiation between the factors considered, with a range from 2.9 to 3.8. This result and a low mean value of 3.25 indicates that there's no clear outstanding reason that stands in the way of an increasing diffusion of the cross-company IdM technology. The reason that is the most important is pretty simple: no need for cross-company IdM. However, the second most important barrier are security concerns which shows that the challenge of security (and behind this maybe trust) is still a major obstacle for this technology. All other categories are rated more or less in the same range reaching values around 3.

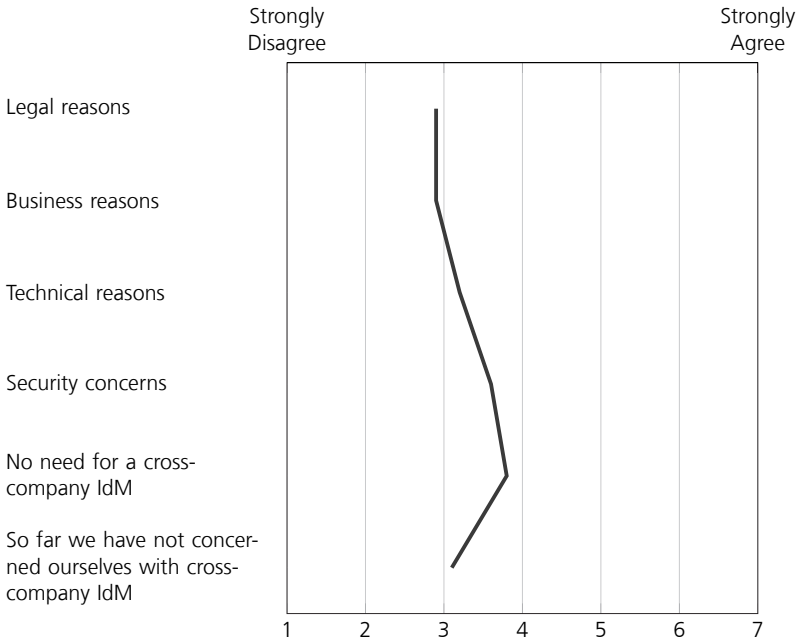

Fig. 11: Barriers to the use of cross-company IdM

5 Conclusion

Our empirical analysis of the diffusion and adoption of identity management and cloud computing technologies in the automotive industry has revealed differentiated results. Private cloud computing solutions are already in use at approximately half of the companies in the sample. However, when it comes to cloud computing with other companies involved, the diffusion is much lower. We showed that with an increasing number of involved parties, the trust in this technology drops significantly. A major reason for this could be the companies' fear of a potential loss of intellectual capital due to trust issues, lack of reliability and as cloud computing is not regarded as well-proven. When looking at identity management technologies, the majority of the companies are using a company-wide IdM with differentiated access rights between internal and external access. The evaluation of authentication methods that are currently in use or planned to be established within the next two years

showed that especially the abolishment of username and password authentication is not intended by most of the companies, which could be seen as a security issue. Regarding more secure authentication methods, a public-key infrastructure is clearly preferred compared to other solutions. Although national electronic identity cards can already be used as credentials and thus offer the potential of cost savings, none of the surveyed companies are using this technique, making this alternative the least attractive solution for this industry branch. Here, solutions like SkIDentity could step in by simplifying the integration of national identity cards for strong authentication. When it comes to cross-company IdM, about half of the surveyed companies stated that they have already established a federated IdM system or state the demand for it. As part of the cooperation with other companies, authentication data of external IdM systems is often used, even though the acceptance of sharing identity data of internal systems is quite low. Hence, we find an immature market with the potential demand for federated IdM. Further investigation of the motivating factors and barriers regarding the use of cross-company IdM shows that the expected benefits are rated quite low and most of the companies still see no need to establish a cross-company solution. Here further research is clearly needed. Moreover, this indicates, that the automotive industry could be sensitized more for the use of these systems in order to achieve a far reaching diffusion. Especially the trustworthiness of federated solutions that can be achieved with solutions like SkIDentity has to be pointed out.

The results of this study are limited by the number of useable questionnaires and the limitation to the automotive industry. In order to reduce potential bias, a numerical extension of the study is recommended. Furthermore, the expansion to other industry branches not directly connected with the automotive industry would be interesting in order to check if the findings of this study are transferable to them.

References

[Ac14] A new era for the automotive industry: How cloud computing will enable automotive companies to change the game.

[Di07] Dillman, Don A: Mail and internet surveys: The tailored design method, volume 47. John Wiley & Sons, 2007.

[FK14] Fähnrich, Nicolas; Kubach, Michael: An Economic Perspective on the State-of-the-Art of Scientific Publications on Identity Management. 2014. Presented at the Scientific Presentation, Open Identity Summit 2014, 4.-6.11.2014, Patras, 2014.

[KÖF14] Kubach, Michael; Özmü, Eray; Flach, Guntram: Secure cloud computing with SkIDentity: A cloud-teamroom for the automotive industry. 2014. Presented at the Scientific Presentation, Open Identity Summit 2014, 4.-6.11.2014, Stuttgart, 2014.

[KRS13] Kubach, Michael; Roßnagel, Heiko; Sellung, Rachelle: Service providers requirements for eID solutions: Empirical evidence from the leisure sector. In: Open Identity Summit 2013 - Lecture Notes in Informatics (LNI) - Proceedings. pp. 69–81, 2013.

[LCW11] Low, Chinyao; Chen, Yahsueh; Wu, Mingchang: Understanding the determinants of cloud computing adoption. Industrial management & data systems, 111(7):1006–1023, 2011.

[Mc15] McKinsey: Gewinne der weltweiten Automobilindustrie im vergangenen Jahr auf Rekordhöhe. 2015.

[Op12] Opitz, Nicky; Langkau, Tobias F; Schmidt, Nils H; Kolbe, Lutz M: Technology acceptance of cloud computing: empirical evidence from German IT departments. In: System Science (HICSS), 2012 45th Hawaii International Conference on. IEEE, pp. 1593–1602, 2012.

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

[Se13] Senk, Christian: Future of Cloud-Based Services for Multi-factor Authentication: Results of a Delphi Study. In: Cloud Computing, pp. 134–144. Springer, 2013.

[Sk14] Skidentity-Project Website, http://www.skidentity.de.

[Vo04] Volpato, Giuseppe: The OEM-FTS relationship in automotive industry. International Journal of Automotive Technology and Management, 4(2-3):166–197, 2004.

[VS02] Volpato, Giuseppe; Stocchetti, Andrea: The role of ICT in the strategic integration of the automotive supply-chain. International Journal of Automotive Technology and Management, 2(3-4):239–260, 2002.

[WRZ14] Wehrenberg, Immo; Roßnagel, Heiko; Zibuschka, Jan: Secure Identities for Engineering Collaboration in the Automotive Industry. Mobility in a Globalised World 2012, 9:202–213, 2014.

[ZR12] Zibuschka, Jan; Roßnagel, Heiko: Stakeholder Economics of Identity Management Infrastructures for the Web. In: Proceedings of the 17th Nordic Workshop on Secure IT Systems (NordSec 2012). 2012.

SSEDIC.2020 on Mobile eID

Michael Kubach[1] Herbert Leitold[2] Heiko Roßnagel[1] Christian H. Schunck[3]
Maurizio Talamo[3]

Abstract: Mobile electronic identity (eID) management solutions are on the rise worldwide and see a rapid take-up by stakeholders. In this paper experts from the SSEDIC.2020 network study and review the status of mobile eID deployment and use in e-government as well as industry with a focus on Europe. The findings demonstrate that mobile eID solutions have the potential to become a major means for digital identification but significant efforts still must be made to drive broad adoption across European member states, to guide secure integration of mobile solutions in the industry and to arrive at dedicated standards.

Keywords: mobile eID, eSignature, eIDAS, secure authentication, identity management, survey

1 Introduction

With the rapidly increasing world-wide use of mobile devices such as smartphones, mobile electronic identity (eID) and mobile signature applications are spreading quickly and are gaining significant traction in the markets where they are deployed. A number of developments further increase the potential of mobile eIDs:

In the EU the eIDAS regulation opens up new application possibilities for mobile eID and signature solutions as notifiable credentials for e-government applications and thus has the potential to drive EU wide adoption of mobile eID solutions [Eu15]. In the US the FIDO Alliance brings forward new technical specifications for online authentication, which are very mobile-friendly and have gained significant traction with the industry [Fi15]. The National Institute for Standards and Technology which hosts the national program office for implementing the National Strategy for Trusted Identities in Cyberspace (NSTIC) [Na15] joined the FIDO Alliance as well and thus connects it closely with the Identity Ecosystem Steering Group (IDESG) [Id15].

However, the opportunities and challenges associated with mobile eID use have not yet been sufficiently addressed within the public and private sectors, as well as regulation and standardization. For this reason SSEDIC.2020 [Ss15a], a large network of experts on digital identity that emerged from the SSEDIC ("Scoping the Single European Digital Identity Community") [Ss15b] thematic network, has decided to expand on the existing SSEDIC theme of mobile eID. The goal is to develop a truly global vision for mobile

[1] Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, firstname.lastname@iao.fraunhofer.de
[2] A-SIT, Inffeldgasse 16a. 8010 Graz, herbert.leitold@a-sit.at
[3] Fondazione Inuit, University of Rome Tor Vergata, Via dell'Archiginnasio snc, 00133 Rome, Italy, firstname.lastname@inuitroma2.it

identity, to point out existing challenges, to encourage best practice sharing and to promote global standardization and interoperability for mobile identity.

This paper is a first step towards developing strategic action plans to encourage adoption in a secure and trusted ecosystem both in the public and private sector and to drive harmonization of mobile authentication mechanisms suitable for eID use. We first look at current deployments of mobile eID in Europe and discuss two exemplary implementations in more detail in section 2, In section 3 we examine the integration of mobile eID solutions in European Commission and government funded research projects. We also analyze the usage of mobile eID in the European industry by example of the automotive sector in section 4 and briefly observe the status of mobile eID in standardization and regulation in section 5, before we summarize our results.

2 Mobile eID in e-government solutions

Mobile identity management solutions have been implemented in more than 35 countries worldwide [Fo15]. In the European Union specific mobile eID solutions have been deployed in four countries: Austria, Estonia, Finland and Lithuania (which adopted the Estonian solution) as well as in the associated country of Iceland [Ge14] and the candidate country Turkey [Gs15]. Compared to the very satisfactory take-up in the countries where these solutions have been released, the number of European countries that have deployed dedicated mobile eID solutions is still small. In the following we will take a closer look at two exemplary cases for these mobile eID initiatives by governments. Austria and Estonia both complemented the traditional smartcard eID with mobile eID. These two mobile eID systems are different both in their technology basis and in organisational aspects.

2.1 Case Study Mobile eID and eSignature in Estonia

In Estonia ID cards and eID are mandatory. All citizens have an active eID card and it is widely used: Since its introduction in 2002, more than 220 million electronic signatures were created and more than 350 million online authentications took place[4]. While the eID card is mandatory, "Mobiil-ID" is optional and was introduced in 2007 [Ma10, Mo15]. Mobile eID needs a special SIM card and the service is charged (1€/month for unlimited transactions). Although there are about ten times less active mobile e-ID users than ID-card/Digi-ID users in Estonia, the mobile e-ID users generate almost one quarter of the total monthly transactions (2.5 million out of 10.5 million transactions[5]). These numbers could in part be attributed to the fact that only those users who are particularly

[4] Figures taken 19 June 2015 at http://www.id.ee: Digital signatures 224 051 414; Active cards: 1 247 479; Electronic authentications: 356 230 150

[5] The data was kindly provided by the Estonian Certification Center Sertifitseerimiskeskus (www.sk.ee) on June 24 2015.

motivated to use their eID credentials very frequently are willing to sign up for a mobile eID at a cost. However, after obtaining the mobile e-ID most people abandon the use of their other Estonian eID credentials almost completely[5]. This strongly suggests that the mobile eID credentials are judged by their users as being the significantly more convenient option. Convenience and user friendliness can in turn be expected to contribute to the observed significantly higher usage rates of mobile eIDs as well.

2.2 Case Study Mobile eID and eSignature in Austria

In Austria eID is voluntary since its introduction in 2003. While there is full penetration of health insurance cards since 2005, its activation (or the activation of other tokens) as eID is a citizen's choice. Mobile eID was first introduced in 2005 by a mobile operator as a charged service, but was ceased in 2008. A similar service got contracted by the government end of 2009. The mobile eID does not need replacement of the SIM and works with any Austrian mobile operator. Both smartcard eID (on the health insurance card) and mobile eID are free of charge for the citizen and include qualified signatures.

The Austrian system is an interesting example for the card eID – mobile eID comparison, as it has similar basic conditions for the citizens for both card eID and mobile eID:

- Practically all citizens possess both tokens (a mobile phone and a health insurance card, probably also other smartcards like student service cards)
- Activation as eID and issuing a qualified signature certificate on it is free of charge for both the health insurance card and the mobile phone
- The activation procedures are comparable (can be done at the same registration offices like tax offices, service centers, etc.; online through the same portals)
- Basically the same eGovernment and private sector services can be used. More than 200 services that can be accessed using either a smartcard eID or the mobile eID are listed at the citizen card portal

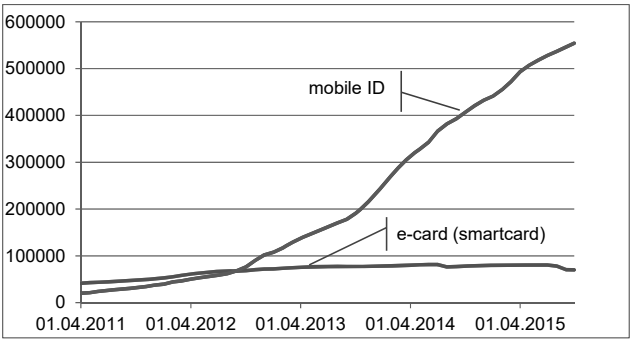

Fig. 1: Active e-cards and mobile eIDs in Austria

A first interesting question when comparing card eID and mobile eID is its take-up by the citizens. The figure above shows the active health smartcard eID (in blue) vs. active mobile eID (in red). As can be seen, mobile eID outperforms smartcard eID by far. This is also the case if considering that other smartcard eIDs exist in Austria that are not shown in the figure (like profession cards of notaries, lawyers, etc.).

Apart from one empirical study on electronic signatures [RH07], which shows that customer segments exist that prefer mobile signatures, no further scientific studies are known to the authors that give a reasoning for these trends. Still it is reasonable to assume that the mobile eID is chosen, as:

- No specific hardware (card-reader) is needed
- No specific software (card-drivers) is needed, just the browser
- Many today's devices like tablets can no longer be used with smartcards
- Mobile eID reflects current lifestyle and Internet access practices like with tablets
- Most citizens carry their mobile phone all the time (most have the health insurance card in their pocket also, though)

3 Mobile eID in selected EU and government funded R&D projects

3.1 SSEDIC Recommendations

SSEDIC.2020 emerged from the thematic network SSEDIC. After an intensive 3-year consultation period together with over 200 European and international digital identity management experts and many stakeholder organizations SSEDIC released a set of recommendations covering four key areas judged as central for the future development of digital identity: mobile identity, attribute usage, authentication and liability [Ta14]. With that SSEDIC recognized mobile identity as key enabler for the adoption of digital identity management solutions. The SSEDIC mobile eID recommendations include suggestions to encourage the acceptance of mobile eIDs as a notifiable credential for eGov use, to review Mobile eSignature/Wireless PKI standards relating to eIDs and to enable access to eGov services via mobile devices regardless of the contractual relationship with mobile providers (similar to emergency calls). The full recommendations are presented in detail in [Ta14].

3.2 FutureID

Practical insights supporting the rising importance of Mobile eIDs come from research in a European identity management-focussed project, where use cases play a major role. In this EU-funded project titled "FutureID - Shaping the Future of Electronic Identity" 19

partners from 9 EU states plus Switzerland and Norway cooperate to build a comprehensive, flexible, privacy-friendly and ubiquitously available identity management infrastructure for Europe to support the EU internal market for online services [Fu15]. The project integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims. The FutureID infrastructure provides benefits to all stakeholders involved in the eID value chain. Users benefit from the availability of a ubiquitously usable open source eID client that is capable of running on arbitrary desktop PCs but also on mobile android-based devices. FutureID allows service providers to easily integrate their existing services with the FutureID infrastructure, providing them with the benefits from the strong security offered by eIDs without requiring them to make substantial investments. To demonstrate the applicability of the developed technologies and the feasibility of the overall approach FutureID has developed two pilot applications as well as a technology demonstrator and is open for additional application services who want to use its technology. Moreover, substantial work on market analysis has been performed in the project. Together with various stakeholders a number of use and business cases have been constructed and evaluated. To this end, qualitative as well as quantitative surveys have been conducted and technology pilots and demonstrators are running. Mobile access is part of some of these use cases. From this look into the practical world of identity management it became even clearer that mobile electronic identity management is vital for secure and trustworthy digital services [Fu14, Fu13a]. This insight is further supported through the findings from the work on Mobile eID and eSignature in Austria [ZTL11].

However, the project does not try to re-invent the wheel. Rather, it builds on already existing elements. Therefore, for example, the Austrian Mobile eID has been integrated into FutureID so that it can be used with the FutureID infrastructure. The Android client is using the Open Mobile API to get access to security modules [Fu13b].

Although a variety of existing and newly developed elements are combined in the FutureID infrastructure, it was determined that it is reasonable to maintain a common user interface on different platforms to minimise confusion. Therefore, a flexible design of the FutureID client enables a similar user experience on different devices that reflect the users' expectations from existing services and functionalities. Therefore, the client has a lightweight GUI that enables platform independence. This is realized through a UI that is based on HTML5 technologies, enabling a responsive design [Fu13c].

3.3 SkIDentity

Another research project that is also working on mobile eIDs is funded by the German Federal Ministry for Economic Affairs and Energy (BMWi) in the "Trusted Cloud" program [Tr15]. The project "SkIDentity – Trusted Identities for the Cloud" is building a stable bridge between electronic identity cards and the existing and emerging cloud computing infrastructures [Sk15]. It aims at providing trusted identities for the cloud and

secure complete business processes and value chains. For this purpose the existing components, services and trust infrastructures are integrated into a comprehensive, legally valid and economically viable identity infrastructure for the cloud and tested in pilot projects. Special attention is given to the demands of small and medium enterprises and public authorities. For example the SkIDentity infrastructure contains an eID-Broker, which will bundle the necessary eID-Services in a form which is accessible even for very small companies and municipal authorities. The project has won several international and German awards like the "European ID and Cloud Award 2015", "EuroCloud Germany Award 2015" and "Land der Ideen" 2014 and 2015 [Sk15].

Using the SkIDentity-Infrastructure, various electronic identity cards like the German eID ("neuer Personalausweis"), the Austrian social insurance card (e-card), the Estonian eID as well as several signature and banking cards from D-Trust, DATEV, S-Trust and GAD can easily be used in cloud and web applications. Moreover, cryptographically secured "Cloud Identities" can be created for pseudonymous authentication or self-determined identity proofing. These "Cloud Identities" can not only be autonomously managed by the user, they can also be transferred securely to almost any smartphone, thereby "mobilising" these eIDs for the use in mobile applications. Service providers that have registered themselves and their online services at the SkIDentity service can allow users to securely identify using their smartphone with the derived mobile eID [Hü15].

3.4 eSENS

The EU Large Scale Pilot (LSPs) eSENS is carried out by twenty EU/EEA member states and candidate countries. The purpose is to consolidate building blocks delivered by sibling LSPs and to pilot these in production environments. Such building blocks are inter alia eID, eSignatures, eDelivery, or eDocuments. eSENS piloting domains are eProcurement, eHealth, business lifecycle, eJustice, and citizen services [Es15]. For the basic building blocks eID and eSignatures eSENS recognises that the success of mobile devices asks for particular attention. One obvious reason is that many mobile devices no longer have the interfaces needed for traditional eID and eSignature means like smartcards. A further reason is a clear preference by users that use mobile devices as their preferred Internet access device.

eSENS addresses the mobile challenge in two dimensions: On the one hand, seamless integration of emerging mobile Id and mobile signature solutions in existing services is needed. On the other hand, states that do not yet have a large scale eID programme may deploy mobile solutions swifter, if they base these on the existing high penetration of mobile devices. The same holds for states that have eID and eSignature solutions but want to augment these as a next generation. The Austrian mobile eID and eSignature solution (cf. section 2.1) can be seen as a showcase: It has been developed in the LSP STORK, design, development, deployment and production integration in services could be achieved in about half a year.

eSENS does not develop mobile eID and eSignature solutions on their own, as little merit is seen if states develop solutions in an area as dynamic as mobile markets. What is developed is reference models on how emerging mobile solutions can be integrated into the states' infrastructure. This included interfaces to the identity basis (like population registers) and the registration infrastructure (like city halls).

4 Mobile eID in Industry and B2B - Automotive sector survey

To shed light on the current market situation for identity management in a business to business context we can present the first results from a quantitative survey in the European automotive industry. The survey in the form of an online questionnaire was conducted in Summer/Fall 2014 and focused on several aspects of electronic identity management in this specific professional context. As the target population was the European automotive industry, we used the customer database of an organization that governs the most important secure communications network of this industry. Respondents were contacted via e-mail and provided with a link to the survey. Follow-up e-mails were used to increase the response rate. Through this approach we received a total of 73 usable questionnaires. A total number of 1122 persons were effectively contacted (subtracting bounced e-mails). Thus, we achieved a response rate of roughly 7 percent. The data were analysed using SPSS. The profile of the respondents and the sample companies is shown in Figure 2 and Figure 3.

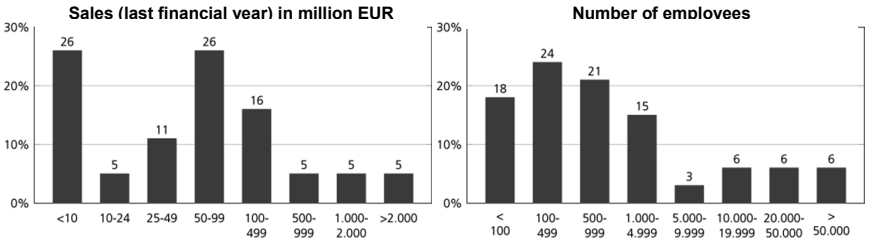

Fig. 2: Size statistics of the sample companies

As can be seen in Fig. 2, our sample covers a wide range of companies, from small to larger ones. Moreover, Fig. 3 shows that companies from different positions in the value chain are represented as well. The main market region of the sample is Europe, with Asia and Northern America being of less importance. This is certainly due to the basic population being customers of the European communication network organization. As SSEDIC 2020 is a project with a European focus this seems appropriate.

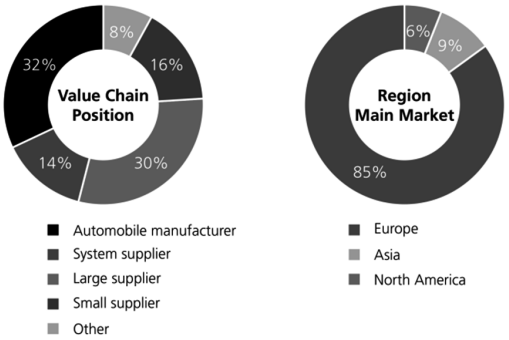

Fig. 3: Value chain position and main market regions of sample companies

The characteristics of the respondents show that most of them work in the IT-department (78 percent), another 13 percent works in the development department (9 percent "other"). IT-security and identity management are very important topics for the development departments due to the sensibility of the development data that is often exchanged with partner companies and the threat of industrial espionage. The respondents on average have 19.6 years of professional experience and work in their company for 14.1 years. Looking at the hierarchical position of the respondents we get a pretty balanced picture and see that 13 percent of the respondents are CEOs/Owners of the companies, 47 percent are on a management level and another 34 percent are employees (6 percent "other"). These data permits us to see the respondents as key informants with sufficient expertise and insight into the topics in question. The key informant approach is a well-established method for conducting survey-research [Ho12]. We can conclude that for a preliminary study the sample is relatively balanced and suitable to give us first insights into the topic.

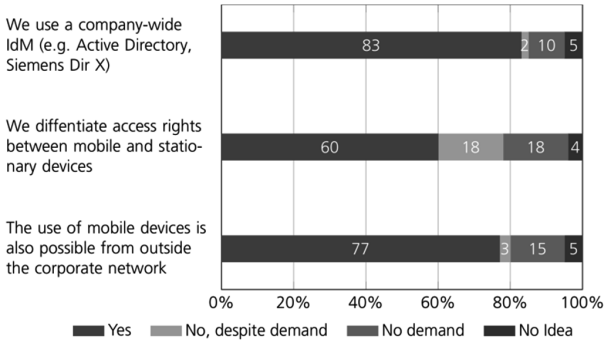

Fig. 4: Use of identity management (IdM) and with mobile devices

In this paper we focus on the parts of the study focusing on mobile aspects in the context

of identity management. Fig. 4 first shows that generally, company-wide identity management is very well-established in the companies included in our sample. More than four-fifths of the companies use such a system. However, it is certainly interesting to note that only 60 percent of the sample companies differentiate in the access rights between mobile and stationary devices. 18 percent of the companies do not differentiate, even though the respondents see a demand for that – a demand that from a security perspective seems to be justified.

In Fig. 5 we show which kind of authentication method the companies in our sample currently used or plan to introduce in the near future (specified as the next two years). Obviously, despite its well-known shortcomings, username and password is still the dominant method for authentication. Three-quarters of the sample companies don't plan to abolish it while only 13 percent plan to do so or already have. As this paper focuses on the mobile aspects we omit a detailed discussion of the various other methods and discuss the use of the mobile telephone as an authentication method. This method, i.e. through SMS-TAN or special software is currently available in 10 percent of the companies. Another 5 percent plan to introduce it in the near future or are in the course of doing so. Thereby, the use of a mobile phone for authentication purposes is less important than all other alternatives to username and password except for national electronic identity cards (that are not yet rolled out in all countries of the European Union and other countries relevant to globally active companies). Public-Key-Infrastructures, One Time Password Generators and Biometric means for authentication are much more common. This means that currently, the relevance of mobile telephones for authentication purposes, despite their ubiquity, is very limited.

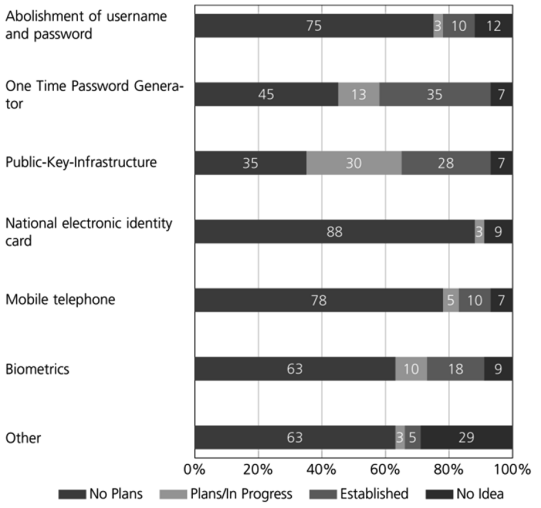

Fig. 5: Authentication method in use, plans to introduce other methods in the near future (approx.

next 2 years)

Summing up the first results from our empirical study we can note that sharing of data, services and application is commonplace in the European automotive industry. However, the development of adequate measures securing this interconnectedness, especially from an identity management perspective, seems to be lagging behind. This becomes especially visible in the mobile sphere. Today, mobile phones are a well-established means for work and are widely used to access (sensitive) data but are rarely integrated into adequate systems for identity management. Hence, mobile electronic identity management is apparently underdeveloped in the European automotive industry which leaves this key industry vulnerable to IT-security threats.

5 Mobile eID in Regulation and Standardization

In regulation and standardization mobile eID and signature solutions are rarely explicitly considered, but are implicitly seen as part of an ecosystem of digital identity management solutions. The eIDAS regulation mentions mobile solutions only once in the context of "innovative solutions and services (such as mobile signing, cloud signing, etc.)". The NSTIC (as a strategy document) mentions cell phones in the context of "existing technology components in wide spread use today" and "identity media". It also states: "mobile phone providers have specific technical needs. Carriers may thus join a trust framework to enable individuals to authenticate using their cell phones as a credential." Overall it appears that the very promising take-up by end-users and industry of mobile eID technologies compared to other approaches is not reflected in the weight given in these documents to mobile eID solutions. This can of course be understood at least in part by efforts to keep such documents as technologically neutral as possible.

Also in standardization domain, specifics of mobile eID solutions are rarely considered in detail. ETSI GS INS 003 "Identity and access management for Networks and Services; Distributed User Profile Management; Using Network Operator as Identity Broker" [Et10] considers mobile carriers and networks as one architecture among others. ISO/IEC 29003 "Information technology - Security techniques - identity proofing" [In12] mentions mobile phones as one of many potential non person entities (NPEs) "or endpoint devices (e.g., mobile phones, PDAs, set-top boxes, laptops)". ITU-T X.1251 "A framework for user control of digital identity" [In13] considers mobile devices together with personal computers as devices into which a user can "plug his/her identity information" in.

However, mobile devices enable a variety of new approaches to identity management that deserve specific attention by standardization bodies. Innovative solutions such as the provision of dynamic attributes through a large variety of sensors [Ta14], efficient means to integrate various biometrics into the authentication process and the integration of dedicated secure elements [Na08] are expected to offer unique and novel opportunities for example to implement efficient step-up authentication. Further, the interaction of

mobile devices with networked services and their support through remote system accessed by mobile devices deserves detailed attention. The latter is currently addressed in the context of mobile signatures by ETSI [Et14].

6 Summary

In summary we have presented strong evidence that mobile devices have a unique potential to drive a large scale take-up of secure digital identity management solutions beyond username/password and smartcard based approaches. The Estonian and Austrian case studies demonstrate that mobile eIDs experience an extraordinarily high acceptance by end users. In both cases the successful take-up is supported by the integration of mobile eIDs in an ecosystem that offers a high number of appealing and convenient use cases.

In sharp contrast to this success stands the small number of European member states that have implemented mobile eIDs. However, the eIDAS regulation is expected to facilitate the roll-out of both mobile eID and e-signature solutions for e-government applications which should drive take-up and support further adoption.

Many national and EU projects actively consider mobile eIDs and have successfully integrated mobile eID solutions. However, mobile eIDs are usually not at the centre of attention. This is surprising as a detailed understanding of the mechanisms that drive the successful take up of mobile eIDs is incomplete. Further mobile devices offer the possibility to integrate a number of novel authentication options including step-up authentication that deserve further and more detailed research and development efforts.

The industry study in this work shows high demand for mobile eID solutions in a key industry sector but also presents evidence that the effective integration of these technologies is currently still underdeveloped. Assuming that these findings also apply to other key European industries a significant industry exposure to IT-security vulnerabilities caused by the non adequate integration of mobile eIDs is highly likely and must be addressed.

Finally, increased efforts dedicated to interoperable mobile eID standards that take advantage of the full range of authentication possibilities offered by networked mobile devices are required.

Acknowledgements

The authors would like to thank all members of the SSEDIC.2020 community and in particular Roger Dean, David Goodman, Hugo Kershot, Tarvi Martens, Daniela Merella, and Jon Shamah for engaging discussions and their ongoing support.

References

[Eu15] EU, „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," 2014. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG. [Access 19 06 2015].

[Fi15] FIDO Alliance, Inc., „FIDO Alliance," 2015. [Online]. Available: https://fidoalliance.org/. [Access 19 06 2015].

[Na15] National Institute of Standards and Technology, „National Strategy for Trusted Identities in Cyberspace (NSTIC)," 2011. [Online]. Available: http://www.nstic.gov. [Access 19 06 2015].

[Id15] Identity Ecosystem Steering Group, Inc., „Identity Ecosystem Steering Group," 2015. [Online]. Available: https://www.idecosystem.org/. [Access 19 06 2015].

[Ss15a] SSEDIC, „SSEDIC.2020," 2015. [Online]. Available: http://www.ssedic2020.eu/. [Access 19 06 2015].

[Ss15b] SSEDIC, „SSEDIC," 2015. [Online]. Available: www.ssedic.eu. [Access 19 06 2015].

[Fo15] N. Foggin, „Exploring the Role of Mobile in Digital Identity Assurance," 2014. [Online]. Available: http://oixuk.org/wp-content/uploads/2014/05/Mobile-White-Paper-final.pdf . [Access 19 06 2015].

[Ge14] Gemalto, National Mobile ID Schemes: Learning from Today's Best Practices, 2014.

[Gs15] GSMA Mobile Identity Team and Turkcell, „Mobile Signature in Turkey: A Case Study of Turkcell," 09 2012. [Online]. Available: http://www.gsma.com/personaldata/wp-content/uploads/2012/09/MI_TurkcellReport_print_FINAL.pdf. [Access 19 06 2015].

[Ma10] T. Martens, „Electronic Identity Management in Estonia Between Market and State Governance," in *Identity in the Information Society*, 2010.

[RH07] H. Roßnagel and O. Hinz, „Zahlungsbereitschaft für elektronische Signaturen," in *Wirtschaftsinformatik 2007 - eOrganisation: Service-, Prozess-, Market-Engineering*, A. Oberweis, C. Weinhardt, H. Gimpel, A. Koschmider, V. Pankratius and B. Schnizler, Hrsg., Karlsruhe, 2007, pp. 163-180.

[Ta14] M. Talamo, S. Ramachandran, M.-L. Barchiesi, D. Merella and C. Schunck, „Towards a Seamless Digital Europe: The SSEDIC Recommendations on Digital Identity Management," in *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI), P-237*, 2014, pp. 62-72.

[Fu15] FutureID Project, „FutureID Project," 2015. [Online]. Available: htttp://www.futureid.eu.

[Fu14] FutureID Project, „Deliverable D21.05," 2014. [Online]. Available: http://futureid.eu/data/deliverables/year1/Public/FutureID_D21.05_WP21_v1.0_Business_and_Use_Case_Analysis.pdf.

[Fu13a] FutureID Project, „Deliverable D21.03," 2013. [Online]. Available: http://futureid.eu/data/deliverables/year1/Public/FutureID_D21.03_WP21_v1.0_Vision.pdf.

[ZTL11] T. Zefferer, P. Teufl and H. Leitold, „Mobile qualifizierte Signaturen in Europa," *Datenschutz und Datensicherheit,* Bd. 35, Nr. 11, pp. 786-773, 2011.

[Fu13b] FutureID Project, „Deliverable D31.02," 2013. [Online]. Available: http://futureid.eu/data/deliverables/year1/Public/FutureID_D31.02%20_WP31_v1.0_Interface%20and%20module%20specification%20and%20documentation.pdf.

[Fu13c] FutureID Project, „Deliverable D34.02," 2013. [Online]. Available: http://futureid.eu/data/deliverables/year1/Public/FutureID_D34.02_WP34_v1.0_DesignMockups.pdf.

[Tr15] Trusted Cloud, „Trusted Cloud," 2015. [Online]. Available: http://trusted-cloud.de/.

[Sk15] SkIDentity Project, „SkIDentity Project," 2015. [Online]. Available: https://www.skidentity.de/.

[Hü15] T. Hühnlein, D. Hühnlein, T. Wich, B. Biallowons, M. Tuengerthal, H.-M. Haase, D. Nemmert, S. Baszanowski and C. Bergmann, „SkIDentity - Mobile eID as a Service," in *D-A-C-H Security 2015, 8./9.9.2015*, St. Augustin, 2015.

[Es15] eSens Pilot, „eSens Pilot Website," 2015. [Online]. Available: http://www.esens.eu/. [Access 01 07 2015].

[Ho12] C. Homburg, M. Klarmann, M. Reimann and O. Schilke, „What Drives Key Informant Accuracy?," *Journal of Marketing Research,* Bd. 49, Nr. 4, pp. 594-608, 2012.

[Et10] ETSI, Identity and access management for Networks and Services; Distributed User Profile Management; Using Network Operator as Identity Broker, 2010.

[In12] International Organization for Standardization, *International Standard Standard ISO/IEC WD1 29003:2012 (E), Information technology - Security Techniques - Identity Proofing,* 2012.

[In13] International Telecommunication Union, „Framework for Discovery of Identity Management Information, Recommendation ITU-T X.1255," 2013.

[Ta14] M. Talamo, M. L. Barchiesi, D. Merella and C. H. Schunck, „Global Convergence in Digital and Attribute Management: Emerging Needs for Standardization," in *Proceedings of the 2014 ITU Kaleidoscope Academic Conference: Living in a Converged World - Impossible Without Standards?*, St. Petersburg, 2014, pp. 15-21.

[Na08] I. Naumann et.al., „Security Issues in the Context of Authentication Using Mobile Devices (Mobile eID), ENISA Position Paper 2008-12-1," European Network and Information Security Agency (ENISA), 2008.

[Et14] ETSI, „Rationalised Framework of Standards for Advanced Electronic Signatures in Mobile Environment, ETSI Technical Report SR 019 020 v0.0.5f," 2014.

[Mo15] Mobile-ID, „Mobile-ID," [Online]. Available: http://mobile.id.ee/ . [Access 19 06 2015].

Detlef Hühnlein et al. (Eds.): Open Identity Summit 2015,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2015 43

Proxied Authentication in Single Sign-On Setups with Common Open Source Systems – an Empirical Survey

René Peinl[1] Florian Holzschuher[1]

Abstract: The paper presents results from an empirical study about the use of a single sign-on (SSO) system in an integrated open source system landscape for supporting team collaboration. A portal solution, enterprise content management system, groupware, business process management and enterprise search engine are used. The investigation shows that although it is easy to achieve SSO with the Web-based user interfaces of the information systems used, none of the systems was prepared to pass authentication tokens to the API of an integrated system or accept SSO tokens instead of username / password pairs for authentication against the API respectively. Different alternatives for achieving the desired functionality are presented and a recommendation for improvement of the affected information systems is derived.

Keywords: single sign-on, double-hop problem, proxied authentication, open source systems

1 Introduction

A modern digital workspace often consists of a number of specialized software systems, capable of solving different problems. In order to minimize overhead, these systems can use a single sign-on (SSO) authentication system, eliminating the need for separately logging into each system. While big vendors' ecosystems, such as Microsoft's, ship with full SSO support throughout, independent open source software's support for SSO is often limited and does not cover APIs. A number of systems supports using an external SSO system for accessing the Web user interface (UI), but still requires passing username and password to integrated systems in the back-end. In a non-SSO setup for example, when a Liferay Portal connects to an external document management system (DMS), the user's credentials entered while logging into Liferay are replayed to authenticate with the DMS. However, in an SSO setup, the user authenticates with Liferay via an SSO token which is only valid for Liferay and cannot be replayed. Furthermore, username and password of the user are not known by Liferay, but only by the SSO system. Therefore, those cannot be used either. A proxied SSO authentication in the user's name would be required.

[1] Hof University, Institute of Information Systems, Alfons-Goppel-Platz 1, 95028 Hof, Germany,
{rene.peinl | florian.holzschuher}@iisys.de

2 Usage scenario

Our target setup for the Social Collaboration Hub (SCHub[2]) project contains, among others, Central Authentication Service (CAS[3]) as a SSO server, Liferay[4] as a portal, Nuxeo[5] as an enterprise content management system (ECMS) and Camunda business process management (BPM)[6] as a workflow engine. Furthermore we use Open-Xchange[7] (OX) as a groupware, with Postfix[8] and Dovecot[9] as its backend. All services are connected to an LDAP server for user account information. Fig. 1 gives a graphical overview of the setup and the communication relations, especially those between server systems. CAS and LDAP have connections to every other system except Dovecot. These are omitted in the figure in order to make it clearer.

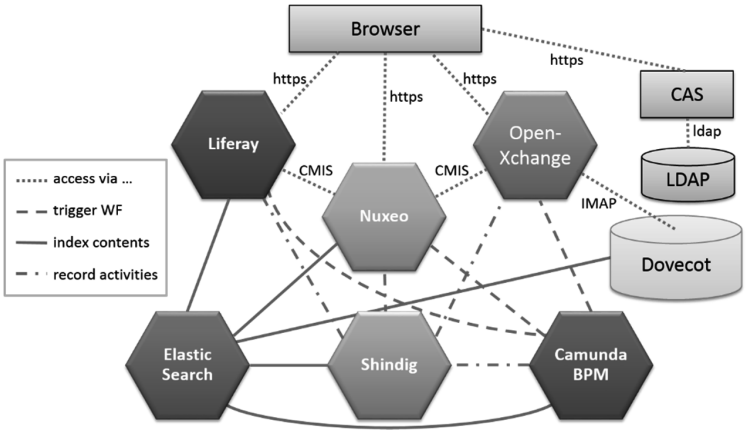

Fig. 1. Communication between systems. CAS relations are omitted (own illustration)

We have several use cases where the problem described above occurs.

1. Access to the ECMS Nuxeo via CMIS[10] from Liferay and OX
2. Triggering workflows in Camunda from Liferay, Nuxeo and OX
3. Storing activities in Shindig from Liferay, Nuxeo, OX and Camunda
4. Accessing emails in Dovecot via IMAP[11] from OX

[2] https://www.sc-hub.de/
[3] http://jasig.github.io/cas/
[4] http://www.liferay.com/
[5] http://www.nuxeo.com/
[6] http://camunda.org/
[7] http://www.open-xchange.com/en/home
[8] http://www.postfix.org/
[9] http://www.dovecot.org/
[10] Content Management Interoperability Services
[11] Internet Mail Access Protocol

In principle, there are also problems when accessing Elasticsearch from the search UI in Liferay, but these can be circumvented by directly accessing the Elasticsearch REST API from the portlet in the browser. Another challenge is indexing the contents of systems that require SSO authentication, but this is not discussed here. In the remainder of the paper the challenges of proxied SSO authentication are investigated, wide-spread authentication protocols are analyzed regarding their support for this scenario and different approaches to securely pass on authentication information are evaluated. Finally the above listed use cases are discussed and a suggestion for enhancements of common open source projects is derived in the conclusion.

3 Challenges

The requirements in the case described are the same as with multi-tiered applications [Hi00]. We need the possibility for a front-end system to access a back-end service under the authenticated user's identity [Au04]. The problem already starts with a commonly accepted term describing it. Microsoft dubbed it "the double hop issue" [Py08], in SAML the feature addressing it is known as delegated authentication [RD10], other authors call it impersonation [FF12] or proxy authentication [Sp11]. However, proxy authentication is an ambiguous term since it usually denotes a proxy that authenticates the user before passing his requests to the application, whereas here it refers to an application passing authentication information to a second application via its API. Delegated authentication is also ambiguous as it also denotes delegating the task of authentication to an external system like CAS. In this paper, the term "proxied authentication" is therefore used to denote the case where a user authenticates with an external single sign-on system for a Web-based application server system. This system in turn passes authentication information to a second back-end server system in order to access its application programming interface (API) with the name and permissions of the logged in user. Usually, common open source systems (OSS) as the ones used in SCHub rely on direct logins into their system. For accessing services of another system, the username and password accepted from the logged in user are often replayed to the second system. However, every application managing its own password replay feature is not only a security flaw but also thwarts the purpose of an SSO setup. Additionally, this replay functionality can be required by libraries used by the system, which open connections to or receive connections from other systems and do not support SSO-compatible authentication methods as is the case with the version of Apache Chemistry library used for CMIS support in Nuxeo. This makes it even more complicated to modify an integrated system so that all components use SSO. Especially the micro-service architectural style [LF14] frequently suggested in the last years [NS14] for Software as a Service (SaaS) scenarios is suffering from this problem. Although the problem is solved from a scientific point of view, the challenge of getting it to work in practice is demanding since it not only requires the usage of an authentication protocol that supports the feature. Both the SSO solution and the server systems must implement that protocol including this specific feature of the protocol as well as be prepared to pass on SSO tokens to external systems and use them for authenticating incoming API requests respectively. Fig. 2 is visualizing the

complex interplay. The user is accessing server system 1 using the browser (1) in order to view information stored in server system 2. System 1 detects that the user is not logged in and redirects the browser (2) to the external SSO system (3). After successful login there (not shown in the figure) the SSO system delivers a user ticket back to the browser (4) that in turn uses it to access system 1 as originally intended (5). However, system 1 needs a proxy ticket instead of the user ticket in order to pass credentials to system 2. Therefore, it has to request it from the SSO system (6) using the user ticket and a process described in section 4.2 but not shown in the figure. Once it got the proxy ticket (7) it can pass it on to system 2 (8) in order to retrieve the data from there (9) or invoke an action and present the result to the user (10). System 2 should be able to validate the ticket without a need to access the SSO system. Ideally, the ticket includes information about the user ID. Otherwise, system 2 would still need to query the SSO system for retrieving user information, which slows down the whole process.

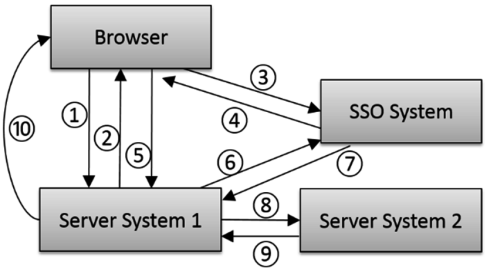

Fig. 2. Communication flow during proxied authentication

The described solution is the cleanest way of achieving the desired result and implemented in SAML 2.0 (section 4.1), Kerberos (section 4.3), as well as CAS proxy tickets (see section 5.2). Another solution, but more a workaround that circumvents the problem, is the usage of system users with fixed credentials. Despite this being relatively easy to implement and partial support for this solution in existing systems, there are several drawbacks. For one, these credentials need to be stored in the configuration of several services and only a part of them may support password encryption (as is the case in SCHub). Moreover, for requests to be handled properly and securely they need to be executed as the right user. But executing requests in a user's name using admin credentials is not widely supported and thus authorization constraints are not in effect and actions may be attributed to an admin, not the user triggering a request. One example for this mechanism is indexing of content stored in Dovecot using the IMAP river plugin of Elasticsearch. We have extended the original plugin[12] provided by Hendrik Saly in order to support the feature of Dovecot to access a user mailbox with an admin account. Such a mechanism is often called impersonation [Ve06]. Normal authentication tokens provided by users cannot be stored and passed on to another service, primarily because they are only valid for the service they were issued to. Furthermore,

[12] https://github.com/salyh/elasticsearch-river-imap

acquiring them through automated logins in the backend without a proper browser session has proven to be very difficult in our tests. The CAS documentation hints[13] at this being on purpose, since passwords have to be known outside of CAS. Otherwise, this mechanism could be easily used for brute force attacks on passwords.

4 Authentication Protocols

4.1 OAuth 2.0

OAuth 2.0 (http://oauth.net/2/) is an authorization protocol/framework, not only supporting Web but also desktop applications. It will be called OAuth in the rest of the paper. The normal authentication flow in OAuth for Web applications is called authorization code grant and works as follows. The server system, the user is trying to access (client in OAuth terms) redirects the user's browser (user agent) to the authorization server. The user is authenticated there presenting an authorization grant (e.g., username / password) and in case of valid credentials gets an authorization code. This code is delivered back to the client which can request the access token and use it to access the resources of the resource server (server system 2), which should be able to verify the access token without needing to contact the authorization server [Ha12]. Optionally, the authorization server can deliver a refresh token together with the access token, which the client can use afterwards to get new access tokens without the need for re-authentication.

In the case of Internet systems, the OAuth authorization server and the resource server are usually the same (e.g. Facebook, Google+). The client is usually a third party Web application that both uses the authorization server as an SSO system as well as the resource server to access additional information about the user or post messages in the name of the user [cf. SB12]. In the use case presented here, however, the authorization server is the SSO system whereas the resource server would be server system 2 and the client server system 1 (see figure 2). Throughout the whole OAuth specification, only the supplement on "bearer token usage" refers to our use case by stating that the bearer token scheme "is intended primarily for server authentication using WWW-Authenticate and Authorization HTTP headers but does not preclude its use for proxy authentication" [JH12]. It seems that OAuth is still missing the clarification of the SAML addendum (see below). Another issue is that the structure of tokens in OAuth is not prescribed and therefore it cannot be guaranteed that two systems will really be interoperable, although both are implementing the specification. Liferay includes an OAuth provider, but it seems to be version 1 only and additionally is working in the wrong direction for SCHub, since it is used to grant other applications access to Liferay [Li00]. There is a plugin for Liferay called oxAuth[14] which allows users to authenticate against an external OAuth provider in order to access Liferay. However, it seems to require OpenID connect support by the authorization server,

[13] https://wiki.jasig.org/display/CAS/Using+CAS+without+the+CAS+login+screen
[14] http://liferay.pbworks.com/w/page/83464783/oxAuth%20plugin%20for%20LifeRay

which is only supported by CAS in the client role up to now[15]. CAS currently supports OAuth 2.0 with the authorization code grant[16]. Consequently, our tests did not succeed to authenticate a user for Liferay using CAS and OAuth. Nuxeo also directly supports OAuth 2.0 and esp. the provider role, which can be used to access Nuxeo from third party applications. However, the CMIS server used in Nuxeo (Apache Chemistry) does not. Astonishingly, we managed to access the Nuxeo CMIS interface using OAuth authentication from a test client. It seems that Nuxeo has linked its own pluggable authentication to the Chemistry library. However, we did not manage to connect the OAuth functionality of Nuxeo with the CAS server and therefore, the use case is not supported.

4.2 SAML 2.0

Security Assertion Markup Language (SAML) 2.0[17] is an XML-based authentication and authorization standard. It was developed to accompany SOAP-based Web services, although it is versatile and can be used to transport arbitrary tokens, e.g. from Kerberos. It supports several profiles[18] for different use cases, but a widely used SSO profile is the Web browser SSO profile introduced in SAML 2.0 [AC08]. The same applies to transport bindings which include SOAP over HTTP as well as HTTP redirect and POST [MR08]. The "Delegated SAML Authentication" described in [MM12] could be used to achieve proxied authentication. It uses SOAP messages, WS-Addressing, public key encryption and signatures to exchange authentication information and user identity assertions. The original SAML specification was not precise enough in this special case, so that an addendum was released later on [Oa09]. CAS fully supports SAML 1.1 and support SAML 2.0 to some extent, especially those features needed for cooperation with Google apps[19]. Liferay is more elaborate in this case and provides a marketplace plugin[20] for the enterprise version that allows Liferay to act both as an Identity Provider (IdP) or Service Provider (SP). Nuxeo provides some SAML support via integration of CAS or Shibboleth and is actively working on providing native support in Nuxeo 7.4 scheduled for September 2015[21]. However, even if all three supported SAML 2.0, Liferay would still need to implement the delegated SAML authentication like uPortal does[22] in order to support our use case.

4.3 Kerberos

Kerberos[23] is an authentication protocol that can be used for SSO. It was not tailored for Web applications, but rather operates on an operating system level, retrieving tickets for

15 https://github.com/Jasig/cas/pull/910
16 http://jasig.github.io/cas/4.0.x/protocol/OAuth-Protocol.html
17 http://saml.xml.org/saml-specifications
18 http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
19 http://jasig.github.io/cas/4.0.x/protocol/SAML-Protocol.html
20 http://www.liferay.com/de/marketplace/-/mp/application/15188711
21 https://jira.nuxeo.com/browse/NXP-14595
22 https://wiki.jasig.org/display/UPM31/00+-+Delegated+SAML+Authentication
23 http://web.mit.edu/kerberos/

supported applications [NT94]. This is not surprising given its year of invention even before the advent of the www [St88]. However, it is versatile enough to be used in modern usage scenarios as well. If the user logs on to her PC using Kerberos and browsers are forwarding the respective ticket, it is possible to achieve SSO on an even deeper level than with Web-based protocols. Internet Explorer does this by default for the local intranet (Windows domain). In Firefox and Chrome it is available, but only after configuring the respective server names in a whitelist. Kerberos is widely used in Windows-based intranets [Py08]. On Linux, it seems less popular, although there are two open source implementations available, which both support Kerberos v5: MIT Kerberos server and Heimdal [Ga03]. Kerberos uses a rather complex, but effective mechanism to solve the problem, similar to the solution described in Fig. 2. Clients get a session ticket, once the user has authenticated successfully against the authentication server. With this, they can obtain a ticket granting ticket (TGT), which in turn allows to get service tickets for the respective services that should be invoked [Ga03, S.21]. It therefore supports proxied authentication. CAS supports Kerberos for clients running in a Windows Active Directory (AD) domain[24]. The CAS mechanism uses the MIT Kerberos stack and is called SPNEGO. Liferay does not support Kerberos by default, but can be configured to use it with an Apache module [Pa14]. Nuxeo even supports it out of the box using a free plugin and the MIT Kerberos server[25]. However, since there is no Windows AD domain in the project setup, this option is not feasible in our use case.

5 Proprietary approaches

CAS supports all of the protocols mentioned above, but uses an own proprietary protocol by default[26]. It uses CAS clients to protect the "casified" applications and retrieve the identity of the authenticated user from the CAS server. The current CAS server v4 uses CAS protocol v3. Key concepts are service tickets (ST) transmitted as parameter in the URL that grant access to a service and ticket granting tickets (TGT) stored in a cookie as a representation of the user session and a means to request new tickets. Thus, it is similar to Kerberos, but uses XML over HTTPS for transport.

5.1 Proxy Authentication

CAS Proxy Authentication[27] is a mechanism through which an application, with a valid TGT, can request a proxy granting ticket (PGT) which it can then use to retrieve proxy tickets for other services [Sp11]. This proxy ticket includes a validation chain that the service must validate in order to prevent impersonation attacks. This mechanism has many advantages, beginning with the fact that no password has to be replayed, making this approach much more secure. Furthermore, the actual user who made the original request is

[24] http://jasig.github.io/cas/4.0.x/installation/SPNEGO-Authentication.html
[25] https://doc.nuxeo.com/display/ADMINDOC/Using+Kerberos
[26] http://jasig.github.io/cas/4.0.x/protocol/CAS-Protocol.html
[27] http://jasig.github.io/cas/development/installation/Configuring-Proxy-Authentication.html

authenticated using a request that transparently shows, by which application the authentication was proxied (authentication chain). This proxy authentication can be configured per service as well. The downside to this approach is the high implementation effort required. Backend systems need to be able to validate proxy tickets (in addition to user tickets) including the proxy chain[28] and proxying systems need retrieval logic for proxy tickets and an additional REST endpoint to receive these additional tickets and attach them to the right request. The callback is used for validating the service using its URL and the certificate for the HTTPS connection.

5.2 CAS ClearPass

CAS ClearPass[29] is the password replay feature of CAS, which can provide services with the user's password captured during login to CAS. This setup is only slightly more secure than leaving password capture to individual services since password storage is centralized and encrypted. It reuses the first part of the proxy ticket mechanism, so that the proxy application needs to retrieve a PGT and a proxy ticket first in order to get the clear text password. Afterwards, this password can be sent to the protected service. Using ClearPass eliminates the need to modify backend applications as long as they authenticate against the same LDAP directory or use the same username/ password combination. Still, the frontend application needs to request the password from the CAS server, extract it and attach it to the user's relayed request. Storing the user's password as an encrypted session variable can help to prevent the SSO system from becoming a performance bottleneck. The use of this feature can be authorized for individual services in order to minimize the potential for abuse.

6 Discussion

6.1 CMIS

Apache Chemistry is the reference implementation for CMIS and provides both a server and a client implementation in Java. Since all systems used in SCHub are mainly developed in Java, it is not surprising that existing implementations in Nuxeo and Liferay both use Chemistry and the developers of Open-Xchange have also decided to use Chemistry as a basis for their own CMIS interface, which is currently under development as part of the SCHub project. Although both Nuxeo and Liferay natively support CAS as well as several other authentication protocols, Chemistry had no working authentication mechanism besides username/password-based authentication at the time of writing. Liferay consequently explicitly states it on the Website[30], that SSO is not supported for connecting to a remote CMIS repository. A review of included Chemistry versions in historic Nuxeo and Liferay versions

[28] http://jasig.github.io/cas/4.0.x/planning/Security-Guide.html
[29] http://jasig.github.io/cas/4.0.x/integration/ClearPass.html
[30] http://www.liferay.com/de/community/wiki/-/wiki/Main/CMIS+Repository

made clear that both systems include fairly recent builds of Chemistry. Given that information, it was clear that the right way to go is contributing to Apache Chemistry instead of making project-specific developments. Fortunately, our discussions with representatives of the Deutsche Wolke working group within the Open Source Business Alliance led us to Grau Data GmbH who are already an active contributor to Chemistry and agreed to implement OAuth 2.0 functionality for Chemistry in order to make it available for their own CMIS-based products. However, we are exploring the use of CAS ClearPass in parallel, since this seems to require the least effort.

6.2 Workflows

The Camunda BPM solution is primarily designed for being embedded into its customers' information systems, although it can be used as a standalone workflow engine as well. Therefore, it doesn't pay special attention to authentication and only provides basic HTTP authentication which is even switched off by default[31]. However, the authentication provider is exchangeable. The cleanest way would be to implement a CAS proxy ticket validation chain as a pluggable provider there. However, the effort to implement the proxy retrieval mechanism in Liferay, Nuxeo and OX is high. Starting from version 7.6.1, OX uses OAuth 2.0 to access subscribed Google calendars[32]. This mechanism could be extended to access Camunda as well. As Camunda is already prepared to work with REST frameworks such as RESTeasy or RESTlet, this could be used to implement OAuth 2.0 for Camunda[33]. Another option would be to embed Camunda into Liferay and use Liferay's authentication features as a wrapper around Camunda similar to Nuxeo embedding Chemistry and combining it with its own authentication mechanism. However, this would counter the project's intention of achieving a micro-service approach, which requires separation of concerns on the level of the deployment unit. Although OX supports SAML 2.0 starting from version 7.8.0[34], it doesn't seem like the right way to go in this case. Kerberos isn't an option here as well.

6.3 OpenSocial

Shindig is the OpenSocial reference implementation and included in both Liferay and Nuxeo as a gadget container and rendering server. Starting with OpenSocial 2.0, OAuth 2.0 was specified as the primary authentication mechanism [Hinc11]. In principle, CAS supports OAuth 2.0 and authentication protocols can be specified per connected system. Shindig currently supports OpenSocial 2.5 and has an OAuth 2.0 service provider implementation[35]. However, we felt it would be a good idea to make our setup more uniform and "casified" Shindig, so that it can be used with the same protocol that was used with

[31] http://docs.camunda.org/latest/api-references/rest/#overview-configuring-authentication
[32] https://oxpedia.org/wiki/index.php?title=Google
[33] http://docs.jboss.org/resteasy/docs/3.0.9.Final/userguide/html/oauth2.html
[34] http://oxpedia.org/wiki/index.php?title=AppSuite:SAML_SSO_Integration
[35] http://bit.ly/1NeU8uE

the other information systems. It therefore seems to be a similar case as for CMIS and workflows. However, the problem is a bit different here. For storing activities in Shindig, it wouldn't be required for the proxy system to impersonate the user. It would be enough to authenticate the server system in order to prevent malicious entries being sent to Shindig. It even doesn't make sense for certain cases to use the logged in user here, since it cannot be guaranteed that there is one in every case (e.g. workflow completed events triggered by a timer event). Therefore, we propose using 2-legged OAuth 2.0 authentication for storing activities in Shindig. For showing the activities, the problem doesn't occur at all, since this is done in the browser using JavaScript and therefore, the service ticket can be used directly without the need to retrieve a proxy ticket.

6.4 IMAP

Although OX is used in many large installations (e.g. at Strato) and it is a common requirement to provide SSO to all services offered by an internet service provider, it seems that none of the existing OX customers demanded it yet. Otherwise, it would have become obvious that OX is not able to access the IMAP server in an SSO scenario, because none of the available IMAP servers is supporting common SSO protocols made for the Web. Dovecot already was the preferred IMAP server for OX before and is now even more after OX has acquired the company behind Dovecot[36]. Out of the above listed protocols, Dovecot supports only Kerberos[37], but OX doesn't. OX provides OAuth 2.0 and recently SAML 2.0 support as stated above. According to Carsten Dirks from OX during our project meeting, customers are trusting on a secure channel between OX server and IMAP server and are using the above mentioned feature to access the mailbox with a root account, but in the name of a normal user.

7 Conclusion

While there are some options for getting a working proxied authentication setup using open source software, compromises sacrificing some security may have to be made for some systems. With sufficient time and effort, at least the Java-based systems and libraries we are using could be modified to fully support CAS proxy tickets. But such in-depth modifications will probably be out of scope for most real world projects. OAuth 2.0 would be a good candidate for a solution, but only recently OpenID connect filled the gap of specifying the exchanged tokens (JSON Web Tokens) and therefore ensuring interoperability in our scenario[38]. CAS is going to support OpenID connect server role in the upcoming version 4.1. Hopefully, Liferay with oxAuth will then work with CAS as well as Nuxeo. If so, it OpenID connect would be our preferred authentication solution. In the

[36] http://www.open-xchange.com/en/dovecot
[37] http://wiki2.dovecot.org/Authentication/Kerberos
[38] http://openid.net/specs/openid-connect-core-1_0.html#IDToken

meantime, we are going to use CAS ClearPass as a workaround. The problem of authentication for scheduled tasks on a user's behalf can be solved with password replay, although this remains an undesirable solution. Thus, the problems of proxied authentication are solveable, but without support from the developers of the individual systems and libraries, the effort required to implement them is immense. With CAS being only one of many open source SSO solutions (e.g., Forgerock OpenAM, Shibboleth, FreeIPA), widespread support for all of its features is unlikely to be implemented in the near future. Although many popular open source systems support one or even several wide-spread authentication protocols, this support often doesn't cover every detail of the specification. Mostly, only one or two profiles or flows are implemented, which is enough for a specific user requirement, but not for general interoperability. We strongly recommend outsourcing the authentication task to third party systems like the application server or at least using some common libraries like RESTeasy or PAC4J that include support for common authentication protocols. Otherwise, the burden to support flexible authentication is too high for a small OSS. The use of JAAS[39] in Nuxeo shows, that this approach is the right way to go and leads to versatile systems. However, including third party components like Apache Chemistry or Apache Shindig requires additional attention in order to prevent limitations regarding overall availability of all authentication options. This wouldn't be the case, if these third party components supported JAAS as well. The recent trend in cloud computing towards "everything as a service" [Scha09] led to "Identity and Access Management as a Service" (IDaaS) [NuAg14] with players such as Octa and PingIdentity [KrWy15] which seem more suitable for use cases such as the one presented here than public Internet providers like Google and Facebook as identity providers. There is also an award winning project in Germany called SkIDentity [KuÖF14], which we are looking to integrate for allowing secure access using the new German identity card or a health insurance card. However, this won't solve problem presented here either.

References

[Ar08] Armando, A.; Carbone, R.; Compagna, L.; Cuellar, J.; Tobarra, L.: Formal analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for google apps. In: *Proc. of the 6th ACM workshop on formal methods in security engineering* : ACM, 2008, S. 1–10

[Au04] Aubry, P.; Mathieu, V.; Marchal, J.: ESUP-Portail: Open Source Single Sign-On with CAS (Central Authentication Service). In: . Ljubljana, Slovenia, 2004, S. 172–178

[FF12] Fan, Z.; Fan, Z.: Security Research about Asp.net Web Application. In: *Proc. of the 2012 Intl. Conf. on Computer Application and System Modeling* : Atlantis Press, 2012

[Ga03] Garman, J.: *Kerberos: The Definitive Guide: The Definitive Guide* : O'Reilly, 2003

[Ha12] Hardt, D.: The OAuth 2.0 authorization framework. http://bit.ly/1L6BYKz

[39] Java Authentication and Authorization Service

[Hi00] Hill, P. B.: Kerberos interoperability issues. In: *Proc. of the 3rd Large Installation System Administration of Windows NT 2000 Conference*, 2000, S. 35–42

[Hi11] Hinchcliffe, D.: *OpenSocial 2.0: Will key new additions make it a prime time player in social apps?* http://zd.net/1LQ6o1f

[JH12] Jones, M. ; Hardt, D.: *The OAuth 2.0 authorization framework: Bearer token usage*, http://bit.ly/1NeUzVK

[KW15] Kreizman, G.; Wynne, N.: *Magic Quadrant for Identity and Access Management as a Service, Worldwide* (Analyst Report). Stamford, CT, USA : Gartner, 2015

[Ku14] Kubach, M.; Özmü, E.; Flach, G.: Secure cloud computing with SkIDentity: A cloud-teamroom for the automotive industry. In: Open Identity Summit 2014. Stuttgart, 2014

[LF14] Lewis, J.; Fowler, M.: *Microservices*. http://bit.ly/1dI7ZJQ

[Li15] *OAuth - User Guide - Liferay.com*. http://bit.ly/1RoZWqN

[MM12] Masi, M.; Maurer, R.: On the usage of SAML delegate assertions in an healthcare scenario with federated communities. In: *Electronic Healthcare* : Springer, 2012, S. 212–220

[MR08] Maler, Eve ; Reed, Drummond: The venn of identity: Options and issues in federated identity management. In: *IEEE Security & Privacy* (2008), Nr. 2, S. 16–23

[NS14] Namiot, Dmitry ; Sneps-Sneppe, Manfred: On Micro-services Architecture. In: *International Journal of Open Information Technologies* Bd. 2 (2014), Nr. 9, S. 24–27

[NT94] Neuman, B.C.; Ts' O, T.: Kerberos: An authentication service for computer networks. In: *Communications Magazine, IEEE* Bd. 32 (1994), Nr. 9, S. 33–38

[NA14] Nuñez, D.; Agudo, I.: BlindIdM: A privacy-preserving approach for identity management as a service. In: *Intl. J. of Information Security* Bd. 13 (2014), Nr. 2, S. 199–215

[Oa09] OASIS: SAML V2.0 Condition for Delegation. http://bit.ly/1X7BnOC

[Pa14] Patou, M.: *Kerberos SSO with Liferay 6.1*. http://bit.ly/1X7BvO5

[Py08] Pyle, N.: *Understanding Kerberos Double Hop*. http://bit.ly/1LnbP8z

[RD10] Rybicki, A.; Dalquist, E.: uPortal 3.1 Manual - Chapter 02-05-06-03-00 - Delegated SAML Authentication, http://bit.ly/1L6wsdK

[Sc09] Schaffer, H. E.: X as a service, cloud computing, and the need for good judgment. In: *IT professional* Bd. 11 (2009), Nr. 5, S. 4–5

[Sp11] Spencer, David: *Proxy CAS Walkthrough*. http://bit.ly/1LwiVLo

[St88] Steiner, J. G.; Neuman, B. C.; Schiller, J. I.: Kerberos: An Authentication Service for Open Network Systems. In: *USENIX Winter*, 1988, S. 191–202

[SB12] Sun, S.-T.; Beznosov, K.: The devil is in the (implementation) details: an empirical analysis of OAuth SSO systems. In: *Proc. of the 2012 ACM Conf. on Computer and Communications Security* : ACM, 2012, S. 378–390

[Ve06] Veeramani, N.: Smart clients versus web forms. In: *Computer* Bd. 39 (2006), Nr. 8, S. 93–95

Detlef Hühnlein et al. (Eds.): Open Identity Summit 2015,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2015 55

Quality Management in Open Source Projects – Experiences from the Open eCard Project

Daniel Nemmert[1] Hans-Martin Haase[1] Detlef Hühnlein[1] Tobias Wich[1]

Abstract: Open Source Software (OSS) has immensely increased in popularity over the years and it is well known, that software with public access to the sources is on average less error prone than closed source software, especially if the project is supported by a large community which peer reviews the sources [Kua02]. For new and smaller projects however there is no large community yet and hence achieving and maintaining sufficient product quality is challenging. Against this background the present paper discusses aspects of product quality management for OSS in general and shares the experiences gathered in the Open eCard project, which has developed an ISO/IEC 24727 based eID client.

Keywords: Open Source, Quality Management, electronic identification (eID).

1 Introduction

Open Source — as a software development model — enables free access to the source code of software published under an appropriate license[2]. Such projects may be used as provided or forked and modified to fit individuals needs. Open Source Software (OSS) has been a success story for over a decade [MP12, CAHM04]. Particularly for Open Source projects with large communities, one of the reasons for this success may be seen in the fact that severe bugs are usually found more reliable and sooner than they would be detected otherwise [Kua02].

For new and highly specialized projects however there is no large community yet and hence achieving and maintaining sufficient quality is challenging. For the Open eCard project for example, which has developed an ISO/IEC 24727 based eID client it is rather unlikely to acquire a large community, because smart card development is still a highly specialized field as smart cards may usually not be used by citizens for individual purposes. Therefore in the scope of the Open eCard project, a development process has been implemented that uses ISO standards with regard to (software) quality as a frame of reference to compensate for the low amount of input from the community.

2 Related Work

Open Source development is not a new topic for scientific research. There have been a number of publications examining the product quality of Open Source projects compared

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

[2] See `http://opensource.org/licenses` for example.

to closed source projects over the years, with other studies examining which factors help an Open Source project to succeed. The subject of most studies tends to focus on projects with larger communities or projects that are developed for a specialized topic that nevertheless tries to solve a pressing need for many people, leading to large amount of feedback albeit the actual development team may be quite small. As a consequence there seems to be a distinct lack of research concerning projects with very small communities and a low amount of feedback from third parties.

After reviewing other empirical research on the scope of OSS, Crowston et al. [CWHW12] come to the conclusion that although OSS is rapidly increasing in popularity and adoption as a software development method, there is still a need to examine Open Source development processes and their "socio-technical work practices."

Aberdour [Abe07] reviewed studies of OSS with the goal to better understand how to improve the software quality of OSS *and* closed source software projects. He draws several conclusions (e.g. creating a sustainable community, testing processes and successful strategies for project management) which will also be investigated further in this paper.

Midha and Palvia [MP12] examine the intrinsic and extrinsic success factors of an OSS project in the first three years of its existence. In their paper they analyze popular assumptions on what contributes to the success of an OSS project. Their work helps to explain the reasons for the low participation by third parties for highly specialized and complex projects. Their research supports the hypothesis that high complexity and focus on niche markets are factors that result in low involvement from the outside.

Jennifer Kuan [Kua02] predicts that the source code of new Open Source projects will surpass the software quality of their closed source counterparts. In her analysis she finds evidence that this prediction holds up for many Open Source projects.

In 2006, Martin Fowler [Fow15] conducted central rules for the software development practice of Continuous Integration (CI), which is used in software development processes popular in the Open Source community, which are inspired by agile methods. Miller [Mil08] provides an example for CI being employed in a closed source project within Microsoft.

Hoffmann [Hof13] provides a comprehensive treatment of aspects related to software quality. He not only covers quality management processes (maturity models and software development methodologies) and software testing but also related topics, such as software bugs, quality assurance and code analysis.

Schneider [Sch08] provides comments on the ISO 9241-110 standard, which addresses software usability.

One of the central standards regarding product quality management is the ISO 9001 [ISO08] standard. It is applicable to virtually every industry and is therefore one of the most often used standards for certification concerning product quality management. Applying the standard to software development, however, proved to be problematic due to the focus of the standard on the manufacturing industry. While the production of goods is the focal

point for product quality management in ISO 9001 (which is barely existent in the software industry), with the design phase beforehand being relatively small compared to the production phase, software development almost completely consists of design and engineering. Therefore the additional guideline ISO/IEC 90003 [ISO14b] was developed at ISO, providing recommendations for the usage of ISO 9001 regarding software development. With ISO/IEC 90003 being only a guideline and not an imperative standard, every additional information provided in the standard is not a strict requirement for a successful certification. However, an auditor may nevertheless ask why certain points from the standard are not implemented in a product quality management system for a software company.

Another standard regarding quality is the ISO/IEC 25000 [ISO14a] series known as "SQuaRE" (**S**oftware product **Qua**lity **R**equirements and **E**valuation) which replaces the old ISO/IEC 9126 [ISO01] and ISO/IEC 14598 [ISO99] standards. The standard offers a framework within which the product quality of software can be evaluated.

The ISO standard defines several procedures and processes to establish a quality management system. The development scenario in the standard is expected to be a typical closed source environment with development being conducted inside a company, ignoring the unique factors that exist in an Open Source context. This leads to the question how ISO 90003 can be applied to OSS development that is driven by a company.

On top of the ISO standards concerning product quality, there are also maturity models to be investigated, which focus in the measurement of the quality of the implemented processes. The following standards are not yet part of the product quality management system of the Open eCard project, but will be analyzed at a later time. One example would be ISO 15504, which is also known as "SPICE" (**S**oftware **P**rocess **I**mprovement and **C**apability d**E**termination). ISO 15504 on its own does not provide a fully defined maturity model but provides a requirements catalog for a fully featured model instead. There are two ISO standards that fulfill the requirements provided by ISO 15504 of which each has a slightly different scope: ISO/IEC 12207 (software life cycle processes) and ISO/IEC 15288 (system life cycle proceses). Besides those two standards, additional viable models that are compliant to ISO 15504 are the Capability Maturity Model (CMM) and Capability Maturity Model Integration (CMMI) by the Software Engineering Institute (SEI).

3 Quality Management in the Open eCard Project

Since the very beginning of the Open eCard Project, one of the goals was to assure a high level of quality through testing and well-defined development guidelines.

The Open eCard App is being developed for as many different platforms as possible. Besides versions for several desktop operating systems (Linux, Windows and MacOSX), there is also an App for Android. Although the platform independence alleviates most of the problems that would be present with more platform dependent languages, there are still enough factors left that may cause complications. Those potential incompatibilities include for example the different versions of Java Development Kits and Runtime Environments — which differ not only between completely different operating systems but also

for example between different distributions of Linux — or the different level of support or quality of the drivers that are necessary to access smart cards.

Additionally, the Open eCard App not only has to be secure from an information security point of view, it also has to follow usability best practices to make the software ”feel safe” to use for users without a strong technical background in information technology. This implies that it is not only necessary to have good and secure code, but to also make the app as user friendly as possible.

3.1 Overview

The Open eCard project orientation is geared towards a process that is aligned with several ISO standards concerning quality in general and standards concerning software quality in particular. One of the most important standards regarding quality management is without a doubt the ISO 9001 standard [ISO08] — and the guideline ISO/IEC 90003 [ISO14b] which expands on and explains ISO 9001 in terms of software development.

The basis for the quality management system of this ISO standard is a ”Plan-Do-Check-Act” (PDCA) cycle as shown in Fig. 1. The model takes the requirements from the customers as input and starts a cycle of continuous improvement starting with the product realization. After a full cycle the product will either be released or the cycle continues until the customer is satisfied with the product. ISO/IEC 90003 provides guidelines for the application of this standard to software.

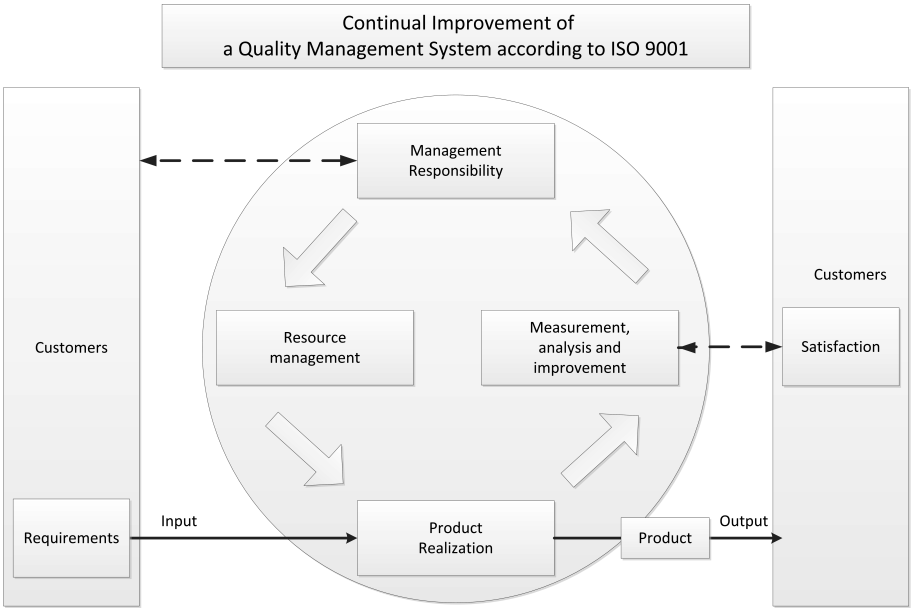

Fig. 1: Process-based Quality Management System according to ISO 9001[ISO08]

The Open eCard Project employs an adapted version of the classic ISO Quality Management System (see Fig. 2) to better reflect the specific requirements within the project. The used system is less strict about the different phases of the PDCA-process with most phases overlapping in some way. This overlap exists as a result of the different phases being partly interconnected with each other. Community interaction, and as a result the recruitment of new developers or testers (contributors) can be a part of the first phase or the first two phases if a new team member is already working on a feature by himself and does so before and after he has been recruited making a smooth transition into the development phase possible. The only isolated phase in the life cycle is the collection of feedback and marketing, which is carried out after a new release and before any new work on the Open eCard App itself begins. After a new release, feedback from users is collected, evaluated and converted into new features, patches or new or refined requirements. In this phase there will usually be announcements for major new versions or related news.

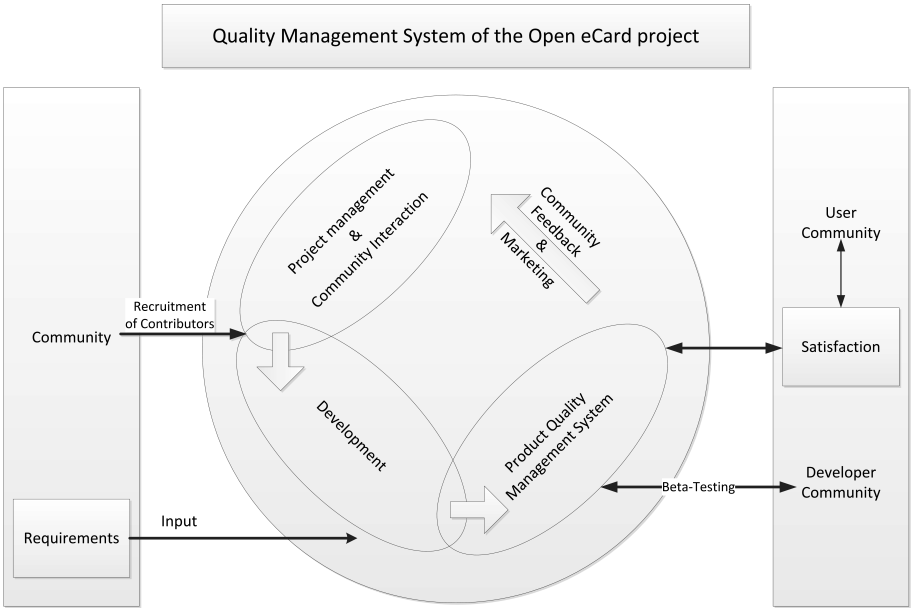

Fig. 2: ISO 9000 inspired QMS as used in the Open eCard project

3.2 Project Management & Community

One of the most important goals for any OSS project is to have a large *and* active community. Aberdour [Abe07] summarizes some of the studies done in terms of OSS quality and proposes that there are certain factors that are common in most successful and high-quality OSS to some degree. The bigger the community, the more new features can be implemented and the more bugs are found — increasing the chances to find and fix potentially devastating vulnerabilities faster than they would be found in a closed source project. This assumption comes with a caveat, though. Projects with rather large communities and the respective quantity of developers require a very good community management to achieve

this goal. Otherwise the sheer size is still useful for finding bugs, but can be a limiting factor that slows down development and deteriorates the general quality of the code base. In addition, a good documentation of everything related to the project is not only essential for closed source projects, but even more so for an OSS project. A good documentation facilitates the participation by other interested developers. Another important success factor is having just the right degree of modularity, which, when done right, facilitates the introduction of new features. While modularity is generally a good thing, "high modularity can lead to greater complexity; therefore, administrators need to keep modularity within an acceptable range." [MP12]

3.2.1 Core Team

The core team consists of the project manager, a maintainer as well as core members acting as developers and testers. Interested parties can gain access to the git-based development repository at GitHub[3] and may easily become tester or developer. Using the example of a new feature the different roles fulfill different tasks in the development process. A ticket for the feature will be created and assigned to a developer. The developer will then implement a solution for the new feature in a given time. Developers are encouraged to provide unit test facilities with their contribution, which will be integrated in the CI system. When the first version of the new feature is implemented, one or more testers (depending on the complexity of the new feature and the available personnel) review the new code and the new functionality with the goal to find any outstanding bugs. After the testing is finished the maintainer will be responsible for the final quality assurance and the integration of a contribution into the corresponding development branch. If any bugs are found in the review phase, a ticket will be created and if possible assigned to the original developer and the process starts from the beginning. The project manager is responsible for making informed decisions about the future direction of the project and assign priorities and new tasks to the rest of the team. Although the number of contributors is quite low, this must be strictly adhered to, because it gives the project a clear structure for each new release and avoids potential chaos in the submission of new features and subsequently in the release of new versions.

3.2.2 Community Add-ons

The Open eCard App also offers the possibility to develop add-ons to the software, enabling everyone to implement new features, without breaking the rest of the core software. Add-on capabilities also make it easier for other companies to develop their own, possibly very specific, additions to the software increasing the potential adoption rate. A company or a group of individuals could for example develop a plugin that enables the Open eCard App to be started before the login to the operating system to use the app for system authentication. In the best case a group of developers will then share their plugin with the original project.

[3] See `https://github.com/ecsec/open-ecard`.

3.2.3 Release Cycle

The best thing that can happen to an OSS project is having an active community. To ensure that, the core team of the project must make sure that release cycles aren't too long. Of course it does not make sense to release weekly new versions without any notable changes. Every OSS project has to try and find the right balance between "exciting" new releases and a release cycle that is short enough to keep its community interested in contributing to the project.

3.3 Development

> "Quality management system planning at the organizational level may include the following: [...] b) defining the work products of software development, such as software requirements documents, architectural design documents, detailed design documents, program code, and software user documentation; [ISO14b]"

3.3.1 Requirements

An initial set of requirements for the Open eCard App has been specified in [KPS+13, WHP+13]. Over time these requirements have been refined and are roughly as follows: The Open eCard App as to support multiple platforms (e.g. Windows 7/8.1 or Mac OS X 10.7 - 10.9 and popular Linux distributions) and a multitude of different cards[4] and especially demonstrate conformity with Technical Guideline TR 03124 [Fed15b, Fed15a] of the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI). Conformity to this technical guideline is especially important in order to ensure the full compatibility with the German eID card (Personalausweis) and may be formally assured by a corresponding certification of the BSI.

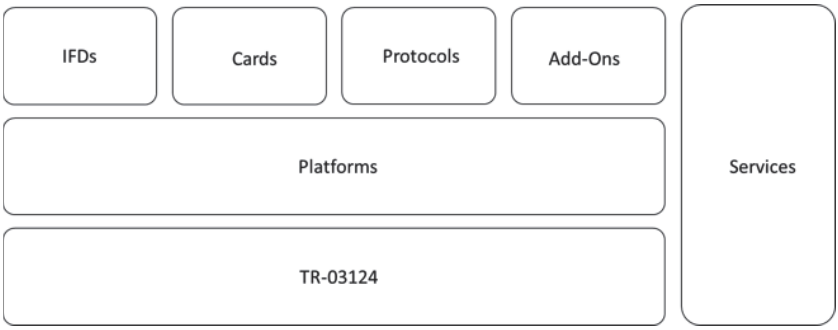

Fig. 3: Overview of requirements of the Open eCard App

At the very beginning of the project there were less planned modules than shown in figure 3. This latest iteration of the specification is a result of a constant evaluation of feedback

[4] A list of the currently supported cards can be found at: `https://www.openecard.org/ecards/`

by the surrounding community and internal evaluations by the core development team. As a result of the ongoing input of ideas and critique the scope of the App is much more complex today. This is an ongoing process that repeats itself for every new version of the App as can be seen in figure 2.

3.3.2 Development Guidelines

Another very important factor for the success of an OSS project is to have well-defined guidelines regarding a variety of development aspects. Without maintaining strict guidelines, having a potentially large community will almost certainly lead to disaster or at least to a huge amount of additional work for the members of the core team, whose time would be better spent on implementing new core features than formatting and rewriting code or rejecting bad code. Defining as strict as possible development guidelines as early as possible leads to a lot less work later on in the project.

In the Open eCard project there are guidelines for the development process, code-style, usage of the repository, and a general guide for developers. Besides those specific guidelines the central rules for general quality assurance governing the area of code commits are:

- Only atomic commits.
- Untested code must not be committed.
- Undocumented code must not be committed.

The developer guide[5] right now consists of two parts: One part provides an overview on how add-on development is realized, giving information for example about the relevant packages and its content. The other is a full documentation of the API of the project in form of a JavaDoc[6]. Again: Having reasonable modular extensibility and good documentation is critical to encourage participation in an OSS project.

The Open eCard project uses the term ”add-on” as a generic description for any type of component that enhances the functionality of the application and makes use of the publicly available API, which is limited to certain features from the full API. This model can be compared to the add-on model popular browsers like Firefox or Chrome are using. As explained in Wich et al. [KPS+13], an add-on can either be an extension or a plug-in, with both fulfilling different purposes. Extensions are directly included into the user interface and can be executed and interacted with by the user. An example for this would be an add-on that provides the functionality to change the pin of a smart card. Plug-ins, on the other hand, are dependent on the context the user utilizes the add-on in. Performing an authentication to a service using a particular smart card, for instance, requires a plug-in which is capable of providing such functionality.

[5] See `https://dev.openecard.org/projects/open-ecard/wiki/Developer_Guide`.
[6] See `https://ci.openecard.org/job/Document/javadoc/`.

Also there is a short explanation on how to begin with add-on development and what to consider before and while developing add-ons for the software.

As mentioned above, it is important for an OSS project to have strict code-style guidelines. If an OSS is adopted by a wide user base, strict code-style guidelines not only help to ”make a good impression” on other users or potential co-developers but also ensure a high readability of the code, which in turn leads to more feedback, which may encourage others to contribute. During the early stages of the Open eCard project, those guidelines have already existed, but weren't enforced in a very strict manner. Which led, in some parts, to code, that is not up to par to the code-style guidelines. As a consequence code-style is one of the most strictly enforced guidelines in the project now. It also facilitates the work of the core team, since newer developers (attracted to the project for various reasons) have access to information on how to format their code fitting to the general style of the project. Furthermore badly formatted code can be instantly rejected based on those guidelines.

The Code-Style guidelines[7] determine how well-formed code has to be formatted for the Open eCard project. In them, general rules are defined governing for example the use of whitespaces, indentations, line endings, file encoding, the language of the code and documentation or other relevant documents. In addition to the general rules, there are more specific rules for document types relevant to the project.

The Open eCard project uses a revision control system, as it is highly recommended for every software development project. The repository is public and hosted on GitHub[8]. Only the maintainer has write permission to this master repository, but every user with git development access, which is provided manually on a case-by-case basis, gets his own repository for development. The development model is similar to the traditional model that is used for the development of the Linux kernel. Additionally, there is the possibility for every interested party to open issues in the central project management and issue tracking tool[9]. The Open eCard Wiki[10] contains more detailed information about the whole process to ease the setup process for less experienced contributors. There are also rules on the correct formatting of the commit messages and other general rules.

3.3.3 Release Cycle

> ”Processes, activities and tasks should be planned and performed using life cycle models suitable to the nature of a software project, considering size, complexity, safety, risk and integrity.” [ISO14b]

The release cycle of the Open eCard project follows several rules. The release versions will be numbered according to Semantic Versioning [SV115]. At the beginning of a release

[7] See `https://dev.openecard.org/projects/open-ecard/wiki/Code-style`.
[8] `https://github.com/ecsec/open-ecard`
[9] access to the Redmine based ”Open eCard Development Center” can be gained by registering at: `http://join.openecard.org`
[10] See `https://dev.openecard.org/projects/open-ecard/wiki/Wiki`.

cycle the project manager assigns tasks to individual developers who then develop the new feature for the upcoming release and he also announces a targeted release date.

To ensure a stable release version, the code is frozen at least two weeks before the end of the cycle by the maintainer. From this point onward, only bug fixes are allowed to be committed to the branch of this release cycle. New features are committed to the branch of the next release. During this two or more week period the release manager and the testers need to test the code thoroughly. If bugs are found, the responsible developer is informed and the testers and developers agree on a person who will be responsible to correct the error. Fixing a bug should not take longer than two working days.

When the tests are completed and all detected errors are corrected, the maintainer is then responsible to build a release version and distribute it to the users. If a bug is found in the current release version, the maintainer and possibly the project manager decide whether its impact is big enough to warrant a bug-fix release or if it is sufficient to correct the error in the following scheduled release version. In case of a bug-fix release the testing stage is repeated: the maintainer contacts the respective developer to fix the bug and gets the new version reviewed by the testers. As soon as the error is fixed the maintainer builds the bug-fix release and again distributes it to the users.

3.4 Quality Assurance

ISO 9000 defines quality assurance as a ”part of quality management (3.2.8) focused on providing confidence that quality requirements will be fulfilled.” [ISO05] In this sense quality assurance is the process which has the objective to guarantee that a product works as intended. The most common and obvious way to achieve this goal is to define and conduct tests. In most software projects it is possible to automate many, if not all, tests required to enable the desired quality level, with the remaining test cases being carried out manually.

Because quality should be the goal of every OSS project that aspires to be successful, quality assurance, and as a consequence testing procedures, must be an important focal point. With limited resources being the most problematic aspect of many OSS projects (apart from projects led by bigger companies) establishing formal testing procedures — like automated tests and continuous integration — is not feasible for every project. Another possibility to improve the quality of the code base is to let the code be reviewed by external parties that have absolutely no connections to the project and do not turn ”a blind eye” to some errors.

The Open eCard project employs a mixture of manual and automated tests in the form of Continuous Integration (CI) and acceptance testing where automation is not feasible. In the scope of this project, a high level of product quality is achieved, when all defined features work as specified and can withstand both phases of the testing procedure.

It is very important to carefully plan and implement a suitable testing procedure right at the beginning of the project. Jenkins, for example, offers the possibility to check if

submitted code follows the defined code-style guidelines. If the code-style check surpasses a defined threshold in terms of warnings, the maintainer is notified via e-mail, whose work is immensely facilitated in consequence of this.

3.4.1 Continuous Integration

> ”Continuous Integration (CI) is a software development practice where members of a team integrate their work frequently, usually each person integrates at least daily - leading to multiple integrations per day. Each integration is verified by an automated build (including test) to detect integration errors as quickly as possible. Many teams find that this approach leads to significantly reduced integration problems and allows a team to develop cohesive software more rapidly.” [Fow15]

Fowler postulates eleven best practices for CI including points such as to maintain a single repository or to automate the build among others. By implementing those guidelines a project can create an efficient development process, that leads to much less integration problems, which is especially important for OSS with multiple contributors, but is also already useful if there is more than one developer working on the software.

Of course a project does not have to fulfill all those best practices at once. Every single step that is used in a software project, mitigates the risk of ending up in an ”integration hell” [Fow15]. The implementation of Continuous Integration is easier than might be expected, because there are very powerful Open Source CI systems available on the market, which may be customized to any needs a specific project might have.

Miller [Mil08], for example, comes to the conclusion that ”teams moving to a CI driven process can expect to achieve at least a 40% reduction in check-in overhead when compared to a check-in process that maintains the same level of code base and product quality.” This reduction alone spares a lot of time not only for bigger projects, but also helps relatively small teams to become more efficient.

The CI process is on the one hand supported by the concept of Mocking and on the other hand by the Open Source CI tool Jenkins[11] Mocking facilitates the testing process by providing mock data required for the testing procedure without the need to have an infrastructure in place that emulates the production environment. As a result, using mock data not only reduces the development costs, it also speeds up the development process because there is no maintenance or setup time involved — or at least less than for e.g. setting up an appropriate database. It is also possible to automate the creation of mock data, eliminating the time needed for creating classes that provide the data necessary to run the tests. Jenkins is one of the most popular CI tools, owing its popularity mainly to the widespread adoption by the Open Source community [Wie11]. The tool enables a development team to implement an extensible CI system facilitating the development process immensely.

[11] See `https://jenkins-ci.org/`.

Most of the testing is done by automated build-testing through a CI-system. In the development process a developer pushes his changes to a central version control system, which in turn informs the CI-system about the presence of changes. The CI-system then conducts the defined tests. If any of the tests fail, the developer is informed so that he can review and edit his changes. If all tests pass the CI-system informs both the developer and the release manager of which the latter then checks the changes and decides about whether to accept or reject the changes.

Both aspects are used in the Open eCard project, albeit limited by external systems that are part of the scope of the project (see section 3.4.2).

3.4.2 Acceptance Testing

The main focus of the acceptance tests is achieving a certification according to the technical guideline TR-03124 Part 2 [Fed15a]. The conformance with the guideline is being verified by using the official test suite issued by the BSI. This is, of course, an extremely specialized certification, which focuses on the conformity with the requirements defined in TR-03124 Part 1 [Fed15b]. Alternative certifications, which are not yet part of the requirements, would include Common Criteria (ISO/IEC 15408 [ISO09]) and NIST FIPS 140-2 [NIS01].

As mentioned earlier, external systems make an almost complete automation of testing very challenging, if not impossible. External systems in this case are primarily the various different smart cards and their integration into the software. Although standards like the ISO/IEC 7816 series related to electronic identification cards with contacts provide guidelines for various characteristics of smart cards the standard itself leaves room for proprietary manufacturer specific aspects which leads to vastly different implementations of the standard. The multi-part standard ISO/IEC 24727 aims to provide normative guidelines for the interoperability between different identity tokens and applications. The standard is an important step towards a more harmonized smart card environment in the future, with governments (e.g. in Germany) already adopting ISO/IEC 24727 for the implementation of their electronic identity card and the related infrastructure. This standard will ease supporting different smart cards easier in the future.

Besides testing different smart cards, the stability of the GUI is tested along with the general behavior of the App. As a last, but nevertheless important, step the cryptographic functionality of the App is being reviewed by experts to limit the possibility of faulty — and as a consequence potentially vulnerable — implementations.

3.5 Community Feedback & Marketing

A large and active community is arguably one of the most import factors which contributes to the success of an OSS project [Abe07]. The community for a successful OSS project is, according to Aberdour, like an onion with the large user base (which uses the software and

notices bugs) as the first layer, a smaller group of bug reporters as the second layer, with the next layer consisting of contributing developers and at the center a core team which leads the project.

The structure of a typical Open Source community is in most cases similar to the onion model described by Aberdour [Abe07]. The community in this model consists of a relatively small core team that is responsible for the main work done on the project. In the case of the Open eCard project this idealized model does not really apply, because not only the project manager and the maintainer would be part of the core team, but also the developers and testers, which are also active developers for the project. Testers are also responsible for bug reports, but so is every member of the team. Having no large and active community surrounding the Open eCard project makes it difficult to apply the most popular community models. As a consequence most development work is done within the core team itself.

An interested developer commonly engages with an OSS project, because the software is missing a feature that is important to him. This engagement can take on multiple forms: from the creation of a ticket or post on the forums, to coding the feature by himself or as part of the OSS team with the goal of implementing in the software, to forking the project and building his own version [Kua02]. This leads, over time, to a more and more ”feature complete” and robust software.

The community of the Open eCard project consists almost entirely of universities and other potentially interested companies. The low participation by private developers may be attributed to the unfortunate introduction of the German eID card and a lack of opportunities to use it for authentication purposes online, leading to a very small potential user base that on top of it all is mostly limited to the universities conducting research in this field and the companies that have financial interest in developing an own solution for card based authentication at the moment. There simply are no features a private developer could need badly enough for him to contribute to the project.

For users that are not interested in being part of the development team there is the possibility to provide feedback via a central issue tracker and via e-mail[12].

Nevertheless, the necessity for making this project open to the public is very high. Making this project Open Source and the code reviewable by everyone imposes a high level of trust in the security of the application, which is essential to the future adoption rate of the application and related eID systems. An application like the Open eCard App that deals with potentially highly sensitive information needs a high level of trust from the general public in order to be widely used for authentication purposes.

4 Conclusions

Implementing a basic product quality management for an OSS project requires less work than one might expect and hence is recommended for any project. The Open eCard project

[12] feedback@openecard.org

has demonstrated that it is even feasible for rather small projects to implement a quality management system as defined by ISO 9001 and ISO/IEC 90003. All factors described above — apart from the costly certification according to [Fed15b] — are possible to implement in almost every OSS project without extensive public funding or funding via relatively new channels like Kickstarter or Indiegogo. The resources required to realize the ISO 9001 inspired quality management system and the automated testing environment are within reasonable limits and should be affordable for almost every OSS project.

After the formal finalization of the certification according to BSI TR-03124 [Fed15b, Fed15a] a future goal may be the systematic examination and improvement of the Open eCard App with respect to usability, which may especially consider ISO 9241-100 [ISO10] and related guidelines.

References

[Abe07] Mark Aberdour. Achieving quality in open-source software. *IEEE Software*, 24(1):58–64, 2007.

[CAHM04] Kevin Crowston, Hala Annabi, James Howison, and Chengetai Masango. Effective work practices for software engineering: free/libre open source software development. In *Proceedings of the 2004 ACM workshop on Interdisciplinary software engineering research*, pages 18–26. ACM, 2004.

[CWHW12] Kevin Crowston, Kangning Wei, James Howison, and Andrea Wiggins. Free/Libre open-source software development: What we know and what we do not know. *ACM Computing Surveys (CSUR)*, 44(2):7:1–7:35, 2012.

[Fed15a] Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik). eID-Client – Conformance Test Specification. Technical Directive (BSI-TR-03124), Version 1.2, Part 2, 2015.

[Fed15b] 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.

[Fow15] Continuous Integration, 2015. `http://martinfowler.com/articles/continuousIntegration.html`, Stand: 16.04.2015.

[Hof13] Dirk W. Hoffmann. *Software-Qualität*. Springer-Verlag, Berlin Heidelberg, 2nd edition, 2013.

[ISO99] ISO. 14598-1:1999 Information technology – Software product evaluation – Part 1: General overview. ISO 14598-1:1999, International Organization for Standardization, 1999.

[ISO01] ISO. 9126-1:2001 Software Engineering – Product Qualiy – Part 1: Quality model. ISO 9126-1:2001, International Organization for Standardization, 2001.

[ISO05] ISO. 9000:2005 Quality management systems Fundamentals and vocabulary. ISO 9000:2005, International Organization for Standardization, 2005.

[ISO08] ISO. 9001:2008 Quality management systems – Requirements. ISO 9001:2008, International Organization for Standardization, 2008.

[ISO09] ISO/IEC. 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. ISO 15408-1:2009, International Organization for Standardization, 2009.

[ISO10] ISO/TR. 9241-100:2010 Ergonomics of human-system interaction – Part 100: Introduction to standards related to software ergonomics. ISO/TR 9241-100:2010, International Organization for Standardization, 2010.

[ISO14a] ISO. 25000:2014 Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Guide to SQuare. ISO 25000:2014, International Organization for Standardization, 2014.

[ISO14b] ISO. 90003:2014 Software engineering – Guidelines for the application of ISO 9001:2008 to computer software. ISO 90003:2014, International Organization for Standardization, 2014.

[KPS+13] Raik Kuhlisch, Dirk Petrautzki, Johannes Schmölz, Ben Kraufmann, Florian Thiemer, Tobias Wich, Detlef Hühnlein, and Thomas Wieland. An Open eCard Plug-in for accessing the German national Personal Health Record. In Detlef Hühnlein and Heiko Roßnagel, editors, *Proceedings of Open Identity Summit 2013*, volume 223 of *Lecture Notes in Informatics*, pages 82 – 94. Gesellschaft für Informatik eV (GI), 2013.

[Kua02] Jennifer Kuan. Open source software as lead users make or buy decision: a study of open and closed source quality. *Stanford Institute for Economic Policy Research, Stanford University*, 2002.

[Mil08] Ade Miller. A hundred days of continuous integration. In *Agile, 2008. AGILE'08. Conference*, pages 289–293. IEEE, 2008.

[MP12] Vishal Midha and Prashant Palvia. Factors affecting the success of Open Source Software. *Journal of Systems and Software*, 85(4):895–905, 2012.

[NIS01] NIST. 140-2: Security Requirements for Cryptographic Modules. ISO 14598-1:1999, National Institute of Standards and Technology, 2001.

[Sch08] Wolfgang Schneider. *Ergonomische Gestaltung von Benutzungsschnittstellen. Kommentar zur Grundsatznorm DIN EN ISO 9241-100:2010*, volume 2. Beuth Verlag GmbH, 2008.

[SV115] Semantic Versioning 2.0.0, 2015. `http://semver.org/`, Stand: 16.04.2015.

[WHP+13] Tobias Wich, Moritz Horsch, Dirk Petrautzki, Johannes Schmölz, Thomas Wieland, and Detlef Hühnlein. An extensible platform for eID, signatures and more. In Detlef Hühnlein and Heiko Roßnagel, editors, *Proceedings of Open Identity Summit 2013*, volume 223 of *Lecture Notes in Informatics*, pages 55 – 68. Gesellschaft für Informatik eV (GI), 2013.

[Wie11] Simon Wiest. *Continuous Integration mit Hudson*. dpunkt.verlag, 2011.

Detlef Hühnlein et al. (Eds.): Open Identity Summit 2015,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2015 71

Using Proxy Re-Encryption for Secure Data Management in an Ambient Assisted Living Application

Hannes Zach[1,2] Philip Peinsold[2] Johannes Winter[3] Peter Danner[2,3] Jakob Hatzl[2]

Abstract: Whenever applications process sensitive user data, secure storage and distribution plays a key role. This paper points out the security demands of an Ambient Assisted Living (AAL) application and demonstrates the usage of proxy re-encryption in order to fulfil its security requirements for storage and distribution of sensitive data. Because AAL systems often exhibit the same security needs as the application developed in the presented project, the described implementation can serve as a point of reference for similar projects.

Keywords: IT Security, Proxy re-encryption, Ambient Assisted Living, secure data storage and distribution

1 Introduction

In the near future, we will have to face a dramatic change in the age structure of our population. Society gets older, while at the same time birth rates are decreasing. As a result of the aging population, the amount of care-dependent people is rising constantly while there are less people to provide care. Ambient Assisted Living (AAL) enables elderly people to live a more convenient and self-determined life, and counteracts the increasing demand for care and an approaching financial crisis due to the increasing costs for professional care. Most AAL systems have to process personal sensitive health data. Hence, careful consideration of security and privacy concerns is required and protection of this data should have highest priority.

DALIA (**DA**ily **LI**fe **A**ctivities at Home) is a research project co-funded by the European AAL joint programme. DALIA works on an integrated home system to support older adults with their daily life activities. One key goal is to provide easy to use, privacy and security aware mechanisms to exchange sensitive data, for example medication data, between older adults and their carers. This paper discusses a work-in-progress approach being developed in DALIA to bring security to an AAL environment.

In order to guarantee data protection, several protective goals have been established and include, among others, confidentiality, integrity and availability [ST07], which has to be

[1] FH Joanneum - University of Applied Sciences, Department of Applied Computer Sciences, Werk-VI-Strasse 46, 8605 Kapfenberg, Austria
[2] exthex GmbH – explore the excellence, Göstinger Straße 213, 8051 Graz, Austria
[3] Graz University of Technology, Institute for Applied Information Processing and Communications (IAIK), Inffeldgasse 16a, 8010 Graz, Austria

guaranteed by the provider of an AAL system. In order to fulfil these needs, many factors have to be considered, especially security and privacy, not only regarding the monitoring of AAL users in their home environment [Mo07] but also in terms of data security.

AAL systems often connect elderly people with their carers. To ensure proper protection of the user's data it is crucial that secure AAL systems employ adequate cryptographic measures to secure network connections and to provide secure data storage capabilities. Transport security can be addressed by using appropriate transport layer protocols, such as TLS/SSL, to realize secure channels that guarantee data-confidentiality, data-integrity and origin-integrity properties between any two network-connected components of an AAL system. Within the scope of this paper, we assume that transport layer security can be solved adequately with secure channels. Secure channels only address security requirements related to *sensitive data in transit* between any two AAL system components. They do not provide any help with storing and sharing data securely.

Secure data storage capabilities are essential for AAL system components to ensure that confidentiality and integrity of sensitive user data is maintained at all times. Encryption of sensitive data stored on servers is one feasible approach to reduce the problem of protecting huge amounts of sensitive data. If proper algorithms and key sizes are used, encryption makes it virtually impossible for an attacker to break confidentiality of *sensitive data at rest*, without knowing the encryption keys.

Secure data sharing capabilities are required to facilitate data exchange between older adults and their carers. Within an AAL system, the data exchange is commonly done indirectly over a cloud-like infrastructure provided by the AAL provider. To protect the privacy and informational self-determination of the end-user, it is essential to have secure data sharing capabilities in the AAL system, which allows them to control sharing of sensitive data.

In order to enable users to store and synchronize their sensitive data in a secure way, it is the providers responsibility to implement an appropriate solution. A relatively new approach to realize a secure data storage is proxy re-encryption. Proxy re-encryption schemes are cryptographic schemes, which allow transformation of ciphertexts, encrypted with one secret key, to ciphertexts that can be decrypted with a different secret key. The ciphertext transformation requires a re-encryption key, which can (only) be derived by the owner of the original secret key.

This paper contains six major sections: Section 1 discusses the motivation for this work and introduces the overall security requirements in the area of AAL. Afterwards, section 2 briefly describes related work in the area of proxy re-encryption, on which this paper builds on. Next, the DALIA security concept and its underlying principles are introduced in section 3. Section 4 contains the main contributions of this paper, which consist of the implementation of the DALIA security framework and its proxy re-encryption library. Section 5 discusses critical aspects of the described implementation. Finally, Section 6 concludes the paper by summing up the advantages of proxy re-encryption in the presented scenario.

2 Related work and our contribution

The first concept of proxy re-encryption was introduced by Mambo and Okamoto in 1997 [MO97]. The authors described a cryptosystem that allows an original decryptor to transform its ciphertext into a ciphertext for a designated proxy decryptor, which is then able to compute a plaintext in place of the original decryptor.

In 1998, Blaze et al. [Bl98] described atomic proxy re-encryption as the currently used scheme for proxy re-encryption. A proxy is able to re-encrypt a ciphertext, produced by the public key of Alice into a ciphertext, Bob is able to decrypt with his own secret key and without actually knowing the secret key of Alice. Therefore, Alice has to create a re-encryption key, which consists of her private key and Bob's public key.

With this basic concept of proxy re-encryption, several possible applications have been explored. Kallahalla et al. [Ka03] examined re-encryption methods for realizing secure file sharing on an untrusted storage. This idea is carried on in DALIA, which is also used as trusted storage for its users, but is, for security reasons, treated as an untrusted entity anyway.

Chow et al. [Sh10] as well as Green and Ateniese [GA07] set the background for realizing a secure distributed storage with proxy re-encryption by examining unidirectional proxy re-encryption. In this concept, which is also applied in DALIA, the data owner does not have to share the private key with the proxy in order to make the data accessible to another user.

Meingast et al. [Me06] studied security risks in healthcare applications and defined relevant questions and requirements that have to be considered by data holders in order to guarantee appropriate data protection in healthcare settings. The key aspects of AAL, that were identified as security relevant, include data ownership, data storage, and data access.

The primary contribution of this paper is twofold: First, we discuss security issues in the area of AAL and show how DALIA addresses these issues. As second part of our contribution, we demonstrate how proxy re-encryption can be used to construct an AAL system that provides a good balance between security requirements, complexity of deployment and usability. Our system architecture enables the user to exercise full control over data sharing, while reducing the computational effort required at the users device to a minimum.

3 DALIA's security concept

One of the key objectives of the DALIA project is to develop an integrated home system supporting older adults as primary end-users in their daily life. To achieve this goal, DALIA incorporates a data storage and distribution framework that allows carers, as secondary end-users of the system, to securely access data produced by the older adults as primary end-users.

The primary DALIA end-users possess smartphones and smart TVs through which they are connected with their relatives or carers. Elderly people can easily stay in touch with their carers, who benefit from a simplified caring process. With DALIA, it is for example possible to automatically disseminate information about changes in the prescriptions of medication for older adults to their carers and relatives. This feature is only possible if all involved participants are able to share sensitive data with each other, in a manner that protects the confidentiality and integrity of the data and the privacy interests of its users.

In DALIA, an older adult can share data or groups of data – called *modules* – like agenda items or emergency contacts, but also sensitive health data like their medications with carers. Sharing data is not unique to DALIA. AAL systems often base on several users who are connected with each other allowing them to share sensitive health data. This is the reason why DALIA relies on proxy re-encryption to make dynamic sharing of data possible. However, unique to DALIA is, that high server-side security mechanisms guarantee for the safety of user data while at the same time ensuring strong cryptographically enforcement of user control over the data distribution. While DALIA enables users to precisely specify where their data may go, it does not demand an unreasonably high level of trust in the intermediate components responsible for the actual data transfer. The remainder of this section discusses the roles and data-flows within DALIA and the usage of proxy re-encryption.

3.1 Roles within the DALIA security framework

The three key roles in DALIA are data subjects, data holders, and third parties with access to the actual data. Data subjects are the producers of sensitive data, respectively the persons who are cared for, also called the “older adult”. The original data subject has full control over what happens to the data. Data holders are professional entities who take care of intermediate and long-term storage and processing of data and should not know the real content of the data. In particular, data holders must not be able to share sensitive data with any unauthorized third parties that were not explicitly approved by the data subject. However, it is possible for data subjects to allow data holders to perform a restricted form of analysis or processing of the data.

The third key role are trusted third parties, typically professional and informal carers or medical services, whom the data subjects trust and explicitly grant access to the data. Those trusted third parties should be able to acquire the relevant data for which they have proper authorization from data holders.

Practical realization of this setting depends on suitable cryptographic methods that allow expressions of trust relationships between the stakeholders by cryptographic means. Therefore, we identified unidirectional proxy re-encryption as such method to realize the DALIA security framework.

3.2 Unidirectional proxy re-encryption

With a re-encryption key, DALIA is able to make data, which is originally encrypted for the older adult, accessible to a carer. In addition, with proxy re-encryption it is possible to share the same ciphertext created by the older adult with different individuals only through re-encrypting the ciphertext with different re-encryption keys.

Proxy re-encryption can be implemented via unidirectional and bidirectional schemes. DALIA uses unidirectional proxy re-encryption because one older adult can have multiple carers to whom the data has to be shared. Bidirectional proxy re-encryption schemes would additionally allow the proxy to re-encrypt the carer's ciphertexts for the older adult. The following figure shows the concept of proxy re-encryption in DALIA.

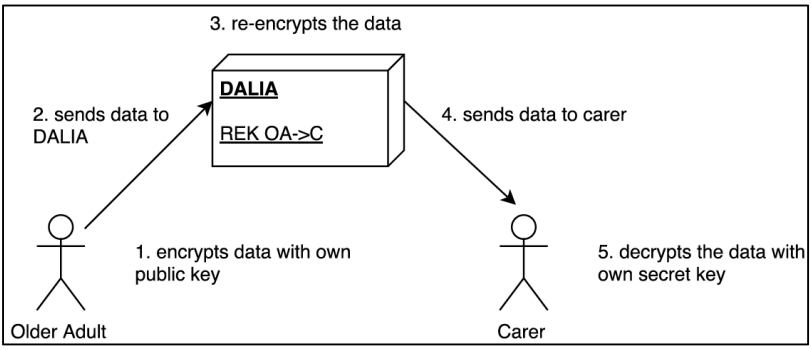

Fig. 1: Proxy re-encryption concept

DALIA uses the re-encryption key derived from the older adults private key and the carers public key (REK AO→C) in order to make the data of the older adult accessible to the carer.

3.3 Encryption and storage of data via proxy re-encryption

In DALIA, the older adult can share several modules with a specific carer. In order to illustrate the proxy re-encryption process in DALIA, the following example explains a typical scenario:

- The older adult creates a new record (e.g. a new medication to be taken).
- The older adult's device creates a key to encrypt the record symmetrically.
- The symmetric key is encrypted with the older adult's public key.
- The encrypted record is put on the DALIA server together with the encrypted symmetric key.

The client encrypts the data symmetrically because of performance reasons. In some cases,

the data could contain binary content like pictures or videos. As a result, the data exhibits a large size and would take much longer to encrypt, decrypt and re-encrypt asymmetrically. The re-encryption of a relatively small key, used for symmetric encryption and decryption, is much more performant than the re-encryption of the actual data.

3.4 Data sharing

An older adult can decide to share a specific module with a carer. To continue the above-mentioned example, an older adult could decide to share all medications with a specific carer and therefore grants access to the medication module. DALIA then allows the carer to receive all medications in an encrypted way. Initially, if a user wants to share data with a carer, the client of the older adult generates a re-encryption key. Only with this re-encryption key, the client of the carer can decrypt the encrypted symmetric key to decrypt the data.

The following picture visualizes the process of sharing data of a specific module of an older adult with a carer.

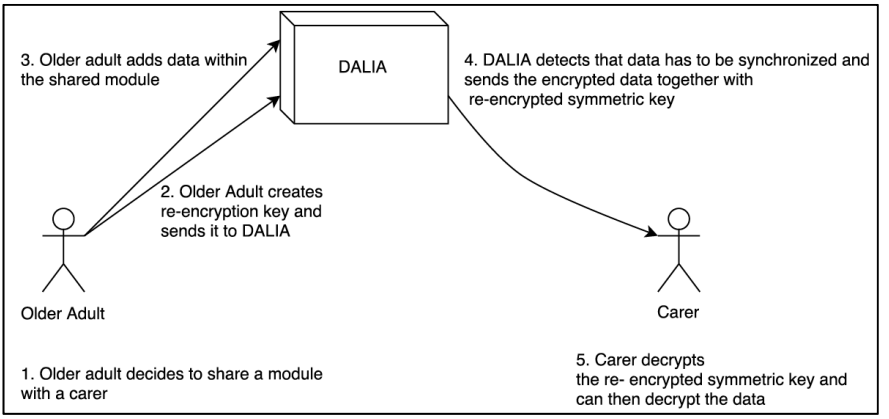

Fig. 2: Encrypted data transfer

Access revocation

DALIA maintains a list that includes a reference between the older adult's modules and the information with whom they are shared.

If an older adult decides that a specific module should no longer be shared with a carer, this reference is simply deleted, which causes DALIA to remove all related data from the carers device. Furthermore, no data is synchronized any longer to the carer.

4 DALIA's security framework

4.1 Proxy re-encryption implementation

In order to generate a proxy re-encryption key, an authentic copy of the carer's public key and the older adult's private key is needed. In the DALIA setting, the owner of the private key (the older adult) always derives proxy re-encryption keys. Therefore, authenticity of private keys is guaranteed implicitly. In order to guarantee that a given public key really belongs to the intended recipient (the carer) explicit authentication is needed. This setting equals other asymmetric encryption schemes, such as RSA, and the solutions to the public key-distribution problem (e.g. PKI).

Proxy Re-Encryption Java Library (reproxy)

We have implemented a standalone Java library (reproxy) to provide the cryptographic primitives for proxy re-encryption in the prototype of the DALIA security framework. This library is designed to abstract the specifics of unidirectional proxy re-encryption schemes behind a scheme-independent simple application programming interface (API).

The reference implementation of our library implements a variant of the unidirectional proxy re-encryption found in Ateniese et al. [At06]. This scheme uses an elliptic curve variant of the El-Gamal encryption scheme in combination with bilinear maps. For elliptic curve and pairing support, our reference implementation uses the open-source jPBC library[4]. No additional external dependencies (apart from the Java Runtime Environment) are used.

The scheme-independent API is the primary interface to the proxy re-encryption library. It contains Java interfaces modelling domain parameters, proxy re-encryption schemes, and the different types of keys (public key, private key and proxy re-encryption key). Operations like key generation, encryption, re-encryption and decryption are modelled as methods on these interfaces.

One challenge that is addressed in the scheme-independent API are the differences between encoding of plaintexts and ciphertexts for different schemes. Depending on the internals of a particular proxy re-encryption scheme the actual message may be mapped to different mathematical objects like integers in some group, points on an elliptic curve, or elements of some finite (extension) field. Even for the same type of mathematical object (like an elliptic curve point) there is often more than one possible way of mapping an arbitrary plaintext byte array to a point. To deal with these differences our scheme-independent API encapsulates plaintext and ciphertext messages that are encoded for a particular proxy re-encryption scheme as Java objects of special type. Encoding and decoding facilities that allow mapping between arbitrary Java byte arrays and these objects are provided as part of the generic proxy re-encryption scheme interface. This design enables library users to work with the library, without noticing the low-level details of the

[4] http://gas.dia.unisa.it/projects/jpbc/

proxy re-encryption scheme in use.

The message encoding facilities of the library also partly address the issue of message length limitations, for example due to the bit-length of moduli. When instantiating a proxy re-encryption scheme, the library user can select a message "codec". That defines how message byte arrays are encapsulated and padded. The reference implementation of our library currently implements four different codec types:

The **"raw"** codec literally maps the message byte array to an unsigned integer value without any further padding. The maximum message length is subject to bit-length limitations (e.g. moduli, group orders) of the scheme, and cannot (automatically) recover the length of the message byte array on decryption.

The **"simple"** and **"oaep"** codecs are based on the PKCS#1 specified padding schemes for RSA encryption. Both of these codecs pad the message byte array, before mapping them to an unsigned integer. The maximum message length is subject to bit-length limitations (e.g. moduli, group orders) of the scheme. For both codecs the padding method allows unambiguous recovery of the length of the message byte array. Decrypted messages will have exactly the same length as the original plaintext byte array used during encryption.

All of the three codecs discussed so far are only suitable for encoding messages, which are shorter than a size limit implied by the choice of domain parameters. To overcome these limitations, our library provides an **"ephemeral"** codec implementing a simple key wrapping scheme: The **"ephemeral"** codec generates a random (ephemeral) key that is encrypted using the proxy re-encryption scheme. The actual message byte array provided by the user is symmetrically encrypted using the ephemeral key. This codec does not have any message length limitations, since the actual payload is encrypted with a normal block cipher. Message integrity can be provided by using a block cipher that supports authenticated encryption (AE), such as AES-GCM.

4.2 Key management

In order to guarantee confidentiality of the stored sensitive data via our proxy re-encryption concept, all participants need to possess a key pair, consisting of a secret key and a public key. Therefore, it is important to define a key distribution concept, which ensures the correct key management in DALIA. The following section describes our approach in more detail.

An older adult usually owns two devices: a smartphone and a smart TV. Both devices have to encrypt their sensitive data via the same secret key, so it is necessary to distribute the keys between them. While there are several concepts available to distribute the asymmetric keys between a system and its users, DALIA generates the key pair for the user. This approach offers a maximum of convenience for DALIA users, while at the same time it demands a certain amount of trust in DALIA. Alternatively, it is possible to create the keys on the client-side or to include a third party into the whole process, as described in

the discussion in section 5. One of the most important aspects of the concept is the recovery password, which DALIA generates randomly. The secret key of a user is encrypted symmetrically with this password to enable DALIA to back up the secret key without having access to it. The user receives the recovery password via mail. With this recovery password, a user can retrieve the encrypted key pair from DALIA and decrypt it. If an older adult receives DALIA for the first time and sets up the devices, each client tries to receive its encrypted key pair. After the setup, the client can use the secret key to decrypt the data and to create re-encryption keys for data sharing.

The actual re-encryption is done on the cloud-server for performance and availability reasons. The client devices used in DALIA, like smartphones and smart TVs, have limited resources and the devices cannot always rely on an available internet connection. Therefore, shared data may not be available for authenticated receivers all the time. This is why the server holds the re-encryption keys and takes care of all re-encryption and data distribution tasks.

4.2.1 Key recovery and backup

If a user loses a device, for example the smartphone, there would normally be no way to obtain the encrypted data, which is stored on DALIA, back on a new smartphone. With the recovery password, the user can easily regain access to the encrypted data with a new smartphone.

The DALIA server has access to the database server, which stores all relevant information about the users like username, hash of the password as well as their encrypted secret key and public key but not the recovery password. After the key pair was initially created and encrypted with a randomly generated recovery password, the recovery password is send to the user but is not stored on the server. Having access to the recovery password would enable unauthorized persons to gain access to the secret key, which then gives access to the encrypted sensitive data. Therefore, only the user has access to the recovery password, which is distributed to the users via a QR-Code that is included in the welcome letter.

4.3 Practical Proxy re-encryption scenarios in DALIA

In DALIA, four different data exchange scenarios can occur. In the first scenario, an older adult creates data within a certain module, either via the smartphone or via the smart TV. This data has to be synchronized to the carer who has access to the module. In this case, DALIA re-encrypts the data in order to make it accessible for the carer. Figure 3 visualizes this case in scenario 1.

Another scenario would be a carer, entering data for a specific older adult. In this case, no re-encryption has to take place because the data created by the carer has a clear destination, which is a specific older adult. Therefore, the data is encrypted with the public key of the older adult and can be decrypted with the older adult's secret key (see scenario 2 in Figure 3). This scenario works similar, regardless whether the data is synchronized to the older

adult's smartphone or the smart TV.

In addition, data which is available on the older adults smart TV has also to be synchronized to the older adult's smartphone. Therefore the older adult's smart TV encrypts the data with the own public key and sends it to DALIA. The smartphone checks regularly whether there exists new data, which has to be synchronized and finds the new entry. DALIA recognizes, that the data comes from the older adult and has to be send to another device of the same older adult. Therefore, no re-encryption is necessary but the data is directly sent to the older adult's smartphone. The smartphone decrypts the data with the secret key and stores it. Figure 3 visualizes this case in scenario 3.

The same synchronization is necessary if a carer adds data on behalf of the older adult via the hosted service and then has to be synchronized to the carer's mobile devices. In this case, the carer encrypts the data with the older adult's public key and stores it on DALIA. In order to access the data on a different device of the carer, the data is again re-encrypted to make a decryption with the carer's secret key possible. Figure 3 visualizes this case in scenario 4.

In all scenarios, DALIA takes care of a possible necessary re-encryption which is always necessary if data of an older adult has to be synchronized to a carer or if data of carer's device 1 has to be synchronized to carer's device 2. The devices of both, the carer and the older adult, always receive the data in a way that it can be decrypted with their own secret key, which is done in the "crypto service". The crypto service is also responsible to encrypt outgoing data with the older adult's public key. Hence, DALIA always encrypts user data with the older adult's public key.

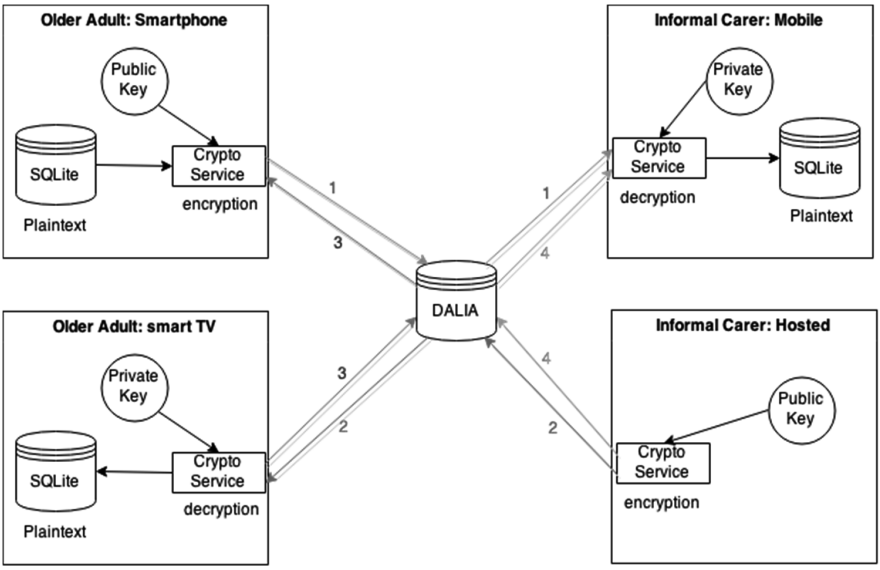

Fig. 3: Data exchange scenarios

5 Discussion

5.1 Alternative key management approaches

Usually, it is common to generate the key pair on the client device. In DALIA, we decided to generate the key pair on the server and to store it in an encrypted way. This approach offers a minimum of user interaction and at the same time ensures that the key pair can never be lost. If the client generates the key pair and the user does not correctly backup the secret key, the loss of the smartphone and hence the secret key has severe consequences. The data, which is stored on DALIA, is only accessible for the older adult with the correct secret key. Because DALIA never has access to the plain data, an unauthorized recovery would not be possible. Relying on the server in terms of key management requires a specific amount of trust in DALIA. This is why a third party should monitor and approve this process to guarantee trustworthiness of DALIA.

Another possibility would be the inclusion of a third, unbiased and trusted party (like a notary) into the key management process. This third party would undertake the task of creating, storing and sending the key pair to the users instead of DALIA. This approach combines both targets, namely usability and security as the user receives again a letter with a QR-Code, which contains the recovery password. The user then only has to scan the QR-Code in order to set up a new device. In terms of security, the whole concept

becomes more reliable because of the exclusion of DALIA from the critical process of key generation.

5.2 Granularity of shared modules

An important aspect of the whole DALIA security framework is the granularity of modules. If an older adult shares a specific module with a carer, all data, which falls into a specific module, is accessible for the carer. At the current state of DALIA, there is no need to make the sharing concept more fine-grained but in some cases, it makes sense to limit the access to the data even within a specific module. An example would be to share just a limited list of medications to a specific carer if the older adult wants to hide specific information like a specific medication, which could indicate a certain medical condition.

6 Conclusion

Because AAL applications often process sensitive health data, secure storage and data protection is essential. Protecting the stored data in an encrypted way and at the same time allowing users to share their data with selected individuals is a highly complex task. In this paper, we investigated the use of proxy re-encryption as one possible solution that can fulfil these requirements. With the DALIA security framework introduced in this paper, users can share specific data sets with selected individuals, while at the same time the data store never has access to the plaintext data. In addition, the presented solution allows users to revoke the granted access to the data easily. Furthermore, it is possible to create a re-encryption key at a later point in time, even for users, which did not exist at the time of encryption. This means, an older adult can store data in a secure way and can share it later with another user like a physician. This approach works because data is always encrypted in the same way, namely with the older adults public key. The server then performs the re-encryption if necessary to make the data accessible for different individuals. This proxy re-encryption approach in combination with the usage of transport layer security (TLS) in the background results in a strongly protected data storage and distribution system. All of the described proxy re-encryption features make the presented concept highly dynamical and easy to use because all of its complexity is hidden for the users, which makes it ideal for Ambient Assisted Living applications.

Acknowledgments: This work has been supported in part by the European Commission through the AAL Joint Programme under contract AAL-2012-5-249 DALIA.

References

[ST07] Sattarova Feruza Y. and Prof. Tao-hoon Kim. IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. International Journal of Multimedia and Ubiquitous Engineering, Vol. 2, No. 2, April 2007.

[Mo07] Moncrieff, S., Venkatesh, S. and West, G. 2007. Privacy and the Access of Information in a Smart House Environment, in Wang, J.Z. et al (ed), Proceedings of the 9th ACM SIGMM International Workshop on Multimedia Information Retrieval (MIR 2007), Sep 24-29 2007, pp. 671-680. Augsburg, Germany: Association for Computing Machinery (ACM).

[MO97] M. Mambo and E. Okamoto. Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 80(1):54-63, 1997.

[Bl98] M. Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. In K. Nyberg, editor, Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques, volume 1403 of Lecture Notes in Computer Science, pages 127-144. Springer, 1998.

[Ka03] Mahesh Kallahalla, Erik Riedel, Ram Swaminathan, Qian Wang, and Kevin Fu. 2003. Plutus: Scalable Secure File Sharing on Untrusted Storage. In *Proceedings of the 2nd USENIX Conference on File and Storage Technologies* (FAST '03). USENIX Association, Berkeley, CA, USA, 29-42.

[Sh10] Sherman S. M. Chow, Jian Weng, Yanjiang Yang, and Robert H. Deng. Efficient Unidirectional Proxy Re-Encryption. In Progress in Cryptology -AFRICACRYPT 2010, volume 6055 of LNCS, pages 316–332. Springer, 2010.

[GA07] Matthew Green and Giuseppe Ateniese. Identity-Based Proxy Re-encryption. In ACNS 2007, volume 4521 of LNCS, pages 288–306. Springer, 2007.

[Me06] Meingast M, Roosta T, Sastry S. Security and privacy issues with health care information technology. Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS ’06); September 2006; pp. 5453–5458

[At06] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Trans. Inf. Syst. Secur.* 9, 1 (February 2006), 1-30. DOI=10.1145/1127345.1127346 http://doi.acm.org/10.1145/1127345.1127346

Detlef Hühnlein et al. (Eds.): Open Identity Summit 2015,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2015 85

Economic Issues of Federated Identity Management – An Estimation of the Costs of Identity Lifecycle Management in Inter-organisational Information Exchange Using Transaction Cost Theory

Sebastian Kurowski[1]

Abstract: Inter-organisational data-exchange is common in inter-organisational value-chains. Currently information providing organizations enrol users of suppliers, in order to enable them to access their services and information. This leaves some users with the issue of handling multiple credentials, introducing risks of password-reuse [Iv04] and weak-passwords [Ne94]. Federated identity management eases this scenario, by enabling users to authenticate against their organizations' identity provider [Hü10]. However, the costs involved in managing the underlying identity and rights lifecycle have hardly been considered. This paper addresses this gap, by using the principal-agent theory, and transaction cost theory, structuring the identity lifecycle using [BS08] [IS05] [IS10], and estimating the management costs. We finally analyse the economic benefits of federated identity management in inter-organisational information exchange. We find that while process costs for executing the identity lifecycle are reduced for the information provider, by introducing federated identity management, the control costs reduce, and in one case even diminish this cost benefit. We briefly discuss our findings, and conclude that further mechanisms and research is required to reduce the efforts in auditing, in order to fully unlock the security and economic benefits of federated identity management.

Keywords: Identity Lifecycle, Identity Management, IAM, Security Management, Access Control, Transaction Cost, Principal-Agent Theory, Entity Assurance, Auditing

1 Introduction

Inter-organisational data exchange is common in inter-organisational value-chains, where suppliers are largely integrated into product development and production processes. The automotive industry, for instance is collaborating in networks, introducing different suppliers, also of competing supply chains [Ku14], [Ku13], [We13]. Authentication and authorization is hereby often handled by the provision of credentials and identities by the information provider. However, this leaves users with multiple credentials, yielding the risk of weak passwords or password reuse [Iv04], [MD08], [Ne94]. Federated Identity Management introduces security advantages, by enabling authentication of users against fewer identity providers, enabling users of suppliers to authenticate against their companies identity provider, while accessing

[1] Institute of labour science and technology management IAT, University of Stuttgart, Competence Team Identity Management, Allmandring 35, 70569 Stuttgart, sebastian.kurowski@iat.uni-stuttgart.de

resources of an information provider [Hü10] , [Hü11]. While the advantages in authentication and security have been largely discussed and acknowledged, the identity lifecycle, including the provision of identities and access rights has been neglected. This paper aims at filling this gap, by addressing the necessary tasks of the identity lifecycle in inter-organizational information exchange, estimating the costs, and then choosing a transaction-cost perspective on federated identity management discussing whether the benefits of federated identity management disperse throughout the whole identity lifecycle, or whether costs induced by opportunism of the suppliers tend to minimize the benefits. We therefore start with discussing the identity lifecycle, and in order to be able to estimate the costs of the identity lifecycle, introducing aspects of information security management [IS05], and authentication assurance [IS05]. We then estimate the costs of the identity lifecycle as such, by using sources regarding the amount of helpdesk employees [MA15], working time required for provisioning tasks [OL10] and price lists of providers for identity document legitimation and verification. For the identification of the tasks we oriented on the assurance levels LoA 3 and 4 of [IS10], arguing that the exchange of information may put the confidentiality of intellectual property and thus of critical knowledge at risk.

2 State-of-the-art

Economic considerations of security has broadly been concerned on information security budgets [An08] [An01], user adoption of security technologies [Hü10], [Ro10], [RZ12], organizational behaviour regarding privacy and security investments [GG05], [Go03], [MR09], [No12], and cost assessment of security technology introduction, such as electronic signatures [RR05a], [RR05b]. While approaches on assessing investment returns of enterprise identity management [Ro13] exist, there is publication, known to the author, regarding the costs of the identity lifecycle as such. The identity lifecycle introduced by [MR08] enables a structured approach on assessing the efforts involved in managing identities and access rights as such. It includes the task of registration, provisioning, usage, deprovisioning and auditing. Registration hereby involves the creation of an identity for a subject, whereas provisioning involves the correlation of required access rights and credentials with the identity. Usage includes all user-related aspects of authentication and credential handling, whereas deprovisioning involves the revocation of access rights, credentials, or identities. Finally regular audits are introduced, in order to ensure the integrity of the identity- and access rights data infrastructure.

The identity lifecycle as such as relatively easy to grasp and should not introduce major issues for organizations. However findings by practicioners, such as [Wa12a] indicate that the introduction of auditing aspects does not necessarily imply a security benefit, as „many IT departments, in the run-up to an audit, apply themselves dilligently to ensuring they achieve the proper compliance“, yet „…once the pressure is off, they tend to neglect compliance throughout the rest of the year“ [Wa12a]. Additionally incidents, such as

[Ze12], where access rights for a suppliers employee, which have not been revoked in time, where used in order to steal intellectual property of the information providing organization, indicates that a mixture of opportunistic behaviour, non-controllability of a suppliers identity lifecycle, and the proper execution of the identity lifecycle may be put in question in some cases.

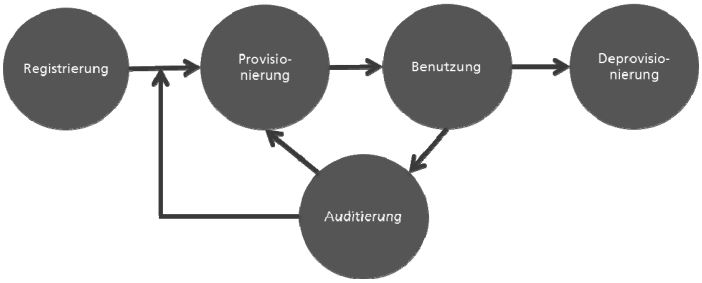

Fig. 1: The identity lifecycle [MR08]

Our research focuses on a distinct scenario, in which an organization integrates suppliers in its' value chain in product development and production tasks. This integration of course requires the provision of critical intellectual property by the organization. Our research hereby focuses on untangling this relationship, identifying the vulnerabilities, and ultimately developing countermeasures in order to avoid leakage of intellectual property to competitors. When turning to economic theories, we are able to characterize the described relationship using the principal-agent theory [LM01]. This theory introduces the concept of a principal which desires the execution of a task, and an agent executing the task. It assumes opportunism, meaning that both the agent and the principal will try to maximize their own utility, even if the utility of the other party is reduced by their actions. Additionally, this setting yields asymmetric information between the principal and the agent. The agent may consist of hidden characteristics, or hidden intentions, which the principal is not able to observe when negotiating the contract. Additionally the agent may execute hidden actions. Under the assumption of opportunism, and being able to hide actions, or meme certain characteristics and intentions towards the principal, enables the agent to maximize the own utility, while the principals utility is being reduced. The principal-agent theory focuses largely on the process leading up to a contract. Actions, characteristics and intentions which may occur ex-post to the contract negotiation in a principal-agent setting, can be described by using the concept of transaction costs [Pi03], [Wi81]. In transaction cost theory we differentiate between the costs which occur ex-ante to a transaction, and costs which occur ex-post to a transaction. Ex-ante costs hereby include costs for initiation of a transaction, and negotiation. Ex-post costs however, include costs for executing a task, adjusting task characteristics, and controlling the task execution. We can further differentiate the relationship between the principal and the agent in being characterized by a hierarchy (integrated organizations whose utility depends on the benefits of the principal), hybrid forms (e.g. sub-organizations, which are competing freely on the

market), and market forms [Pi03]. The latter will be the most interesting integration form in our case, as supplier integration yields large benefits due to the access to competing, and thus improving suppliers [Ku13] [We13], requiring an open market, and thus a low degree of integration by the principal.

3 Scenario

Knowing the characteristics of the relationship between an organization and its' suppliers in inter-organizational value chains, we are now turning towards our scenario, which involves a principal, providing information, and an agent using this information in order to execute a task. The principal requires the agent to handle the information adequately, including proper management of the identities and access rights. The agent however, will aim at maximizing its' own utility, minimizing costs and thus may aim at cost savings of the identity lifecycle. This of course leads to access rights, and identities not being revoked, criminals potentially impersonating employees, and credentials not handled correctly. In order to stress the roles of the principal and the agent, we will in the following refer to the principal and being the Information Provider (IP), and the agent as being the Information User (IU). We further involve the observation, that collaboration in value-chains may be characterized by a full mesh, indicating that a IP may exchange information with multiple IU, even from competing supply chains [We13]. We will consider the identity lifecycles of the IU and the IP in two different cases, involving the use of federated identity management (in the following referred to as the "Federated Identity Management" Scenario), and the provisioning of access-rights and identities by the IP (In the following referred to as the "Extranet" Scenario). In both scenarios our cost analysis focuses only on the costs arising out of the collaboration scenario. This means, that we only consider identity lifecycle costs for external employees. Therefore we neglect the costs for identity lifecycle management of the IPs employees in the "Extranet" scenario.

4 Costs of identity and access rights lifecycle management

In order to assess the impact of transaction costs on identity and access rights lifecycle management in federated identity management, we aim at identifying the process costs involved for the IP and the IU, as well as the costs for control and communication. In our approach we therefore consider the structure of the identity lifecycle, controls from [IS10] and [IS05] to identify the tasks. We then discuss these tasks and estimate the process costs, by considering costs and execution frequencies from [OL10].

Throughout our analysis and articulation of included tasks in identity lifecycle management we identified the following process fields: (1) Identity Proofing and identity information verification [IS10], (2) Credential renewal and/or replacement [IS10], (3) Registration [IS10], (4) Credential creation [IS10], (5) Credential activation

[IS10], (6) Credential issuance [IS10], (7) Deprovisioning [IS10], (8) Security training and awareness [IS05], (9) Provisioning of a central contact for security events [IS05], and (10) Auditing [IS05] [IS10]. Hereby the process (1) is being considered as enrolment in the identity lifecycle. The processes (3), (4), (5), and (6) are being considered as provisioning in the identity lifecycle. Processes (8) and (9) are being considered as usage, and processes (7) and (2) are being considered as deprovisioning. Finally, process (9) is considered as the auditing phase in the identity lifecycle [MR08].

The whole structure of the identity lifecycle using ISO/IEC 29115 controls for LoA 3 and 4 would exceed the limits of this paper. Yet, we will in the following try to briefly describe the associated tasks, the respective cost drivers and estimated costs per identity lifecycle area. Hereby we only consider process costs of the organization, e.g. costs for capturing or validating attributes. Costs of the entity are being omitted, as we aim at identifying the costs for the IP as a reference for our analysis, whereas costs of the entities are costs of the IU, which are omitted in our considerations.

Enrolment

During enrolment the identity of the subject is being verified, by identity proofing and identity information verification [IS10]. This task can hereby be carried out off-site, or on-site, whereas in LoA 4 an on-site verification is mandatory. Viewing the controls for identity proofing and identity information verification, we concluded that these included for the off-site case: Provisioning of identifying and other attributes, validation of the attributes, provisioning of secrets, and validation of the secret by a trusted third party. The on-site case includes the provisioning of an authoritative document, validation of the documents' validity and genuineness, provisioning of identifying and other attributes, validation of these attributes, provisioning of contact details, and validation of the contact details. Additionally, in LoA 4 on-site verification and the provisioning of a second authoritative document is mandatory. The controls of identity proofing therefore mainly includes tasks of comparing and capturing attributes, validating attributes, and validating documents. In the case of on-site proofing we shall additionally include the task of scheduling an appointment. Using these abstract tasks, we are able to state the following assumptions (A1) to (A3): **(A1)** If we assume automation in capturing attributes, e.g. by using a web portal, and in validation, e.g. by using web services for validating authoritative documents, we assume that no further process costs are introduced. Although the transaction costs of using third parties and validation services can be significant[2], we focus mainly on the created process costs, neglecting these costs for comparing and capturing attributes, and for validating attributes. However, in the case of manual capturing and comparison, and validation of attributes we estimate 5 working minutes for entering the attributes, submitting these to a validation service[3], and

[2] For instance the German PostIdent service which enables off-site identity verification costs between 3,50€ and 8,90€ per transaction. For a list on prices of the PostIdent service, please refer to https://www.deutschepost.de/content/dam/dpag/images/P_p/Postident/Postident%202015/preisliste-postident-20150526.pdf

[3] For a list on web services for validation of authoritative documents (in German) please refer to: http://www.bundespolizei.de/DE/01Buergerservice/Dokumentenpruefung/_dokumentenueberpruefung_anmo

assessing the outcome of the validation. Hereby, capturing and comparing attributes may largely depend on the complexity of the attribute, and the familiarity of the capturing individual with this attribute. E.g. a very long personal ID number may be more time consuming to capture, than very short familiar attributes such as sex or dates of birth. **(A2)** Validating documents includes validating the genuineness and the document itself. Depending on the familiarity of the individual with the document the required working time may be negligible. However, if the individual is required to use databases on authoritative documents[4], e.g. if the individual is completely unfamiliar with the document, we estimate the validation to require 5 working minutes. **(A3)** Finally, we estimate the scheduling of an appointment to require at least 5 working minutes for initiating and finding a suitable date and at most 10 working minutes in the case of multiple required transactions. Using these assumptions we can estimate, that in the off-site case, 0 to 5 working minutes are required for capturing and validating identifying and other attributes under assumption (A1). Capturing and validation of secrets is regarded as capturing and validation of attributes and thus creates additional costs of 0 to 5 working minutes. We can therefore conclude that the off-site case introduces process costs of 0 to 10 working minutes for identity proofing.

The on-site cases however, additionally requires the scheduling of an appointment, which costs 5 to 10 working minutes under assumption A3, along with the provisioning and validation of an authoritative document (0 to 5 working minutes under assumption A2). Additionally, the identifying and other attributes must be captured and validated which creates costs from 0 to 5 working minutes under assumption A1. Contact details must be captured and validated which, when treated as attribute capturing and validation creates costs from 0 to 5 working minutes under assumption A1. Finally, in the case of LoA 4, which has been omitted for off-site verification as on-site verification is mandatory in LoA4, the additional capturing of attributes from a second authoritative document is required, creating additional costs of 0 to 5 working minutes under assumption A1. We can therefore conclude that the process of identity proofing and identity information verification introduces costs between 0 working minutes in the case of off-site proofing and LoA 3, and 30 working minutes in the case of on-site proofing and LoA 4.

Provisioning

The Provisioning phase consists of the registration, which includes the creation of an identity, the creation of a credential, the issuance of the credential, and the activation of the credential by the entity. According to [IS10] credentials should involve two-factor authentication, limiting the producible credentials to PKI based smartcards, secured software credentials, unprotected software tokens, biometric tokens with password, and hardware OTP tokens. Credential production hereby additionally includes access control

d.html

[4] One example for such databases is the PRADO database, which holds information on characteristics of authoritative documents. The database can be found at: http://www.consilium.europa.eu/prado/de/prado-start-page.html

to the credential inventory, in order to prevent credential theft. Therefore an additional identity management infrastructure is required for managing access rights to the credential inventory. In order to estimate the costs of the tasks involved in credential creation, we are using the following assumptions: **(A4)** Only one credential is issued per user. **(A4a)** Production costs for unprotected software OTP files are negligible. Production costs for Secured Software Credentials are estimate to be 70€ per user. Production costs for PKI credentials are assumed to be negligible and are thus reduced to the operation costs of Public Key Infrastructures which are 150€ per user [Ve05]. Finger-vein and palm-vein devices are estimated to cost up to 3.000€ per user including template creation and devices [Si15]. Therefore production costs for a credential can be between 0€ and 3.000€ per user. **(A4b)** In the case of biometric credentials we additionally assume negligible working time for the template creation, and up to 1 minute for template creation. **(A4c)** The costs for the required access control to the credential inventory is estimated to be the costs of registration, which can create costs between 6,6 and 12,4 minutes per user [OL10]. Using these assumptions we can estimate that the costs for credential creation are between 6,6 and 13,4 working minutes per year under assumption A4c and A4b. Additionally, the costs of the credentials can range between a negligible amount up to 3.000€ per user und assumptions A4 and A4a.

Issuance of the credential can be done in-person or impersonal, whereas impersonal issuance may include the usage of internal issuance infrastructures, or external services such as (express) mail. In the case of in-person issuance, scheduling an appointment is necessary, along with identity proofing acknowledgement of receipt. Additionally, in the case of LoA 4, acknowledgement of receipt of the credential is required. The costs for credential issuance are being estimated using hypotheses A5 to A8: **(A5)** Impersonal issuance requires verification of the recipients address [IS10]. The transactions included for address verification requires the organization to provide multiple attributes to a third party, and receive and interpret the verification result. We assume no automation and therefore estimate the consumed working time to be at least 5 working minutes and at most 10 working minutes, depending on the amount of required attributes[5]. **(A6)** Impersonal issuance done via internal mailing systems creates negligible costs. **(A7)** If the impersonal issuance is done using an external party, service ordering and packaging of the credential according to the third parties rules, may consume between 5 and 10 working minutes. **(A8)** Receipts of acknowledgement are handled by the third party and are thus neglected.

Therefore we can conclude that for impersonal issuance, which requires address verification (A5), packaging and service ordering (in the case of a third party) (A7), and creation of an acknowledgement of receipt (A8) consumes at least 5 working minutes (in the case of using the internal mail infrastructure) and up to 20 working minutes. Personal issuance on the other hand, requires scheduling an appointment, which can be assumed

[5] Required attributes for address verification, e.g. at federal authorities may include the provisioning oft he full name, and the birth date, along with costs about 8€ to 10€. For a full price list please refer to: https://www.verwaltungsservice.bayern.de/dokumente/leistung/66886554503

to consume between 5 to 10 working minutes under assumption A3. Additionally, identity verification of the recipient and the creation of a receipt of acknowledgement are required. Arguing that for identity verification, the sender may verify the recipients identifying document, and neglecting the costs for creating a receipt of acknowledgement we are able to estimate this activity to consume up to 5 working minutes. Therefore we are estimating the costs for personal issuance of a credential to be between 5 and 15 working minutes.

Activation of the credential creates requires the entity to follow an activation process, usually involving entering of an issued activation code. However, as these costs mainly occur at the entity, and since the entity in scenario is not associated with the IP, we neglect the costs for activation of the credential.

Last, but not least the registration includes the provisioning of the partial identity and of access rights for the partial identity. According to [OL10] we differentiate between the provisioning of access rights for new identities, the provisioning of not yet existing access rights for existing identities, and the provisioning of existing access rights for existing identities. Using [OL10] we estimate the costs for the registration process to be within 6,6 to 12,4 working minutes, depending on the availability of RBAC.

Usage
Apart from credential characteristics, as the usage of a secured channel throughout authentication, or the absence of identity information transmission, credential storage, and credential handling by the entity is crucial for avoidance of unauthorized access. Therefore security training and awareness (SETA) programmes must be maintained within the organization [IS05]. Additionally, the implementation of a central security event contact, where users can provide observations regarding security lacks in the organization is beneficial for improving the handling and secure storage of credentials [BS08]. Therefore we estimate the costs for the usage phase, by estimating the costs for SETA, and a central security event contact. According to [Bu10], [Ar08], [Wa12b] the success of awareness programs largely depend on their ability to implement a security culture. Therefore all employees, including managerial staff must attend SETA events. Additionally, [Em05] show that the frequency of SETA events may positively impact the user behaviour. **(A9)** We estimate an awareness training to consume between 2 and 5 hours of working time per user. Additionally we estimate a frequency of the trainings to be between 3 monthly and yearly trainings. As every employee should attend this training, we can therefore assume between 120 and 1200 working minutes per year. Additionally, we assume that the preparation of the trainings require up to 24 working minutes per user per year, as the preparation may be neglectable, in the case of using security training software[6].

For the security event contact, we assume that the main tasks are to receive notifications on security-related observations by users, to analyse and document these notifications, and to escalate the events towards incidents or even problems. This similarity with

[6] An example application can be found at http://www.e-sec.at/de-at/virtualtrainingcompany/elearningsoftware

service desk processes, as in [TS11] enable us to estimate the costs for this contact by using a service desk ratio of 1 employee per 70 users, as in [MA15]. Using a monthly working time of 160 hours, we are able to receive a working time of 34,23 working minutes per user, per week. Assuming that we may have at least 1 observed security event per year, and at most 1 observed security event per week, we can estimate the costs for the security event contact to be between 34,23 working minutes and 1369 working minutes per user, per year.

Deprovisioning
Deprovisioning consists of the revocation of identities, access rights and credentials, along with identity proofing for eventually replacing, or renewing identities, as in [IS10]. The costs for deprovisioning can be estimated using [OL10], who estimate at least 4,7 working minutes for the termination of access rights. The revocation of credentials, requires the deactivation, destruction and disposal of the credential along with documentation of the credentials status. Using assumption A1 and no automation we estimate this task to include transactions between credential status information systems and receiving the credential itself. Therefore we estimate the costs for revocation of credentials to be between 5 and 10 working minutes per credential, depending on the availability of information, and the usability of inventory and credential status information systems. According to the controls of ISO/IEC 29115, credential renewal and replacement can be minimized to identity proofing and identity information verification. Yet, the required controls for LoA 3 and LoA 4 credential renewal, include LoA 2, and LoA 3 information proofing and validation, which does not require the provisioning of additional documents. Therefore one task including attribute capture is not required. Yet, initiation and proofing possession of the credential is mandatory [IS10]. Arguing that proofing the possession may include the provisioning of a credential id, or in the case of PKI based credentials may be fully automated we can estimate these additional costs to be negligible and at most 5 working minutes under assumption A1. Therefore credential renewal and replacement consumes at least 0 to 30 working minutes, similar to identity proofing and identity information verification.

Auditing
Regular auditing is crucial for maintaining the integrity of the identity and rights data infrastructure. In order to be able to identify the appropriateness of identities and access rights, auditors require information on the employees' current project status, and access rights requirements. Therefore an auditor, in the best case simply compares the employee data with the identity and access rights infrastructure. In the light of [IS10], an additional audit on the validity and appropriateness of the credentials is required, which includes an audit of the credential statuses. We estimate, that if an auditor receives the information in an easily accessible form, the audit is reduced to simply comparing information between the identity and access rights data infrastructure, the credential statuses, and the employee data, and thus estimate the effort to be 5 working minutes per identity. However, if the auditors are required to consolidate the required information themselves, we estimate about 15 working minutes per user. Additionally, the frequency of audits influences the quality of the identity and access rights data infrastructure, as room for

complacency, as [Wa12a] puts it, is reduced. Assuming a yearly, up to a monthly-frequency, we can thus estimate the costs for an audit to be between 5 and 180 working minutes per user. Having estimated the costs partially on a per user, per year, partially on a per year basis we are finally assuming that: **(A10)** The observed organization is stable in growth and structure, including the frequencies of deprovisioned identities, renewed credentials, and provisioned identities are equal. Although this assumption is unrealistic, it enables us to use a neutral view on the organization, leaving out factors such as organizational adaption towards markets and competitive scenarios, which would raise the complexity of the regarded issue, while not necessarily contributing to the considerations of transaction costs. Using A10 we can use frequencies of 0.2 for enrolment, 0.2 to 0.21 for provisioning, and 0.17 to 0.2 per user, per year for deprovisioning activities [OL10]. A complete list of the resulting costs can be found in Annex A1.

For the "Extranet" scenario, in which the IP handles the identities of the entities associated with the IU, we can conclude that the costs for executing the identity lifecycle may vary between 163,669 working minutes in the best case, and 2797,36 working minutes per user, per year in the worst case. These costs can be relaxed under the assumption that the IP is neither providing SETA, nor a central contact for security events for the entities associated with the IU. In this case, the costs account for 9,439 working minutes per user per year in the best case, up to 204,16 working minutes in the worst case for the IP. In our transaction analysis we will consider both scenarios.

5 Transaction costs of federated identity management

In the "Extranet" scenario, the IP is providing credentials, identities, and access rights for entities associated with the IU. Assuming that the entities are working off-premise, SETA and provisioning of a central contact for security events can be neglected. In our following analysis we will consider both the "Extranet" and the "Federated Identity Management" scenario. Hereby we will distinguish between process costs (depicted with P), control costs (depicted with C), documentation costs (depicted with D) and communication costs (depicted with CO). Process costs are hereby costs for carrying out a certain task, as analysed in our cost estimation of the identity lifecycle. Control costs arise out of a sphere of uncertainty between two parties and include costs for controlling, and establishing control mechanisms. In our considerations, control costs are mainly costs for auditing identity and lifecycle management. Documentation costs are directly associated with control costs, consolidating and articulating information required to efficiently carry out an audit. Finally, communication costs are costs associated with provisioning of information, e.g. for initiation of a task. Tab. 1 provides an overview on the different cost types in both scenarios. In our "Extranet" scenario, the IP is responsible for providing identities, credentials, and access rights. SETA and a central contact for security events may be provided by the IP or the IU. Finally, as the identity and rights data infrastructure is completely administered by the IP, auditing is also

included in the IPs costs. The IU is only responsible for initiating the enrolment of an entity, creating communication costs in “Enrolment”, and initiating the deprovisioning for an entity. If the IU is carrying out SETA and provides a central contact for security events, the only costs arising for the IP are control costs, e.g. by auditing the existence and contents of both controls.

	Extranet Scenario		**Federated Identity Management Scenario**	
Phase	**IP**	**IU**	**IP**	**IU**
Enrolment	P	C	C	P, D
Provisioning	P		C, P	P, D
Usage	(P),(C)	(P)	C	P, D
Deprovisioning	P	C	C, P	P, D
Auditing	P		C, CO, P	P, CO, D
Worst Case process costs (per user, per year)	204,16 minutes (2797,36 minutes)	(2593,2 minutes)	185,48 minutes	2797,36 minutes
Best Case process costs (per user, per year)	9,439 minutes (163,669 minutes)	(154,23 minutes)	7,119 minutes	163,669 minutes

Tab. 1: Comparison of the cost types associated with the "Extranet" and the "Federated Identity Management" scenario

In the case of the “Federated Identity Management“ scenario however, the IU is providing its‘ own credentials, and identities. The only processes carried out by the IP are the provisioning and deprovisioning of access rights. Regarding the costs for identity lifecycle management, this means that the IP is still responsible for auditing the access rights data infrastructure, provisioning, and deprovisioning of access rights. Process costs are hereby lower than in the “Extranet” scenario, both in the worst and best case scenario. Overall, the IP only requires 90.85% of the process costs of the “Extranet” scenario using the “Federated Identity Management” scenario.

However, the IP yields additional costs in the “Federated Identity Management” scenario, in terms of control costs. Outsourcing the tasks of enrolment, identity creation, credential creation, revocation of identities and credentials, and auditing of the identity data infrastructure adds to uncertainty between the IP and the IU, contributing to the IUs opportunism [Pi03]. In order, to verify that the tasks are not subject to negligence, creating critical security issues, the IP is now required to invest control costs, e.g. carry

out additional audits on the identity creation and revocation processes and products. Therefore ten additional audit aspects may be required on correct execution and existence of credential renewal, identity proofing, registration, credential creation, activation, issuance, deprovisioning, SETA, central contact for security events, and auditing of the identity data infrastructure by the IU.

Using our estimation from Section 4 we can assume that the audit costs may vary between 50 to 1800 working minutes for the IP per user, per year. This variation may be up to the quality and availability of information as documented by the IU. This means, that even in the considerations of the audit costs, uncertainty is induced by the IP and IU relationship. If we use this additional workload for the IP, we see that the savings of process costs of the "Federated Identity Management" Scenario, quickly diminish. If we consider audit rates between yearly audits, and three-yearly audits, whereas the latter may leave too much room for complacency in identity lifecycle management [Wa12a], we yield additional audit costs between 50 and 1800 working minutes (yearly audits), and 16,66 and 600 working minutes (three-yearly audits). In the case of yearly audits, the resulting total costs for the IP now vary between 52,119 working minutes in the best case, and 1805,48 working minutes in the worst case. For three-yearly audits, the best case are 18,779 working minutes and 605,48 working minutes in the worst case.

Scenario	"Federated Identity Management" (Best Case)	"Federated Identity Management" (Worst Case)
"Extranet" Scenario (Best Case)	~198%	~641%
"Extranet" Scenario (Worst Case)	~9,2%	~296%

Tab. 2: Comparison of the "Federated Identity Management" and "Extranet" scenario with additional audit costs (3-yearly audits)

Tab. 2 provides a comparison of the costs induced by the „Extranet" scenario, compared with the costs of the „Federated Identity Management" scenario, using 3-yearly audits. The only strategy, in which the „Federated Identity Management" scenario yields advantages, includes the comparison with inefficient identity lifecycle management in the „Extranet" scenario, and very efficient auditing in the „Federated identity management" scenario. Apart from this strategy, the „Federated Identity Management" scenario yields increases in costs between 200% and 641% compared to the costs of the „Extranet" scenario.

However, audits may vary in their characteristics. Such as the VDA Information Security Assessment, for instance contribute to reducing auditing efforts. Additionally, audits may not involve the process product but only focus on the process itself. However, in the "Federated Identity Management" scenario audits are obviously the only control

mechanism available for ensuring integrity of each identity and credential provided by the IU, as required by ISO/IEC 29115 [IS10]. This may induce the requirement for auditing all identities handled in the respective processes at the IP. Yet, for practicability reason, and if the assessment of process quality is able to sufficiently indicate its' product quality, assessment of process existence and documentation may be sufficient.

Still the consideration of necessary control costs shows, that the success of federated identity management systems in industrial scenarios, may largely depend on its' accompanying mechanisms. Audit trails can, for instance reduce the uncertainty involved in audit costs, enabling organizations to unlock cost savings through federated identity management, and making partial outsourcing of the identity lifecycle beneficious for the IU [Pi03].

6 Conclusion

Our contribution was able to provide a structured overview on the process fields involved in the identity lifecycle, and estimate the costs per user, per year for managing the identity lifecycle. Our cost analysis shows, that by considering process costs, federated identity management provides clear benefits for an IP, as most of the identity lifecycle management task are carried out by the IU. However the opportunism implied by the principal-agent [LM01] scenario between the IP and the IU, yields additional costs regarding communication and control. Even when neglecting the communication costs, and observing only the control costs, we were able to identify that the required audits tend to minimize, and even overweigh the economic benefits of federated identity management. Controls in federated identity management, can no longer only focus on the status of the identity- and rights-data infrastructure, but must ensure the correct execution of the depicted processes as required by [IS10], in order to ensure correct handling of the credentials, and avoid delay of revocation, along with the risk of impersonation, and unauthorized access to credentials and intellectual property. These findings indicate, that while federated identity management may offer economic benefits for the IP, along with security benefits by avoiding password-reuse [Iv04], and increasing user acceptance [Hü10], unlocking these benefits may require further research in the field of audit-trail provisioning, and integration of these mechanisms into the identity lifecycle management processes of the IU.

Acknowledgment

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

[An08] Anderson, R. et al.: Security Economics and the Internal Market. European Network and Information Security Agency(2008).
[An01] Anderson, R.: Why information security is hard- An economic perspective. Computer Security Applications Conference. pp. 358–365 , Las Vegas, Nevada, USA (2001).
[BS08] BSI: IT-Grundschutz-Vorgehensweise. Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn (2008).
[Bu10] Bulgurcu, B. et al.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. Manag. Inf. Syst. Q. 34, 3, 523–548 (2010).
[Ar08] D'Arcy, J. et al.: User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Inf. Syst. Res. 1–20 (2008).
[Em05] Eminagaoglu, M. et al.: The positive outcomes of information security awareness training in companies - A case study. Inf. Secur. Tech. Rep. 14, 223–229 (2009).
[GG05] Gal-Or, E., Ghose, A.: The economic incentives for sharing infomration security information. Inf. Syst. Res. 16, 2, 186–208 (2005).
[Go03] Gordon, L.A. et al.: Sharing information on computer systems security: an economic analysis. J. Account. Public Policy. 22, 461–485 (2003).
[Hü10] Hühnlein, D. et al.: Diffusion of Federated Identity Management. Sicherheit 2010. Berlin (2010).
[Hü11] Hühnlein, D. et al.: SkIDentity - Vertrauenswürdige Identitäten für die Cloud. D-A-CH Security 2011. P. Schartner und J. Taeger. 293–304 (2011).
[IS05] ISO: Information technology -- Security techniques -- Code of practice for information security management. , Geneva, CH (2005).
[IS10] ISO/IEC 29115: Information technology - security techniques - Entity authentication assurance framework. (2010).
[Iv04] Ives, B. et al.: The Domino Effect of Password Reuse. Commun. ACM. 47, 4, 75–78 (2004).
[Ku14] Kubach, M. et al.: Secure Cloud Computing with SkIDentity: A Cloud-Teamroom for the Automotive Industry. Scientific Presentation, Open Identity Summit 2014, 4.-6.11.2014. , Stuttgart (2014).
[Ku13] Kurowski, S.: Access rights and identity management in collaborative, distributed and digitized value chains in production. Presented at the 8th International IFIP Summer School on Privacy and Identity Management for Emerging Services and Technologies , Berg en Dal, Netherlands June (2013).
[LM01] Laffont, J.-J., Martimort, D.: The Theory of Incentives: The Principal-Agent Model. Princeton University Press (2001).
[MD08] Maler, E., Drummond, R.: The Venn of Identity: Options and Issues in Federated Identity Management. IEEE Secur. Priv. Mag. 6, 2, 16–23 (2008).
[MA15] Matchett, C., Ashok, P.: Best Practices for Determining Your IT Service Desk

Staffing Ratio. Gartner Inc. (2015).
[MR08] Meints, M., Royer, D.: Der Lebenszyklus von Identitäten. Datenschutz Datensicherheit DuD. 32, 3, 201 (2008).
[MR09] Muntermann, J., Roßnagel, H.: On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market. In: Proceedings of the 14th Nordic Workshop on Secure IT Systems (NordSec 2009). pp. 1–14 , Oslo, Norway (2009).
[Ne94] Neumann, P.G.: Risks of Passwords. Commun. ACM. 37, 4, 126 (1994).
[No12] Nofer, M. et al.: The Economic Impact of Privacy Violations and Security Breaches - A Laboratory Experiment. (2012).
[OL10] O'Connor, R.C., Loomis, R.J.: 2010 Economic Analysis of Role-Based Access Control. NIST, Gaithersburg, MD, USA (2010).
[Pi03] Picot, A. et al.: Die Grenzenlose Unternehmung: Information, Organisation und Management. , Wiesbaden (2003).
[Ro10] Roßnagel, H.: The Market Failure of Anonymity Services. In: IFIP. pp. 340–354 (2010).
[RR05a] Roßnagel, H., Royer, D.: Investing in Security Solutions: Can Qualified Electronic Signatures be Profitable for Mobile Operators. In: Proceedings of the 11th Americas Conference on Information Systems. pp. 3248–3257 AIS, August, Omaha, Nebraska (2005).
[RR05b] Roßnagel, H., Royer, D.: Profitability of Mobile Qualified Electronic Signatures. In: Proceedings of the 9th Pacific Asia Conference on Information Systems (PACIS 05). pp. 1345–1355 AIS, Bangkok (2005).
[RZ12] Roßnagel, H., Zibuschka, J.: Assessing Market Compliance of IT Security Solutions: A Structured Approach Using Diffusion of Innovations Theory. Strateg. Pract. Approaches Inf. Secur. Gov. Technol. Appl. Solut. 13–33 (2012).
[Ro13] Royer, D.: Enterprise Identity Management - Towards an Investment Decision Approach. Springer Berlin / Heidelberg, Berlin / Heidelberg (2013).,
[Si15] Sicherheit.info: Biometrische Lösungen für Zutrittskontrolle, http://www.sicherheit.info/artikel/1105111. (2015).
[TS11] TSO: ITIL Service Operation 2011 Edition. The Stationery Office (2011).
[Ve05] VeriSign: Total Cost of Ownership for Public Key Infrastructure. (2005).
[Wa12a] Wallix, N.L.: Access rights - protect access to your data or lose it: serious misconceptions about information security. Comput. Fraud Secur. 8–0 (2012).
[Wa12b] Waly, N. et al.: Improving Organisational Information Security Management: The Impact of Training and Awareness. Presented at the June (2012).
[We13] Wehrenberg, I. et al.: Secure Identities for Engineering Collaboration in the Automotive Industry. In: Mobility in a Globalized World. , Bamberg (2013).
[Wi81] Williamson, O.E.: The Economics of Organization: The Transaction Cost Approach. Am. J. Sociol. 87, 3, 548–577 (1981).
[Ze12] Zetter, K.: Toyota contractor accused of sabotaging company network, stealing data, http://www.wired.com/2012/08/toyota-alleges-sabotage/. (2012).

A Annex

A.1 Overview on the costs of the identity lifecycle per user, per year

Process field	Effort of identity lifecycle managing organization per user	Estimated frequency per user, per year	Effort per user, per year
Credential Renewal and / or replacement	0..30 minutes	0,2	0..6 minutes
Identity proofing and identity information verification	0..30 minutes	0,2	0..6 minutes
Registration	6,6..12,4 minutes	0,2..0,21	1,32..2,48 Min.
Credential Creation	6,6..13,4 minutes / 0€..3000€	0,2	1,32..2,68 Min. / 0..600€
Credential Activation	0	0,2	0
Credential Issuance	5..20 minutes	0,2	1..4 minutes
Deprovisioning	4,7..10 Min.	0,17..0,2	0,799..3 minutes
SETA	120..1224 Min.	1	120..1224 minutes
Central contact for security events	34,23..1369,2	1	34,23..1369,2 minutes
Auditing	5..180 Min.	1	5..180 minutes
Overall effort per user, per year			163,669..2797,36 minutes / 0..600€

Detlef Hühnlein et al. (Eds.): Open Identity Summit 2015,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2015 101

Topology of Dynamic Metadata Exchange via a Trusted Third Party

Daniela Pöhn[1]

Abstract: Federated Identity Management is an effective technology that allows multiple organizations to share resources. Deployments of the protocol Security Assertion Markup Language (SAML) practically require the pre-exchange of aggregated metadata files, making federations to fixed trust boundaries. Dynamic metadata exchange between identity provider and service provider via a trusted third party (TTP) overcomes these barriers. In this paper, we contrast dynamic metadata exchange with other state-of-the-art approaches and present the topology of the dynamic metadata exchange via a TTP. Furthermore, a distributed dynamic metadata exchange is proposed, in order to enhance the current protocol and provide a scalable solution for large-scale infrastructures.

Keywords: Metadata, Security Assertion Markup Language, Identity Management, Federated Identity Management, Metadata Exchange

1 Introduction

Focusing on cognitive scalability, in addition to technical scalability, is key to the success of identity management systems. This is one of the seven flaws of identity management, discovered by R. Dhamija and L. Dusseault [DD08]. Although on-demand and scalability are important requirements, many federated identity management (FIM) solutions do not provide these technical aspects.

A researcher, e.g., works in a specific research field and is part of the associated research community. This community, also called virtual organization (VO), provides services, which are essential for the work. The researcher's home institution, also called identity provider (IDP), is member of a national federation operated by the national research and education network (NREN). Other IDPs and service provider (SPs) are part of this national federation. As most research and education (R&E) federation, this federation is based on the protocol Security Assertion Markup Language (SAML), while commercial providers prefer OpenID Connect. Although SAML does not require aggregated, pre-exchanged metadata files, it is common practice. The metadata contains information about the communication endpoints, e.g., Uniformed Resource Locator (URL) and certificate information. Therefore, the national federation collects and aggregates the metadata of the members and distributes the metadata set to its members. As the national federation with most of its members is part of an inter-federation, e.g., eduGAIN, the metadata of all participating federations is again aggregated and then distributed.

[1] Leibniz Supercomputing Centre, Boltzmannstr. 1, 85748 Garching n. Munich, daniela.poehn@lrz.de

Consequently, services can only be used within these trust boundaries. The VO of the researcher consists of members inside and outside the inter-federation. As a result, the researcher's VO either needs to participate in the inter-federation as a whole or set-up their own virtual federation.

This example explains the main problems of the current deployments of SAML federations in R&E. The coverage of the inter-federation is lacking, while in the same time the scalability of the metadata exchange is reduced. The size of the aggregated metadata file is growing, as more federations are participating. The size slows down hardware, especially older versions or when the aggregated metadata file has significantly grown. As many web service are provided on-demand, the relevant question is, if the SAML metadata can be exchanged on-demand as well. The following chapter contrasts the architecture of a trusted third party (TTP) for dynamic metadata exchange with current state of the art and practical approaches. Chapter 3 concentrates on the topology of such a TTP and while Chapter 4 extends the core workflow, in order to overcome current limitations. Last but not least, this paper concludes with the summarized results and further research questions.

2 Dynamic Metadata Exchange by a Trusted Third Party

SAML does not specify the aggregation and pre-exchange of metadata, as mentioned above. Nevertheless it is current practice to exchange these large metadata files within NREN federation. The Swiss federation SwitchAAI was the first NREN federation to develop a web service called Resource Registry [Hä06], where entities have to register their metadata and update entity information. The national metadata file is aggregated, based on all uploaded metadata files. The participants can then download the aggregated federational file as well as the eduGAIN inter-federational metadata file, which was aggregated by the Metadata Distribution Service (MDS) of GÉANT. Though the web service helps entities to manage their information, many manual steps are required and the local configuration needs to be updated manually. Furthermore, the metadata exchange is not scalable and on-demand. A newer practical solution is the Public Endpoint Entities Registry (PEER) by Young et al. [YJ09]. The implementation of PEER is called REEP and can be used by any entity, independent of the federation and protocol used. Although this approach helps entities participating in several federations, the metadata is still aggregated by federations and inter-federations. Another drawback are the manual steps, which are required. The approach of a TTP for dynamic metadata exchange works as public resource registry, where any entity can register and upload their metadata. In order to establish dynamic, on-demand metadata exchange, the TTP extends the currently used localization service, formally known as WAYF (Where Are You From?). This localization service is used by the SP to localize the user's IDP. The user expresses his will to access a specific service at the SP, hence he triggers the metadata exchange between IDP and SP, if they do not have a technical trust relationship yet established. The localization service then knows both entities and their

communication endpoints. These are the required information for on-demand metadata exchange, also described in [PMH14c], [PMH14a] and [PMH14b], where the state of the art, basic concepts, workflows and database design were explained. As only the necessary metadata is exchanged, this effectively avoids performance bottlenecks and improves the scalability of the metadata exchange.

Young submitted an Internet-Draft (I-D) called Metadata Query Protocol [Yo15]. Another I-D describes the profile for SAML. The metadata can be retrieved by HTTP GET requests, allowing dynamic metadata distribution and therefore this approach solves the problem of huge aggregated metadata files. The TTP can re-use the Metadata Query Protocol in order to let the IDPs and SPs query the metadata on-demand. The metadata is either stored at the TTP or the TTP knows the metadata location at the entity. The authenticated user then triggers the metadata exchange by an extended IDP discovery workflow. The authentication is necessary, in order to avoid inappropriate metadata exchange, e.g., a denial-of-service attack. The user-triggered metadata-exchange is described in the I-D Dynamic Automated Metadata Exchange (DAME) [Pö15]. The I-D does not only specify how the user triggers the metadata exchange, but also the integration workflow. As a result, DAME extends the Metadata Query Protocol.

Federated Attribute Management and Trust Negotiation (FAMTN) by Bhargav-Spantzel et al. [BSSB07] assumes that every SP can act as an IDP. Internal users of FAMTN are supposed to perform negotiations by exploiting their single sign-on (SSO) ID without repeating identity verifications. External users need to declare all their user information during the first communication, in order to receive a temporary user ID. The SSO ID is exploit during further communication, though the stored information could be a target of attacks. It might appear that a SP needs less or more attributes, leading to violations of data minimization or further negotiations between the SP and the user. Furthermore, it is user unfriendly for externals to state all user information in the beginning. The approach Trust Service Provider (TSP) by Jian Jiang et al. [Ji11] requires each entity to register at the central TSP service. The TSP brokers the trust of two entities during runtime. The metadata is downloaded from the TSP and might be stored in the cache of an entity. If a user wants to make use of a service, which is offered by a SP, the SP needs to check his local cache, if he has the metadata of the IDP. If this is not the case, the SP sends a request to the TSP. The IDP is required to send another request, in order to fetch the metadata of the SP. The metadata have version numbers. If the IDP is outside the federation, the SP of the home federation of the IDP can be used as an IDP-Proxy for indirect authentication. This also means that the SP needs to cache the assertion of the home IDP and that each SP needs to run an IDP-Proxy. Additionally, the version number is unnecessarily added to the metadata's name. The TTP, in contrast, automates the technical integration of new metadata on the SP as well as on the IDP side. In order to integrate these information automatically, an extension of existing software is needed. The extension of the software can automate the manual steps by the information already included into the metadata. This eliminates the manual workload for SP and IDP administrators and avoids waiting time for the end users. This is particularly the case as the metadata can be exchanged across current federations' boarders.

The TTP is basically a central service to store and retrieve SP and IDP metadata on-demand. The advantages of TTP over the current practical solution and scientific approaches are, e.g.:

- scalable metadata exchange,
- user triggered, on-demand metadata exchange,
- based on standard SAML workflows,
- not involved in authentications and further communication,
- widen the trust boundaries, and
- automates manual workflows.

The proof of concept implementation of the TTP is tailored for SAML, which is the FIM standard in research federations, but it could be adapted to other FIM protocols without changing the core functionality. In the case of the researcher, this means that, as a prerequisite, his IDP and the SPs have registered at the TTP and implemented the extension. When the researcher wants to make use of a new service, he is forwarded to the discovery service running at the TTP. He chooses his IDP, while he automatically triggers the metadata exchange between IDP and SP at the same time. When both have configured a fully automated metadata exchange, the metadata is exchanged on-demand and directly integrated into the local configuration. This heavily reduces the size of the metadata files exchanged and the waiting time for the user, if IDP and SP are not within the same trust boundaries. The TTP is designed as a central service, used by SPs and IDPs, which extends the discovery service. Although the TTP is designed as a central party, it can have different topologies: one global TTP, distributed connected TTPs or one TTP per federation. The topology of the TTP is discussed in the following section and the focus of this paper.

3 Topology of the Trusted Third Party

In order to decide on the topology, the MNM (Munich Network Management) service model is introduced. The MNM service model [Ga01] is a generic model for IT service management, defining service-related terms, concepts and structuring rules. It allows to model specific services for the purpose to analyze needs and demands in regards of an appropriate service management. As it is a generic view, it also gives an overview of the architecture, which can later onwards be used for further analysis. In order to understand and explain the topology, first the basic service model of inter-federated identity management (IFIM) and the central TTP is explained. Afterwards, the service view of a central TTP is used to discuss the topology.

3.1 Basic Service Model

The basic service model contains the relevant roles and associations. It distinguishes between customer side, provider side and the side independent service. The customer side consists of the basic roles customer and user, while the role provider is part of the provider side. The provider makes the service available to the customer side, whereas more details about the service are provided by two different views.

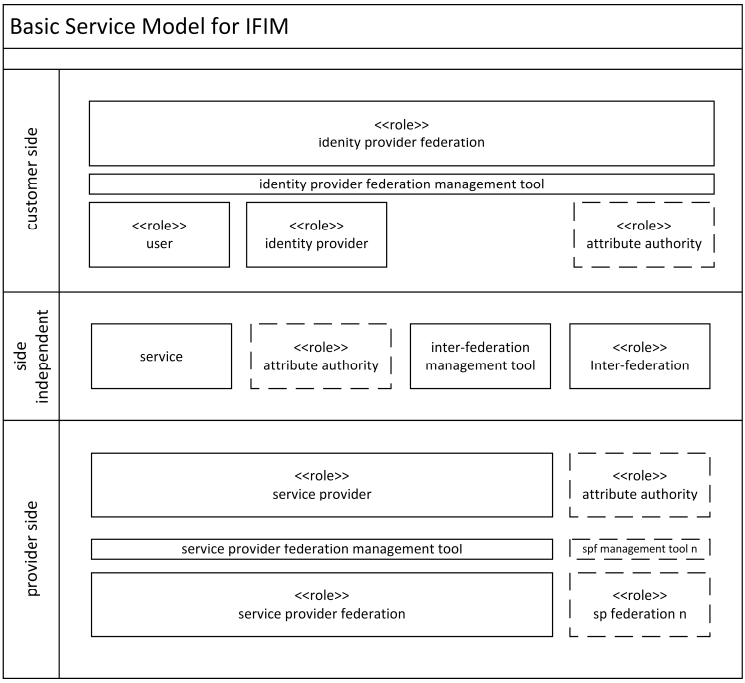

Fig. 1: Basic Service Model for IFIM

Fig. 1 shows the basic service model of inter-federations. User and Identity Provider are part of the customer side. An IDP is normally member of a federation, the identity provider federation. Each federation has different tools, like Resource Registry and PEER, to manage the federation, which also means different tools for the entities to upload and download metadata files. An attribute authority (AA) might be part of the identity provider federation. The provider side consists of a service provider, one or more service provider federations and their management tools. If the researcher of our example is part of the CLARIN community, the SP is member of 15 federations, which leads in the worst case to 15 different management tools. Besides the side independent service, independent AAs, the inter-federation and its management tool belong to this neutral side.

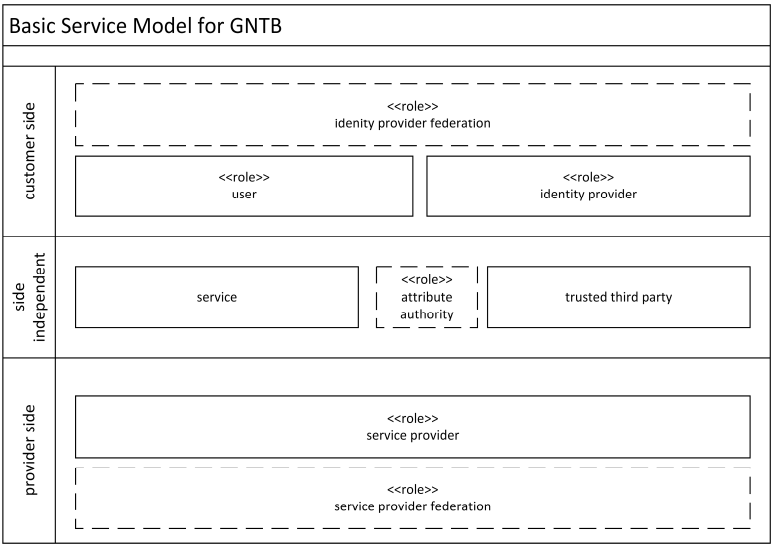

Fig. 2: Basic Service Model for TTP

In contrast to the basic service model for inter-federated identity management (IFIM), the service model for the TTP reduces the amount of management tools, as shown in Fig. 2. The identity provider federation and the service provider federation use the management tool of the TTP. Each federation might still run an AA. In case of CLARIN, the SP federation of the community joint several federations in order to reach the needed coverage. If they use the TTP, joining several federations is obsolete, as the metadata is exchanged on-demand between IDP and SP. Federations might still exist out of legal requirements, but it is technically not necessary anymore. The TTP is seen as a neutral service, as it should be run by a neutral party and it's neutral to IDP and SP.

3.2 Topology described on Service View

The service view contains the functionality of the service, i.e., usage for the role user and management functionality, which is accessed by the role customer. There are two access points, i.e., service access point and customer service management access point, for the customer side to access the usage and management functionality. The customer service management is a concept of a single management interface between customer side and provider side providing a mean to exchange management information. One such information associated to each service is a list of quality of service parameters, which have to be met by the service.

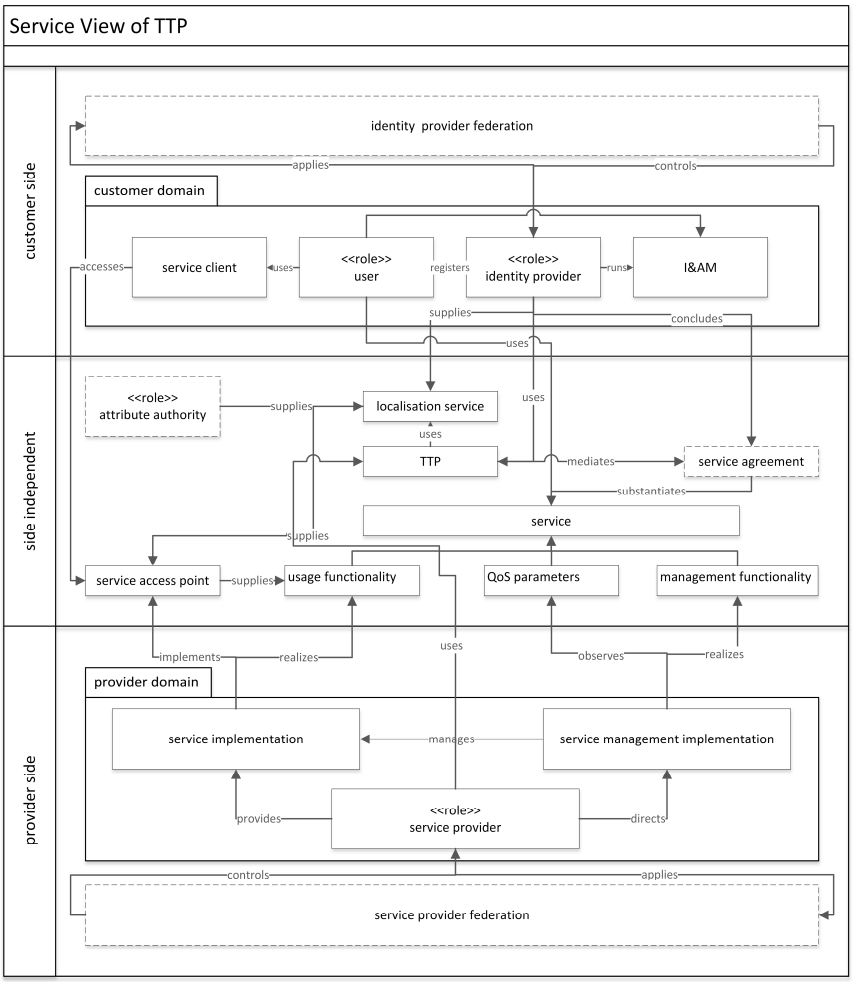

Fig. 3: Service View for TTP

The service view is customized for identity management by the TTP (Fig. 3). As customer service management is relatively unimportant for no-cost web services, it is omitted for better overview. Service client, Identity & Access Management (I&AM) as well as the customer domain are added. The user accesses a service via a service client, which is normally a web browser. The IDP stores user information in a local I&AM. These information are accessed by the FIM software of the IDP. Service client, user, IDP and I&AM are combined to the customer domain, as they belong to one organization.

The service provider on the provider side provides a service implementation, which implements a service access point, e.g., a login page, and provides the usage functionality. The SP also directs the service management implementation, which observes quality of service parameters and realizes the management functionality. The SP utilizes the localization service to locate the user's IDP. The TTP uses the localization service at the same time to exchange the metadata of IDP and SP on-demand. Therefore, the TTP mediates a service agreement. An AA might supply the localization service. Both, IDP and SP, use the TTP to manage their data. If IDP or SP belong to a federation, it might interact with the TTP to manage its members.

Depending on the topology of the TTP, the service view for a global scenario might differ. Possible topologies for the implemented dynamic metadata exchange are:

- A global TTP, where all IDPs and SPs need to register. Fig. 3 already shows this topology.
- Isolated TTPs per federation, where each federation or inter-federation runs an own TTP.
- Distributed TTPs, which communicate in order to enable distributed exchange of metadata.

A global TTP can use the DAME protocol to initiate the metadata exchange, while the metadata exchange itself is done by the Metadata Query Protocol. Monitoring and statistics are easy to manage, as all important data is stored at the global TTP. The topology of the global TTP is rather simple, as you can see in the Fig. 3. On the other hand, a world-wide federation is an utopia [YJ09]. A world-wide used TTP seems like another utopia. It would need a neutral operator and become a bigger target for attacks. As the global TTP is used for all users, IDPs, and SPs around the world, lots of data is collected, which can be miss-used. User profiles can easily be generated and censorship can exclude users, IDPs, and services by the operator of the TTP or a hacker. This can be the case, if, e.g., a government of a country wants to exclude another country or the government of a country wants to observe their people. Last but not least it is possible that the operator of the TTP shuts-down the TTP, stopping all metadata exchanges at once.

The Service Model for isolated TTPs would look similar to a global TTP, besides the fact, that many TTPs exist in parallel with closed trust boundaries. Some IDPs and SPs might be member of several federations. For isolated TTPs per federation, the same positive affects apply as for a global TTP. In contrast, every federation could run a TTP, building up the same boundaries as in the current situation, as there are many TTPs in parallel with closed trust boundaries. From the point of view of our researcher, he would need to use different TTPs for his work. Therefore, his IDP respectively SPs needs to register at all the TTPs, where the user's SPs or IDP are registered. As a result the dynamic of the metadata exchange is decreasing.

The Service Model for distributed TTPs consists of several TTPs, though each IDP and

SP is only registered at one TTP. The TTPs are communicating with each other. Distributed TTPs would need another protocol or an extension of the DAME protocol for this communication. At the same time, it would increase the coverage in comparison to isolated TTPs as there are no closed trust boundaries. The TTPs run by federations or other organizations would communicate and allow the metadata exchange between different TTPs. A distributed TTP is a less interesting target for attacks, user profiling, and censorship than a global TTP. As the data is distributed between several TTPs, it is much harder to collect all the data. Therefore, user profiling is impossible. If, e.g., the government of a country wants to exclude another country, it has to convince all operators.

Given that the topology of isolated TTPs is not as scalable as both other approaches and the disadvantages of a global TTP, the TTP should be distributed.

4 Distributed Dynamic Metadata Exchange

The distributed TTPs can be run by different groups, like federations, projects and commercial sectors. Though the operators of the distributed TTPs do not necessarily need to cooperate besides running these distributed TTPs, it would be advisable to have different inter-organizational processes in place. Inter-organizational security management and service management are two examples, which are already explored by other approaches. It is essential, that all other distributed TTPs are known, since they need to communicate and exchange sensible information. The knowledge about all TTPs is considered in the next subsection. Afterwards, the current DAME protocol is explained, which is then extended in the following subsection.

4.1 Metadata Feed

Discovery services currently use metadata feeds to extract trusted IDPs. The URL of the metadata feed, basically the aggregated metadata file, is added to the local configuration by the operator. This functionality can be used to build a registrar of TTPs by:

- having the operators manually adding the URL of the metadata feed all other TTPs into the local configuration or
- implementing an automated registration for all TTPs, which then generates a feed. In order to automate the registration, the TTPs need an additional functionality, which contacts automatically the TTP registrar.

As the metadata between IDP and SP is exchanged on-demand via a TTP and then automatically added to the local configuration, the automated, dynamic registration is chosen. If, e.g., the TTP of the national federation of the researcher, the TTP of his VO, and the TTP of another VO (VO2) communicate, the metadata feed would contain these three TTPs. All three TTPs register themselves automatically at the registrar, which then

generates the metadata feed. The researcher would choose his IDP within his federation, while another researcher from VO2 would choose the IDP of his community, when using a service of the researcher's VO. The TTP registrar could be DNSSEC. The Domain Name System (DNS) is used to resolve the name, i.e., internet protocol (IP) address to domain and vice versa. Different DNS server are connected via delegation. DNSSEC is used against Cache Poisoning. The DNS entries are signed in order to detect forgery. The resolver validates the answer with DNSSEC. Incorrect signed entries cannot be resolved and therefore the forgery is detected. TTPs can be registered in such DNSSEC servers. At the same time it protected against specific attacks, the connected TTPs are queried dynamically, and no central authority has control over all entries.

4.2 Dynamic Automated Metadata Exchange

In order to exchange the metadata in a distributed way, the DAME protocol needs to be extended. The workflow is currently as follows:

Step 1: The researcher wants to access a service. Therefore, he requests access.

Step 2: The SP redirects to the extended discovery service.

Step 3: The researcher selects his IDP and triggers the core workflow.

Step 4: The TTP informs the SP about the chosen IDP. The SP sends then an authentication request.

Step 5: The TTP caches the authentication request and sends a new generated authentication request to the IDP.

Step 6: The researcher successfully authenticates at the IDP.

Step 7: The IDP sends the authentication response to the TTP.

Step 8: The TTP triggers the metadata exchange. It is recommended that the IDP starts integrating the metadata.

Step 9: Both entities indicate the status of the integration.

Step 10: When both have successfully integrated the metadata and updated the configuration, the cached authentication request is sent to the IDP.

Step 11: As the user has a valid session, the IDP sends the assertion with the user information to the SP and the SP grants access to the user.

4.3 Distributed Dynamic Automated Metadata Exchange

For the approach of distributed TTPs, the same workflow is applied, if IDP and SP are

registered at the same TTP. If the IDP is registered at TTP1 and the SP is registered at TTP2, the same workflow looks as described below. Both entities have one trusted TTP they definitely know, therefore it is their communication endpoint. The IDP normally communicates with the TTP1, while the SP communicates with the TTP2. The distributed TTPs act similar to proxies in this case. The only exception is the metadata exchange itself. As the metadata request is, according to the Metadata Query Protocol, directly sent to the responder, the TTP with the relevant metadata should trigger the exchange. This means that TTP1 triggers the metadata exchange for the IDP's metadata and the TTP2 triggers the exchange for the SP's metadata.

Step 1: The researcher wants to access a service. Therefore, he requests access.

Step 2: The SP redirects to the extended discovery service of his TTP2.

Step 3: The researcher selects his IDP and triggers the core workflow.

Step 4: The TTP2 informs the SP about the chosen IDP. The SP sends then an authentication request to TTP2. The authentication request is forwarded to TTP1 by the TTP2 by a HTTP Redirect.

Step 5: Both TTPs cache the authentication request and TTP1 sends a new generated authentication request to the IDP. TTP2 sends an internal HTTP Request to TTP1.

Step 6: The researcher successfully authenticates at the IDP.

Step 7: The IDP sends the authentication response to the TTP1, which is forwarded to TTP2 as internal HTTP Response.

Step 8: Both TTPs trigger the metadata exchange. TTP1 triggers the metadata exchange for the SP, while TTP2 triggers the metadata exchange for the IDP. It is recommended that the IDP starts integrating the metadata.

Step 9: Both entities indicate the status of the integration to the TTP, which triggered the metadata exchange. TTP1 sends TTP2 about the status and vice versa. This is done by integration request and response messages.

Step 10: When both have successfully integrated the metadata and updated the configuration, the cached authentication request is sent to the IDP by TTP1. TTP1 forwards the request to the TTP2 by an internal HTTP Request, in order to close the metadata exchange, which is answered by an internal HTTP Response with a status code.

Step 11: As the user has a valid session, the IDP sends the assertion with the user information to the SP and the SP grants access to the user.

The SAML HTTP Redirect Binding and HTTP Requests can be used to forward the message. HTTP Redirect Binding utilizes the user agent to forward a message. The internal HTTP Requests and Responses are suitable for messages without the

involvement of the user. As the distributed DAME is, similar to DAME, only used for the initial metadata exchange, normal SAML workflows can be applied afterwards.

5 Conclusion and Outlook

Distributed TTPs enable dynamic metadata exchange for large-scale infrastructures. The approach facilitates the fully automated technical setup for FIM without the boundaries of federations. The scalability of the metadata exchange is increased in comparison to the pre-exchanged aggregated metadata files. By operating distributed TTPs, the federations still can have control over the registered IDPs and SPs, while improving the situation of the users at the same time.

The researcher's IDP is registered at the national TTP1, while the SPs of the VO use TTP2. As TTP1 and TTP2 communicate, the metadata is exchanged on-demand between the researcher's IDP and a new SP of the VO. When the researcher cooperates with another community, which operates TTP3, the same mechanism applies, reducing the waiting time for the researcher.

While a central TTP for dynamic metadata exchange is implemented, deployed and tested, the distributed setup still needs to be implemented. The duration of metadata exchange with a central TTP took on average 3 seconds during our tests. A comparison of the duration of metadata exchange in a central and a distributed environment should be done. Distributed TTPs for dynamic metadata exchange is a technical solution for the problem of scalable metadata exchange. Nevertheless, a LoA framework needs to be in designed, in order to easily compare different LoA schemas and help the entities to determine the trust-worthiness of the other entity. As different federations use different LoA schemas, the schemas do not necessarily overlap nor does typical LoA standards fit, a simple mapping is not always possible. Last but not least, more user-friendly approaches, like User Managed Access, should be regarded and applied.

Acknowledgement

The authors wish to thank the members of the Munich Network Management (MNM) Team for helpful comments on previous versions of this paper. The MNM-Team, directed by Prof. Dr. Dieter Kranzlmüller and Prof. Dr. Heinz-Gerd Hegering, is a group of researchers at Ludwig-Maximilians-Universität München, Technische Universität München, the University of the Federal Armed Forces, and the Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities.

References

[BSSB07] Bhargav-Spantzel, A.; Squicciarini, A. C.; Bertino, E.: Trust Negotiation in Identity Management. IEEE Security and Privacy, vol. 5, no. 2, pp. 55–63, 2007.

[DD08] Dhamija, R.; Dusseault, L.: The Seven Flaws of Identity Management: Usability and Security Challenges. IEEE Security & Privacy, vol. 6, no. 2, pp. 24–29, 2008.

[Ga01] Garschhammer, M.; Hauck, R.; Kempter, B.; Radisic, I.; Roelle, H.; Schmidt, H.: The MNM Service Model – Refined Views on Generic Service Management. Journal of Communications and Networks, IEEE, vol. 3, no. 4, pp. 297–306, 2001.

[Hä06] Hämmerle, L.: SWITCHaai: Shibboleth-based Federated Identity Management in Switzerland. In: Proc. CESNET 2006 Conference. 2006.

[Ji11] Jiang, Jian; Duan, Haixin; Lin, Tao; Qin, Fenglin; Hong, Zhang: A federated identity management system with centralized trust and unified Single Sign-On. In: Communications and Networking in China (CHINACOM), 2011 6th International ICST Conference on. IEEE, pp. 785–789, 2011.

[PMH14a] Pöhn, D.; Metzger, S.; Hommel, W.: Géant-TrustBroker: Dynamic, Scalable Management of SAML-Based Inter-federation Authentication and Authorization Infrastructures. In: ICT Systems Security and Privacy Protection. Springer Berlin Heidelberg, pp. 307–320, 2014.

[PMH14b] Pöhn, D.; Metzger, S.; Hommel, W.: Project GÉANT-TrustBroker – dynamic identity management across federation borders. In: Networking with the World, The 30th Trans European Research and Education Networking Conference, 19-22 May, 2014, Dublin, Ireland, Selected Papers. TERENA, 2014.

[PMH14c] Pöhn, D.; Metzger, S.; Hommel, W.: A SAML Metadata Broker for Dynamic Federations and Inter-Federations. In: Proceedings of INFOCOMP 2014, The Fourth International Conference on Advanced Communications and Computation. IARIA, pp. 132–137, 2014.

[Pö15] Pöhn, D.: Dynamic Automated Metadata Exchange – draft-pohn-dame-03. Work in Progress, 2015.

[YJ09] Young, I. A.; La Choi, Chad: Interfederation and Metadata Exchange: Concepts and Methods, http://iay.org.uk/blog/2009/05/concepts-v1.10.pdf, 09.06.2015.

[Yo15] Young, I. A.: Metadata Query Protocol – draft-young-md-query-05. Work in Progress, 2015.

Open Identity Summit 2015

Further Conference Contributions

Detlef Hühnlein et al. (Eds.): Open Identity Summit 2015,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2015 117

Automatic Recognition, Processing and Attacking of Single Sign-On Protocols with Burp Suite

Christian Mainka[1] Vladislav Mladenov[2] Tim Guenther[3] Jörg Schwenk[4]

Abstract: SAML, Mozilla BrowserID, OpenID, OpenID Connect, Facebook Connect, Microsoft Account, OAuth — today's web applications are supporting a large set of Single Sign-On (SSO) solutions. Some of them have common properties and behavior, others are completely different. This paper will give an overview of modern SSO protocols. We classify them into two groups and show how to distinguish them from each other. We provide EsPReSSO, an open source Burpsuite plugin that identifies SSO protocols automatically in a browser's HTTP traffic and helps penetration testers and security auditors to manipulate SSO flows easily.

1 Introduction

Using username/password combinations to authenticate on websites is still dominating the Internet. From the security point of view the management of plethora login credentials is not a trivial task and carries many risks – users tend to use weak and easy to remember passwords or reuse passwords between different sites. Even if password managers are used, attacks are still applicable [Si14, Li14].

SSO systems simplify login procedures by using an Identity Provider (IdP) to issue authentication tokens which can be consumed by Service Providers (SPs). Thus, instead of managing multiple username/password combinations for each website, a user just needs an account at an IdP which can then be used to log in on an SP.

The importance of SSO has become more important in the recent years, since large companies like Facebook, Google, Microsoft and Salesforce offer different SSO services. For instance, Facebook's SSO service *Facebook Connect* allows its users to connect their Facebook account with various applications. More than 7 million applications use this protocol[We]. Additionally, a non-academic overview [Ja13] claims that 87% of U.S. customers are aware of SSO and more than half have tried it.

Today, there are several different SSO protocols. The most widespread are Kerberos, SAML, OAuth, OpenID, and OpenID Connect. Kerberos is provided in Microsoft's products like Active Directory Federation Service (ADFS) but rarely used in web applications.

[1] Horst Görtz Institute, Ruhr-University Bochum, Germany, christian.mainka@rub.de
The research was supported by the *German Ministry of research and Education (BMBF)* as part of the VERTRAG research project.
[2] Horst Görtz Institute, Ruhr-University Bochum, Germany, vladislav.mladenov@rub.de
The author was supported by the SkIDentity project of the German Federal Ministry of Economics and Technology (BMWi,FKZ: 01MD11030).
[3] Horst Görtz Institute, Ruhr-University Bochum, Germany, tim.guenther@rub.de
[4] Horst Görtz Institute, Ruhr-University Bochum, Germany, joerg.schwenk@rub.de

SAML is a flexible and well standardized protocol offering extensive interoperability features commonly used in enterprise solutions, governmental services and large companies. OAuth, OpenID and OpenID Connect are less complex than SAML and easy to deploy. Thus, these protocols are mostly used for delegated authentication and authorization for websites and mobile devices. In recent years, companies have created and pushed their own SSO protocols: Facebook designed Facebook Connect on top of the OAuth specification. With Microsoft Account, Microsoft also offers an SSO protocol which is based on OAuth. Only Mozilla developed their SSO protocol Mozilla BrowserID from scratch.

In summary, SSO is commonly used in all areas – desktop and web applications, mobile devices, government institutions and enterprise environments. In this focus we mainly concentrate on web applications. Figure 1 depicts a common example of what is called *social login* on a website. The user can either login using its username and password, or use one of his existing accounts (Microsoft, Facebook, Google, ...). The hidden part of the *social login* is the underlying protocol: The user does not see (because it is not necessary) which exact SSO protocol is used. However, this information is important when it comes to security audits: a security auditor (pentester) needs to know which protocol is used so that he can evaluate its security.

Fig. 1: Modern websites offer multiple login possibilities.

A plethora design flaws and implementation errors in Kerberos [Sl01, Sh02], SAML [Ma14, So12], OpenID [WCW12, TT07, SHB12], OAuth [Eg13, YZ14], OpenID Connect [MM15c, MM15b, MM15a], Mozilla BrowserID [FKS14], and Facebook Connect [ZE14] led to critical vulnerabilities.

There exist different approaches to analyze SSO: (1) Via formal analysis the according protocol can be depicted, different threat scenarios can be automatically evaluated and protocol design flaws plus risks can be discovered. Unfortunately, implementation flaws cannot be detected via formal analysis. (2) Many researches concentrate on the analysis of existing implementations. The authors tend to introduce a novel tool, which provides an automated way to provide the security analysis. Unfortunately, such tools are limited to only *one* SSO protocol or *one* attacker model. An additional limitation is the extensibility in order to support more attack vectors and the false positive or false negative rates according the discovered flaws.

The limitations mentioned above are relevant for researchers elaborating novel attacks and security penetration testers, evaluating different services. Such analysis requires: (1) Recognition of protocols and relevant messages, (2) automated decoding of messages and security relevant parameters, (3) a flexible approach enabling the manual manipulation of different messages and parameters within the authentication protocol and (4) a set of existing attack vectors, which can be used for attacks.

To cover these limitations, we created a tool EsPReSSO[5] which is able to (1) detect and highlight SSO messages in the browser's traffic flow (i.e. the SSO token in the HTTP parameters) (2) determine the used SSO protocol. It currently supports all major SSO protocols that are used in modern web applications. (3) Additionally, EsPReSSO detects supported SSO protocols by just loading a website, e.g. a login page. (4) After the recognition of the SSO protocol EsPReSSO facilitates the manipulation of the related messages and automatically decodes and encodes them.

The main challenge tackled by EsPReSSO is the distinction between the different SSO protocols. This task requires an in-depth analysis of all protocols and detailed knowledge of the differences between them. For example, OpenID Connect and Facebook Connect are both based on OAuth and similar. Thus, a simple verification if an OAuth parameter is transmitted will not be able to distinguish between these protocols. Our paper will therefore give a detailed overview of recent SSO protocols and how they can be identified.

Contributions. The main contributions of this paper are the following:

- We provide an overview of seven modern SSO protocols. We classify them into *OAuth family* and *other protocols* and show, that the general protocol can be divided into a few generic steps among all those SSO protocols.
- We have created EsPReSSO, an easy to use open source Burpsuite plugin that automatically identifies SSO protocol messages and classifies them, so that security audits of modern web applications can benefit from it.

2 Foundations

2.1 Single Sign-On

SSO is a concept to login a user on an SP without storing any credentials on the SP. SSO therefore uses an IdP as a trusted third party. The IdP creates an SSO token, sends it back to the user, who passes it to the SP.

A generic description of SSO protocols is depicted in Figure 2. We will give more details on the concrete protocols in section 3. Figure 2 illustrates an abstract and generic protocol flow for modern SSO protocols like OpenID, OpenID Connect, SAML and Facebook Connect.

(1.) The user starts a login request using his user agent (UA) on the SP, for example by submitting his email address (Mozilla BrowserID) or his identifier URL (OpenID, OpenID Connect). (2.) Some SSO protocols then contact the IdP directly (server to server communication). This phase can be used to establish key material which is later used to sign and verify the messages or to determine the endpoint interfaces of the IdP, which will be used. Such an endpoint is for instance the login page at the IdP for the user. (3.) The SP responds to the first message with a token request. This message is then forwarded to the

[5] `https://github.com/RUB-NDS/BurpSSOExtension`

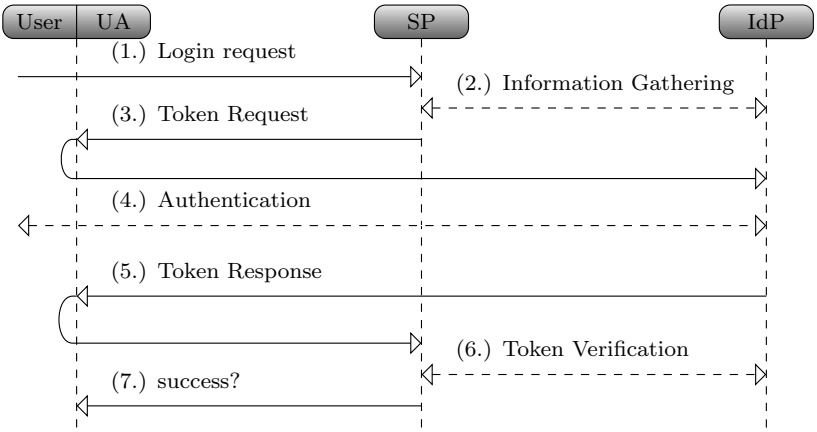

Fig. 2: Generic protocol flow for SSO protocols.

SP by the user (to be more precise, by his UA.). (4.) The user then authenticates to his IdP, typically by entering his username/password combination. Some protocols and IdPs require further user interaction in order to authorize the access to user's data like email address, nickname, birthday or gender. This step is often transparent for the User if he is already authenticated on the IdP. (5.) Next, the IdP sends the token response. This message contains all information that is necessary for the SP to identify the user. The message is forwarded to the IdP. (6.) The SP can then optionally contact the IdP again to verify the token response. Depending on the protocol, this is not necessarily (e.g. in SAML), because the token response contains a signature that can be verified.

2.2 Burpsuite

Burpsuite (Burp) is a penetration test tool by Portswigger[6]. It is available in a free and a commercial professional version. Burp acts as an intercepting proxy. This way, Burp can be configured on any UA as a proxy to log, intercept, display and modify HTTP traffic. The most commonly used UAs for Burp is a web browser, but it is also possible to configure it for any other application (e.g. Thunderbird, Skype, ...). In this paper, we use the free version of Burp. Features of the professional version are not necessary for our research.

Burp is often used by security auditors, researchers and penetration testers for the analysis of different systems. The core functionality of Burp is to intercept and display HTTP messages in a structured manner. Thus, a tester gets a quick overview of the target system, all transmitted messages and parameters. In addition, Burp provides a GUI allowing the full control over all messages - drop, forward, repeat, modify, send later, etc.. Thus, a tester can design different attack scenarios and execute them manually via Burp. The results of the attacks can be seen directly in the UA and analyzed by the tester.

[6] `http://portswigger.net/`

Simple parameter manipulations are supported by Burp and can be executed manually. However, more complex scenarios like decoding, manipulating and signing messages cannot be started in automated manner. In addition, manually analyzing each HTTP message can be time consuming and is often not necessary. In order to facilitate more complex scenarios Burp offers extension points, which allow writing custom features for it. Burp extensions can monitor and analyze any HTTP message that is passed through its proxy. Extensions can modify them and create new UI elements to display them.

3 SSO Protocols

This section will give a short overview of existing SSO protocols used in the web and introduces the necessary details used in EsPReSSO to identify them.

3.1 Protocol Classification

EsPReSSO is able to distinguish between seven different SSO protocols. We therefore classified them into two categories as shown in Table 1: (1.) SSO protocols belonging to the **OAuth-Family** and (2.) **other protocols**.

OAuth-Family		**Other**	
Decentralized	Monolithic	Decentralized	Monolithic
OAuth OpenID Connect	Facebook Connect Microsoft Account	OpenID SAML	Mozilla BrowserID

Tab. 1: Overview on existing SSO protocols used in the web and their classification.

The *OAuth-Family* consists of four different protocols. (1.) OAuth itself [RF] and (2.) OpenID Connect, which is an extension of the original OAuth protocol [Th14]. Both protocols can be used *decentralized*. By decentralized, we mean, that the protocol is independent of a specific provider. (3.) Facebook Connect [Mo08] and (4.) Microsoft Account [Mi08] in contrast are *monolithic*, because they relay on the Facebook resp. Microsoft servers. *Other protocols* are (1.) OpenID [sp07] and (2.) SAML [Or05], which are both decentralized, and Mozilla BrowserID, which is monolithic[7].

3.2 OAuth-Family Protocol Description

The following sections will give a quick overview of protocols of the OAuth family. We do not provide details on how the protocol works, but rather concentrate on the aspects that are necessary to distinguish them from each other. Our results are summarized in Table 2 on Page 124.

[7] Mozilla BrowserID allows one to setup one's IdP (*Primary IdP*-feature), but even in this use-case, the protocol contacts the Mozilla server at `login.persona.org` first.

3.2.1 OAuth

OAuth is an authorization framework that allows delegating access on specific resources to a third party. OAuth itself is not an SSO protocol [Sal14], but since previous research has shown, that developers tend to falsely use it for SSO [Ch14], we decided to add OAuth to the list of supported SSO protocols by EsPReSSO. Taking Figure 2, OAuth follows this protocol flow:

(1.) The user sends his login request to the SP.[8] (2.) The OAuth protocol does not use the *information gathering* phase, because all information on the IdP[9] is configured once beforehand. (3.) According to the specification [RF] within the token request the following parameters are required:`response_type` and `client_id`. The parameter `response_type` determines the *flow* that is going to be used. The most common flows are `code` and `token`. Other flows can be found in the specification [RF]. The parameter `client_id` is a unique string identifying the SP. Further optional parameters, which can be used to identify an OAuth token request are: `scope` for requesting permissions (e.g. the address-book or the calendar), `state` and `redirect_uri`. (4.) Then, the user has to authenticate to the IdP and authorize the requested permissions (`scope`) to the SP. (5.) The IdP generates the token response. If the *code* flow is used, the token response contains a `code` parameter. For the *token* flow, it contains a `access_token` parameter. (6.) The SP uses the received `code` or `access_token` to retrieve information about the user from the IdP and to authenticate him.

3.2.2 OpenID Connect

OpenID Connect is a decentralized SSO protocol by adding an authentication layer to OAuth [Th14]. The general flow is almost identical to OAuth as described in the previous section. Thus, the distinction between OpenID Connect and OAuth is not trivial and requires fine granular comparison.

According the specification a OpenID Connect token request must contain the following parameter: `scope, client_id, response_type, redirect_uri`. Unfortunately, the parameters are commonly used in OAuth too. Thus, the distinction on this level is not possible. However, in OpenID Connect the token request must contain the value *openid* in the `scope` parameter. Additionally, the token request can contain the parameter `nonce`, which is required within the *token* flow. Based on these characteristics the token request can be recognized.

The recognition of OpenID Connect token responses is more complicated and requires more detailed distinction. Within the *token* flow an additional parameter `id_token` will be sent by the IdP to the SP. The `id_token` is used only in OpenID Connect and provides information about the authenticated user. Thus, the identification of the token response is simple.

[8] In the context of OAuth, the *user* is commonly referred to as the *Resource Owner* and the SP as the *Client*. To simplify the description and to unify all SSO protocol, we strictly use user/SP naming.

[9] Again, we use the term *IdP* instead of the OAuth term *Authorization Server*. We also use the term IdP for the *Resource Server*.

The OpenID Connect token response within the *code* flow is identical to the OAuth flow. The only way to provide the distinction is to check the according token request sent before and bind both messages. This binding can be done by using parameters like `client_id`, `state and redirect_uri`, which are sent in the token request and token response.

3.2.3 Facebook Connect

Facebook Connect is a monolithic SSO protocol. It is based on OAuth and uses the same protocol flow as described in subsubsection 3.2.1.

The token request within the Facebook Connect protocol can be recognized by the following characteristics:

- The `scope` parameter can contain the value `signed_request`.
- In addition to the required OAuth parameters within a token request, the following parameters are sent: `domain, origin, sdk, app_id`.

Identical to OpenID Connect, the recognition of the token response is not trivial. Within the *token* flow, the parameter `signed_request` can be used. The value of this parameter is a JSON Web Token (JWT) containing information about the authenticated user. Similar to OpenID Connect the binding between the token request and token response via parameters like `client_id, state, redirect_uri` can be used.

Since Facebook Connect is monolithic, calling the public known SSO endpoints of Facebook's API can be used to identify the flow, for instance `https://graph.facebook.com`.

3.2.4 Microsoft Account

Microsoft Account is monolithic SSO protocol. It is based on OAuth and uses the same protocol flow as described in subsubsection 3.2.1. Microsoft Account token request can be easily detected by observing the `scope` parameter, which contains one of the following values: `wl.basic`, `wl.offline_access`, `wl.signin`.

Identical to OpenID Connect, the recognition of the token response is not trivial. Within the *token* flow, the parameter `authentication_token` can be used. The value of this parameter is a JWT containing information about the authenticated user. Similar to OpenID Connect the binding between the token request and token response via parameters like `client_id, state, redirect_uri` can be used.

Since Microsoft Account is monolithic, calling the public known SSO endpoints of Microsoft can be used to identify the flow, for instance `https://login.live.com/oauth20_authorize.srf`.

Protocol	Message Type	Recognition
OAuth	Token Request	Parameter: `response_type`
	Token Response	Parameter: `code` OR `access_token`
OpenID Connect	Token Request	Parameter: `scope` contains *openid*, `nonce`
	Token Response	Parameter: `id_token`
Facebook Connect	Token Request	Parameter: `domain`, `origin`, `sdk`, `app_id`, `scope` contains *signed_request*
	Token Response	Parameter: `signed_request`, `domain`, `origin`, `sdk`, `app_id`
	URL	`http://static.ak.facebook.com/connect/xd_arbiter`
		`https://graph.facebook.com`
Microsoft Account	Token Request	Parameter: `scope` contains *wl.basic, wl.offline_access* or *wl.signin*
	Token Response	Parameter: `authentication_token`
	URL	`https://login.live.com/oauth20_authorize.srf`
		`https://apis.live.net`
		`https://www.contoso.com/callback.htm`

Tab. 2: OAuth-Family message recognition and distinction

3.3 Other SSO Protocols

In the following sections, we describe SSO protocols that are not based on OAuth. We again focus on the properties which are important to identify the protocol rather than giving a complete protocol description.

3.3.1 SAML

SAML is a decentralized SSO protocol that uses XML to describe the security token. In the SAML protocol flow, there is commonly no interaction between the SP and the IdP [10], so Steps (2.) and (6.) in Figure 2 are skipped. The protocol flow is as follows: (1.) The user submits his login request to the SP. (3.) The SP generates the token request which contains a parameter `SAMLRequest`. The value of the parameter is basically XML and contains information on the to be used IdP (e.g. its URL). It is compressed using the deflate algorithm [De96] (optional), then encoded using Base64 [Jo06] followed by an URL-encoding [BLFM05]. (6.) The IdP generates the token response. This is again XML that is encoded using Base64 and optionally using URL-encoding. The result is stored in a parameter named `SAMLResponse`.

[10] An exception to this is the SAML Artifact Binding [Or05, Section 4.1.3]

3.3.2 OpenID

OpenID is a decentralized SSO protocol, but in contrast to, for example, SAML, it is *open* for dynamically using an IdP without any pre-configuration. By this means, anyone owning an OpenID can submit his identifier, which is an URL, to an SP in Step (1.) as shown in Figure 2. The SP will then discover the IdP in Step (2.) . He browses the URL and retrieves in this way the URL of the IdP. (3.) Next, the SP generates the token request and sends it back to the user. OpenID messages are easy to distinguish from other SSO protocols, since relevant all parameters start with `openid.*`. Message (3.) can be identified by the parameter `openid.mode=checkid_setup`. Authentication to the IdP is provided as usual in Step (4.) . The IdP then generates the token response in Step (5.) . This message can be identified due to the presence of a signature with parameter `openid.sig`. (6.) The SP can optionally send the token response to the IdP and sets `openid.mode=check_authentication` or he can choose to verify the signature on its own.

3.3.3 Mozilla BrowserID

Mozilla BrowserID is a monolithic SSO protocol developed by Mozilla and using Mozilla's server as an IdP during the authentication process. Interestingly, in Mozilla BrowserID using arbitrary IdPs is possible. However, Mozilla's SSO API is always called within the protocol flow.

The recognition of Mozilla BrowserID is possible by the detection of the HTTP parameter `assertion` containing information about the authenticated user within a JWT and a cookie named `browserid_state`. In addition, a JSON message containing key material can be used for the detection. The following parameters occurs within the message: `pubkey`, `p`, `q`, `g`, `algorithm`, `duration` and `email`.

4 EsPReSSO

This section provides a closer look on the design our Burp extension EsPReSSO.

4.1 Idea and Motivation

The Burp **E**xten**s**ion for **P**rocessing and **Re**cognition of **S**ingle **S**ign-**O**n Protocols (EsPReSSO), simplifies the analysis of SSO protocol flows. During our manual analysis of SSO, we often meet the problem to do the same repetitive work over and over again to determine the used protocol. To speed up the identification and to help inexperienced penetration testers, we decided to develop EsPReSSO.

Its simple idea is to have an automatic scanning utility that passively inspects a browser's traffic by scanning HTTP parameters and keywords. In the background the analyzing algorithm processes checks on the messages. If specific keywords and parameter-value pairs

occur, the request/response is highlighted and marked as the recognized protocol. Additional we recognize SSO login possibilities by searching HTTP body responses, to track entry points for further research.

4.2 Design

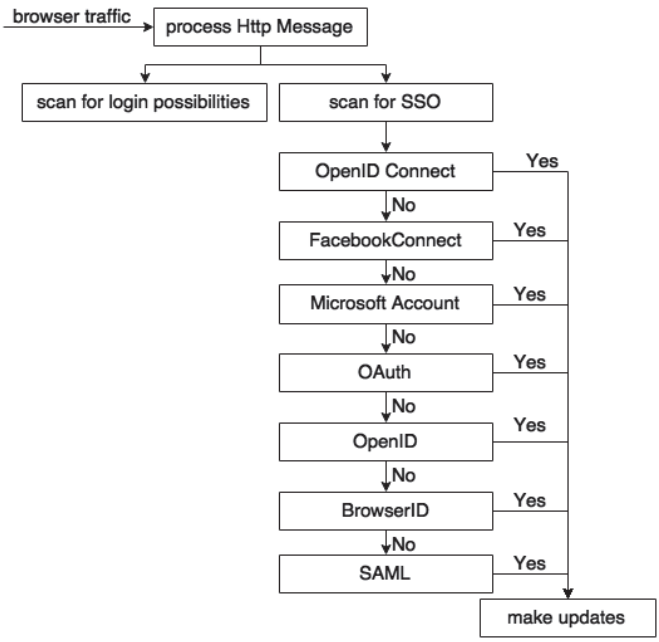

Fig. 3: Setup of the scanner.

EsPReSSO's core functionality is its scanning engine and the presentation of the results. One of our design goals is to stick as close as possible to Burp's user experience. By this means, we used existing structures like the logging mechanisms, the proxy history and its entries.

4.2.1 Scanner

The scanner carries out the detection of the SSO protocols according the described characteristics in section 3. Initially, the scanner uses Burp's interfaces and automatically receives all incoming traffic. Consequentially, it analyzes every loaded website for SSO login possibilities. Simultaneously, it scans the HTTP parameter and detects a SSO authentication process and the according SSO protocol.

The first submodule checks for the possibility to login with a specific SSO module, for example OpenID or Facebook Connect. This is implemented by searching the HTTP response messages through regular expressions for specific key words.

The second submodule inspects the HTTP traffic for specific properties that identify SSO protocols. It therefore searches successively for characteristics that are unique in each SSO protocol (cf. section 3). Please note the order of the given SSO modules, because distinguishing between protocols which partly base on the same protocol is difficult. *OAuth* is part of the protocols *OpenID Connect*, *Microsoft Account* and *Facebook Connect*, therefore we check these protocols first.

In addition, the scanner collects all collected information about the recognized SSO protocols, which allows the analysis afterwards.

4.2.2 Visualizer

Once SSO relevant parameters are detected, they have to be visualized. The Visualizer carries out this task by handling and filtering the collected data, converting the informations in human readable format (e.g. Base64-decoding or inflating) and calling different Burp APIs to display the results.

In detail, the Visualizer includes the following features:

Burp History Burp provides a history tab containing all intercepted messages. Thus, security auditors get an overview of the entire communication and can statically analyze the intercepted data. The Visualizer facilitates the evaluation process by highlighting the SSO relevant messages and by providing additional information about the recognized protocol.

SSO History A new Burp history window displays recognized protocols with additional data, for example, the used token and the protocol name. In comparison to the SSO History window, only SSO relevant messages will be displayed. The Visualizer provides more information about the messages, for example, the relation to other messages and the decoded content.

Follow SSO Flow By right clicking on a SSO History item a new tab is dynamically attached to the view with the complete protocol flow of the entry.[11] Token requests and responses will be assigned to each other, which facilitates the analysis of the entire protocol.

JSON Tab By analyzing the MIME-type of the HTTP messages, the Visualizer detects JSON messages and displays them. This feature is often used in OAuth to transmit data to the SP.

JWT Tab Protocols that are known to make use of JSON Web Tokens (JWT) get automatically a new tab to view the decoded JWT.

SAMLResponse/Request Tab Extra tab that displays the fully decoded and deflated SAML Request/Response messages.

[11] This feature is inspired by Wireshark's *follow TCP stream* feature

All new tabs come with syntax highlighting[12].

4.2.3 Manipulator

Security auditors often have to manipulate HTTP messages in order to simulate different attacks. Thus, in addition to the visualization of the protocols, EsPReSSO offers the possibility to modify the content of the messages.

In order to process the manipulations, the Manipulator offers the following features:

- Editable area containing all relevant parameters and enabling the modifications.
- Modifications will be detected and the old content will be replaced. The flexible architecture of EsPReSSO allows the manual or semi-automatic execution of modifications by choosing an attack vector from a predefined set of attacks.
- Data, which is transformed in a human readable format, will be transformed back to the original format. For instance, SAML tokens will be automatically decoded and — if necessary — deflated.

5 Related Work

SSO Security Tools. In 2013, Bai et al. [Ba13] have proposed AuthScan, a framework to extract the authentication protocol specifications automatically from implementations. The authors concentrated on Man-in-the-Middle (MitM) attacks, Replay attacks and Guessable tokens. More complex attacks like token manipulations were not considered. In the same year, Wang et al. [Xi13] developed a tool named *InteGuard* detecting the invariance in the communication between the client and SP to prevent logical flaws in the latter one. Another tool similar to *InteGuard* is *BLOCK* [LX11]. Both tools can detect and mitigate attacks, but cannot be used for penetration testing of existing implementations and manipulating the traffic. Zhou et al. [YZ14] published on USENIX'14 a fully automated tool named *SSOScan* for analyzing the security of OAuth implementations and described five attacks, which can be automatically tested by the tool. Further SSO protocols are not considered. In 2014, Mainka et al. [MM15d] published a fully automated tool acting as a malicious IdP for analyzing the security of OpenID implementations and described two novel attacks.

SSO extensions. In 2015 an extension called "SAMLyze" was published at Black Hat [Ba15]. Its goal is to pentest SAML SPs fast and easy against XXE, DTDs and to perform automatically a variety of SAML validations. In 2015 another extension analyzing SAML SPs was published [Bi15]. It contains two core functionalities: Manipulating SAML Messages and manage X.509 certificates.

However, both extensions concentrate on SAML but to not consider further SSO protocols.

[12] We use RSyntaxTextArea: `http://sourceforge.net/projects/rsyntaxtextarea/`

6 Conclusion and Future Work

EsPReSSO is the initial approach to create a tool capable to analyze different SSO protocols according their characteristics, to display all relevant parameters in a human readable format, and to manipulate the intercepted data in order to simulate different attacks. Thus, EsPReSSO facilitates the security analysis of SSO protocols.

EsPReSSO contains three different modules: Scanner, Visualizer and Manipulator. Each of these components can be easily extended. Thus, the detection of further protocols, further features regarding the depiction of the messages and manipulation possibilities can be added.

To the best of our knowledge, EsPReSSO is the first tool capable to detect, display and modify multiple different SSO protocols at the same time.

In future, EsPReSSO's functionality will be tested on a large set of websites and if needed modifications approving the detection will be implemented. Another issue is the enlargement of the available attacking set by considering attacks like XML Signature Wrapping (XSW) or attacks on JWTs.

References

[Ba13] Bai, Guangdong; Lei, Jike; Meng, Guozhu; Venkatraman, Sai Sathyanarayan; Saxena, Prateek; Sun, Jun; Liu, Yang; Dong, Jin Song: AUTHSCAN: Automatic extraction of web authentication protocols from implementations. NDSS, February, 2013.

[Ba15] Barber, Jon: , SAMLyze, August 2015.

[Bi15] Bischofberger, Roland: , SAMLRaider, Juli 2015.

[BLFM05] Berners-Lee, T.; Fielding, R.; Masinter, L.: , Uniform Resource Identifier (URI): Generic Syntax. RFC 3986 (INTERNET STANDARD), January 2005. Updated by RFCs 6874, 7320.

[Ch14] Chen, Eric; Pei, Yutong; Chen, Shuo; Tian, Yuan; Kotcher, Robert; Tague, Patrick: OAuth Demystied for Mobile Application Developers. In: Proceedings of the ACM Conference on Computer and Communications Security (CCS). ACM – Association for Computing Machinery, November 2014.

[De96] Deutsch, P.: , DEFLATE Compressed Data Format Specification version 1.3. RFC 1951 (Informational), May 1996.

[Eg13] Egor Homakov: , How we hacked Facebook with OAuth2 and Chrome bugs, Februrary 2013.

[FKS14] Fett, Daniel; Kusters, Ralf; Schmitz, Guido: An expressive model for the Web infrastructure: Definition and application to the Browser ID SSO system. In: Security and Privacy (SP), 2014 IEEE Symposium on. IEEE, pp. 673–688, 2014.

[Ja13] Janrain: , 2013 Consumer Research: The Value of Social Login, 2013.

[Jo06] Josefsson, S.: , The Base16, Base32, and Base64 Data Encodings. RFC 4648 (Proposed Standard), October 2006.

[Li14] Li, Zhiwei; He, Warren; Akhawe, Devdatta; Song, Dawn: The emperor's new password manager: Security analysis of web-based password managers. In: 23rd USENIX Security Symposium (USENIX Security 14). 2014.

[LX11] Li, Xiaowei; Xue, Yuan: BLOCK: A Black-box Approach for Detection of State Violation Attacks Towards Web Applications. In: Proceedings of the 27th Annual Computer Security Applications Conference. ACSAC '11, ACM, New York, NY, USA, 2011.

[Ma14] Mainka, Christian; Mladenov, Vladislav; Feldmann, Florian; Krautwald, Julian; Schwenk, Jörg: Your Software at my Service: Security Analysis of SaaS Single Sign-On Solutions in the Cloud. In: Proceedings of the 6th edition of the ACM Workshop on Cloud Computing Security, CCSW '14, Scottsdale, Arizona, USA, November 7, 2014. pp. 93–104, 2014.

[Mi08] Microsoft: , One account for all things Microsoft, May 2008.

[MM15a] Mainka, Christian; Mladenov, Vladislav: , Connect2id Acknowledgement, 2015.

[MM15b] Mainka, Christian; Mladenov, Vladislav: , CVE-2015-0959, 2015.

[MM15c] Mainka, Christian; Mladenov, Vladislav: , CVE-2015-0960, 2015.

[MM15d] Mainka, Christian; Mladenov, Vladislav: , Do not trust me: Using malicious IdPs for analyzing and attacking Single Sign-On (Full Version with Attachments), 2015. [online] `http://bit.ly/maliciousIdPs_fullversion`.

[Mo08] Morin, Dave: , Announcing Facebook Connect, May 2008.

[Or05] Organization for the Advancement of Structured Information Standards: . Security Assertion Markup Language (SAML) v2.0, 2005.

[RF] RFC6749, IETF: , The OAuth 2.0 Authorization Framework.

[Sal14] Salesforce.com, inc. Inside OpenID Connect on Force.com, 2014.

[Sh02] Shiflett, Chris: , Passport Hacking Revisited, 2002.

[SHB12] Sun, San-Tsai; Hawkey, Kirstie; Beznosov, Konstantin: Systematically breaking and fixing OpenID security: Formal analysis, semi-automated empirical evaluation, and practical countermeasures. Computers & Security, 31(4), 2012.

[Si14] Silver, David; Jana, Suman; Chen, Eric; Jackson, Collin; Boneh, Dan: Password managers: Attacks and defenses. In: Proceedings of the 23rd Usenix Security Symposium. 2014.

[Sl01] Slemko, Marc: , Microsoft Passport to Trouble, 2001.

[So12] Somorovsky, Juraj; Mayer, Andreas; Schwenk, Jörg; Kampmann, Marco; Jensen, Meiko: On Breaking SAML: Be Whoever You Want to Be. In: Presented as part of the 21st USENIX Security Symposium (USENIX Security 12). USENIX, Bellevue, WA, pp. 397–412, 2012.

[sp07] specs@openid.net: , OpenID Authentication 2.0 – Final, December 2007.

[Th14] The OpenID Foundation (OIDF): , OpenID Connect Core 1.0, February 2014.

[TT07] Tsyrklevich, Eugene; Tsyrklevich, Vlad: , Single Sign-On for the Internet: A Security Story, July and August 2007.

[WCW12] Wang, Rui; Chen, Shuo; Wang, XiaoFeng: Signing Me onto Your Accounts through Facebook and Google: A Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services. In: Proceedings of the 2012 IEEE Symposium on Security and Privacy. SP '12, IEEE Computer Society, Washington, DC, USA, 2012.

[We] Websites using Facebook Connect. visited on 2015-05-25.

[Xi13] Xing, Luyi; Chen, Yangyi; Wang, X; Chen, Shuo: InteGuard: Toward Automatic Protection of Third-Party Web Service Integrations. In: Proceedings of 20th Annual Network & Distributed System Security Symposium. 2013.

[YZ14] Yuchen Zhou, David Evans: Automated Testing of Web Applications for Single Sign-On Vulnerabilities. In: 23rd USENIX Security Symposium (USENIX Security 14). USENIX Association, San Diego, CA, August 2014.

[ZE14] Zhou, Yuchen; Evans, David: SSOScan: Automated Testing of Web Applications for Single Sign-On Vulnerabilities. 23rd USENIX Security Symposium, 2014.

Detlef Hühnlein et al. (Eds.): Open Identity Summit 2015,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2015 133

Evaluating Complex Identity Management Systems – The FutureID Approach

Rachelle Sellung[1] Heiko Roßnagel[2]

Abstract: This in-progress paper will discuss the importance of evaluation methods in complex large scale projects, specifically those regarding identity management systems and electronic Identities (eIDs). It will depict the advantages of using a Design Science methodological framework approach and show how the EU project FutureID has utilized this methodology to bring multiple disciplines perspectives together in a harmonized evaluation.

Keywords: Design Science, Large-Scale projects, Evaluation approach, eID's

1 Introduction

A common problem found in many technology-based research projects, specifically in information security, is the sole focus only on the technological aspects. These solutions address mainly issues, such as, security, privacy and reliability [ZR12]. They fail to elicit and consider other requirements such as business and usability requirements. As a result, this approach often veers away from user's needs, markets, and economic contexts. Consequently, there have been multiple security and privacy technologies, which have been designed in a way that often results in market failures; such as, electronic signatures [Ro06] or web anonymity services [FFSS02]. Another strong point mentioned by [ZR12], is that the assumption concluding a technologies market success is solely reliant on their technological sophistication is not satisfactory. When reducing the effort put forth into creating a well-designed business model for the market, it often leads to important factors either not being addressed or not initiated to the best of its capabilities. For example, [GORR04] mentions how technologies often fail to address the user's needs and requirements appropriately with respect to usability and accessibility for both individuals and organizations. In addition, the classical initiation of a technology base project is having the evaluation of the project results being based on a sole evaluation of the pilots. Furthermore, the evaluation results of the pilots are often assumed to be an accurate implication or even forecast on how it would perform in a real market scenario. When including a wider range of disciplines within an evaluation, it becomes quickly apparent that this approach is no longer viable to serve as a well-rounded evaluation for a large complex research project. The FutureID project has taken an alternative approach to address these concerns and challenges. FutureID is a large scale EU project that

[1]Fraunhofer IAO, Identity Management, Nobelstraße 12, 70569 Stuttgart, Germany
firstname.lastname@iao.fraunhofer.de

strives to build a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe. Following a viable security approach [ZR12], FutureID considers the interests of all the stakeholders involved in the eID ecosystem to facilitate economic conditions for wide take-up of its results. It combines experts from seven different disciplines that each provided a requirement analysis for three defined artifacts of the project which depict three levels of the project as a whole. These requirements were considered during the design of the artifacts and serve as a basis for the evaluation approach. As a result the project needed to address these needs with a rigorous, flexible, and comprehensive evaluation method. To put into perspective of importance, FutureID's pilots only show a subset of what the results of this project has to offer, specifically in its reference architecture and the implementation. Further, the Design Science Approach is the process decided to address this task. This research in progress paper focuses mainly on the Design Science Evaluation method, specifically how this was addressed in FutureID. The rest of this paper is organized as follows; section two will include the challenges faced, section three goes into detail on the methodology, section four expands on the FutureID approach, section five serves as a discussion and limitations section, and lastly section six is a conclusion.

2 Challenges

Including a variety of disciplines naturally leads to a more complex evaluation. The disciplines included in the FutureID evaluation are Socio-economic, Security, Legal, Privacy, Usability, Accessibility, and Technical. With that, FutureID has faced many challenges in initiating a comprehensive evaluation its artifacts. First, FutureID is a large project that includes 19 different partners from 11 different EU countries. Having such a diverse consortium in many different ways, often leads to challenges regarding harmonizing and compromising all perspectives to create artifacts that are comprehensive and flexible. Second, FutureID aims at having a flexible Reference Architecture, however with that it increases difficulties in initiating an evaluation method that can be just as flexible. For instance, the Reference Architecture evolved throughout the duration and evaluation process of the project due to the increasing needs of requirements from the different disciplines, going beyond what was originally proposed in the project plan. As a result it was not possible to implement all of the new features defined in the Reference Architecture, due to the limited amount of available resources. Further, due to the flexibility of the architecture many different configurations and different forms of deployment are possible, which of course makes an evaluation even more challenging. While FutureID is capable of supporting many different use and business cases, the two pilot applications only focus on two exemplary use cases. One pilot provides Citizen Services in the e-health domain and the other one focuses on e-Learning Services for Enterprises. As a result these pilots are not capable to showcase all of the possibilities. With this conclusive set of challenges, FutureID faced the largest challenge of finding and applying an evaluation approach that would fulfill its comprehensive and flexible needs.

3 Methodology

FutureID uses the Design Science research approach as they are presenting three novel artifacts and a suitable evaluation that address the artifact's appropriateness to contribute to the problems' solution [NCP91] [ZRMS11]. Design Science research is a set of analytical techniques and perspectives that was originally designed for Information Systems. Design Science's achieves knowledge and understanding of a problem domain by building and application of a designed artifact [MMG02] [HMPR04]. The artifact is created to be used as a tool to better understand the problem and to re-evaluate the problem to improve the quality of the design process and to be able to start the process over again [MMG02]. The overall goal of this approach is to create a design process that is a sequence of expert activities that produces an innovative product [WSE09]. Referring to Figure 1, the Design Science research model satisfies two cases; the business needs (relevance) and the knowledge base (rigor). The knowledge base feeds on creating applicable knowledge that will be able to be used to better an artifact that is used in different real world situations. The knowledge base's objective is to be rigorous in a way that the research built upon existing knowledge and then it further contributes as applicable knowledge to an artifact or theory. After it is applied, then it assists in assessment and refinement to further justify and evaluate in a more scientific manner. The knowledge resulting from this process is added to the knowledge base. Simultaneously, the environment side serves more the business-needs assessment of the model. Its goal is to apply the artifact or theory in a relevant way and real world situations. In the Design Science Research model, business needs are assessed and evaluated in consideration of organizational strategies, structures, cultures and already existing business processes [HMPR04]. Furthermore, business needs go through the same process as the knowledge base did, as it is further assessed and refined to justify and evaluate the artifact or theory. The difference with the Environment side is that afterwards it the result is applied in an appropriate environment and then what is learned is returned to the Environment side. This model shows how these two processes work simultaneously and perpetually together to continuously make a method or artifact stronger and more comprehensive. Furthermore, the Design Science Evaluation methods, which are shown in Table 2, are divided into five broad categories; observational, analytical, experimental, testing, and descriptive. These categories cover a wide variety of evaluation methods; such as, case studies, dynamic analysis, simulation, functional testing, or informed argumentation. Each evaluation method shouldn't be considered or weighed at the same consistency as an informed argument is not as credible or reliable as a field study. An advantage to the Design Science evaluation method is that these five categories are flexible enough to be applied in many different disciplines despite the range of different techniques. These methods can be applied to a wide variety of research fields whether it's in law or in a more technical field. The Design Science evaluation methods are flexible, but organized. This provides a strong argument to how one can organize a variety of interdisciplinary evaluation methods. Overall, Design Science has a strong and comprehensive research model, dependable guidelines, and wide spread evaluation methods. In the FutureID project, we have 7 discipline teams of experts, who

follow this approach and apply their own evaluation techniques within the realm of the Design Science Evaluation Methods. As a result of this application, each discipline creates a list of requirements that each artifact would have to fulfill. This results in a basis from a Design Science Methodology framework for the interdisciplinary evaluation of the main artifacts of the FutureID project.

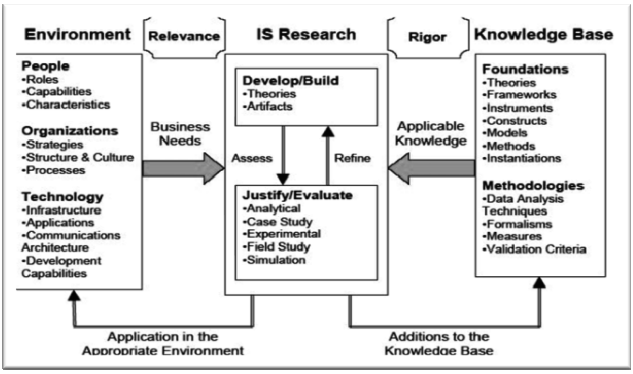

Fig. 1: Design Science Research Model [HMPR04]

Observational	Case Study: Study artifact in depth and business environment
	Field Study: Monitor use of artifact in multiple projects
Analytical	Static Analysis: Examine structure of artifact for static qualities (e.g. complexity)
	Architecture Analysis: Study fit of artifact into technical IS architecture
	Optimization: Demonstrate inherent optimal properties of artifact or provide optimality bounds on artifact
	Dynamic Analysis: Study artifact in use for dynamic qualities (e.g. performance)
Experimental	Controlled Experiment: Study artifact in use for dynamic qualities (e.g. usability)
	Simulation: Execute artifact with artificial data
Testing	Functional (Black Box) Testing: Execute artifact interfaces to discover failures and identify defects
	Structural (White Box) Testing: Preform coverage testing of some metric (e.g. execution paths) in the artifact implementation
Descriptive	Informed Argument: Use information from the knowledge base(e.g. relevant research) to build a convincing argument for the artifacts utility
	Scenarios: Construct detailed scenarios around the artifact to demonstrate its utility

Tab. 2: Design Science Evaluation Methods [HMPR04]

4 FutureID Approach

FutureID has dedicated a significant effort to evaluate its results in a rigorous manner (e.g. Test beds for the Pilots, Evaluation WP). To provide an overhead of results, FutureID has dedicated part of the Sub-Project Transfer tasks to Consolidation and Evaluation. The work packages dedicated to these tasks present the 'big picture' of the major results for the entire large-scale project of FutureID. The consolidated view forms the basis to give a systematic evaluation. The FutureID Evaluation approach using a Design Science Methodology framework has been a valuable tool in organizing and harmonizing multiple disciplinary evaluation approaches.

To provide a closer look, FutureID has simplified its evaluation process into three easy steps. First, they identify each of the Artifacts, which in their case are two pilots, a reference architecture, and implementation. Second, they clarify where each interdisciplinary team considers the artifacts and develop requirements regarding their disciplinary. This step is ranked regarding importance and is utilized by using the Evaluation Wiki Tool. Lastly, they Re-evaluate, which is when each requirement identified will be reevaluated on whether they should be really implemented or initiated in each artifact. Of course, with the complexity of some of the artifacts a noble evaluation could not be sufficiently executed with just this process, therefore, FutureID has used extra evaluation steps to properly consider specific needs of some of the artifacts. For example, they have used testbeds in grasping a better outlook of the pilots. The Evaluation Wiki tool is a quality control mechanism that has been used for the core evaluation of FutureIDs results. It has a variety of different beneficial functions that lead to a practical and more optimal evaluation method. On the practical side, it presents an easy to read and adjust, while still being a comprehensive solution for documentation of the evaluation requirements needed for each artifact. Each artifact can be sub categorized into viewing each of the importance levels of requirements (must, should, may, all) on the main page of the tool. It classifies each requirement, from which interdisciplinary team it's from, comment section, and its rank of importance. While collaborating with multiple disciplines, harmonizing and consolidating a wide spectrum of requirements proved to have some difficulties and major conflicts. In order to resolve this problem, FutureID included another addition to the Evaluation Wiki tool and to the Evaluation work package. The additions was an added deliverable that focused on the clarification of which requirements are either similar to, relates to, or conflicts with other requirements. This is a necessary task that all large scale interdisciplinary projects should have in harmonizing requirements in evaluations. This task helped provide insight on how all of the requirements can cooperate and be applied all together. In addition to these processes, the testbed has proven to be a great technical method in testing the implementation and pilot applications. It is built of three different levels of testing; unit testing, integration testing, and system testing. The implementation artifact is tested using the unit, integration, and system testing. While, the pilots are tested on only the system level testing, the form of evaluation methods between different artifacts obviously varies. However, the Design Science Evaluation methods are broad enough to cover a wide range of techniques.

5 First Results and Limitations

As FutureID is an ongoing project, this section will elaborate on first results in FutureID and limitations. Until now, the requirements have been formed and harmonized for the evaluation of all of the FutureID artifacts. The advantages could be seen as premature, but as the Design Science Methodology framework has provided mostly positive feedback in research, the outcomes are promising. Overall, this could be seen as one of the main limitations presented in this in-progress paper and application, even though until now there has been promising first results. Continuing, FutureID has already gain first results on the Reference Architecture, which has provided encouraging results. As a way of evaluation, each discipline represented in FutureID established requirements that should be met for each artifact. The Reference Architecture passed all of the requirements in all 'must, may, should' categories regarding the Socio-Economic Requirements. Regarding the Technical Requirements, it also passed 92 % of the 'must, may, should' categories for both the Reference Architecture and the Implementation artifacts. Overall, most of the disciplines displayed similar positive remarks regarding the application of requirements. Even though FutureID is currently in the stage of concluding the evaluation of both the Implementation artifact and the Pilots, it can be foreseen that similar positive results are also to emerge.

6 Conclusion

This research in-progress paper discussed the need for technical projects to focus on multiple disciplines in order to be more inviting to the market. Further, the paper takes a practical focus and goes into detail how the project FutureID has applied a Design Science Evaluation approach to better evaluate, re-evaluate, and harmonize the needs and demands of different disciplines and different perspectives. As the project and this paper are still in progress, only first results were able to be presented. However, FutureID will be concluding its work by fall of 2015, where larger results of this inter-disciplinary evaluation application can be seen and interpreted.

References

[GORR04] Greenwald S, Olthoff K, Raskin V, Ruch W. The user non-acceptance paradigm: INFOSEC's dirty little secret. Proceedings of the 2004 workshop on New security paradigms. ACM, Nova Scotia, Canada 2004. p35-43

[HMPR04] Hevner A, March S, Park J, Ram S. Design science in information systems research, MIS Quarterly 2004. p 75-105.

[FFSS02] Feigenbaum J, Freedman M, Sander T, Shostack A. Economic barriers to the deployment of existing privacy technologies (position paper). Proceedings of the Workshop on Economics of Information Security; 2002.

[Fu14] FutureID- Shaping the Future of Electronic Identity, [Internet]. 2014. Available: http://futureid.eu/.

[NCP91] Nunamaker J, Chen M, Purdin T. Systems development in information systems research. Journal of Management Information, 1991.

[MMG02] Markus ML, Majchrzak A, Gasser L. A design theory for systems that support emergent knowledge processes, Mis Quarterly, 2002. p. 179–212.

[Ro06] Roßnagel, H. On Diffusion and Confusion – Why Electronic Signatures Have Failed. Trust and Privacy in Digital Business; 2006. p. 71-80

[WSE09] Watts S, Shankaranarayanan G, Even A. Data quality assessment in context: A cognitive perspective. Decis Support Syst., 2009. p. 202–211.

[ZR12] Zibuschka J, Roßnagel H. A Structured Approach to the Design of Viable Security Systems. ISSE 2011- S Wiesbaden: Vieweg+ Teubner; 2012. p.246-55.

[ZRMS11] Zibuschka, J., Roßnagel, H., Muntermann, J. und Scherner, T. Mobile Emergency Management Services Targeting Large Public Events. International Journal of Service Science, Management, Engineering, and Technology (IJSSMET). 2011.

Detlef Hühnlein et al. (Eds.): Open Identity Summit 2015,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2015 141

Innovative Building Blocks for Versatile Authentication within the SkIDentity Service

Detlef Hühnlein[1] Max Tuengerthal[1] Tobias Wich[1] Tina Hühnlein[1] Benedikt Biallowons[1]

Abstract: Accepting arbitrary electronic identity cards (eIDs) and similar authenticators in cloud and web applications has been a challenging task. Thanks to the multiply awarded "SkIDentity Service" this has changed recently. This versatile authentication infrastructure combines open technologies, international eID standards and latest research results with respect to trusted cloud computing in order to offer electronic identification and strong authentication in form of a trustworthy, simple to use and cost efficient cloud computing service, which supports various European eIDs as well as alternative authenticators proposed by the FIDO Alliance for example. The present contribution exposes innovative and patent pending building blocks of the SkIDentity Service: (1) The "Identity Broker", which eases the integration of authentication, authorization, federation and application services and in particular allows to derive secure credentials from conventional eID cards, which can be transferred to mobile devices for example. (2) The "Universal Authentication Service" (UAS), which allows to execute arbitrary authentication protocols, which are specified by the recently introduced "Authentication Protocol Specification" (APS) language, (3) the "Cloud Connector" which eases the integration of federation protocols into web applications and last but not least (4) the "SkIDentity Self-Service Portal", which makes it extremely easy for Service Providers to configure the necessary parameters in order to connect with the SkIDentity Service and use strong authentication in their individual applications.

1 Introduction

As the inherent weaknesses of password-based authentication [Ne94, IWS04] are about to become obvious in practice (see [Fe14a, Fe14b, CN14] for example) there seems to be a trend towards implementing strong authentication for web-based applications [Go11, Am13b, Mi13, Li13, FI] using a variety of protocols and authentication means. While supporting versatile authentication technologies certainly promotes the diffusion and adoption in practice [HRZ10], it also imposes the new challenge how to integrate and handle the large variety of involved technologies in an efficient manner. A basic strategy for handling this kind of complexity is to introduce appropriate interfaces, which allow to decouple certain services and modules, which can be developed, maintained and integrated in an independent manner. On a macro scale this approach has lead to the versatile authentication infrastructure designed and developed within the SkIDentity project, which has been supported by the German government within the "Trusted Cloud"[2] programme (see Section 2

[1] ecsec GmbH, Sudetenstraße 16, 96247 Michelau, Germany, {firstname.secondname}@ecsec.de
[2] See `http://trusted-cloud.de`.

This work was partly supported by the German Federal Ministry of Economics and Energy (BMWi) within the Trusted Cloud project **SkIDentity** (01MD11025A) (see `https://skidentity.com`) and the European Union within the 7th FP project **FutureID** (ICT-318424) (see `https://futureid.eu`).

and especially Figure 1) and on a micro scale to the highly modular and extensible Open eCard App (see [Wi13]), which allows to support arbitrary smart cards and authentication protocols in an efficient manner.

Against this background we will go one step further here and expose some innovative and patent pending building blocks of this versatile authentication system in Section 3: (1) The "Identity Broker" (see Section 3.1), which allows to integrate arbitrary services for authentication, authorization and federation and in particular allows to derive secure credentials from conventional eID cards, which can be transferred to mobile devices for example. (2) The "Universal Authentication Service" (UAS) (see Section 3.2), which allows to execute arbitrary authentication protocols, which are specified by the recently introduced "Authentication Protocol Specification" (APS) language [AM13a, AM15]. (3) The "Cloud Connector" (see Section 3.3) which eases the integration of federation protocols into web applications and last but not least (4) the "SkIDentity Self-Service Portal" (see Section 3.4), which makes it extremely easy for Service Providers to configure the necessary parameters in order to integrate with the SkIDentity Service in order to use strong authentication. Section 4 summarizes the main aspects of the present contribution and provides an outlook towards future developments.

2 Overview of the SkIDentity system

The main contribution of the present paper is to expose some innovative and patent pending building blocks of the SkIDentity system as outlined in [Sk12] and Figure 1. For this purpose we start by briefly recalling the main aspects of the SkIDentity Reference Architecture.

The SkIDentity system is depicted in Figure 1 and builds upon the concept of Federated Identity Management as explained in [MR08, HRZ10, Ca05a]. It refines the classical components "Client", "Service Provider" and "Identity Provider" in order to support arbitrary authentication mechanisms, eID-tokens, credential technologies and federation protocols.

There are components at the Client, the Service Provider and within the SkIDentity Service.

2.1 System Components at the Client

The system of the User (Client) comprises the *User Agent* (UA), which can be realised by an arbitrary browser, and an appropriate *eCard-App* (eCA), such as the Open eCard App [Hü12, Wi13], which enables the User to authenticate at an *Authentication Service* (AS) using some Credential. Due to the modular architecture based on ISO/IEC 24727 [IS08] it is easy to support various smart cards and authentication protocols. Using the add-on framework introduced in [Wi13] it is also easy to add application-specific logic[3], which can be accessed via corresponding interfaces.

[3] See [Ku13] for an example.

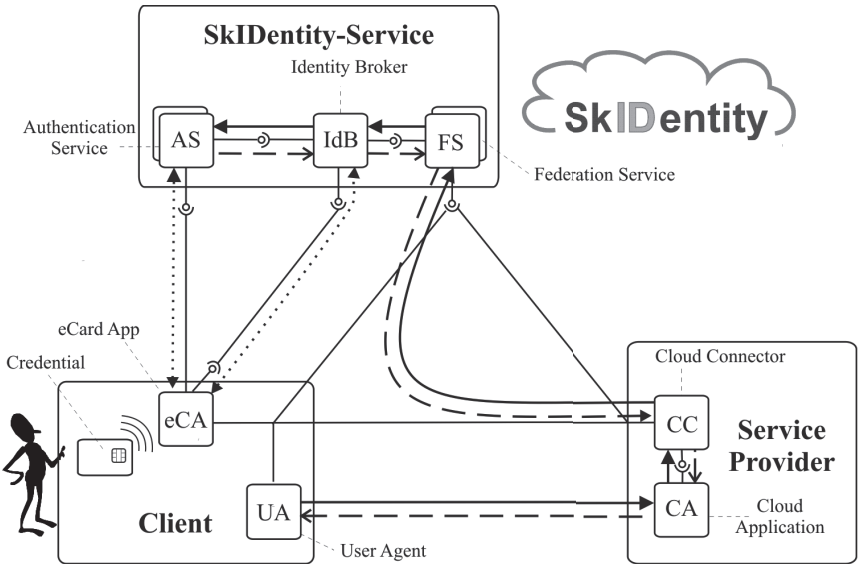

Fig. 1: SkIDentity Reference Architecture

2.2 System Components at the Service Provider

The system of the Service Provider (SP) comprises the *Cloud Application* (CA) and an appropriate *Cloud Connector* (CC) (see Section 3.3), which allows to communicate with an appropriate *Federation Service* (FS) in the SkIDentity Infrastructure using an appropriate federation protocol such as SAML [Ca05a], OpenID [Op] or OAuth [HL10, Ha12, HJ12] for example.

2.3 SkIDentity Service

Within the SkIDentity Service there are various *Federation Services* (FS) and a variety of *Authentication Services* (AS), which are connected via the *Identity Broker* (IdB) (see Section 3.1). The Identity Broker acts as information intermediary and provides the different eID-Services in a bundled and rehashed way. This offers the possibility to use the different services and tokens (electronic identity cards, electronic health cards, health professional cards, bank and signature cards, company ID tokens and last but not least FIDO's U2F token [FI]) with an easy and consistent interface for the secure authentication in cloud based applications.

3 Innovative Building Blocks of the SkIDentity Service

This section exposes innovative and patent pending building blocks of the SkIDentity Service. The "Identity Broker" is discussed in Section 3.1, the "Universal Authentication Ser-

vice" is subject of Section 3.2, the "Cloud Connector" is subject of Section 3.3 and the "SkIDentity Self-Service Portal" finally is introduced in Section 3.4.

Fig. 2: Identity Selector within the Identity Broker

3.1 Identity Broker

As depicted in Figure 1 the Identity Broker (IdB) is the central component within the SkIDentity Service, which receives authentication requests from some FS and forwards this request to an appropriate AS. This service performs the authentication of the User and returns the result to the IdB, which will return the received data to the calling FS. The selection of the AS is performed based on (1) the authentication options acceptable by the Service Provider, (2) the technical capabilities of the Client (e.g. whether an eID client software is present or not) and finally (3) the credential selected by the User among the possible options as depicted in Figure 2. Based on this information the IdB is able to determine a suitable AS, which will perform the authentication of the User.

The set of acceptable authentication options and requested attributes is specified by the Service Provider using the SkIDentity Self-Service Portal (see Section 3.4), which translates the choices to corresponding XML-based SAML Metadata structures, as outlined in [HTW14].

The IdB may not only act as a dispatcher, which simply forwards messages to some AS, but the IdB may also initiate the derivation of a cryptographically protected credential from a conventional eID card. Such a "Cloud Identity" can be securely stored on the User's system, transferred to another device of the User (e.g. his personal smart phone) and it may be bound to an additional cryptographic hardware token, in order to enhance security. A Cloud Identity may be seen as a cryptographically secured copy of an original eID, which may substitute a real eID in various online scenarios, while supporting a high level of usability. As a Cloud Identity can be transferred to arbitrary smart phones, this approach turns SkIDentity into a "Mobile eID as a Service" platform.

3.2 Universal Authentication Service

The Universal Authentication Service (UAS) is a specifically powerful Authentication Service, which has been developed within the FutureID project and which makes it easy to support arbitrary authentication protocols.

As the existing eID cards, eHealth cards, and eSign cards already support a large variety of different authentication protocols and it is expected that future authentication tokens will support other credentials and authentication protocols, it would be close to impossible to implement all required protocols using a conventional approach, because this would require a specialized program module for each authentication protocol.

In order to solve this problem, protocols are described in the Authentication Protocol Specification (APS) language [AM13a, AM15]. The APS descriptions of the authentication protocols in turn refer to appropriate Basic Services, such as cryptographic primitives or smart card commands according to ISO/IEC 7816 [IS]. As the different authentication protocols are all composed of a rather limited set of Basic Services, the problem of supporting arbitrary authentication protocols is reduced to providing this limited set of basic functionality and providing appropriate APS descriptions for the different authentication protocols.

Another advantage of specifying authentication protocols in the APS language is that the APS language is directly supported by state of the art formal protocol analysis tools, such as OFMC [MV09], that can be used to prove security properties of the authentication protocols.

The core component of the UAS is the Job Execution Environment (JEE) (see Section 3.2.2), which runs authentication protocols specified in the APS language. This makes it possible to support arbitrary protocols in a very efficient manner.

3.2.1 Authentication Protocol Specification Language

Describing the APS language is beyond the scope of this paper and we refer to [AM13a, AM15] for details. Instead, in Listing 1, we present an example which demonstrates the

flavor of describing authentication protocols in APS. In this protocol, two parties (PCD and PICC) want to authenticate each other using an authenticated Diffie-Hellman key exchange protocol. The specification in Listing 1 consists of (1) the protocol name, (2) type declarations, (3) message formats, (4) the initial knowledge of the participants, (5) the actions that describe the message that are sent/received by the parties (this is the main part of the specification), and (6) the goals (security properties) this protocol must satisfy.

```
Protocol: EAC
Types:
  Nonce RpiccTA, RpiccCA;
  ...
Formats:
  eac1input( Msg, ImpData, ImpData, ImpData, ImpData );
  eac1output( ImpData, ImpData, ImpData, efcardaccess, Agent, Nonce );
  ...
Knowledge:
  PCD:  cert(PCD,pk(PCD),ca), pk(PCD), pk(ca), ...;
  PICC: cert(PICC,exp(g,sk(PICC)),ca), pk(ca), sk(PICC), ...;

Actions:
  [PCD]*->*[PICC]: eac1input( cert(PCD,pk(PCD),ca), CertDesc, ... )
  [PICC]*->*[PCD]: eac1output( RC, CHAT, CAR, EFCA, IDPICC, RpiccTA )
  let PK_PCD = exp(g,X)
  let S_PCD  = sign(inv(pk(PCD)),(IDPICC,RpiccTA,comp(PK_PCD)))
  [PCD]*->*[PICC]: eac2input( CertChain, PK_PCD, S_PCD )
  let PK_PICC = exp(g,sk(PICC))
  let K       = exp(PK_PCD,sk(PICC))   # = exp(PK_PICC,X)
  let Kmac    = kdf(K,RpiccCA)
  let Tpicc   = mac(Kmac,PK_PCD)
  [PICC]*->*[PCD]: eac2output( cert(PICC,PK_PICC,ca), Tpicc, RpiccCA )

Goals:
  PICC authenticates PCD on Tpicc
  PCD authenticates PICC on Tpicc
  K secret of PICC, PCD
```

List. 1: The EAC protocol specified in the APS language.

3.2.2 Job Execution Environment

The Job Execution Environment (JEE) is able to load and execute protocols that are defined in the APS language. Since the JEE is not able to execute the abstract APS directly, it must first be compiled to some kind of executable script code. For this purpose the JEE supports JavaScript to which an APS file is compiled to be executed.

An important feature of the JEE is the possibility to access and execute the Basic Services (BS) which provide different functions for common tasks, e.g. to compute a hash value, obtain the status of a certificate via Online Certificate Status Protocol (OCSP) or to create a certain Application Protocol Data Unit (APDU), which is to be sent to an Interface Device (IFD) component, which in turn communicates with a smart card. Furthermore

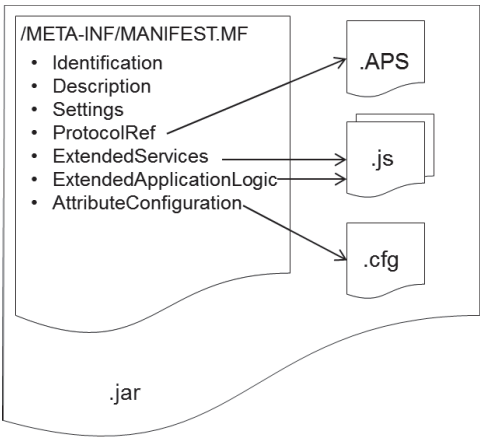

Fig. 3: Structure of a Credential-specific APS (CAPS) package.

the JEE may be equipped with additional JavaScript-based Extended Services (ES), which combine several calls and hence may be used to provide higher level functionality.

The difference between the Extended Services and the Basic Services is that the Basic Services are available in the Universal Authentication Service per default. Extended Services are usually more light-weight and are shipped together with a specific APS file. The environment that is needed by a specific protocol can be specified within the manifest file, which is distributed together with the APS file, which specifies the authentication protocol. The JEE uses this configuration file to set up a context in which the authentication protocol is executed. Every instance of a protocol has its own context so that the different instances do not interfere with each other.

Protocol descriptions are distributed in Java Archive (JAR) files that can be loaded by the Job Execution Environment during runtime. Since the leading factor when determining the protocol (and, hence, the JAR file) to be used for authentication is the type of the credential (i.e., the type of an eID card or some other authentication token) that is used for authentication, we call these JAR files Credential-specific APS (CAPS) packages. Besides the script files that define the protocol and the configuration that is used to set up the context for the protocol, a CAPS package can optionally contain additional Extended Services, which can be provided in form of JavaScript files. Furthermore, it optionally contains information about extended application logic that is to be executed after the authentication has been performed. For example, in case the credential is an eID card, the application logic might communicate with the card to sign messages or to obtain attributes from the card. Obtaining attributes using secure messaging established during authentication is the most common use case. It is therefore possible to provide an attribute configuration which provides information about how attributes are obtained and extracted from eID cards. The structure of a CAPS package is depicted in Figure 3.

We now describe the processing within the JEE in more detail. It can be structured into three phases: (1) Initialization, (2) Execution of the Authentication Protocol and (3) Execution of the Application Logic.

Initialization. In the initialisation phase, the JEE loads the CAPS package, creates an initial (job execution) context, for the protocol to be executed, and compiles the authentication protocol that is specified in the APS language into executable JavaScript code.

Execution of the authentication protocol. In this phase, the JEE first executes initialization code (if provided) and then executes the authentication protocol, i.e., the previously generated JavaScript code. During this execution, the JavaScript code may call predefined functions (crypt, decrypt, hash, etc.) to perform basic cryptographic operations. The JEE translates these function calls into calls to corresponding Basic Services (BS) or Extended Services (ES). Which algorithm to call (e.g., SHA-256 for hashing) is determined by the JEE during runtime using the settings given in the CAPS package (it may depend on the context, in particularly on messages received from the client). To generate and parse messages that are sent to/received from the client, the JavaScript code may use the message format objects that are provided by the CAPS package. Furthermore, the JavaScript code may call functions to send and receive messages to/from the network.

3.3 Cloud Connector

If the Cloud Application already supports a standardized federation protocol, such as SAML [Ca05a] or OAuth [HJ12] for example, it can directly communicate with the corresponding Federation Service within the SkIDentity Service. If not, it may perform the integration using the Cloud Connector (CC).

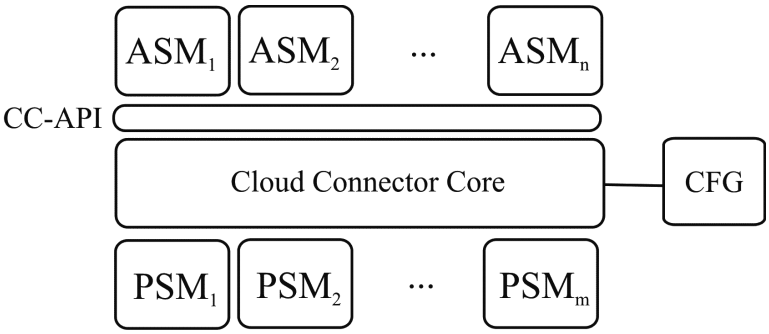

Fig. 4: Architecture of the SkIDentity Cloud Connector

As depicted in Figure 4, the CC is a modular integration library, which is available for different platforms, such as Java, PHP or .NET for example, and consists of a central component (Cloud Connector Core), which is accessible via a simple CC-API, which allows to

- request the authentication of the User (`authenticate( )`),
- get the identifier of the User determined during authentication (`getNameId( )`),
- access a particular attribute (`getAttribute($name)`) or all attributes of the User (`getAttributes( )`) or
- logout and redirect the User to a particular URL (`logout($return)`).

While the Platform Specific Modules (PSM_i) implement the different federation protocols (SAML, OAuth etc.), the Application Specific Modules (ASM_j) take care about the final integration into some application. There are various Application Specific Modules for popular Open Source applications, including Joomla, WordPress, ownCloud, MediaWiki, TYPO3, phpBB and Magento for example.

3.4 SkIDentity Self-Service Portal

While the integration of eIDs into cloud and web applications has been a challenging task, the SkIDentity Self-Service Portal[4] makes it easy for Service Providers to configure the parameters, which are required for the smooth integration of an individual service. The configuration can simply be performed by a responsive web application, which allows to specify (1) the information which is displayed to the User (see Figure 2), (2) the acceptable credentials and required attributes and (3) the corresponding technical parameters required for the federation protocol. As standardized SAML Metadata structures according to [Ca05b, Ca12] are used for this purpose, it is easy to import existing SAML Metadata files and export the generated data to another standardized system.

4 Summary and Outlook

The present paper exposed some innovative and patent pending building blocks of the multiply awarded SkIDentity Service, which makes it easy to accept eID cards and similar authenticators in cloud and web applications. In particular it was shown above that this system comprises an Identity Broker (see Section 3.1) which makes it easy to integrate arbitrary services for authentication and federation and create cryptographically protected derived credentials, which can be securely transferred to mobile devices for example. This gives rise to an innovative "Mobile eID as a Service" offering. Using the innovative Universal Authentication Service (see Section 3.2) one can support arbitrary authentication protocols, which are described by an appropriate "Alice and Bob"-like language as outlined in Listing 1. Last but not least it is easy to integrate cloud and web applications with the SkIDentity Service by using the convenient Self-Service Portal (see Section 3.4) and an appropriate Cloud Connector (see Section 3.3), if necessary.

[4] See `https://sp.skidentity.de`.

While the current focus of the SkIDentity Service is to provide strong authentication, future developments will extend the service in order to support authorization and provisioning as well as electronic signatures and in the long term perspective also the management of more complete business processes.

References

[AM13a] Almousa, Omar; Mödersheim, Sebastian: , Future AnB: The projected APS Language of FutureID. FutureID – WP42 / D42.3, 2013. http://futureid.eu/data/deliverables/year1/Public/FutureID_D42.03_WP42_v1.0_Design%20of%20formal%20APS-language.pdf.

[Am13b] Amazon Inc.: , AWS Multi-Factor Authentication, 2013. http://aws.amazon.com/de/mfa/.

[AM15] Almousa, Omar; Mödersheim, Sebastian: , Alice and Bob: Reconciling Formal Models and Implementation. submitted for publication, 2015. http://www.imm.dtu.dk/~samo/SPS.pdf.

[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; Moreh, Jahan; Philpott, Rob; Maler, Eve: , Metadata 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-metadata-2.0-os.pdf.

[Ca12] Cantor, Scott: , SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0. OASIS Committee Specification 01, 2012. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/sstc-saml-metadata-ui-v1.0.pdf.

[CN14] CNET: , eBay hacked, requests all users change passwords. Press Release 21.05.2014, 2014. http://www.cnet.com/news/ebay-hacked-requests-all-users-change-passwords/.

[Fe14a] Federal Office for Information Security: , Million-fold Identity Theft: Federal Office for Information Security offers security test for email addresses. Press Release 21.01.2014, in German, 2014. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Mailtest_21012014.html.

[Fe14b] Federal Office for Information Security: , New Case of large-scale Identity Theft: Federal Office for Information Security informs victims. Press Release 07.04.2014, in German, 2014. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Neuer_Fall_von_Identitaetsdiebstahl_07042014.htmll.

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

[Go11] Google: , Advanced sign-in security for your Google account, 2011. http://googleblog.blogspot.de/2011/02/advanced-sign-in-security-for-your.html.

[Ha12] Hardt, D.: , The OAuth 2.0 Authorization Framework. Request For Comments – RFC 6749, 2012. http://www.ietf.org/rfc/rfc6749.txt.

[HJ12] Hardt, D.; Jones, M.: , The OAuth 2.0 Authorization Framework: Bearer Token Usage. Request For Comments – RFC 6750, 2012. http://www.ietf.org/rfc/rfc6750.txt.

[HL10] Hammer-Lahav, E.: , The OAuth 1.0 Protocol. Request For Comments – RFC 5849, April 2010. http://www.ietf.org/rfc/rfc5849.txt.

[HRZ10] Hühnlein, Detlef; Rossnagel, Heiko; Zibuschka, Jan: Diffusion of Federated Identity Management. In: Tagungsband "Sicherheit 2010". volume 170 of LNI. GI, pp. 25–37, 2010. http://www.ecsec.de/pub/Sicherheit2010.pdf.

[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.

[Hü12] Hühnlein, Detlef; Petrautzki, Dirk; Schmölz, Johannes; Wich, Tobias; Horsch, Moritz; Wieland, Thomas; Eichholz, Jan; Wiesmaier, Alexander; Braun, Johannes; Feldmann, Florian; Potzernheim, Simon; Schwenk, Jörg; Kahlo, Christian; Kühne, Andreas; Veit, Heiko: On the design and implementation of the Open eCard App. In: Sicherheit 2012. GI-LNI, 2012. http://subs.emis.de/LNI/Proceedings/Proceedings195/95.pdf.

[IS] ISO/IEC 7816: , Identification cards – Integrated circuit cards – Part 1-15. International Standard.

[IS08] ISO/IEC: , ISO/IEC 24727: Identification cards – Integrated circuit cards programming interfaces – Part 1-6, 2008.

[IWS04] Ives, Blake; Walsh, Kenneth R; Schneider, Helmut: The domino effect of password reuse. Communications of the ACM, 47(4):75–78, 2004.

[Ku13] Kuhlisch, Raik; Petrautzki, Dirk; Schmölz, Johannes; Kraufmann, Ben; Thiemer, Florian; Wich, Tobias; Hühnlein, Detlef; Wieland, Thomas: An Open eCard Plug-in for accessing the German national Personal Health Record. In: Open Identity Summit 2013. volume 223 of GI-LNI, 2013.

[Li13] Lindemann, Rolf: Not Built On Sand – How Modern Authentication Complements Federation. In: Proceedings of Open Identity Summit 2013. volume 223 of Lecture Notes in Informatics. GI e.V., pp. 164–168, 2013.

[Mi13] Microsoft Inc.: , Microsoft Account Gets More Secure, 2013. http://blogs.technet.com/b/microsoft_blog/archive/2013/04/17/microsoft-account-gets-more-secure.aspx.

[MR08] Maler, Eve; Reed, Drummond: The Venn of Identity: Options and Issues in Federated Identity Management. IEEE Security & Privacy Magazine, 6(2):16–23, 2008.

[MV09] Mödersheim, Sebastian; Viganò, Luca: The Open-Source Fixed-Point Model Checker for Symbolic Analysis of Security Protocols. In (Aldini, Alessandro; Barthe, Gilles; Gorrieri, Roberto, eds): FOSAD. volume 5705 of Lecture Notes in Computer Science. Springer, pp. 166–194, 2009.

[Ne94] Neumann, Peter G.: Risks of passwords. Commun. ACM, 37(4):126, 1994.

[Op] OpenID Foundation: , OpenID Authentication 2.0. Final, December 5, 2007. http://openid.net/specs/openid-authentication-2_0.html.

[Sk12] SkIDentity-Team: , SkIDentity - Reference Architecture. Version 1.0, 2012.

[Wi13] Wich, Tobias; Horsch, Moritz; Petrautzki, Dirk; Schmölz, Johannes; Hühnlein, Detlef; Wieland, Thomas; Potzernheim, Simon: An extensible platform for eID, signatures and more. In: Proceedings of Open Identity Summit 2013. volume 223 of Lecture Notes in Informatics. GI e.V., pp. 55–68, 2013.

Detlef Hühnlein et al. (Eds.): Open Identity Summit 2015,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2015 153

Towards a Secure Cloud Usage for Financial IT

Marcus Hilbrich[1] Ronald Petrlic[2] Steffen Becker[3]

Abstract: Cloud Computing and Big Data are the current hot topics in research and industry. Based on the enormous amount of preliminary work, ranging from grid and distributed computing to data mining and clustering, to name only a few approaches, cloud computing has become a de-facto standard for computing in general and data-intensive industry tasks in particular. Thus, a lot of questions about how to develop and implement such systems are already answered, but nonetheless, there is reservation to adopt such techniques in some business areas. Most of the reservations are due to security reasons, as in certain areas, like in the banking sector or in the health industry, high levels of security standards have been met for decades and those standards must not be weakened. This is the reason why we investigate—closely together with partners from the industry—how to overcome security concerns in the adoption of cloud computing in the financial industry. An introduction to our strategies is given with this paper.

Keywords: Cloud Computing, Security, Financial IT, Scalability, Elasticity, Distributed Infrastructure, Services, Storage

1 Introduction

In many commercial computing environments it is a common concept to pay for on-demand resource usage. This avoids to over-provision resources and pay for under-utilised hardware. The concept also supports an outsourcing of IT tasks that are not the primary concern of the business. In short, the operation of hard- and software is replaced by services from a provider. Overall, this approach allows for a concentration on the core business and it constitutes a variable and often more cost-efficient usage of exactly the amount of resources that are required in a specific situation. A common solution to this issue is the usage of cloud systems.

In a typical scenario for an IT-assisted enterprise, it is usual to store and process both the customers' and the company's data, which are mainly related to a concrete business. The access to the data has to be restricted. The services can be self-developed and be part of the company's knowledge base or be general or purchased. Depending on the categorization, the services are strongly business-related or be commonly available tools. In most cases, the operation of computing resources, though, does not constitute a core business. Otherwise, it is needed to have enough resources available at all times, even under rare events, which appear just once a year like, e.g. during Christmas shopping period or balancing of accounts. Thus, in case the hardware is provisioned, the mean

[1] Software Quality Lab (s-lab), Universität Paderborn, marcus.hilbrich@uni-paderborn.de
[2] Software Quality Lab (s-lab), Universität Paderborn, ronald.petrlic@uni-paderborn.de
[3] Software Engineering Chair, Technische Universität Chemnitz, steffen.becker@informatik.tu-chemnitz.de

utilisation is often very low.

Considering cost, utilisation, flexibility, and availability, it is often a good decision to use cloud systems with a pay-per-use pricing model. However, cloud technologies also bring new challenges. Many of them are already addressed and have to be adapted to the concrete situation, others need the introduction of innovative ideas. However, we expect that we can handle all the challenges and strongly benefit from using cloud technologies.

The following aspects need to be considered when your data is not under your physical control. You have to avoid a locked-in syndrome [PC09], you have to care about Service Level Agreements (SLAs) [Be11] and you have to establish mutual trust with your service and resource providers.

We are working in the project "Securing the Financial Cloud"[4] (SFC)[5]. The aim of the project is to explore how the advantages of cloud-like systems can be utilised by computing and storage systems of financial IT. This means we have to deal with data from e.g. Automatic Teller Machines (ATMs), bank transfers, balance of accounts, inter-bank transfers, and commercial papers. This data is highly valuable in terms of money, has a very high protection demand defined by the stockholder, and a bulk of legal restrictions.

Besides the data, we have to deal with the analysis performed by services. We have different kinds of aspects of such services. From simple ones that balance an account or calculate interests, which have a low protection demand[6] up to services that estimate the financial standing of a bank-related customer or support strategical investment decisions that hold strong intellectual properties and need an according protection.

To allow stakeholder with different security demands to have separate and shared data in a cooperatively used system, a multi-mandatory support has to be realised. This allows e.g. inter-bank communication (for transferring money from one bank to another one and so on). To avoid a locked-in syndrome, the data have to be sorted by different resource providers and data processing has to be realised independent from a concrete resource provider. In concrete we want to enable a provider independent usage of private and public clouds (hybrid cloud concepts) [Ro11] and cloud brokers [BRC10].

So we have to deal with the already known challenges of scalability, elasticity, and fulfilment of SLAs in a cloud-based environment which has to be matched to a context with very strong demands on safety and security. In concrete, we have to investigate within the project the following concepts:

- Geographical storage locations of all data have to be known and have to be restricted based on SLAs.

[4] Funded by BMBF under grant ID 16KIS0062
[5] http://www.vdivde-it.de/KIS/sichere-ikt/sicheres-cloud-computing/sfc
[6] This holds only for the security level of the algorithm, not for the data the algorithm runs on.

- All data is stored encrypted, so even in case of an SLA violation the data are protected.
- Data is never overwritten or deleted, updates are performed by providing an additional version of a file.
- Analysis processes are realised as services which allow that different companies can use the same software [PC09].
- Multiple execution zones have to be supported, e.g. local computing centre, private clouds, public clouds and hybrid clouds.
- The integrity of the data can be validated based on cryptographic methods.

2 Preconditions and Actual Situation

During the arrangement and the beginning of the SFC project we worked out the conditions for a later realisation phase. One of the terms we have to fulfil is a legal one. For a large part of the data, the geographical location of storage and processing is restricted [Re00, Hi06], e.g. to the country the data is accrued. This can be considered by cooperating with local cloud operators that ensure a concrete data location.

Another aspect is the required security level from the stakeholder of the data. Often the protection level can be ensured by SLAs [BA11]. In some cases, especially for financial data it is also common to demand that an external resource provider is not able to read the data. In this case a cryptographically secure solution has to be established.

For the project, so-called Hardware Security Modules (HSMs) can be used. These are trust anchors that can store cryptographic keys and perform encryption and decryption. Based on the hard- and software based security arrangement, these operations can be considered as secure because in case of an attempt to breach the modules, their data are destroyed. The modules provide security even when not physically controlled by the stakeholders. So they can be offered as a special service by a cloud provider which needs a secured initialization process. In a preceding work, members of the project group have already covered the security aspects of the client-side, i.e. security of ATMs, making use of Trusted Platform Modules (TPMs) that served as trust anchors [PS14].

Moreover, we make use of a relatively new cryptographic approach called attribute-based encryption (ABE). Such ABE schemes allow for a fine-grained access control. Data are encrypted under certain access structures and only users/processes that possess private keys with the corresponding attributes that fulfil the access structure of the ciphertext allow for a decryption. The private keys can only be issued by a central key server.

3 Envisioned Target Architecture

As a starting point, a general architecture which mainly focuses on the functional view was developed. This architecture can receive input data that are financial transactions, e.g. from ATMs or inter-bank communication. The output data are e.g. account balances or the result of automatic analysis processes, which is often determined knowledge about the bank customer's behaviour or knowledge-based decisions. To realise the in- and output mechanisms, a communication layer is intended (see Fig.1).

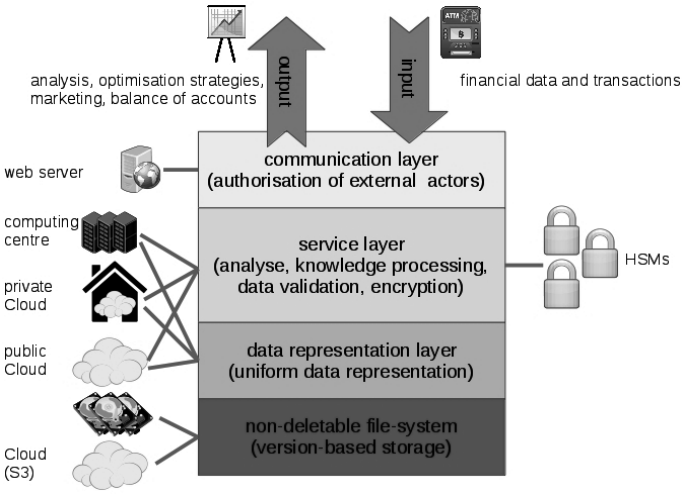

Fig. 1: Layer-based view of the SFC Concept

An additional layer is the service layer. This layer realises information and knowledge generation and processing, which are the demanded services from the stakeholders. Another important task is the validation of the input data, e.g. checking source signatures or transaction order, which is also realised as a service. Based on the fact that this layer has to do the data processing, this layer needs to be able to decrypt the data. This is realised by using the HSMs. The main reason for making use of HSMs in our scenario is due to a separation between the cloud provider, i.e. the provider performing the computations on the data, and the data owner, i.e. the bank that outsourced the processing of its data to the cloud provider. The HSM is in full control of the bank, i.e. the cloud provider is not able to retrieve the bank's private keys that are stored on the HSM. Based on the fact that the other layers do not realise data processing, it is not needed to decrypt data in any other layer. Thus, this is the only layer which needs access to the HSMs. We will establish a multi-agent-based system to realise flexible and efficient data processing combined with a blackboard design pattern for communication and data access. From a research perspective, there are two challenging tasks that we currently deal with at the service layer. First, we need to find a way to virtualize HSMs.

The hardware HSMs constitute the trust anchors of those virtualized HSMs. Therefore, we need to find a way to provide as strong security guarantees for virtualized HSMs as they hold for hardware HSMs. The second challenge is to find out to which extent we can implement our developed attribute-based encryption scheme on state-of-the-art HSMs.

The data representation layer offers a uniform and up-to-date view to the data. Based on the current state of the project, it is planned to represent the data as a POSIX-based file system. This allows a very simple and general interface to realise and adapt services to the infrastructure of SFC. Another aspect is the sufficient performance and scalability of modern distributed file systems known from cloud and High Performance Computing (HPC) context. This even allows a communication of services on different locations via the uniform file-system view. The data representation layer also guarantees that data is not deleted or overwritten. To realise this property, an additional layer is used. This additional layer is a non-deletable data storage which holds all versions of a value. The data representation layer provides a view to this data storage which only holds the last version of the data. As already described, the data storage and representation layer only work on encrypted data and do not need to access HSMs. Data validation is not part of this layer. A high level validation based on cryptographic integrity tests is provided as a service which probably needs access to HSMs and low level data safety is provided by the file system layer described next.

To realise the non-deletable file-system, open source tools like Ceph[7] will be evaluated. These tools also have to offer an additional property which is demanded by the SFC system. For realising a safe storage of the data, it is needed to realise a replication-based physical storage strategy. Therefore, it is needed to distinct between different geographical locations to avoid that copies of data are written to the same physical location. This concept of replication and distinction of geo-locations is e.g. supported by Ceph. This avoids to reimplement a distributed storage strategy as part of the SFC-project.

In the layers of the SFC Infrastructure, different execution environments will be supported. An example is the service execution. Therefore, it is needed do distinct between the service description, which holds all the information to run the service, and the execution system. The service description can be a virtual machine image or a container image. Such an image can be started on a server or a container execution system (e.g. Docker[8]) to operate an instance of the service. So the same service can be executed in different environments, e.g. local computing centres or the public cloud. In this way it is even possible to have the same service with different security contexts, depending on the execution environment. Another example is the data storage where different storage systems like e.g. cloud storage, servers with disks, and nodes with network attached storage can be used to form a uniform file system.

[7] http://ceph.com/
[8] http://www.docker.com/

4 Conclusion and Future Work

To provide a relevant contribution to the field of secure cloud architectures, in future work, we will show that even financial data can be processed. Thus, we develop a cloud-based infrastructure taking into account security constraints in particular. As part of future work, we will investigate how attribute-based encryption can be combined with high security modules in an efficient way, i.e. we will need to analyse which tasks need to be performed on the HSMs and which tasks can be executed on the "ordinary" machines. Moreover, we also need to come up with a holistic security approach that includes organizational security aspects additionally to technical measures. Based on the security concept we also develop a prototype which will be able to process and store data in a scalable, elastic and efficient manner. So we can prove to benefit by using cloud environments even under hard security and safety constraints.

References

[Ba11] Badger, Lee; Bohn, Robert; Chu, Shilong; Hogan, Mike; Liu, Fang; Kaufmann, Viktor; Mao, Jian; Messina, John; Mills, Kevin; Sokol, Annie; Tong, Jin; Whiteside, Fred; Leaf, Dawn: NIST Special Publication 500-293, US Government Cloud Computing Technology Roadmap, Release 1.0 (Draft), Volume II Useful Information for Cloud Adopters, November 2011.

[Be11] Bernsmed, K.; Jaatun, M.G.; Meland, P.H.; Undheim, A.: Security SLAs for Federated Cloud Services. In: Availability, Reliability and Security (ARES), 2011 Sixth International Conference on. pp. 202 –209, aug. 2011.

[BRC10] Buyya, Rajkumar; Ranjan, Rajiv; Calheiros, Rodrigo: InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services. In (Hsu, Ching-Hsien; Yang, Laurence; Park, Jong; Yeo, Sang-Soo, eds): Algorithms and Architectures for Parallel Processing, volume 6081 of Lecture Notes in Computer Science, pp. 13–31. Springer Berlin / Heidelberg, 2010.

[Hi06] Hildebrandt, Mireille: Profiling: From data to knowledge. Datenschutz und Datensicherheit - DuD, 30:548–552, 2006. 10.1007/s11623-006-0140-3.

[PC09] Parameswaran, A. V.; Chaddha, A.: Cloud Interoperability and Standardization. In: SETLabs Briefings, Vol. 7, 2009.

[PS14] Petrlic, Ronald; Sorge, Christoph: Establishing user trust in Automated Teller Machine Integrity. IET Information Security, 8(2):132–139, 2014.

[Re00] Rehm, Gebhard Marc: Just Judicial Activism? Privacy and Informational Self-Determination in U.S. and German Constitutional Law, January2000. Available at SSRN: http://ssrn.com/abstract=216348 or http://dx.doi.org/10.2139/ssrn.216348.

[Ro11] Rochwerger, B.; Breitgand, D.; Epstein, A.; Hadas, D.; Loy, I.; Nagin, K.; Tordsson, J.; Ragusa,C.;Villari, M.;Clayman,S.;Levy,E.;Maraschini,A.; Massonet,P.;Muõandoz, H.; Tofetti, G.: Reservoir - When One Cloud Is Not Enough. Computer, 44(3):44 –51, march 2011.

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 Adhoc-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 inforrmatische 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
I²CS 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^2CS) – 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^2CS)

P-187 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
4. DFN-Forum Kommunikations-technologien, 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 Kommunikations-technologien
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 Kommunikations-technologien 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-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

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