Secure Cloud Computing with SkIDentity: A Cloud-Teamroom for the Automotive Industry

Michael Kubach and Eray Özmü, Fraunhofer IAO
Nobelstr. 12, 70569 Stuttgart
firstname.lastname@iao.fraunhofer.de

Guntram Flach, Fraunhofer IGD
Joachim-Jungius-Str. 11, 18059 Rostock
guntram.flach@igd-r.fraunhofer.de

Abstract: A major security-challenge in the automotive industry is to enable the secure and flexible engineering cooperation with changing partners in complex development projects. Therefore an effective interorganizational identity management is needed to control access to cooperative development platforms. This identity management has to be based on reliable identification of engineers of various partners with different credentials. The SkIDentity-Project, that aims to build trusted identities for the cloud, addresses this scenario. By integrating the existing components, services and trust infrastructures into a comprehensive, legally valid and economically viable identity infrastructure the technology enables to provide trusted identities for the cloud and secure complete business processes and value chains. One pilot-application of the project is the "Cloud-Teamroom for the Automotive Industry". It is adjusted to the specific requirements of the value chains in the automotive industry. Thanks to the SkIDentity-Technology, and via the so-called eID-Broker, engineers from different partners can access the cloud-teamroom. For the required strong authentication they can use the credentials that are already available in their company. This paper presents the SkIDentity-technology and exemplifies it by means of the pilot application.

1 Introduction

Trustworthy cloud computing requires secure and reliable mechanisms for authentication. At the same time user interfaces and authentication processes have to be designed as user-friendly as possible to achieve a high user acceptance [1]. Only systems that are accepted by users and that are actually used can make the authentication to cloud computing systems sustainably safer. This highlights that security is not merely a technological challenge. Therefore the goal is a solution that combines good usability with high technical security.

The SkIDentity project[1] accordingly strives to create an architecture that is designed from the basis to flexibly work together with solutions from multiple vendors [2].

[1] SkIDentity is among the winners of the "Trusted Cloud" technology competition (www.trusted-cloud.de) of the Federal Ministry of Economics and Energy (BMWi) and aims at providing trusted electronic identities for cloud computing services. It brings together an interdisciplinary team of experts led by the ecsec GmbH with the participation of the ENX Association, the Fraunhofer Institutes IAO and IGD, the Open SignCubes GmbH, Ruhr University Bochum, the University of Passau, the Urospace GmbH and VDG Versicherungs-

Through a federated identity management (FidM), organizations will be able to offer one or multiple authentication services or make use of external identity information and authentication for applications operated by them; a multitude of combinations being possible. Both the technical and organizational aspects, as well as the legal requirements are taken into account by the project. As a result, the user should be able to use their preferred "identity card" (credential) for strong authentication in various applications. This reduces the number of authentication information to remember or credentials to manage by the individual user. Moreover, it saves her from having to become acquainted with new authentication procedures with every new service she uses. At the same time this simplification increases security because the authentication steps and sequences are always familiar, comprehensible, understandable, and recognizable for the user.

However, the user is not the only stakeholder that has to be considered for an identity management system. As Roßnagel and Zibuschka have argued, all relevant stakeholders for an identity management system have to be taken into account [3]. This means that we have to look at the service providers' requirements as well. They have to implement and operate the system, which means that they have to make significant investments in terms of money and other resources [4]. Therefore, they will only be willing to implement a specific identity management system if these investments are likely to pay off. So there needs to be a business case for the service providers to implement the identity management system. For example this could be (a) the possibility to raise the number of potential customers or users of the provided service or (b) to reduce the costs induced by the authentication process. The SkIDentity-Technology enables both: (a) As users can perform a strong authentication with the service using the credentials they already possess, the number of potential users and customers is raised. And (b) the handling of credentials is facilitated as there is no need for the service to give out its own credentials. Already available credentials such as national electronic ID-Cards (eIDs) or other identity tokens such as OTP-Generators or even mobile phones can be easily integrated. Therefore cost savings can be achieved.

The third relevant stakeholder for an identity management system is the identity provider. It can be assumed that the goal of the identity provider is to gain a large base of users and service providers that rely on its identity provision services. The business model of the identity provider could be that both or one of these groups of users pay for the identity provider's service. Thus, a higher number of users and service providers should raise the revenue of the identity provider. At the same time, as we have already described above, a higher number of users is in the interest of the service provider as well. Moreover, a higher number of potential services that can be used with a specific credential already in the hands of a user is in the interest of the user. From an economic science perspective this illustrates that network effects apply to identity management systems so that in this case we are faced with a multi-sided market [3], [5], [6].

---

wirtschaftlicher Datendienst GmbH. Additionally, the SkIDentity-project is supported by relevant organizations such as the Federal Association for Information Technology, Telecommunications and New Media (BITKOM), EuroCloud Deutschland_eco e.V., ProSTEP iViP e.V. and TeleTrusT – IT Security Association Germany e.V. and renowned companies such as DATEV eG, easy Login GmbH, media transfer AG, SAP AG und SiXFORM GmbH.

The article shows how the SkIDentity-Technology achieves what is described above and exemplifies this by means of the pilot application. Thus, it is organized as follows. Section 2 outlines the scenario in the automotive industry in greater detail. In section 3 we describe the system architecture of the SkIDentity-Technology. Subsequently, in section 4, we present the pilot application "Cloud Teamroom" as realized in the project, before we conclude our findings in section 5.

2 Pilot-Application Scenario: Automotive Industry

The automotive industry can be characterized as highly competitive and globalized. A relatively small number of car makers (original equipment manufacturers – OEMs) are spread over the world. Most of them target markets around the world and therefore compete against each other on a global scale. This industry has always been driven by new technologies and technological advances are often quickly adopted into new products. Within the last one or two decades, this led to a tighter integration and interconnection of simple parts into more complex systems. The OEMs have reacted to these new challenges by outsourcing the production and even the development of those systems. Thus, the tasks of the suppliers have grown from manufacturing simple parts to manufacturing complex systems. As these systems require a highly specialized knowledge, they are often not only made, but also designed by the supplier according to the OEM's specification [7], [8].

The development described above has led to the current situation in which a significant amount of the value is not generated by the OEM itself, but by the extended workbench consisting of its suppliers. Yet, these suppliers (Tier1-suppliers) usually have an extended workbench with suppliers (Tier2-suppliers) as well. Here, we can see the distributed value chain of the automotive industry [8].

The intense competition in the automotive industry makes a continuous reduction of the time-to-market of new products imperative. This is achieved inter alia through an interactive collaboration between the engineers at OEMs and suppliers in multi-user applications [9]. However, due to the complex network-like structure of competition in the automotive industry, OEMs, Tier-1 and Tier2-suppliers at the same time cooperate for different components each with numerous competing partners. For this reason, an effective access control for sharing and collaboratively editing of technical specifications and component design is absolutely necessary to protect the intellectual capital of each partner.

The effective interorganizational access control that is required already constitutes a major challenge for the identity management (IdM) inside of a single organization. However, if several independent companies (OEMs, Tier1-, Tier2-suppliers and, where appropriate Service/Cloud providers) are involved, the complexity of the task of a trusted authentication of all engineers involved increases significantly. For example, different companies use their own authentication methods and security policies that must be implemented by service/cloud providers. In addition, dependent on the specific demand, engineers are assigned to or withdrawn from projects by their mother company.

Therefore, access rights and permissions permanently have to be kept up-to-date (Enrolement/De-Provision/De-Enrolement). The economic and technical capabilities, particularly of smaller organizations without major IT departments thus quickly reach their limits, due to the variety of requirements that need to be fulfilled. Moreover, the complexity of the task can provoke errors, leading to security problems and, in the end, costly loss of intellectual capital or the termination of working relationships.

In a scenario as depicted, a SkIDentity-based solution could address the identity management-specific challenges. But before this solution is presented, we'll outline the system architecture of the SkIDentiy-Technology in the following section.

3 SkIDentity System-Architecture in Brief

SkIDentity builds upon the concept of Federated Identity Management (FIdM) [10]. The architecture enables the use of various authentication methods, services and protocols in a consistent and secure way in any application. Particularly, the SkIDentity-technology renders it possible to use government-issued electronic Identity Cards (eIDs) for a great variety of services. These eIDs or similar documents, such the German "neuer Personalausweis" (nPA), are increasingly available in the general population all over Europe, as they are being issued by more and more states [11]. Thanks to the official trust anchor, due to being issued by the public authorities, these credentials are perceived as very save and over time they will be widespread. The design of the SkIDentity system-architecture therefore pays particular attention to compliance with the requirements of the German eID-law.

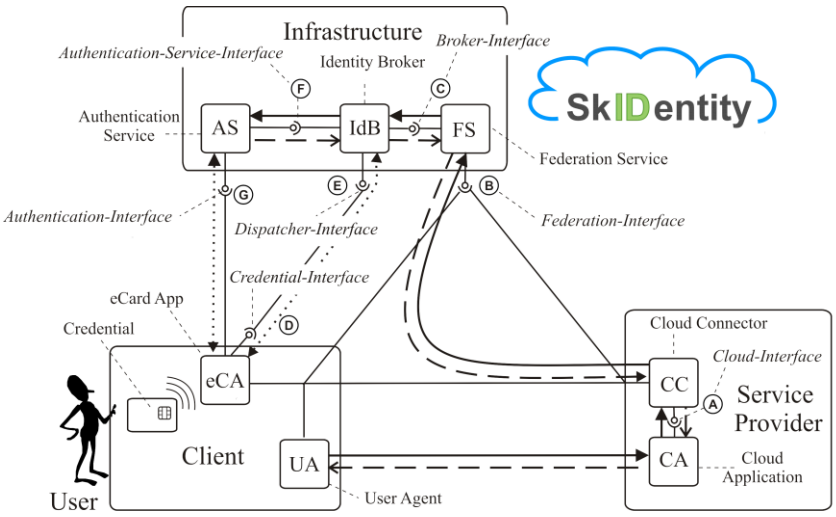

Figure 1: SkIDentity reference-architecture

The SkIDentity reference-architecture for strong and trustable authentication in the cloud can be broken down into three major components. As shown in Figure 1, these are located at the user/client, the service provider and infrastructure components.

Identity Broker (IdB)

The IdB is the central component in the SkIDentity-infrastructure. When an authentication request is sent by the CC or FS, he determines which credentials are available from the user, so that an appropriate service for the user authentication can be selected.

Federation Service (FS)

The FS is an optional service that supports protocols for identity federation such as [12], [13], or [14]. If the authentication policy supports it, a single-sign-on becomes possible. In this way a user only needs to authenticate once to use a multitude of applications (for a certain time).

Cloud Connector (CC)

Via the CC, the Cloud Application (CA) is integrated into the SkIDentity-infrastructure. The CA represents the cloud application that the user actually wants to access. The CC is operated at the CA. It enables the CA to use Identities and Authentication with a protocol that is supported by an IdB or a FS. CAs that already support such functionality have already implemented a CC. But the CC can also be integrated directly into a CA afterwards by using a program library if the functionality hasn't been implemented right from the start. Alternatively, it can work as an independent process that receives the data from an IdB or FS to transmit it in a compatible format to the CA.

Authentication Services (AS)

To perform the actual user authentication the IdB calls the AS. Dependent on the credential, a suitable authentication protocol is used for this communication. As an example: to authenticate with the nPA the Extended Access Control (EAC) protocol according to [15] is used.

The following chapter will show how the now outlined SkIDentity system-architecture can be used to build an application that addresses the challenges of the automotive scenario described in earlier in the paper.

4 Pilot-Application: Cloud-Teamroom for the Automotive Industry

The pilot-application that has been developed in the SkIDentity project is a cloud-teamroom for the automotive industry. It provides a cloud-based collaborative workspace that can be accessed by different users with specific, variable permissions. By utilizing the Identity Broker for the authentication, credentials that are already available in the organizations can be used. It is not necessary to give out (and after termination of

the project collect) special credentials to engineers of partner organizations that are supposed to work on the platform. The cloud-teamroom was integrated into the architecture of SkIDentity and developed in a way so that it can serve as an experimental system for further research and development work in the sense of agile software development [16] as well as public presentations.

The overall concept of the cloud-teamroom is pictured in Figure 2. One or more companies in a manufacturer-supplier network in the automotive industry opt for the use of the SkIDentity-infrastructure for the secure authentication at a shared cloud-service. The cloud-teamroom of the realized pilot-application is an example for this application scenario.[2] The cloud-application is based on the Open Source software system ownCloud for cloud storage and data synchronization [17].

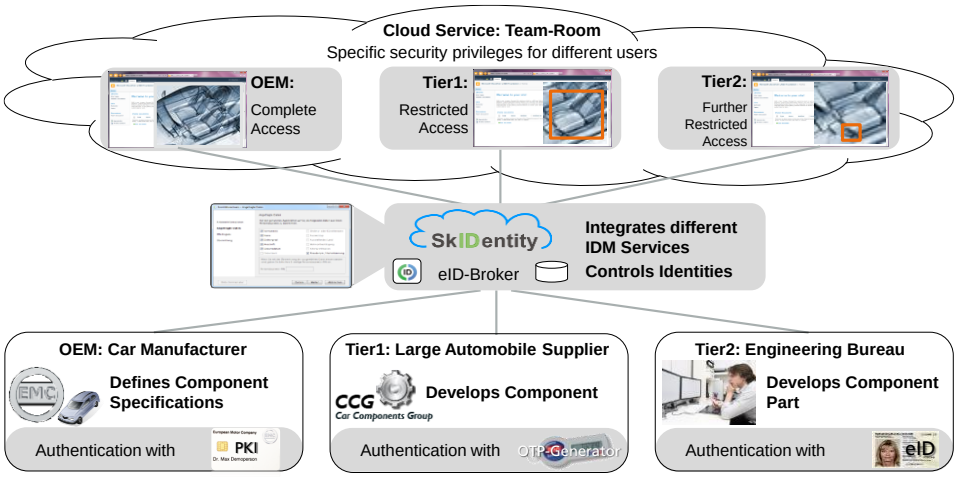

Figure 2: Concept of the Cloud-Teamroom for the Automotive Industry

The authentication through SkIDentity to log on to the service can be done by clicking on the SkIDentity-Button embedded into the login-screen of the cloud-service. The SkIDentity Identity Selector pops up to show the user which credentials are available for authentication at the cloud service (see Figure 3). After the user has selected his available/preferred credential he gets redirected to the IdP to perform the authentication process there. If the authentication is successful, the user is granted access and he gets logged on to the service to use it as intended. Specific read/write-permissions for individual engineers are handled in the cloud service (here: the ownCloud solution), not through the SkIDentity-Technology.

The Open Source platform ownCloud which is originally designed for data storage in the cloud was customized to fit the needs of users in an automotive scenario. Depending on the role a user holds, the design and the functions presented in the cloud-teamroom vary.

[2] The pilot application can be accessed via: https://www.skidentity.de/de/demo/ .

By using the SkIDentity-infrastructure each user obtains a unique ID which is used inside ownCloud as the specific user id. This user ID corresponds to an ownCloud user which then can be authorized inside the ownCloud user management settings. By assigning the user to a user group the administrator can easily manage their access rights and available functions inside the cloud-teamroom.

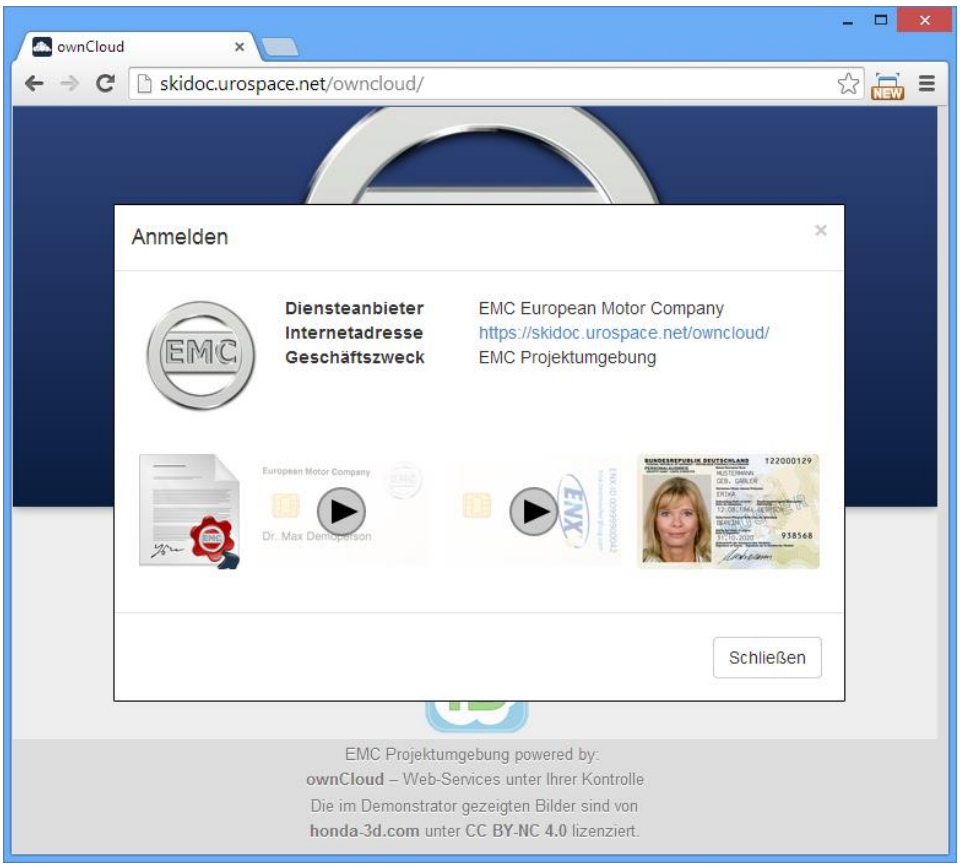

Figure 3: Login to the Cloud-Teamroom with the Identity Selector by SkIDentity

In a fictitious case study for the pilot-application three companies from the automotive cooperate in a development project. The cloud-teamroom is operated by the fictitious car maker EMC – European Motor Company. It is a big global player in the automotive industry with a highly capable IT-department and considerable resources. In the development project it cooperates with CCG - Car Components Group and Ingenieurbüro Schneider on a new car component. CCG is a Tier1-Supplier of medium size. Ingenieurbüro Schneider is a small independent engineering bureau that is very specialized on a specific part of the component (Tier2-Supplier). In the pilot case four possible credentials are available:

1. A software certificate, stored on the desktop PCs of EMC. This OEM operates the cloud-teamroom in this case study and his desktop PCs are operated in a safe environment and protected by physical as well as software (PKI-based) access control. Therefore a software certificate is highly convenient while at the same time being very secure.
2. EMC-Company Smartcard, based on a PKI-Infrastructure. This Smartcard allows engineers of EMC to access the cloud-teamroom from any computer with a suitable card-reader that fulfils the company's security policy.
3. CCG-Smartcard, provided to the company by the ENX-association. ENX is a respected organization in the automotive industry that already provides a secure communications network to the industry [18]. Moreover, as it is founded and supervised by most major OEMs and suppliers it serves as a trust anchor for the electronic Identities assigned with the Smartcard. Thus, ENX serves as an IdP for CCG. Engineers of CCG can use this Smartcard to use internal services as well as to access the cloud-teamroom.
4. German national ID-Card: neuer Personalausweis (nPA). As Ingenieurbüro Schneider is a Company with only a hand full of employees it doesn't have an IT-department, not to mention a PKI-Infrastructure. However, the engineers possess an nPA which they can use for strong authentication at the cloud-teamroom.

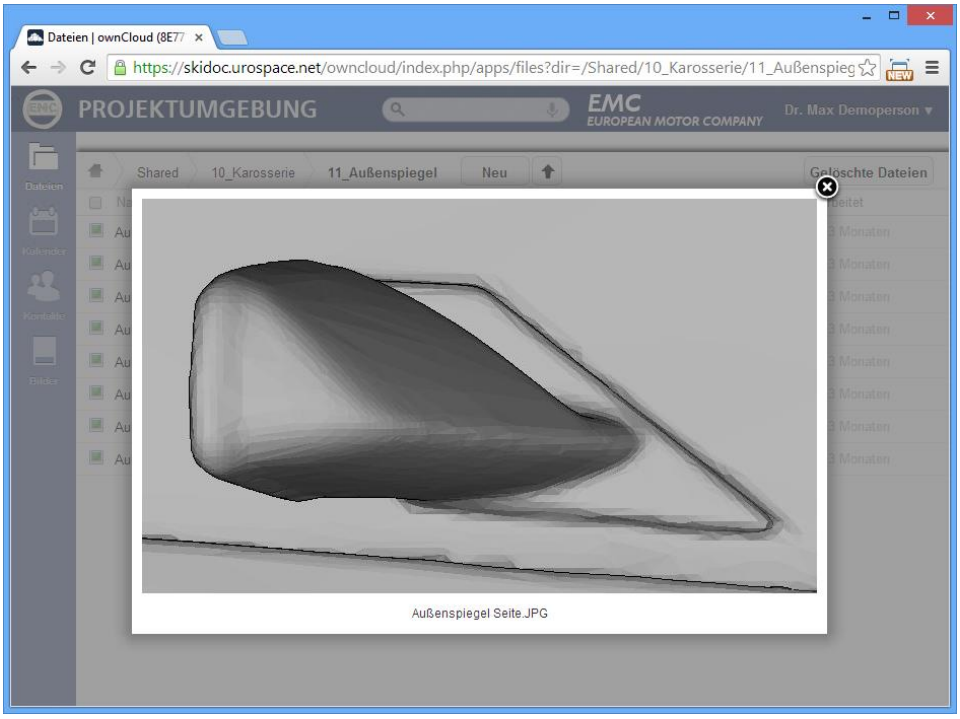

Figure 4: Exemplary functionality of the Cloud-Teamroom: view of 3D-Model-Data

This shows how strong authentication in the complex value chain of the automotive industry can be achieved by making use of the SkIDentity-technology and with limited resources. Each partner just uses the credential that is most convenient for him. At the same time a high level of security and trust is achieved.

4 Conclusion

With the example of a cloud-teamroom for the automotive industry, this paper has shown how an effective interorganizational identity management can be realized with the SkIDentity-technology. The approach enables reliable identification of engineers of various partners with different credentials while being easy to implement into existing structures and processes.

In addition to the evaluation of the approach used in the current pilot-application, future work will be especially concerned with the further analysis of the results of a qualitative market study on Federated Identity Management in the automotive industry. First results of this analysis have already been integrated into the design of the pilot-application. The combined results will be used to revise the SkIDentity reference-architecture as a whole. Moreover, they will be used to iteratively refine the pilot-application and to conceptualize business models for SkIDentity in the successive project phases.

References

[1] C. Senk, "Future of Cloud-Based Services for Multi-factor Authentication: Results of a Delphi Study," in *Cloud Computing*, vol. 112, M. Yousif and L. Schubert, Eds. Springer International Publishing, 2013, pp. 134–144.

[2] SkIDentity, "Skidentity-Project Website," *Skidentity-Project Website*, 2014. [Online]. Available: http://www.skidentity.de/.

[3] J. Zibuschka and H. Roßnagel, "Stakeholder Economics of Identity Management Infrastructures for the Web," in *Proceedings of the 17th Nordic Workshop on Secure IT Systems (NordSec 2012)*, Karlskrone, Sweden, 2012.

[4] M. Kubach, H. Roßnagel, and R. Sellung, "Service providers' requirements for eID solutions: Empirical evidence from the leisure sector," in *Open Identity Summit 2013 - Lecture Notes in Informatics (LNI) - Proceedings*, D. Hühnlein and H. Roßnagel, Eds. Bonn, 2013, pp. 69–81.

[5] A. Hagiu, "Two-sided platforms: Pricing and social efficiency," 2004.

[6] D. S. Evans, "The Antitrust Economics of Two-sided Markets," *Yale J. Regul.*, vol. 20, no. 2, pp. 235–294, 2003.

[7] I. Wehrenberg, H. Roßnagel, and J. Zibuschka, "Secure Identities for Engineering Collaboration in the Automotive Industry," presented at the MIGW 2012 - Conference on Mobility in a Globalised World, Bamberg, 2012, pp. 1–12.

[8] G. Volpato, "The OEM-FTS relationship in automotive industry," *Int. J. Automot. Technol. Ldots*, vol. 4, no. 2/3, pp. 166–197, 2004.

[9] G. Volpato and A. Stocchetti, “The role of ICT in the strategic integration of the automotive supply-chain,” *Int. J. Automot. Technol. Manag.*, vol. 2, no. 3/4, p. 239, 2002.
[10] D. Hühnlein, H. Roßnagel, and J. Zibuschka, “Diffusion of Federated Identity Management,” in *Sicherheit 2010*, F. C. Freiling, Ed. Bonn: Köllen Druck + Verlag GmbH, 2010, pp. 25–36.
[11] FutureID Project, “Survey and Analysis of Existing eID and Credential Systems, Deliverable D32.1,” 2013.
[12] D. Hardt, Ed., “The OAuth 2.0 Authorization Framework, IETF RFC 6749.” 2012.
[13] OpenID Foundation, “OpenID Authentication 2.0.” 2007.
[14] S. Cantor, J. Kemp, R. Philpott, and E. Maler, *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0*. 2005.
[15] Federal Office for Information Security (BSI), “Advanced Security Mechanism for Machine Readable Travel Documents - Extended Access Control (EAC), Password Authentication Connection Establishment (PACE), and Restricted Identification (RI),” Technical Directive (BSI-TR-03110) Version 2.10, 2012.
[16] F. Paetsch, A. Eberlein, and F. Maurer, “Requirements engineering and agile software development,” in *2012 IEEE 21st International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 2003, pp. 308–308.
[17] ownCloud, “ownCloud, Your Cloud, Your Data, Your Way!,” 2014. [Online]. Available: www.http://owncloud.org/.
[18] ENX Association, “ENX Association,” *ENX - The communications network of the European automotive industry*, 2014. [Online]. Available: http://www.enxo.com/.