ENX ID – An Architecture for Practical and Secure Cross Company Authentication

Michael Kubach & Heiko Roßnagel, Fraunhofer IAO
Lennart Oly & Immo Wehrenberg, ENX Association

michael.kubach@iao.fraunhofer.de
heiko.rossnagel@iao.fraunhofer.de
lennart.oly@enx.com
immo.wehrenberg@enx.com

Abstract: This paper introduces a development approach and a novel architecture for cross company identity management and authentication. It aims to design an architecture, which is practically implementable in the highly collaborative environment that exists in the automotive industry. The paper sketches the conducted marked research to obtain such a model and presents an architecture design based on a trusted intermediary.

1 Introduction

The automotive industry was among the first industries that had a high need on authentication, as it was among the first to rely on internetworked information technology to optimize its supply chain even across company borders [KWB03].

Today, use of internetworked IT is no longer limited to supply chains. It has been extended to many applications starting with the exchange of research and development data, reaching to real-time collaboration using telepresence and live collaboration systems like multi-user CAD systems, and even administration of production systems – the so called "shop-floor IT" [SRW05a]

A detailed description of the dense mesh of collaborating companies that exists in the European and worldwide automotive industry today is given in [WRZ12]. This mesh of interconnections is especially relevant to the development of new systems and whole cars. Nowadays, about 300 companies are involved in the development of a new car and more than 80 percent [IK07] of the value in a typical new car project is created by suppliers.

Generally, IT systems are secured by two major measures:

Perimeter-based security is the outermost security measure possible. It prevents even basic access to systems by limiting the access possibilities to a network. The most common method is to restrict critical systems to a non-public network – often enforced by firewalls. In the collaboration with many partners, these internal networks are no longer company-internal but instead cross-company as well [MR08].

Authentication to the system in question is the second measure. The most common authentication method again is username and password-based authentication [MO07].

In the automotive industry, as in all other industries, perimeter security is enforced by firewalls. Moreover, the automotive industry has an additional method of perimeter security that is called the *ENX Network*.

The ENX Network is a secure, interoperable and at the same time cross-company and multi-provider network. ENX Network access is restricted to user companies within the industry. Communication within the network is protected by cryptographic measures. Every user company connected to the network is authenticated cryptographically by a public key infrastructure. The network and its central services are controlled by an industry-steered independent association: the ENX Association [Ri11].

ENX Association is neither controlled by one particular company of the industry, nor controlled by a profit-oriented provider but instead by its members consisting of large automotive companies and associations. This made it possible in a unique way to create a global, widely accepted industry standard that reduces complexity significantly.

The ENX Network is an important building block of the increasingly interconnected structure in the automotive IT. However, even such a very strong perimeter protection is no longer sufficient to cope with all the different threats faced by the industry. Therefore, authentication as the second line of defense becomes more and more important. The significance of password-based authentication that came with its broad adoption as the standard IT authentication method has also revealed its many weaknesses [IWS04], [Pe94], [RR06].

Authentication is a vital part of identity management (IDM) as it ensures that the identity (ID) and its associated capabilities can only be used by the legit entity [Sc06]. If authentication fails, an ID may be stolen and used maliciously. A stolen ID enables all kinds of attacks on computer systems that cannot only create damage in computer systems, but has significant economic impact as well [ADS08]. It can even become a matter of life and death if one thinks of manipulated production robots within the shop-floor IT or gas-based fire extinction systems.

Therefore, it is evident that stronger methods of authentication are necessary [CF07]. From the user experience perspective, it is desirable to limit the number of authentication methods and credentials per user [DD08]. However, authentication methods and credentials are often difficult to implement across company borders or even industry-wide.

This paper presents an economically, legally and technically viable architecture to enable industry-wide authentication based on secure multi-factor authentication. The paper is structured as follows. In section 2 we describe the conducted research to identify the industrial requirements of the ENX ID cross company IDM architecture described in section 3. We conclude the paper in section 4 by summarizing the major results and discussing the limitations of our work.

2 Expert Interviews

2.1 Methodology

We chose the method of a qualitative analysis based on semi-structured interviews. The respondents were IT specialists with expertise in identity management (IDM) working for car manufacturers and suppliers in the automotive industry. The goal of the qualitative analysis was to reconstruct how these respondents see the challenges and chances of a viable IDM. Because the theoretical foundation of this topic is so far relatively underdeveloped, this approach does not aim to test concrete pre-formulated theories or hypotheses. Instead, the creation of a deeper understanding for the research subject was considered appropriate. For these reason, semi-structured interviews are the tool of choice for this research project. Interviews of this form constitute an established research-tool for such tasks [MN07].

The guide for the semi-structured expert interviews included targeted and open-ended questions and left room for further inquiries. It was derived from the theoretical analysis from the work in [Ro14], [WRZ12], and [RZ12].The interviews were conducted in the period from mid-2012 to mid-2013. Each interview took approx. 120 minutes. In three cases, the respondents agreed to an audio recording of the interview, which was fully transcribed. Audio recordings of other interviews were not possible due to company regulations, so the three interviewers each took handwritten notes, which were later combined.

Three interviews were conducted with three European automobile manufacturers and two European automotive suppliers. Geographically the focus of the study was located in and around Germany. Together with their Asian and American competitors, European automotive companies certainly are the leaders of the industry. Our respondents represent major and influential companies and are therefore well suited for our approach.

Most of the interviewees held senior positions in middle management with relations to IT security. In one case, we directly spoke with the Chief Information Officer (CIO). It can be assumed that the respondents have the necessary competence in terms of both function and of their position. Thus, we are following a key informant approach [Ho12].

The evaluation of the resulting transcripts from the interviews was carried out using MAXqda in version 11, a software for qualitative data analysis. We followed a thematic coding process, as there was no predefined coding scheme due to the underdeveloped theoretically foundation of the research. Without a set of established theories, no coding scheme could be derived ex-ante.

2.2 Results

Four main clusters where identified while looking at the results of the expert interviews: State-of-the-art, the drivers, the hurdles and the challenges for federated IDM.

State-of-the-art: The protection of intellectual property is a top priority for the companies in the automotive industry and has been gaining importance in the last years. Corporate IDM systems are state-of-the-art in our sample. Moreover, a clear trend towards strong and multi-factor authentication is evident. A respondent stated: *"Especially the security issue is on the rise. There is a trend away from passwords towards strong authentication. However, it always depends on the area of application."*

The close connection of the value-chain was made clear as well. Engineering departments of suppliers directly work in the development environments of the manufacturers. Smaller engineering bureaus access development data of larger suppliers via web-access. For strong authentication often own company smart cards or one-time-password-tokens are issued to partner companies. Traditional password-based authentication is used if handing out smart cards or tokens is not viable.

Drivers: The distributed value chain and the changing of partner causes a lot of work adjusting the IDM to different partners. In general, the transaction costs for enrolment/de-enrolment are significant. One respondent said that for smaller partners it is not always worth the effort. Strong authentication with PKI smart cards given out by one company is not always feasible. A security expert from an automobile manufacturer explained it like that: *"We have 2,500 supplier users. We cannot distribute 2,500 PKI smartcards to externals. This is logistically impossible as they are distributed all over the world."* Asked if ID federation allowing supplier company users to use their company tokens to authenticate and use services of the manufacturer would be seen as possible, the security specialist replied*: "I think so, but we care a lot about our security."*

These factors can be seen as drivers for a federated IDM. All companies in the sample have therefore started to think about ID federation. Some have completed or at least started pilot projects. A large association of the automotive industry is running a project on federated IDM. However, no company is using it in larger production processes yet.

Hurdles: Several hurdles for federated IDM were mentioned in the interviews. Security and control are major issues in this sensible area. Companies want to stay in control and are hesitant delegating to other partners that might be competing in some areas. As one respondent stated: *"We are blessed to work with foreign partners, but we are clearly obliged to define what is necessary to limit the access and the authenticity of the exchange."*

Other aspects that the respondents mentioned are more of legal or organizational nature. One respondent from an automotive supplier said that while technical challenges had been solved in a pilot project it went into hibernation in the hands of their lawyers. *„From a technical point of view everything worked in the end. Organizational and legal challenges were the problem."* Questions of liability in case of incidents like security breaches or downtimes are seen as difficult. The challenge of intra- and inter-organizational coordination between the divisions responsible for what and how the processes work in the case of such incidents are mentioned as additional hurdles.

Challenges: There are challenges related to the different systems and standards used by applications at different partners. These challenges were not seen as insurmountable. The

technical problems in pilot projects of companies in the sample were solved or seen as not too significant. Frameworks like SAML are seen as valuable here.

Privacy is seen as an issue, as it is not yet clear which personal information can be shared with other organizations. First ideas how this could be solved by restricting the visibility of certain details of the information exist.

Organizational and control aspects are an issue when sensitive functions are to be delegated to customers or even competitors for the federation of identities. Interorganizational trust plays a major role here. Some of the respondents indicated that such a delegation could be possible with an independent intermediary serving as a trust anchor. A respondent from an automobile manufacturer stated*: "Definitely, I would prefer a model with an independent authority that is able to deliver identity or authentication. From my point of view, it's a longer process to go through alliance-partner Y and the process isn't preferred. Also, it's difficult to trust the competitor in this matter or a third party because it is trusted by our competitor."*

3 The ENX ID Architecture

3.1 Architecture Design Considerations

As confirmed in the interviews, companies already use corporate identity management (IDM) systems and do already support multiple secure multi-factor authentication methods. So far, all of these identities are limited to the particular companies itself. The solution to make these authentication methods available across multiple IT infrastructures is called federation. In the standard federation scenario, two companies would federate their IDM systems in order to make the identities from one domain available to the other and – if necessary – vice versa.

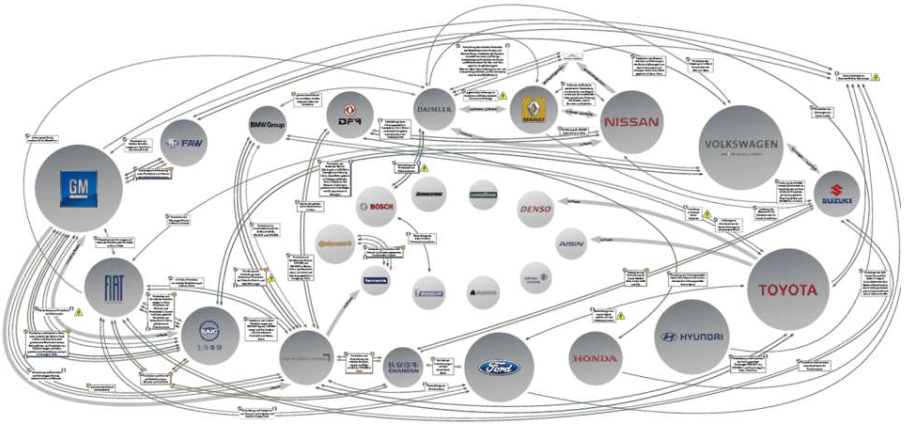

Figure 1: Who Cooperates With Whom - The Largest Automotive Manufacturers and the 10 Largest Suppliers [Vi12]

In the automotive scenario, this might be sufficient for individual cooperation between the manufacturers and large suppliers, but it is not practical to create an industry-wide direct federation. In that case, any company in the industry would have to federate with all its business partners. Figure 1 shows large development projects between the largest OEMs and the 10 largest suppliers. Even only focusing on those, the figure visualizes that this is already very complex. If one also considers simple contract work and includes the smaller and more specialized suppliers, it immediately becomes clear that such a setup would be far too complex to be practical.

Moreover, becoming relying party of a federated system requires trust in the assuring parties regarding the identities and authentication assurances received from the federated system. It was clearly stated in all interviews, that the establishment of this trust is seen as one of the biggest challenges for a broad federation. As shown in the interviews, this trust must be established in multiple areas:

Trust in the technical construct is the trust in the technical security and soundness of the architecture and all the systems involved. This trust can be established by creating clear and transparent criteria required to participate and an openly and transparent designed architecture. The compliance to these requirements must be auditable. As these audits especially at participating companies might reveal sensitive information, they must be conducted by an independent and trusted third party.

Trust in the legal construct can be established by creating a fitting, reliable, and transparent contractual construct. The contractual model must not require all companies to be direct contract partners but has to ensure a fair distribution of liability. Additionally, ID data is personal data and protected by law, so the architecture must respect data protection regulations. This becomes even more challenging as the automotive industry is actively engaged around the world and with that affected by several data protection laws.

Trust in the economical construct can be established by creating an architecture that supports a realistic business model and is backed by economically stable and conservative organizations.

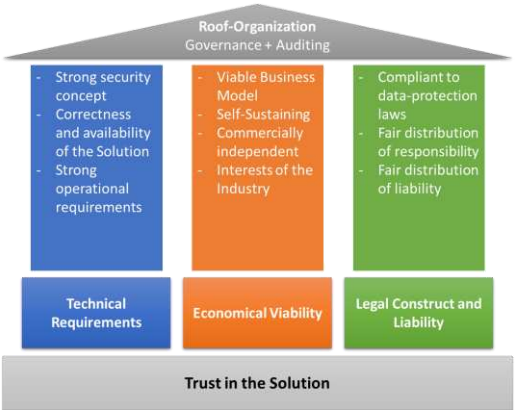

Figure 2: Three Pillars to Establish Trust

In all of these areas, the easiest way to establish trust is using a trust anchor. The trust anchor governs the whole construct, defines or assesses the technical criteria and conducts or coordinates the audits for the technical construct. Moreover, the trust anchor designs and is part of the contractual construct to distribute the liability reasonably. It also develops a business model, ensures that economic interests of all involved parties are addressed and with that, the economic viability of the architecture is ensured. The trust anchor must be accepted by all parties. As supported by the results of the interviews, the OEMs, representing different interests as they are in direct and strong competition, are unlikely to become a joint trust anchor for the architecture. Similarly, service providers having an interest to exploit the federated setup commercially are not well suited. A good trust anchor would be an established third party that represents the interest of the industry and does not represent the interest of a specific company.

ENX Association was founded by the industry for exactly this purpose within the ENX Network. The axiom of ENX Association is that cross-company services in a branch with the size and the level of cross-linking as given in the automotive industry have to be

- Sufficiently standardized and centralized in order to reduce complexity
- Offer the branch or industry a fair level of steering in order to govern the service and to the trust anchor
- Open enough in order to allow for competition among services offered

Therefore, ENX Association is proposed to take over a comparable role concerning the architecture described here.

3.2 Identity Intermediary for Federation of Existing Identity Management Systems

In order to reduce the complexity, the architecture does not aim to federate all companies with each other directly. Instead, companies federate with a central identity (ID) intermediary. This intermediary reduces complexity by requiring only one federation per partner instead of one for each partner at each partner. It can reduce complexity even further by solving two major challenges:

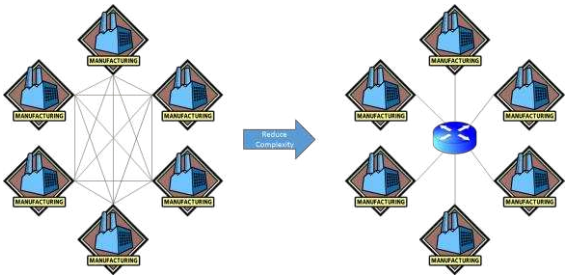

Figure 3: Complexity Reduction by Introduction of an Intermediary

To sanitize and normalize the input received by the parties that participate in the federation. As the federated parties have different systems and protocols are not always 100 percent compatible, the intermediary is able to sanitize the information received and forward it in a normalized way that is appropriate to the receiving party.

To translate different protocols. There are several ID federation protocols in different modes and versions available. The most important protocol nowadays is a specific mode of SAML 2.0. Examples for other protocols are OAuth, OpenID and WS-Federation. The intermediary allows participating parties to focus on one federation protocol and resolves the necessity of an industry-wide agreement on one. Figure 3**Fehler! Verweisquelle konnte nicht gefunden werden.** visualizes the complexity reduction by the intermediary.

3.3 One or More Independent Sources for Multi-Factor Authentication Methods

As explained before, the technical and procedural requirements for the federation are significant. This is completely acceptable for larger companies that have similar requirements on their internal IT. However, a important part of the automotive industry consists of small and medium-sized enterprises with very limited IT capabilities. For most of those, it would require a serious investment to fulfill the requirements.

This would consume the benefits of the participation in such a system. To overcome this challenge, the architecture proposed includes one or more identity providers (IDP) that supply identities to foreign users. This centralized IDP would issue secure ID tokens to its customers in a way compliant with the federation requirements. To ensure the highest security requirements, two-factor authentication is necessary. The interviews 3.1.2 have indicated that the industry sees ENX Association as an appropriate IDP. In the pilot implementation of the architecture, the IDs ("ENX-IDs") will therefore be issued indeed by ENX Association. In an advanced production environment, a model with several competing IDPs offering different kinds of authentication methods federated with the central component in a varying manner is appropriate.

On a technical level, ENX Association has chosen modern cryptographic smart card based authentication method for the pilot. As described before, cryptographic smart cards provide high security based on a PKI, in this case the existing ENX PKI that is already trusted by the ENX user companies, which are a significant part of the industry.

The processes and IT policies of medium-sized to large companies can make it very difficult to install security-relevant software on the client systems and almost impossible to integrate new hardware. Therefore, it was necessary to choose a solution that works with most hardware already available and requires minimal software support. Therefore, the chosen ENX-ID smart card can communicate using the contact-based interface as standardized in ISO/IEC 7816 as well as the contactless interface standardized in ISO 14443 and commonly referred to as NFC. The prototype card is running with the CardOS 5.1 operating system from ATOS due to its widely adoption and therefore minimizes the software requirements on the client systems.

The key feature of the ENX-ID is its ability to authenticate against the ENX-ID provider. The ENX-ID therefore hosts a secret RSA key suitable for authentication coming with a certificate issued by the ENX PKI. This certificate can also be used to authenticate to a Windows domain that is configured accordingly.

Smart cards are commonly used for other purposes that benefit from a secure key storage method. To add further value to the ENX-ID smart card, it can also be equipped with a key and a corresponding certificate of the ENX PKI for email signing. Finally, the user may store its email and hard disk encryption keys on the ENX-ID smart card.

3.4 Business Model

The business model structured according to [OP09] is outlined in Figure 4. In [Ro13] the different aspects of the business model are described in more detail.

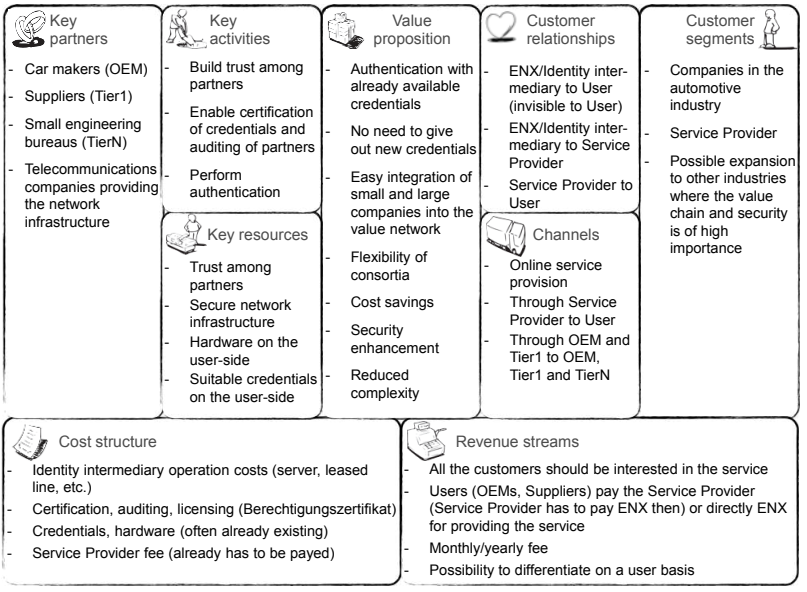

Figure 4: Business Model Overview – Presentation Based on [OP09]

Even though ENX Association is operating the architecture as a service for the automotive industry without the need to maximize profit, it must nevertheless be able to cover its expenses for running the infrastructure. A possible business model with respect to the trust services builds on ENX Association's existing structure. Again, ENX Association can fill the role of the legal and organizational roof of a business model based on competition among service providers.

Following the general ENX approach, central authentication services can be provided by ENX Association while implementation of central ID services like the ENX-ID could be executed through specialized and certified ID service providers. Additionally, any application provider can use the central authentication services for a variety of individual use cases if the usage complies with the general usage policies and legal regulations.

If implemented in this way, the ENX Association will use its position of trust and apply it to new business. The complexity of the authentication between business partners in the

industry is significantly reduced, without interfering with the free competition of providers and users and without restricting users in their selection of the service providers or services itself.

The cash flows in this model are initially similar to the original ENX business model. The stream of revenue goes from the automotive companies to the IDP who is charged by ENX Association for providing the central authentication service. Moreover, the companies participating directly in the federation would pay directly to ENX for the use of IDs from the central infrastructure. At least for an initial pilot period where ENX Association acts also as a central IDP, costs for direct management of individuals, organizational units, legal entities, credentials, roles and rights are expected to be higher compared to the current cost of the present model as it is based on the administration of corporate identities only.

3.5 Legal Aspects

Federated IDM including a third party that mitigates between different companies can be considered critical regarding data protection as personal data is distributed to a third party. However, [Sä13] shows, that the architecture is at least in Europe legally feasible if the contracts are designed carefully.

It is well imaginable to reuse the existing ENX contractual triangle as shown in Figure 5**Fehler! Verweisquelle konnte nicht gefunden werden.**. The performance and the cash flows are terminated by the triangle between ENX Association, certified service providers (CSPs) and users. All service components making up ENX today are offered to the user by a CSP in a bundle. Accordingly, a continuing obligation in respect of all recurring deliverables exist between service providers and users.

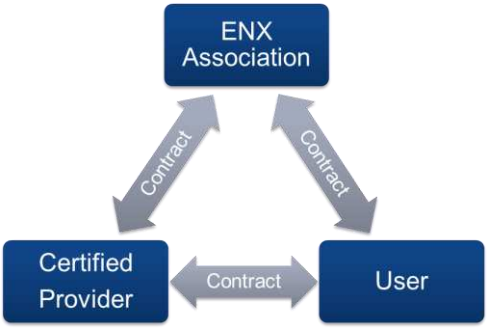

Figure 5: Contractual Relationship between the Involved Parties in the ENX Network

The ENX CSP provides these services to its customer. Based on an elaborate key (number of connections, bandwidth, quality levels, etc.) the service provider then pays a fee to the ENX Association for the central services in the overall construct.

The responsibilities of the participating parties are much higher than in the ENX Network scenario and have to be distributed fairly and carefully. It will be a major task of a

pilot installation to include all legal requirements and to establish a working and agreeable contractual model that is trustworthy to all involved parties, supports the described setup and fits into the economic model.

4 Conclusion

The ENX ID architecture is an approach to make identities available in a community consisting of many companies of all sizes. It aims to reduce the complexity of secure authentication in a whole industry significantly and thus to make it practical for many applications. This is done by two key design decisions.

First of all, the ENX ID architecture reduces the federation configuration complexity per user from O(n) to O(1) by introducing an intermediary. Companies can chose to federate with this intermediary and immediately are able to accept user information and authentication data from all other federated companies.

Secondly, the architecture introduces one or more identity provider with secure multi-factor authentication methods that are also federated with the intermediary. These identity providers can be used by companies that are not federated with the intermediary.

The architecture relies on the ENX Association as an independent but controllable third party to generate trust. The ENX Association enables companies to trust into the federation by ensuring trustworthiness in three key areas. It enables the technical security by defining strong security criteria as a perquisite for federation and it certifies and audits. It ensures economical trust by establishing a business model that has proven its viability in a similar setup already. It will finally enable legal trust by a carefully designed contractual model and a careful analysis of the data protection law relevant issues.

References

[ADS08] Anderson K.B.; Durbin E. und Salinger M.A. (2008): Identity Theft. *Journal of Economic Perspectives*, 171-192.

[CF07] Clarke N.L. und Furnell S.M. (2007): Advanced user authentication for mobile devices. *Computers & Security 26*, 109-119.

[DD08] Dhamija R. und Dusseault L. (2008): The seven flaws of identity management: usability and security challenges. In: *IEEE Security & Privacy*.. S. 24-29.

[Ho12] Homburg C.; Klarmann M.; Reimann M. et al. (2012): What Drives Key Informant Accuracy? *Journal of Marketing Research*, 49. S. 594-608.

[IK07] IKB Deutsche Industriebank (2007): *Investitions-Outsourcing in der Automobilindustrie von Automobilindustrie*. http://www.automotive-rheinland.de/content/TOP_2_Kraus_IKB_071113.pdf2,

[IWS04] Ives B.; Walsch K.R. und Schneider H. (2004): The domino effect of password reuse. *Communications of the ACM 47(4)*, 75-78.

[KWB03] König W.; Wigand R.T. und Beck R. (2003): Globalization and E-Commerce: Environment and Policy in Germany. *Communications of the AIS 10*, 33-72.

[MN07] Myers M.D. und Newman M. (2007): The qualitative interview in IS research: Examining the craft. *Information and Organization*, 17. S. 2-26.

[MO07] Mannau M. und Oorschot P.C.v. (2007): Using a personal device to strengthen password authentication from an untrusted computer. In: *Conference of Financial Crypto*. Scarborough Trinidad and Tobago: S. Dietrich; R. Dhamija. S. 88-103.

[MR08] Maler E. und Reed D. (2008): The venn of identity: options and issues in federated identity management. In: *IEEE Security & Privacy*.. S. 16-23.

[OP09] Osterwalder A. und Pigneur Y. (2009): *Business Model Generation*. Amsterdam.

[Pe94] Neumann P.G. (1994): Risks of passwords. *Communications of the ACM 37(4)*, 126.

[Ri11] Riske A. (2011): ENX: Geschützte Datenübertragung in der Industrie. *iX 8/2011*.

[Ro13] Rossnagel H.; Sellung R.; Fähnrich N. et al. (2013): *FutureID Deliverable D21.5 Business and Use-case Analysis*.

[Ro14] Roßnagel H.; Zibuschka J.; Hintz O. et al. (2014): Users' willingness to pay for web identity management systems. *European Journal of Information Systems*, 23. S. 36-50.

[RR06] Recordon D. und Reed D. (2006): OpenID 2.0: a platform for user centric identity management. In: *ACM Workshop on Digital Identity Management*. Alexandra VA: ACM Press. S. 11-16.

[RZ12] Zibuschka J. und Roßnagel H. (2012): Stakeholder Economics of Identity Management Infrastructures for the Web. In: *Proceedings of the 17th Nordic Workshop on Secure IT Systems (NordSec 2012)*. Karlskrone, Sweden.

[Sä13] Sädtler S. (2013): Identity management in cloud computing in conformity with European Union law? Problems and approaches pursuant to the proposal for a regulation by the European Commission on electronic identification and trust services for electronic transactions in the i. In: Hühnlein D. und Rossnagel H. (Hg.): *OpenIdentity Summit*. Kloster-Banz. S. 116-127.

[Sc06] Schläger C.; Sojer M.; Muschall B. et al. (2006): Attribute based authentication and authorisation infrastructures for e-commerce provides. In: Bauknecht K.; Pröll B. und Werthner H. (Hg.): *E-Commerce and Web-Technologies*. Berlin: Springer. S. E-Commerce and Web Technologies.

[SRW05a] Spath D.; Renner T. und Weisbecker A. (2005): Inter-company business processes and ecollaboration. In: *The Pratical Real-Time Enterprise*. Berlin: Springer. S. 13-28.

[Vi12] Viavision (2012): Wer mit Wem? Die Verpflechtungen der Autobranche. *Viavision 04*.

[WRZ12] Wehrenberg I.; Roßnagel H. und Zibuschka J. (2012): Secure Identities for Engineering Collaboration in the Automotive Industry. In: *MIGW 2012 - Conference on Mobility in a Globalised World*. Bamberg. S. 1-12.