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.

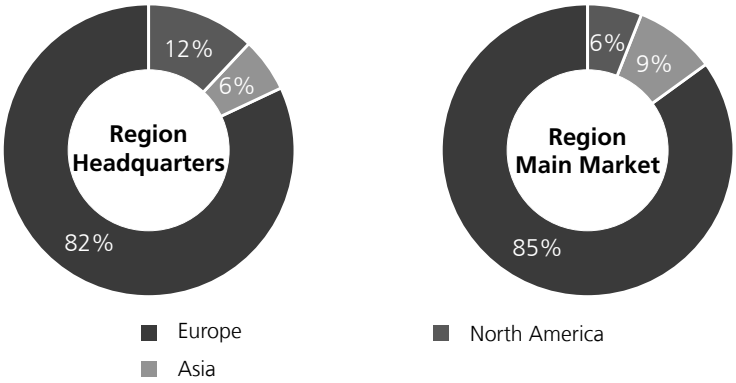

Fig. 1: Headquarters and main markets of sample companies

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.

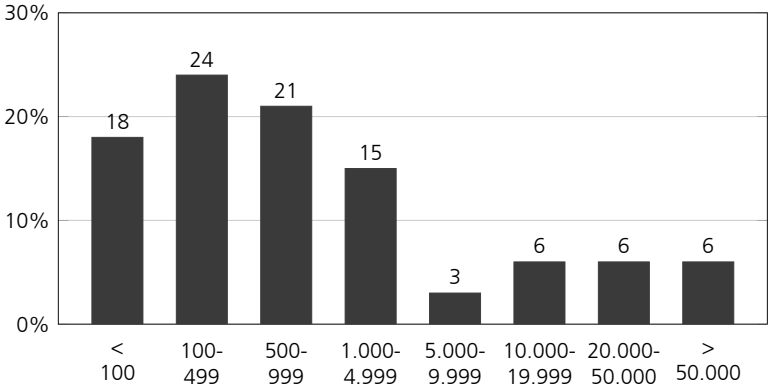

Fig. 2: Size distribution (number of employees) of sample campanies

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.

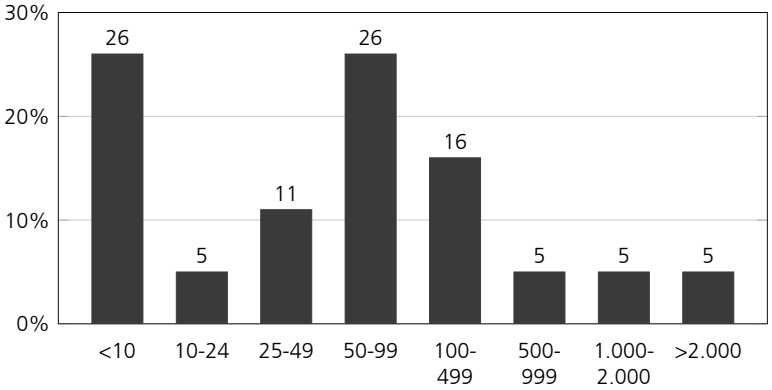

Fig. 3: Size distribution (sales last financial year in million euro)

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.

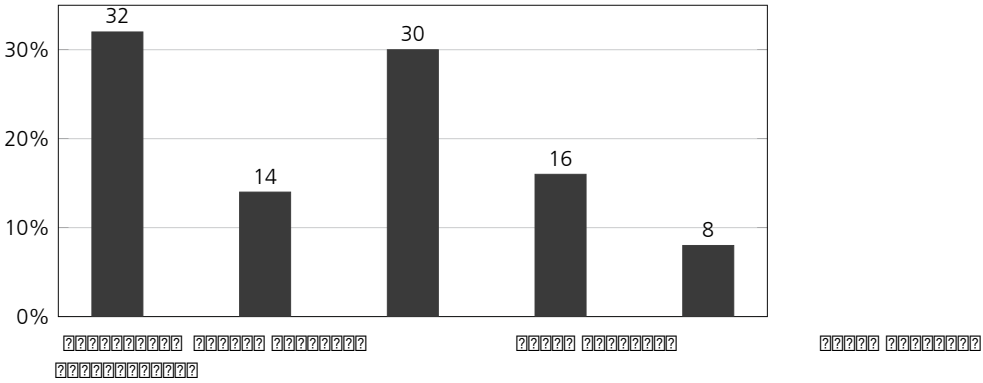

Fig. 4: Value chain position distribution in the sample

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.

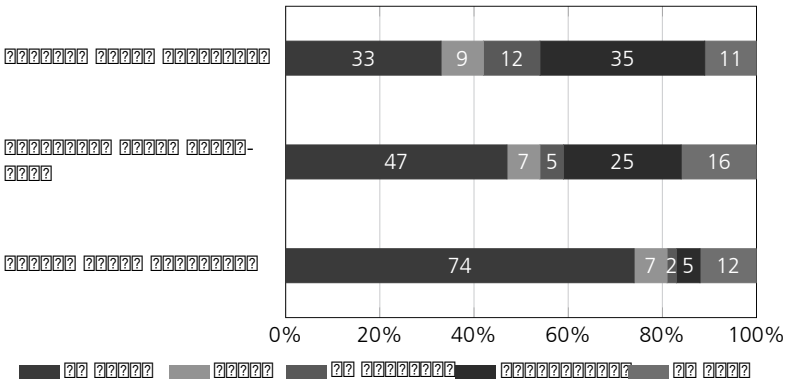

Fig. 5: Diffusion of cloud computing

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.

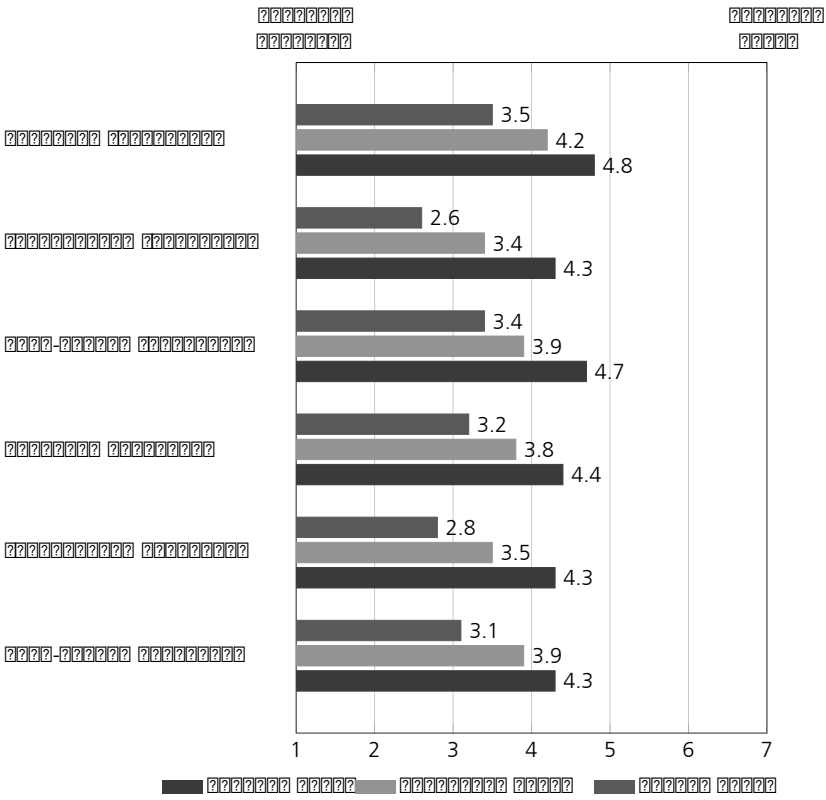

Fig. 6: Perceptions of cloud computing

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.

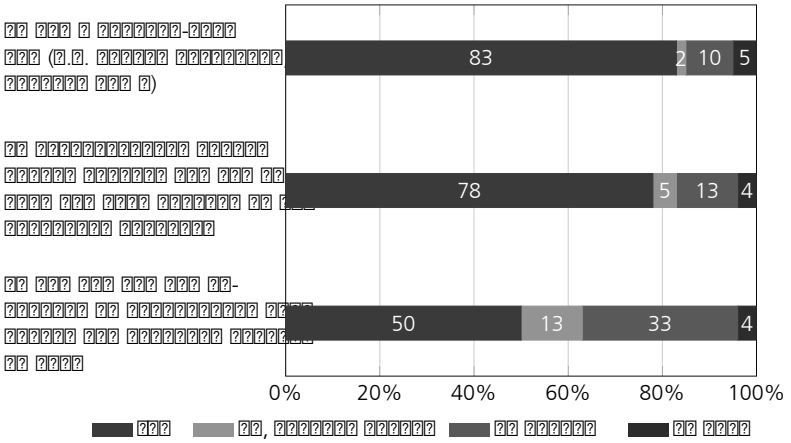

Fig. 7: Use of identity management technologies

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 %.

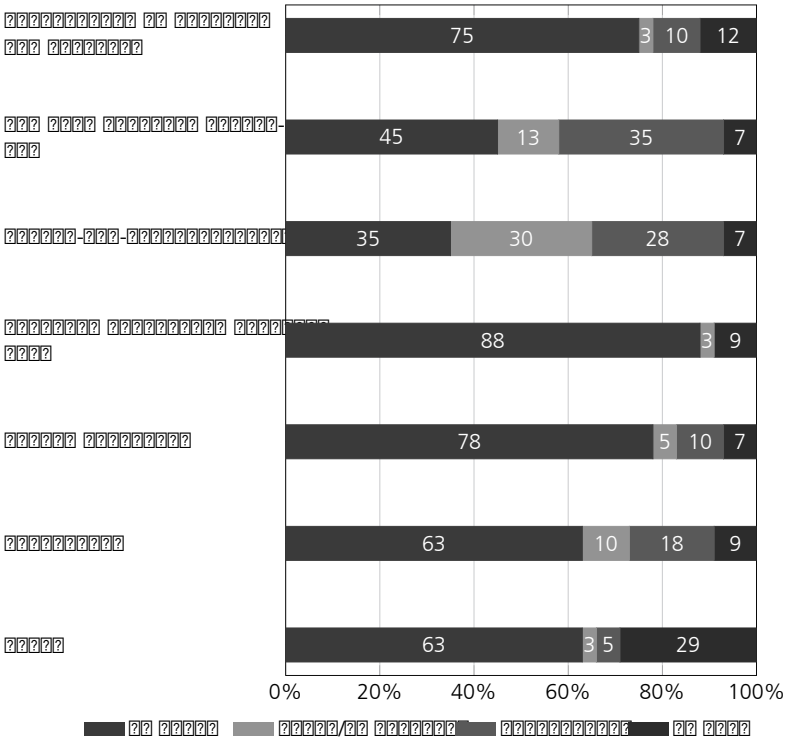

Fig. 8: Status and future (next two years) of authentication methods

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.

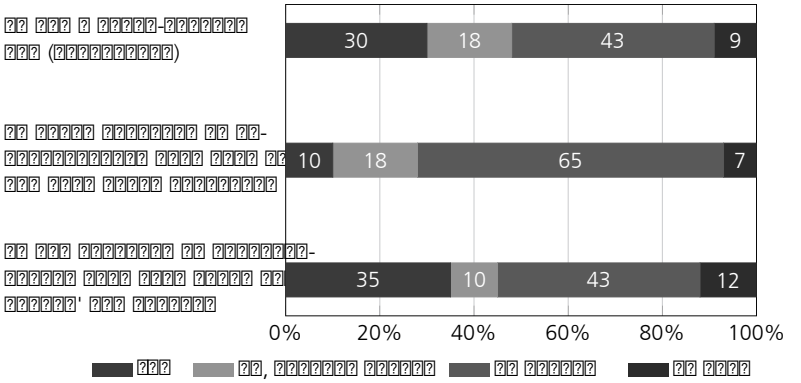

Fig. 9: Cross-company IdM

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.

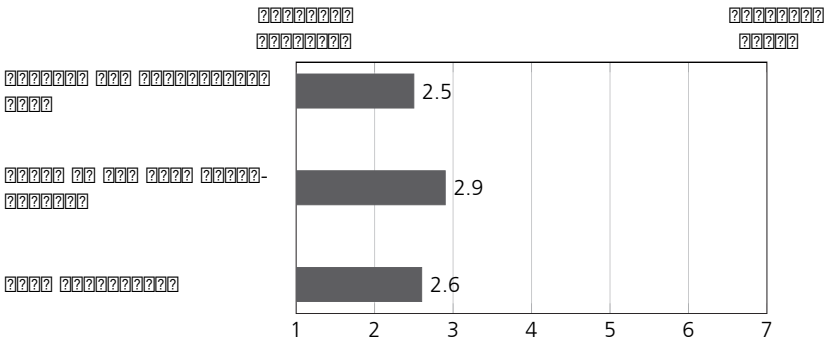

Fig. 10: Motivating factors for the implementation of cross-company IdM

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.

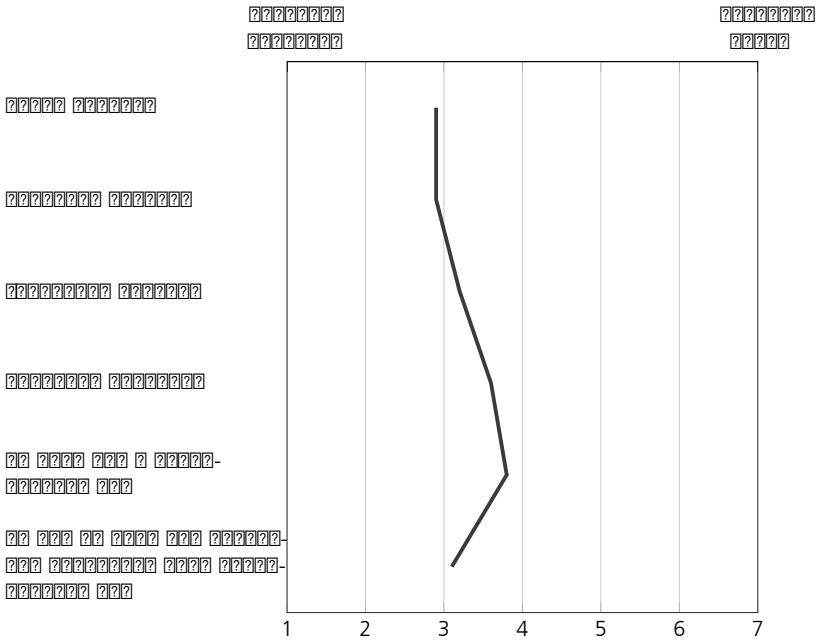

Fig. 11: Barriers to the use of cross-company IdM

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.