Preserving Privacy in Production

Moritz Christian Müller

Preserving Privacy in Production

Moritz Christian Müller
Fraunhofer IAO
Competence Team Identity Management
Nobelstraße 12
70569 Stuttgart
Germany
moritz.cm@gmail.com

Abstract. In modern manufacturing environments, new technologies are introduced that bring machines, analytics and people closer together. As a consequence, a rise in productivity, flexibility and efficiency is expected. However, these technologies raise new privacy concerns as well. We look at AssiEff, a tool to reduce the energy consumption of production systems, analyse its privacy issues and requirements regarding authentication and propose two approaches in order to address these issues. The first approach is based on anonymous credentials; the second follows an organisational approach. Both approaches are evaluated in regards to security-, privacy- and economic-aspects. In the end, we draw the conclusion that although anonymous credentials fulfil all security and privacy requirements, the organisational approach is the more appropriate solution in most scenarios. Costs are low and the privacy of the employees is protected sufficiently.

Keywords: Authentication, Anonymous Credentials, Industrie 4.0, Privacy

1 Introduction

The rising trend of the Industrial Internet[1] and Industrie 4.0[2] is promising among others to bring machines, analytics and people closer together in manufacturing environments. This is achieved by connecting machines with sensors and software applications, by connecting people, for example with the help of mobile devices like tablet computers and by connecting both through advanced analytics. Thereby people get a better insight in the production process, are able to react faster to changing requirements and are able to communicate with co-workers, suppliers and customers more efficient. A rise in productivity, flexibility and efficiency is expected [1].

Several research projects have the goal to increase flexibility or to increase the energy efficiency in production [2].

Among those is the project AssiEff, which is focusing on the energy consumption of production systems in small and medium enterprises (SME). A study by [3] is stating that energy consumption in production can still be decreased up to 50 %.

[1] www.ge.com/mindsandmachines
[2] www.bmbf.de/de/19955.php

AssiEff is analysing especially components of production systems. A back-end service is automatically looking at the utilization of each component and is checking if the component still fits the needs of the production process. By turning components off or by exchanging them with components which are more efficient, energy and therefore money can be saved. The operators of the production systems, who are responsible for the production system on the shop floor get notified about ways to reduce the energy consumption on a tablet-computer and are able to act based on this information. For example, a recommendation can be sent out to turn off a component for the next hour. A machine operator has the possibility to follow this recommendation, which is then confirmed to the AssiEff back-end services [4].

Most applications, which are developed as part of the *Industrial Internet* and *Industrie 4.0*, have in common that they gather a lot of data about machines but also about people, who are interacting with them. With the help of this data, detailed profiles of each employee could be created. This raises privacy concerns. In the last years, several incidents made the news, where employees unduly have been recorded by hidden video cameras or their behaviour has been monitored [5,6]. Industrie 4.0 technologies could increase the range of surveillance further.

Although some of these measurements might be legal, they can affect the relationship between the employee and the employer. Studies have shown that some employees, who are monitored by their employer may feel that "they are denied the self-respect that comes with being trusted to do their jobs correctly on their own" [7].

For these developments to be successful, it is necessary to bare these privacy concerns in mind and to develop solutions that respect their concerns and provide privacy by design [8]. In case of the basic AssiEff-architecture, an employer has the possibility to examine which employee has followed how many recommendations and could use this data, to track the employees' behaviour, compare and rank them. It is very likely, that this functionality is not embraced by the employees and the staff council. Therefore, we want to look at solutions, which address with these concerns, fit into the existing AssiEff architecture and still provide the necessary security. The final version of AssiEff should then make use of the recommended solution.

In this research, we discuss the requirements of AssiEff from the view of an employee but also from the view of an employer, describe how the current authentication architecture is designed and how it could be extended in order to fulfil the requirements. Then we want to evaluate an approach, based on anonymous authentication and an approach which is based on pseudonym authentication. The proposed architectures are evaluated and compared by security, privacy and socio-economic standards. At the end of the research, we will recommend an approach, based on the evaluation and give a short summary.

2 Methodology

The introduced relevant privacy and security concerns for assistant systems in manufacturing are addressed by providing two IT artefacts. These two artefacts are developed and evaluated based on the Design Science approach as proposed by Hevner et al. [9]. The first artefact includes a novel authentication system based on

anonymous credentials (ACs); the second includes an authentication system, following an organization approach. The technical principles, on which these approaches based, have been proven to fulfil high privacy and security requirements. The feasibility of these approaches is rigorously evaluated within the given environment. The environment includes the different stakeholders of the AssiEff system, processes within the system and the infrastructure. Business needs are derived from this environment. A knowledge base provides existing frameworks and techniques which will be applied on the development of the artefacts. From this knowledge base the requirements are derived as well. Furthermore, the business needs and the knowledge base are the foundation for the evaluation of these artefacts.

3 Related Work

We base our work on several studies discussing the effects of employee monitoring [10,7,11]. Similar to [12], we look at privacy issues in manufacturing environments, but contrary to this paper, we are examining the effects of monitoring the general behaviour of employees and how to minimize them. The environment we describe has been developed and introduced by [4].

One way to protect privacy of employees are ACs. The basic technique behind ACs was introduced by [13] and [14]. For evaluation, the acceptance of such a solution, the barriers, benefits and costs play an important role. These issues have already been discussed in [15] and [16].

4 Basic Architecture

The basic architecture of AssiEff includes two components: The AssiEff mobile application, which runs on a tablet-computer and the AssiEff-Server. The AssiEff server analyses production systems and production schedules and is looking for ways to reduce energy. If ways have been identified, it generates a recommendation, which notifies the user, how energy can be saved. On shop floor level, every employee is carrying a tablet-computer, which receives these recommendations.

Based on the username, employees can be identified at any time and any action can be linked. Also every user is a member of a role, which limits their actions in the AssiEff service. All user accounts are managed by the AssiEff-Server.

At the beginning of a work day, employees receive tablet-computers on which they sign in with their username and password. The AssiEff server verifies their accounts and grants them access to the AssiEff app, depending on the role they are assigned to. To keep users accountable for the tablet computer, the server also takes note, which tablet the employee is currently using. When they receive a recommendation on their tablet, they are able to follow the recommendation and confirm this action to the server. In the basic architecture, the server logs, which recommendation has been followed or declined by the user.

The following figure shows the structure of the current AssiEff architecture.

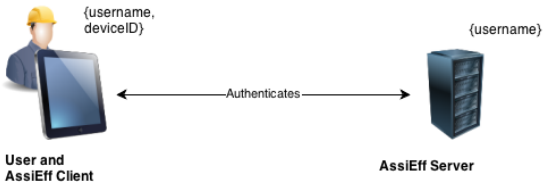

Fig. 1. Basic AssiEff architecture

5 Requirements

5.1 Basic Requirements

To restrict access to critical information and parameters, a role based user model is introduced, which allows the administrator of the system to define which kind of user has access to what kind of information [17]. Therefore, an authentication system must verify the users' role, when they want to sign in to the system [17].

Also, it must be possible to hold employees accountable for their actions. Thus employees have to log in to the authentication service with a unique identification.

These are the basic requirements of the AssiEff authentication system regarding authentication, authorization and accountability. They are already fulfilled by the existing AssiEff architecture. Also, it must be possible to hold employees accountable for their actions. Thus employees have to log in to the authentication service with a unique identification.

5.2 Extended Requirements

Additionally, not only security but also privacy and usability issues have to be addressed.

In AssiEff, employers could track how many recommendations an employee has followed. This data could influence decisions of personnel administration and may have negative effects for the employee. As stated earlier, it is very likely that this functionality is not embraced by the employees and may even be prohibited by the work council or labour courts. A closer analysis of this topic by legal experts is desirable but is not part of this paper. Therefore, solutions have to be found, which respect the privacy of the employees, but also guarantee secure authentication.

Furthermore, one has to bear in mind that AssiEff is focusing on small and medium enterprises (SME) with only a small number of manufacturing systems. Such enterprises may not have the money or expertise to set up and maintain elaborate IT-infrastructures. First unpublished measurements have shown that AssiEff might reduce the energy consumption of productions systems up to 40%. As an example, such a system might consist out of five small robots with a payload of 15kg. Each

robot may consume 1.3kW energy on average and is run daily for 8 hours, 350 days per year [18]. In total all robots run 14,000 hours per year. This makes an energy consumption of 18,200 kWh. The energy costs for one kWh in typical companies in Germany are around 12 cent/kWh [19]. As a consequence the energy costs for these five robots are about €2184.00 for one year. Assuming, that the energy costs of these components can be reduced by 40% with the help of AssiEff, the energy costs can be reduced by €873.60.

Thus, the costs for expanding the basic architecture in order to achieve the aforementioned requirements must not exceed the amount of money, which can be saved with AssiEff.

Below, the requirements of the system are summarised.

- **Secure authentication:** Only valid users must be allowed to access the system.
- **Authorization:** Access-restrictions for specific areas must be possible.
- **Privacy protection:** Employer must not be able to trace the behaviour of its staff.
- **Accountability:** Administration must be able to hold users accountable for their actions with their tablet computer.
- **Economic aspects:** The cost for setting up and maintaining the authentication and authorization system should not exceed the amount of money that can be saved by AssiEff.

6 Extended Architecture

In order to fulfil the requirements, we want to propose and discuss two different approaches.

6.1 Anonymity

The first approach is based on ACs as first introduced by [20] and refined by [13].

ACs are based on the idea that a user can obtain a credential and then proves the possession of this credential to an organisation. The organisation does only know that the user possesses such a credential but does not know the identity of the user. Even if a user wants to demonstrate the possession of such a credential several times, the demonstrations cannot be linked.

The architecture of ACs consists out of three basic entities.

- **The User**, who wants to prove to an organisation, that she owns a certain attribute.
- **The Verifier**, which wants a proof from the user, that she owns a certain attribute.
- **The Issuer**, which can certify that the user owns a certain attribute.

Applying ACs to AssiEff, the user, which is in case of AssiEff the employee, wants to prove to the Verifier, which is in case of AssiEff the AssiEff-Server that she is a designated member of a certain role. This proof is provided by the Issuer, where the User has authenticated herself earlier. The verifier only knows that the user is a designated member of the role, but does not know who the user is. As a consequence, the user cannot be linked to her actions.

The following figure show, how such an infrastructure could look like.

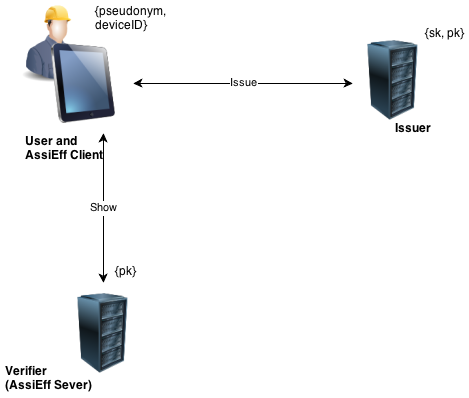

Fig. 2. AssiEff architecture with anonymous credentials

There are different entities who could act as an issuer. On the one hand the issuer can be hosted within the enterprise IT-infrastructure. There, the enterprise has full control over issued credentials and their revocation. On the other hand, third parties could also act as an issuer. For example, governments could support ACs and could issue credentials for their eIDs or eIDs could even implement an AC infrastructure itself as proposed by [21].

To hold users accountable in case of loss or damage of the tablet computer, the Issuer additionally has a table, where the device ID, the name of the user and the current date is stored. At the beginning of the work day, the user confirms to the Issuer, which device she has taken.

6.2 Pseudonymity

The second approach follows an organisational solution instead of a technical solution. Instead of full anonymity, it only provides pseudonymity for its users. In comparison to the first approach, transactions could still be linked to a unique user in case the real identity behind a pseudonym is being revealed.

Pseudonymity is achieved by separating authentication from the actual AssiEff server to an additional Authentication Server. There, the real name is mapped to a pseudonym. This Authentication Server is under control of an entity, which is trusted by the employees. The entity is the only instance, which has insight into the mapping of real-name to pseudonym and should not reveal this information to the employer.

Figure 3 shows the AssiEff architecture based on the pseudonym approach.

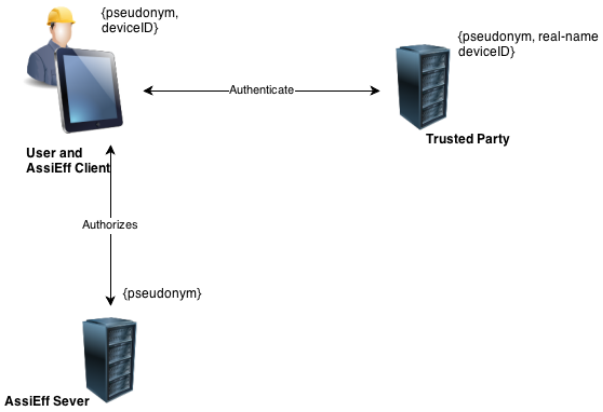

Fig. 3. AssiEff architecture based on pseudonym approach

At the beginning of a workday, users take a tablet computer and initiate the authentication process by using their user-name and password. The Trusted Party verifies the credentials. In case that the authentication was successful, the trusted-party sends a token with the pseudonym to the AssiEff client. It proves to the AssiEff server that the user is a designated member of a certain role. The client forwards this token to the AssiEff server which authorizes the user. The token does not include any information about the real identity of the user but a pseudonym. Only the Trusted Party knows the real identity of the user.

In order to prevent that the token can be forged, it must be encrypted with a pre-shared key. Thereby the use of an expensive PKI is avoided. Access to the authentication server must only be granted to the Trusted Party.

The role of the Trusted Party could be taken by the work council. Usually the work council is elected by the work force and enjoys the trust of the employees. The trust may vary from company to company and has to be built up over years [22].

7 Evaluation

Now it is examined, if the approaches fulfil the requirements for a secure authentication, support the described role-model and if they can be implemented within the limitations of the basic AssiEff architecture, in order to restrict access to the AssiEff services properly.

Second, it has to be evaluated, how the solutions fulfil the privacy concerns.

Because AssiEff is focusing on small and medium enterprises, the costs for planning, setting up and maintaining these authentication services play a crucial role and are being evaluated as well.

7.1 Evaluating Anonymous Approach

Security. First of all, the discussed solutions have to fulfil all requirements regarding a secure authentication of users at the AssiEff assistant as listed in 5.1.

The AssiEff back-end is based on Java and therefore an anonymous authentication implemented in Java is preferred. [14] proposes such an authentication framework called idemix. It provides all protocols, which are necessary to implement ACs in AssiEff. It has been proven that ACs are secure and therefore fulfil the requirement as mentioned earlier in 5.1. The required role model can be implemented seamlessly. The Issuer provides tokens to users, which proves that they are member of a certain role. Then, this token is being shown to the Verifier. The Verifies checks if the token is signed by the Issuer.

Because ACs are relying on a PKI, IT-administration have to guarantee, that the underlying public keys are distributed and the private keys are stored in a secure manner.

Privacy. Authentication based on ACs fulfils high standards of privacy and anonymity. Even if Verifier and Issuer are residing within the same organisation or pooling their data, as it is most likely the case in AssiEff, unlinkability between the provided credential and the real name is still guaranteed [14]. Even two successful logins, which were initiated by the same user, cannot be linked.

To make sure that anonymity of the users is fully guaranteed, the underlying communication channels must support anonymity [14].

It has to be taken in mind that AssiEff might be used by companies with only a small number of employees. Therefore it might be the case that only a few people are assigned to a certain role. By comparing shift schedules or attendance lists with the log of the Verifier, conclusions about the identity of the user could be drawn and unlinkability is not guaranteed anymore.

Pseudonyms can be implemented with ACs as well, if it is of interest of the company.

Economic. The focus of AssiEff on SMEs requires that the costs and efforts for applying an anonymous authentication system should be as low as possible.

However, the PKI which is necessary for ACs is costly. Costs for such an infrastructure include IT staff time, hardware, security measurements and facility [23]. [24] estimates the costs for an in-house PKI at $157 (~€120[3]) per user and year. Although this estimation was made for 5000 users, similar costs for SMEs are expected. Thus a PKI environment with 10 users would cost €1200 per year. In comparison to the example as described in 5.2, this would exceed the costs by €326.40. This could put the willingness of the company at risk, to include AssiEff in their infrastructure. The costs can vary depending on the available hard- and software. Also a PKI might be used for other purposes, for example E-Mail signatures or log in for ordinary workstation computers. This reduces the total cost of ownership.

[3] As at May 10, 2013

Besides the direct costs, there might be indirect costs caused by ACs as well. Issuing, showing and verifying credentials takes time. Measurements conducted with a prototype of idemix demonstrated that showing an AC can take up to 8.2 seconds [14]. The AssiEff client is running on low-powered tablet computers which are not designed for complex computations. This slows down the login process significantly and might lead to frustrated users. It is important that the acceptance is not reduced by bad usability.

7.2 Evaluating Organisational Approach

Security. The organisational approach relies on basic and approved security mechanisms. The authentication process can be secured with adequate cryptographic mechanisms without implementing sophisticated authentication mechanisms. The authentication server and the underlying communication channel must be properly secured. The required role model can be easily implemented.

Privacy. The achieved level of privacy depends on the Trusted Party. If it is assumed that the Trusted Party holds any information about the identity of the user confidential, then the employer is not able to track their behaviour. A work council could take over the role as a Trusted Party. However, 57.2% of all medium sized enterprises in Germany do not have a work council [25]. In these cases, it might be hard to find an entity, which is trusted enough by the employees. Also, as mentioned in 6.2, trust between the work-council and the work force depends on several influences and may vary from company to company.

Economic. The costs for this approach are relatively low. Besides an additional server for a Trusted Party, no additional hardware is necessary. It only must be guaranteed, that the server is protected from unauthorized access. Also it can be assumed that even untrained IT-personnel is able to set up and maintain such an infrastructure.

Even though the direct costs might be relatively low, this approach might cause indirect costs. These may occur due to an informational asymmetry between the employees and the Trusted Party. Because of the design of the organisational approach, employees cannot verify if the Trusted Party fulfils its task and holds the information confidential. Based on the Principal-Agent-Theory, the employee takes over the role of the principal and the Trusted Party takes the role of the agent.

In order to balance the informational asymmetry between principal and agent, the agent should take actions that make the principal easier to verify, if their information is handled with care. Actions may include the evaluation of the infrastructure by a third party, setting up logging mechanisms to track who accessed the server of the Trusted Party, or introducing harsh punishments if the trust between the user and the Trusted Party has been abused. These actions may cause agency costs and will raise the total costs of such an approach.

8 Discussion

Based on the evaluation in section 7, it has been shown that although ACs provide the best protection of the employees' privacy, the costs for implementing such an infrastructure exceed the cost saved by AssiEff by far. Thereby the main reason to use AssiEff is at risk and it will be hard to justify the implementation. This solution only makes sense, if an authentication system based on ACs is already available or companies are driven by ideological reasons.

Also, as described in [16], legal requirements might enforce a more strict protection of the employees' privacy which could be a reason for choosing this approach.

In most cases, the organisational approach is the more appropriate solution because costs are low and the employees' privacy is protected in a sufficiently manner.

9 Conclusion

In this paper, we have introduced the privacy challenges in the upcoming trend of highly interconnected machines, analytics-software and people. As an example, we have chosen AssiEff, an assistant to reduce the energy consumption of production systems. We have looked at its security requirements, privacy concerns and its basic architecture.

An anonymous authentication system, based on ACs and a pseudonym authentication system was proposed to address these issues. Both solutions have been evaluated based on security, privacy and economic aspects.

The anonymous approach guarantees full privacy of employee whereas the organisational approach can only provide pseudonymity. The main difference between these solutions is the costs of implementation. The anonymous approach relies on a PKI, which causes more costs than the organisational approach. We have come to the conclusion that addressing the privacy concerns is essential for the success of systems like AssiEff. The user's privacy is not protected in the basic architecture thus both solutions improve the privacy. Which solution will be chosen depends on several factors including the size of the company, the individual costs for the solution and the willingness of the company to protect the privacy of their employees. In our opinion the organisational approach is the more adequate solution for most companies.

References

1. P. C. Evans and M. Annunziata, Industrial Internet: Pushing the Boundaries of Minds and Machines. 26-Nov-2012.
2. S. Gerlach, »KAPAFLEXCY« Für die Industrie 4.0, IAO-News, no. Dezember 2012 / Januar 2013, p. 3, 2012.
3. C. Schmid, Energieeffizienz in Unternehmen. Zürich, Switzerland: vdf Hochschulverlag AG, 2004.

4. U. Laufs, P. Schneider, and J. Zibuschka, Design of a system for energy-efficient production in SMEs, in ICPR 2011 - Conference Proceedings, 2011.
5. T. Wilke, Apple gewinnt Big Brother Award 2013 für „besonders dreiste Form von Videoüberwachung, GIZMODO, 14-Apr-2013.
6. P.-M. Ziegler, Datenschutzverletzungen: Lidl fällt als Wiederholungstäter auf, heise online, 26-Mar-2008.
7. S. S. Ariss, Computer monitoring: benefits and pitfalls facing management, Information and Management, 2001.
8. A. Cavoukian, Privacy by Design … Take the Challenge. Information and Privacy Commissioner Ontario Canada, 2009.
9. A. R. Hevner, S. T. March, J. Park, and S. Ram, Design Science in Information System Research, MIS Quarterly, vol. Vol. 28 No 1., pp. 75–105, 2004.
10. G. Lasprogata, N. J. King, and S. Pillay, Regulation of Electronig Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada, Standford Technology Law Review, vol. 4–2004, 2004.
11. G. S. Alder, T. W. Noel, and M. L. Ambrose, Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust, Information and Management, 2006.
12. D. Lucke, E. Westkämper, M. Eissele, T. Ertl., and O. Siemoneit, Privacy-Preserving Self-Localization Techniques in Next Generation Manufacturing, presented at the 10th Intl. Conf. on Control, Automation, Robotics and Vision, Hanoi, Vietnam, 2008.
13. J. Camenisch and A. Lysyanskaya, An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. 2001.
14. J. Camenisch and E. V. Herreweghen, Design and Implementation of the idemix Anonymous Credential System, presented at the CCS'02, Washington, DC, USA, 2002.
15. H. Roßnagel, J. Zibuschka, O. Hinz, and J. Muntermann, Users' Willingness to Pay for Web Identity Management Systems, European Journal of Information Systems, 2014.
16. The European Commission, Ed., Study on the economic benefits of privacy□enhancing technologies (PETs). Jul-2010.
17. U. Laufs, J. Zibuschka, and P. Schneider, Decision support for energy efficient produciton in SME, Mobility in a globalised world: University of Bamberg Press, pp. 135–144, 2012.
18. P. Poonyapak, J. M. J. McDill, and M. J. D. Hayes, Improving Robot Efficiency to Reduce Energy Consumption. 2007.
19. S. Bolay, C. Grajetzky, H. Hüwels, K. Andrea, and S. Lechner, Faktenpapier Strompreise in Deutschland. 20012.
20. D. Chaum, Security without identication: Transaction systems to make big brother obsolete., Communications of the ACM, vol. 28(10), pp. 1030–1044, Oct. 1985.
21. P. Bichsel, J. Camenisch, T. Groß, and V. Shoup, Anonymous credentials on a standard java card, in Proceedings of the 16th ACM conference on Computer and communications security, Chicago, IL, USA, 2009, pp. 600–610.
22. U. Rami and A. Hunger, Vertrauen als Legimitation für die Betriebsarbeit, Industrielle Beziehung, no. Jahrgang 18, Heft 3, pp. 167–189, 2011.
23. E. G. Carayannis and E. Turner, Innovation diffusion and technology acceptance: The case of PKI technology, vol. technovation, 2005.
24. VeriSgin, Ed., White Paper: Total Costs of Ownership for Public Key Infrastructure. 2005.
25. Hans-Böckler-Stiftung, Ed., Betriebsräte in mittelständischen Unternehmen weithin akzeptiert, Böcklerimpuls, no. 16/2007, 2007.