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

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

Sebastian Kurowski[1]

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

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

1 Introduction

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

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

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

2 State-of-the-art

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

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

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

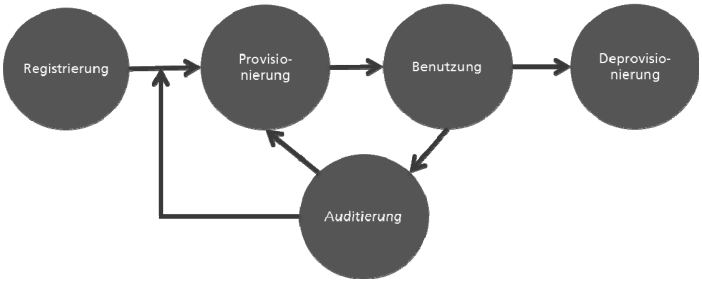

Fig. 1: The identity lifecycle [MR08]

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

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

3 Scenario

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

4 Costs of identity and access rights lifecycle management

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

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

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

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

Enrolment

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

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

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

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

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

Provisioning

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

d.html

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

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

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

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

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

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

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

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

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

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

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

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

Deprovisioning

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

Auditing

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

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

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

5 Transaction costs of federated identity management

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6 Conclusion

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

Acknowledgment

The research leading to these results was supported by the "German Ministry of research and Education (BMBF)" as part of the VERTRAG research project.

References

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

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

A Annex

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

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