Supporting Compliant and Secure User Handling - A Structured Approach for In-House Identity Management

Ludwig Fuchs, Günther Pernul
Department of Information Systems, University of Regensburg, Germany
{Ludwig.Fuchs|Guenther.Pernul}@wiwi.uni-regensburg.de

Abstract

The catchword "compliance" dominates the actual debate about Identity Management and information security like few before. Companies need to comply with a variety of internal and external standards and regulations like the US SOX act. Identity Management is seen as a main provider of compliance in modern companies. However, its organisational aspects are underestimated in many projects, lacking a comprehensive approach to introduce in-house Identity Management. This work is based on the experiences gained from industry projects using Identity Management functionalities to strengthen security and to reach a high level of compliance. We develop a structured process-oriented methodology for introducing an Identity Management Infrastructure for organisations using drivers from IT security management to evaluate, rank, and implement subprojects. The methodology consists of an iterative process which enables even large and unstructured organisations to reach a suitable and profitable level of Identity Management by emphasising on organisational aspects rather than taking a merely technical approach.

1. Introduction and Motivation

Identity Management (IdM) is one of the most challenging topics in today's modern society. The secure and efficient administration of numerous personal attributes that make up digital identities is one of the key requirements in open and closed networks. Identity Management in open networks like the Internet has received remarkable attention throughout the last years with researchers focussing on Identity Federations based on different open standards. In addition to that, projects like FIDIS (http://www.fidis.net/) or PRIME (https://www.prime-project.eu/) flesh out the importance of IdM for the society. Although considered important, Identity Management in closed networks, however, has not gained comparable significance within the research community. The lack of academic penetration on the one hand and experience gained in industrial projects on the other hand were the major motivation for performing this research.

Our engagement in different IdM projects has revealed the need for careful planning and a modularised introduction of an in-house Identity Management Strategy and Infrastructure. Together with an international company employing over 35.000 users, we started to introduce IdM as a means to meet information security and compliance demands. A methodology was derived showing the necessary steps to introduce IdM and supporting the project team in planning the implementation of further IdM modules. Coming across the same problems within other organisations, independent from the companies' size or class of business, we experienced the need for a reference model to cope with Identity Management in a structured and company-wide manner. This led us to the development of an approach for the introduction of IdM which is presented in this paper. Our goal is to provide a reusable process-oriented reference model for IdM in closed networks that takes recurring organisational issues into account and therefore is generally able to assist companies in their Identity Management issues.

Organisations today are getting increasingly under pressure to control, manage, and audit their information flows. We experience a new level of taken precautions, officially certified processes, and strategic changes in IT having their roots in information security issues, legislative acts, or pressure from customers and partners. Among the most known drivers for changes in IT and information control systems are the U.S. Sarbanes-Oxley Act (SOX) of 2002 [1], Basel II [2], BSI Grundschutz [3], the Directive 95/46/EC of the European Parliament [4], ISO IT Security standards (such as ISO 27002), and internal regulations. The effort to conduct business and manage IT systems in accordance with these standards and demands is called *compliance*.

Addressing the major aspects of computer- and information security, which are confidentiality, integrity, and availability, is of paramount importance for getting compliant. Especially in respect to confidentiality and integrity, the users themselves, rather than popular external threads like viruses, phishing, or pharming attacks represent the main risk [5]. As a result of incorrect account management and inadequately enforced security policies users accumulate a number of excessive rights within the organisations' IT systems over time, violating the principle of the least privilege [6].

Identity Management is a means to reduce such risks, representing a vital part of a company's security and auditing infrastructure [7]. Based on processes, policies, and the used technology, the aim is to restrict and control access to resources and identify all actions by their issuer. In addition, IdM strengthens security through stronger authentication, enforcing least privilege and thereby minimising potential misuse. Identity Management itself consists of various modules starting with Single-Sign-On (SSO), secured provisioning processes, and more. It is often seen as a merely technical approach but looking closer, the issue is indeed a strategic decision - affecting security, human resource provisioning, process flows, organisational structures, and software license costs.

This paper is structured as follows. In section 2, related work is presented, organisational aspects are addressed and drivers for Identity Management are analysed. Section 3, subsequently, introduces IdM technologies. Section 4 explains the developed reference model for introducing Identity Management in organisations. Finally, conclusions and future work are given.

2. Related work and basic definitions

2.1. Identity Management

In particular big companies have to deal with a large amount of digital identities accessing their information systems. We define the term *identity* according to [8] as a subset of attributes or characteristics of an entity which make the entity, e.g. a person, uniquely identifiable within a set of entities. Electronic representatives for physical individuals are needed to administer users, grant permissions and control, regularise, and protocol their actions. In practice users often do not own only one single identity, but several identities in order to work with the productive applications. Every identity has its own access information and has to be created, maintained and erased separately. This situation results in a so called identity chaos in many organisations which needs to be faced by implementing a centralised Identity Management Infrastructure (IdMI). The IdMI represents the realisation of the defined processes and policies using adequate technical measures.

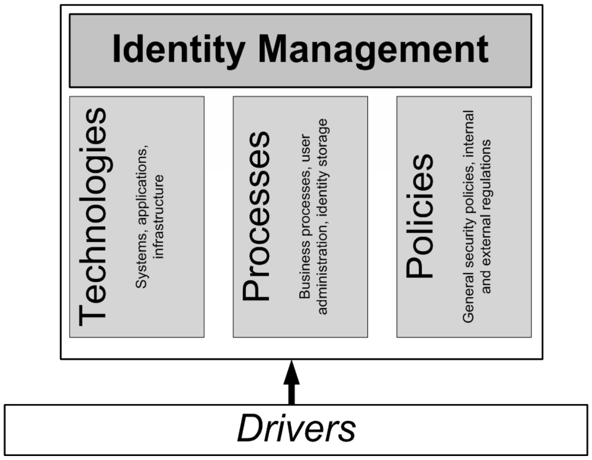
Identity Management
Technologies
Systems, applications, infrastructure
Processes
Business processes, user administration, identity storage
Policies
General security policies, internal and external regulations
Drivers

Figure 1. Identity Management environment

Identity Management has grown up over the last years and established itself as a core component of enterprise security management. It has evolved into an integrated, comprehensive framework, based on three pillars: Processes, well-defined policies and used technologies (as shown in Figure 1). Influenced by organisational and technical drivers, it deals with the storage, administration and usage of digital identities during their lifecycle. This covers rather simple tasks like automatic allocation and revocation of user resources, i.e. Windows accounts. However, it also includes sophisticated duties like role development on an organisational level. Practical experience has shown that the usage of roles and role patterns bears significant improvements in the area of user management as administration overhead and IT-risks are reduced [9]. The role concept assigns users to roles based on their function within the organisation instead of allocating access rights directly to them. The roles themselves are connected with access rights to certain resources [10]. A large body of work has gone on in the last years in this area covering different role models, administration concepts and role development strategies. However, going into detail about role-based IdM is out of scope of this paper and will be researched in our future work.

2.2. Organisational aspects of IdM

Before presenting technical components in chapter III, this sub-chapter focuses on the organisational side of IdM. Processes and policies valid within the organisation form the basis for a subsequent implementation of Identity Management. According to given strategic goals, they regulate the usage of electronic identities and their possible actions within the systems. Organisational Identity Management has to address security issues in order to build a stable basis and gain management commitment for IdM technologies like infrastructural elements, functional modules or connectors. Controlled and compliant processes and *policies* are needed to make technological measures efficient and meaningful.

Identity Management *processes* deal with user management, organisational as well as technical approval workflows, and escalation procedures. They form the main administrative workload as they comprehend the management of the whole user lifecycle. Besides IT-resources, responsible managers are affected by Identity Management processes. In terms of information security, proper analysis and representation of the processes play the central role for reducing the number of security breaches and possible risks. After their definition, technical and organisational approvals are mapped to the IdM workflow module in order to empower the managers to allow or deny user requests using a central administrative component. Furthermore, the existence of escalation plans is a mandatory aspect of Identity Management. Processes that define emergency procedures ensure ongoing system operation in case of technical malfunction, unexpected process delays or policy violations.

In order to regulate identity-related information flows and processes, *policies* have to be defined, consolidated and harmonised on different levels within the organisation: Process-level, IdM-level, IT-level or global level. Their grade of abstraction is dependent on their scope: Within Identity Management, for example, policies express regulations for user management processes, delegation issues or general security requirements. Abstract IT or global security guidelines are essentially direction-giving documents in an organisation defining the broad boundaries of information security. In contrast to that, policies at the process-level need to be implemented within the workflow component of an IdM solution and are therefore more system-specific.

However, political problems accompany the definition and enforcement of policies and processes as human factors play an important role in the process of policy definition and consolidation [11]. Factors like data ownership or the fear of future restrictions caused by a modern and comprehensive IdM solution makes policy-related tasks a time-consuming, communication-intensive and crucial challenge for the project team.

2.3. Drivers for Identity Management

Investigating the drivers for Identity Management from figure 1, one can distinguish between technical and organisational aspects. Technical goals could be security, scalability, system performance, and process automation while organisational aspects stem from the management perspective and include an overall increased security level, lower system administration costs and more efficient user administration processes.

Looking at driving forces for high level management commitment reveals compliance and increased information security as central drivers for the introduction of IdM. Closely related with each other, national and international law together with internal guidelines force enterprises to be able to provide proof of evidence about who has access to vital data within the companies' information systems and who has granted permissions to whom. Central IdM functionalities, like automated user management, are able to address these requirements and support organisations in becoming compliant. Implementation projects like [12] and popular studies [13] show that major security risks arise because of staff gaining unauthorized access to resources as a result of manually handling user accounts. Moreover, user management processes are rarely documented and most of the time carried out differently. Application-specific rights management increases security risks within the organisation and complicates comprehensive auditing tasks.

A good example for neglecting organisational aspects is the implementation of a Single-Sign-On solution in combination with strong password policies. If the necessary reorganisation of the provisioning processes is not taken into consideration, it remains an ineffective stand-alone solution, at least regarding information security. If employees that left the company months ago still have access to their user accounts, the Single-Sign-On system does not improve information security: The former employees are still able to get unauthorized access to internal data. This prime example shows that both, provisioning and deprovisioning processes, have to be optimized and enforced, so that additional measures on the technical level are able to unfold their full potential.

3. Technologies of Identity Management

Some years ago, stand-alone SSO modules or meta-directories quite often already were branded with the term Identity Management. Lately researchers as well as software vendors have realised that companies need more than just one or two single functional components to solve the identity chaos: Organisations need a comprehensive, integrative and standard-based Identity Management Infrastructure that contains several functional modules each serving a different purpose [14]. In addition to that, the emerging demand for sharing identity information between organisations results in a greater need for standardized data exchange channels. State-of-the-art identity federation therefore must rely on open standards, such as the XML-based protocols SAML [15] or SPML [16], essentially connecting different IdMIs. However, federation is out of the scope of this paper and will not be discussed in further detail.

The IdMI presented in figure 2 is an output of one of our industry projects with the overall goal to provide a structured view onto technical Identity Management within the enterprise. It reveals *Directory Services*, *User Management*, and *Access Management* as the central IdM modules.

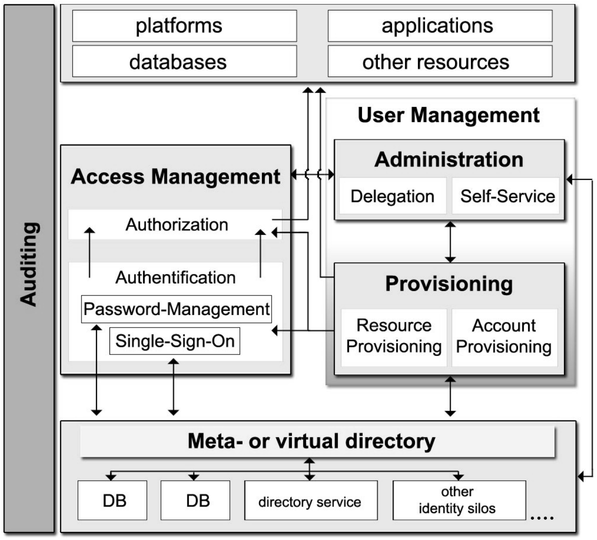

Figure 2. IdMI within an organisation

3.1. Directory services

Directory services provide synchronised information about users and resources forming the fundament of a comprehensive IdMI. The main challenge for the central data repository is to integrate user- or resource information from different target systems in a timely and consistent manner. This can be done by using either meta- or virtual directory technologies. Meta directories utilise connectors or agents to exchange data with the target systems and store the information by creating a copy in a central repository. The virtual-directory approach omits resulting redundancies by only storing pointers to the pieces of information in the target systems without working with physical copies.

3.2. User Management

The data provided by the directory services is facilitated by other functional IdM components like *User Management*, *Access Management* or exchange of user information across organisational borders. User Management deals with the process of managing the digital identities throughout their lifecycle, starting with the creation of accounts, the maintenance, i.e. by processing change requests, up to the deactivation or termination. It can be split into an administrative and a provisioning component. The latter includes the allocation and revocation of accounts or resources (IT and non-IT). When electronic identities are no longer needed, e.g. after employees left the organisation they are deactivated by a de-provisioning process. This way the provisioning system ensures that access rights of inactive users are locked or revoked immediately and reduces security vulnerabilities.

From an administrative point of view a delegation concept allows for passing on administrative rights to local persons in charge. The final step of this decentralisation process is a Self-Service component which enables users to alter their personal details on their own or request several resources without involving administrative staff.

3.3. Access Management

Together with the User Management and the directory services, an *Access Management* component is the third main module of an Identity Management Infrastructure. It deals with the authentication and authorisation of users, controlling access to connected resources. State-of-the art solutions are able to work with roles [6], granting access to information based on roles rather than individual IDs. Modern SSO modules incorporate different methods of authentication including passwords, digital certificates, and hardware or software tokens. Relying on global and local security policies, Access Management components also include Password Management and synchronisation as well as web or enterprise SSO functionality.

4. Introducing Identity Management

After pointing out the basic organisational and technical concepts and components of IdM, this chapter presents a method for setting up an IdMI and integrating it into the existing IT-infrastructure of an organisation. Our approach alters and extends an existing model [17] that is used for implementing an enterprise directory. The proposed methodology (figure 3) is not intended to be a project-management strategy but a rather generic high-level approach that considers special IdM requirements. One main purpose is to emphasise the need for organisational restructuring throughout the whole implementation process. Based on our project experience a technical approach that neglects the management side is leading to a situation where developed processes and policies remain unused and theoretical while on the other hand a solely management focused approach disregards central implementation issues like integration problems between different Identity Management modules.

4.1. Model overview

The complexity of the IdM components and the interaction together with the large amount of target systems and digital identities that have to be administered in big companies enforce a step-by-step introduction of an IdMI. On the one hand the policy and management side has to set up processes, and handle organisational issues while technology and architecture on the other hand have to focus on integrating and testing new functionalities within an existing IT-infrastructure. This dual concept needs to be taken into consideration as it is crucial for the development of Identity Management in general.

Based on two pillars (*technology/architecture* and *policies/management*) our approach consists of several process loops (from hereinafter called subprojects), each representing the implementation of one single IdM module (e.g. a provisioning component). Single process loops can differ in their complexity and length depending on the functionality and its cross connections with other loops. Complex Identity Management modules like a global user directory usually are implemented in a more time consuming subproject compared to the rather straightforward rollout of a user Self-Service functionality. The IdMI implementation is guided by a global strategy (top box, figure 3) that is influenced by long-term drivers and goals. In the centre of our model three basic process-steps form a subproject for implementing a single IdM module:

- Step 1: Subproject planning, preparations, and requirements engineering.
- Step 2: Development of (integration) processes and policies.
- Step 3: Technical integration into existing infrastructure, enhancement of policies and processes.

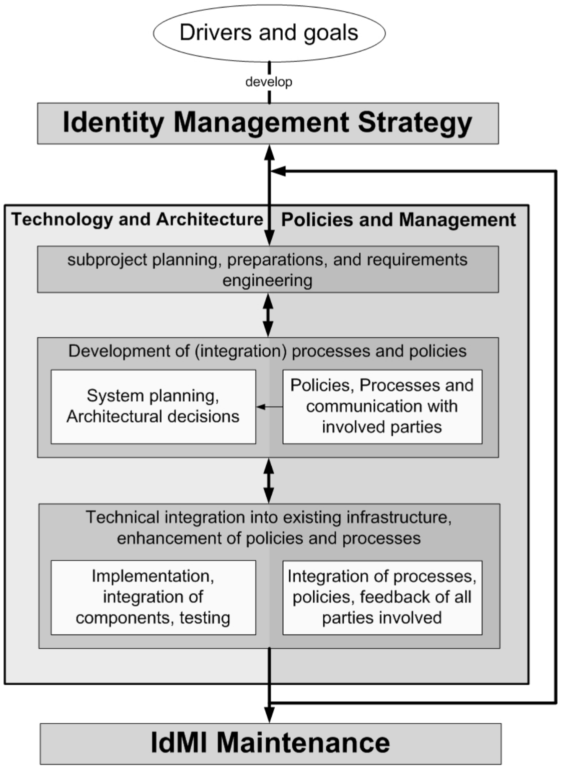
Drivers and goals
develop
Identity Management Strategy
Technology and Architecture
Policies and Management
subproject planning, preparations, and requirements engineering
Development of (integration) processes and policies
System planning, Architectural decisions
Policies, Processes and communication with involved parties
Technical integration into existing infrastructure, enhancement of policies and processes
Implementation, integration of components, testing
Integration of processes, policies, feedback of all parties involved
IdMI Maintenance

Figure 3. Structured Approach for IdM

During one subproject it is likely that the implementation team has to loop back and refine previous work after coming up against problems. If e.g. throughout step 3 the project team realizes that needed policies haven't been defined in the development phase (step 2), they have to go back, create the policy, and complete the remaining tasks of step 2 for this policy. After successfully completing one subproject the new module enters the IdMI Maintenance in which administrators have to deal with everyday's issues such as fixing minor bugs, adding some functional extensions (like scripts) or adapting the module to new hardware devices.

4.2. The Identity Management Strategy

One special characteristic of Identity Management projects is their strategic, trans-organisational alignment crossing the boundaries of single IT-systems. This integrative orientation enforces the existence of a global Identity Management Strategy that has to be developed before the individual components can be deployed. This strategy defines the sequence of implementation, the structure of the IdMI, and has to provide a stable organisational environment and commitment for the project itself. Besides general definitions, business and technical drivers together with the associated goals interact with the Identity Management Strategy. This way factors that are gaining more and more importance within the company influence the organisation's IdM goals and the global long term strategy. The current movement within risk management and governmental regulations e.g. requires comprehensive auditing and controlling capabilities within the IdMI. Therefore, the organisation might have to change the implementation sequence, introducing an auditing module earlier, and postponing the implementation of a SSO component. In general, the presented functional modules of an IdMI as seen in figure 2 have to be analysed for how they could assist in order to reach the current Identity Management goals.

4.3. Subproject planning, preparations, and requirements engineering

The first step of a subproject affects both, the management and the technical side of Identity Management in the same way. One key task is to define the scope of the subproject technically and from a business point of view and thereby frame which goals have to be achieved within this iteration. Basic preparations include the appointment of a project team and allocation of responsibilities. The requirements for the actual subproject are defined according to potential previous iterations and the overall system and process architecture which is specified in the global Identity Management Strategy.

The most important task in step 1 is to bridge the gap between the long term strategy and the short term project work. In our use cases this first process-step also included tasks like setting up contact with vendors of IdM solutions. On a technical level this helps the IdM team to get to know the capabilities of available solutions. While tasks like the allocation of responsibilities and the listing of affected policies are mainly located on the management side, staff responsible for the technical issues has to make a list of all information systems that are affected during the actual iteration. Possible interdependencies between other active process loops have to be taken into consideration. Looking at step 1 from the information security perspective leads to tasks like defining the possible risks related to the current subproject, i.e. which new security issues arise, which risks can be minimized or at least are reduced by the module that is to be implemented. The management side has to figure out business risks, while technicians have to deal with security risks that stem from the module integration, the potential usage, and exchange of identity data among connected IT systems.

4.4. Development of (integration) processes and policies

After the subproject planning has been finished, integration processes, new IdM related processes, and policies have to be developed in the next phase. The main goals of this step are the refinement and transformation of the results from step 1 in order to bridge the gap between high-level subproject goals and the actual software implementation. The organisational basis for step 3 is set up by concretising requirements, analysing the actual processes and policies, re-engineering, and documenting them subsequently.

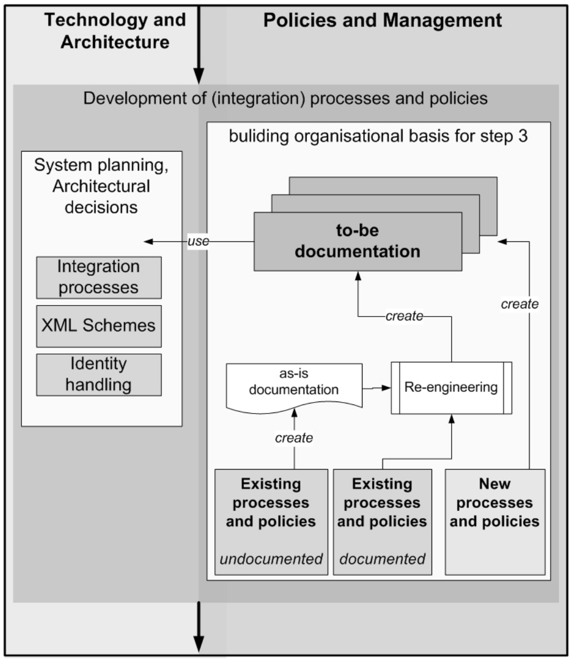
Technology and Architecture
Policies and Management
Development of (integration) processes and policies
buliding organisational basis for step 3
System planning, Architectural decisions
Integration processes
XML Schemes
Identity handling
use
to-be documentation
create
create
as-is documentation
Re-engineering
create
Existing processes and policies
undocumented
Existing processes and policies
documented
New processes and policies

Figure 4. Developing the organisational basis for an IdM module

Figure 4 particularises the second step of a subproject and shows the different kinds of process and policy states that organisations face: Undocumented, documented, as well as new processes and policies that have to be defined and enforced in the context of IdM. Knowledge about existing processes and policies that are undocumented has to be made explicit in an *as-is documentation*. Afterwards a *re-engineering* phase tries to optimise the current state and generate the *to-be documentation* which is needed for further technical system planning and architectural decisions. These tasks require communication on the organisational side of the project while the definition of integration processes that structure the linkage between the new component and existing systems, is a mainly technical issue. Such architectural decisions and basic system planning has to be conducted in order to ensure a seamless integration of the new Identity Management module into the existing IT-infrastructure. An enterprise directory e.g. has to maintain bidirectional communication channels with each connected subsystem. For the exchange of identity information XML schemes usually have to be developed as different attributes are normally called or spelled differently throughout the involved systems.

From an organisational point of view, the IdM team has to figure out how existing policies are affected by the new component and which new policies have to be defined during its implementation. According to the requirements given, all involved parties, i.e. not just the management, have to agree upon a consistent definition, the scope of each policy and the point where it is enforced. The processes and policies that are created form the basis for enforcing security measures and therefore reducing the risks and getting compliant. One policy could e.g. require that the currently implemented provisioning system has to log all administrative activities regarding account creation, maintenance and termination and store the information within a separate database. This has to be defined by the management but enforced by the module in question. Hence an issue of major importance in step 2 is the interaction and the collaboration of the technical and the organisational pillar.

4.5. Technical integration into existing infrastructure, enhancement of policies and processes

Technically spoken, step 3 represents the actual functional enhancement of the IdMI. In the previous steps the project team has defined how and where identity information has to be synchronised or provided for the new module and where new policies and processes have to be implemented. Therefore, the main technical task of this step is testing the component and ensuring the seamless integration into the existing IdMI. A test environment in which the new functionality can be reviewed in detail has to be set up. In addition to that, a roll-back plan has to be developed to ensure business continuity. This task is of paramount importance, because the management support for the Identity Management itself is going to decrease in case of dysfunction of the IdMI and even faster decrease if the users cannot continue with their everyday's work.

On the organisational side the technical integration is accompanied by a process and policy adaptation. It is of major value that not just the functionality of the productive IT-Systems is ensured. In addition, the affected business processes also have to be reviewed for further enhancement in terms of Business Process Re-engineering. The IdM team has to communicate with stakeholders (end users, administrators, etc.) in order to get feedback if the new functionality is accessible and works properly. Furthermore, the project team needs to check if all implemented security policies are fully enforced. This can be done by investigating audit logs or identity data within the repositories. Step 3 is closely related to the following IdMI Maintenance phase. After one subproject is finished, the new component enters the maintenance phase and needs to be monitored for potential problems and enhancements.

4.6. Practical experiences

After investigating the IdMI implementation process, this chapter closes by presenting some practical experiences. Our project work has shown that it is e.g. a quite common situation that different subprojects of our model coexist. During testing and setting up connections between data repositories as part of the meta-directory roll-out, the IdM team already was dealing with the implementation of a provisioning component. Nevertheless, it seems rational to take interdependencies between single functional modules into consideration when planning an Identity Management roadmap. We found it very useful to start an IdM project with the introduction of a global user repository which stores identity data of all employees. Currently one industrial partner is following the proposed approach and working on the second iteration of the model after completing the roll-out of a meta-directory. During the first iteration of the model suboptimal user management became obvious. We experienced e.g. certain ignorance for the documentation and re-engineering of existing processes in the context of IdM. However, it is of paramount importance to have a reliable process and policy documentation before the actual implementation of an IdM module is carried out.

5. Conclusion

The paper contains a structured approach for in-house IdM. It is our goal that this approach develops to some reference model which could help analysts and parties involved in IdM projects to better plan and structure their efforts. In general, an IdMI is implemented with the global aim to get compliant and reduce risks during user handling. Nevertheless, many organisational problems slow down the development of a comprehensive IdMI. Applying our reference model and considering the managerial as well as the technical aspects helped to better organise future work and delegate sub-tasks to persons in charge. From our experiences we know about the applicability of the proposed approach, but it turned out that following it is an intensive and time-consuming "political" task in an organisation as different stakeholders have to agree upon standardized workflows.

Focussing on information security and compliance, this paper has shown the importance of in-house IdM. The introduction of a global user directory at one project partner led to the identification and deletion of numerous orphan accounts. Centrally available and consistent user data now gives administrators an overview over all the electronic identities independent from different naming conventions in the connected sub-systems. This was a big step further because the initial situation with local identity silos made it impossible to bring together information about the users' accounts in an automated way. No one within the company was able to present a list of an employee's accounts in order to give evidence about his access rights within the IT systems. Obviously, this situation didn't comply with the mentioned legal regulations. Our project partner is currently working on the roadmap for integrating global provisioning into the IdMI. For future work we will monitor our user partner's IdM implementation closely. Several studies are scheduled to assure ongoing compliance. Investigating the implementation of role-based user administration will be the main aspect of our future work. Especially the process of role-development is going to be researched in detail.

References

[1] Paul S. Sarbanes and Michael Oxley: *Sarbanes-Oxley Act of 2002 (Pub. L. No. 107-204, 116 Stat. 745).* Available: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf (2002).

[2] Bank for International Settlements: *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework*. Available: http://www.bis.org/publ/bcbs128.pdf (2006).

[3] Federal Office for Information Security (BSI): *IT-Grundschutz*. Available: http://www.bsi.bund.de/english/gshb/index.htm (2004).

[4] European Union: *Directive 95/46/EC of the European Parliament and of the Council. Journal of the European Communities 23.Nov.1995 No L. 281 p. 31.*. Available: http://www.cdt.org/privacy/eudirective/EU_Directive_.html (1995).

[5] Jeffrey M. Stanton, Kathryn R. Stam, Paul Mastrangelo, and Jeffrey Jolton: *Analysis of end user security behaviors*. Computers & Security 24(2): 124-133 (2005).

[6] David F. Ferraiolo, Richard D. Kuhn, and Ramaswamy Chandramouli: *Role-Based Access Control*. Artech House computer security series, ISBN 1-58053-370-1 (2003).

[7] D. A. Buell and R. Sandhu: *Guest Editors' Introduction: Identity Management.* IEEE Internet Computing, vol. 07, no. 6, pp. 26-28 (2003).

[8] A. Pfitzmann and M. Köhntopp: *Anonymity, unobservability, pseudonymity, and identity management – a proposal for terminology*. Lecture Notes in Computer Science, Volume 2009, Springer, Heidelberg (2000).

[9] M.P. Gallaher, A.C. O'Connor, and B. Kropp: *The economic impact of role-based access control.* Planning report 02-1, NIST, Available: http://www.nist.gov/director/prog-ofc/report02-1.pdf (2002).

[10] R. S. Sandhu, E.J. Coyne; H.L. Feinstein; C.E. Youman: *Role-Based Access Control Models*. IEEE Computer 29(2): 38-47. IEEE Press (1996).

[11] Charles P. Pfleeger and Shari L. Pfleeger: *Security in Computing*. Third Edition, Prentice Hall: Upper Saddle River, NJ, ISBN 0-13-035548-8 (2003).

[12] E. Axel Larsson: *A Case Study: Implementing Novell Identity Management*. Proceedings of the 33rd annual ACM SIGUCCS conference on User services. November 6–9, Monterey, California, USA (2005).

[13] Gurpreet Dhillon: *Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns*. Computers & Security, Volume 20, Issue 2, Pages 165-172 (2001).

[14] Marco Casassa Mont, Pete Bramhall, and Joseph Pato: *On Adaptive Identity Management: The Next Generation of Identity Management Technologies*. Tech Report: HPL-2003-149, Hewlett-Packard Laboratories Bristol (2003).

[15] Organization for the Advancement of Structured Information Standards (OASIS): *Service Assertion Markup Language (SAML)*. Available: http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip (2005).

[16] Organization for the Advancement of Structured Information Standards (OASIS): *Service Provisioning Markup Language (SPML)*. Available: http://www.oasis-open.org/committees/download.php/17708/pstc-spml-2.0-os.zip (2006).

[17] Ann West: *Identity Management Systems: Components and Constituents*. Available: http://www.nmi-edit.org/roadmap/dir-roadmap_200510/index-set.html (2005).