Sanna Virkkunen

A GUIDE FOR REQUIREMENT SPECIFICATION OF IDENTITY AND ACCESS MANAGEMENT IN HEALTH CARE

A GUIDE FOR REQUIREMENT SPECIFICATION OF IDENTITY AND ACCESS MANAGEMENT IN HEALTH CARE

Sanna Virkkunen
Master’s thesis
Spring 2014
Degree Programme in Information Technology
Oulu University of Applied Sciences

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Information Technology

Author: Sanna Virkkunen
Title of thesis: A Guide for Requirement Specification of Identity and Access Management in Health Care
Supervisor: Teemu Korpela
Term and year of completion: Spring 2014 Number of pages: 79

The object of this Master's thesis was to describe the basic functionalities provided by identity and access management system (IAM) and their suitability for a health care environment. Specifying and defining the IAM project began in the Northern Ostrobothnia Hospital District in 2007. The preliminary work for enabling identity and access management automation has been done ever since. Most of the requirement specification work was done during the autumn 2013 for the IAM SSO project in the Northern Ostrobothnia Hospital District.

The work consisted of studying various aspects of identity and access management and also analyzing the current state and describing the target state. The studying process consisted of understanding and describing authoritative requirements of IAM in health care, discovering the special features of IAM in Finnish health care and defining the basic IAM use cases in health care.

The result of the study was that identity and access management processes should be guided with strict working period or service period information. They are the master data for both internal and external users. They can be used to define user rights, access rights and their active and inactive periods. The quality of the master data affects the whole IAM process. Attaching smart cards to AD enables network and domain login but also managing complicated multi-role identities.

IAM is a never-ending process. After critical and key systems have been integrated to an IAM system, there will always be yet another integration to be built. New information systems will be deployed and they need to be integrated to the IAM system. The legislation changes all the time, and the organization structures will also change from time to time. All these affect IAM processes and the functionalities of the IAM system. A properly maintained IAM system will help dealing with the changes.

Keywords:

Identity management, user rights management, access management, provisioning, master data, access control, health care system

CONTENTS

TERMS AND ABBREVIATIONS

ABAC	Attribute-Based Access Control
ACL	Access Control List
AD	Active Directory
APM	Active Perso Manager
DAC	Discretionary Access Control
EHR	Electronic Health Record
ESB	Enterprise Service Bus
eSSO	Enterprise Single-Sign On
HIS	Hospital Information System
HR	Human Resources
IAM	Identity and Access Management
IDM	Identity Management
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
NOHD	Northern Ostrobothnia Hospital District
PRC	The Population Register Centre
RA	Registration Authority
RBAC	Role-Based Access Control
RIS	Radiology Information System
SOA	Service-Oriented Architecture
UPN	User Principal Name attribute
VPN	Virtual Private Network

PREFACE

This Master's Thesis was made for the Department of ICT Management in the Northern Ostrobothnia Hospital District (later referred to as NOHD). Thesis materials will be used to further develop the identity and access management system and processes in the area of Oulu University Hospital's special responsibility. The aim of this thesis was to describe the process of designing an identity and access management project as well as writing a requirement analysis for an identity and access management system in health care environment. This work was made to deepen the knowledge in identity management technologies and processes at my work Department of ICT Management in the Nothern Ostrobothnia Hospital District as an IAM SSO project manager. The thesis was created after office hours during the autumn 2013.

I would like to thank Mr. Pekka Mattila, Planning Manager of Northern Ostrobothnia Hospital District for enabling this thesis work and supervising it on behalf of NOHD, Mr. Teemu Korpela, Lecturer of Oulu University of Applied Sciences, for acting as a supervising teacher and Ms. Kaija Posio for acting as a language instructor. I would also like to thank my colleagues for the information and support given during the process. Finally, I would like to thank my husband Heikki and my family for arranging me enough time to accomplish my studies.

Oulu, Finland, January 2014
Sanna Virkkunen

1 INTRODUCTION

1.1 Prelude

Identity and access management (IAM) is not a new thing in industrial world. Managing access in different software has been available from the first second the software programmers created user names and passwords to the software. Identity management means managing digital identities – their roles, rules and groups through their entire life cycle. Identity and access management itself can be a manual or an automated process. IAM processes have been made to protect organizations from threats coming from inside and outside.

Identity and access management has not been systematically organised at different platforms until recent years. Identity and access management projects have had a bad reputation due to a high failure rate. Projects have exceeded their budgets, as well as their schedules. In the worst cases the identity and access management software has never been ready for deployment. The reasons for this have varied from forgetting the HR point of view in the project to clumsy IAM systems. However, a successful IAM project improves the security and productivity in the whole organization as the costs in managing users and their attributes and credentials decrease. Systemizing identity management processes by using a sophisticated, agile IAM system can decrease costs of access management, control risks in identity management and make access rights processes less time-consuming.

Identity and access management in health care is usually a widely spread and mostly manual process across the whole organization. This makes it inefficient and uncontrolled, albeit the information processed in health care information systems is deeply confidential by nature and should be kept highly secure according to the law. It is impossible to create a flawless identity based log file without a proper IAM system. Typically it takes several work months per year to create and maintain user rights manually for every occasional short-term employee, medical student and substitute in a health care organization. External users cause yet another issue for access management processes.

The Northern Ostrobothnia Hospital District (NOHD) owns and operates three different hospitals: Oulu University Hospital, Oulaskangas Hospital and Visala Hospital. The preliminary analysis of

IAM was started at NOHD’s ICT development unit in 2007. The preliminary work for enabling an identity and access management automation has been done ever since.

Oulu University Hospital represents all medical specialities and is the centre of special responsibility area in Northern Finland. All five northern hospital districts have been collaborating with identity and access management for several years. This collaboration has been valuable giving a possibility to gain knowledge and support from each other working on the same substance. This thesis focuses on creating a safe requirements analysis which will be suitable for the identity and access management needs of most health care organizations in Finland.

1.2 Roadmap for developing identity and access management in health care

Developing an identity and access management roadmap is necessary for the organization to deploy the organization-wide system successfully. As can be seen in Figure 1, the roadmap will help to see the overall picture of strategic requirements more clearly as well as to avoid pitfalls. It is easier to determine whether the IAM system will be deployed before the eSSO or vice versa after developing the roadmap thoroughly. In NOHD it was decided to deploy the IAM system first. This decreases the amount of time needed for user training concerning the eSSO system for each user. There are some prerequisites for the health care organization before the IAM development can begin. For example, the organization should have an enterprise architecture description and smart cards in use or at least distributed to the staff.

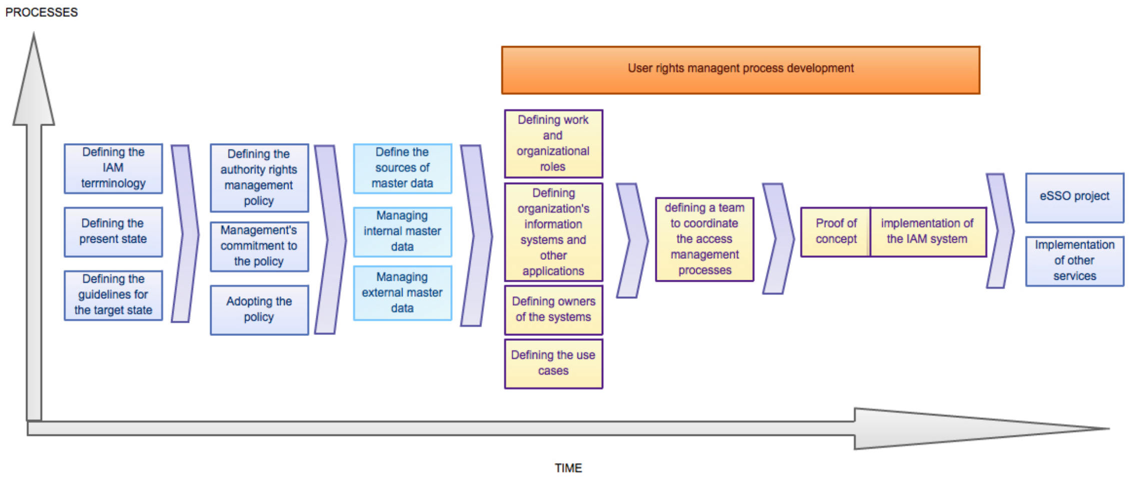

PROCESSES
User rights managent process development
Defining the IAM terrminology
Defining the present state
Defining the guidelines for the target state
Defining the authority rights management policy
Management's commitment to the policy
Adopting the policy
Define the sources of master data
Managing internal master data
Managing external master data
Defining work and organizational roles
Defining organization's information systems and other applications
Defining owners of the systems
Defining the use cases
defining a team to coordinate the access management processes
Proof of concept
implementation of the IAM system
eSSO project
Implementation of other services
TIME

FIGURE 1. Example of a roadmap (Virkkunen Sanna, 2014)

A roadmap development will begin by learning and defining the terminology used in identity and access management. Understanding the terms used within the substance is essential for a successful project. After this step it is important to clarify the present state and define the guidelines for the target state.

The next step is to define the authority rights management policy for the organization. This is the very basis for all identity and access management procedures and decisions within the organization. The policy has to have a full support from the management of the organization. Adopting the policy can be initiated right away even without the IAM system.

The next step is to manage the personnel master data. This has to be initiated by defining the sources of the master data. Inconsistent raw data has to be noted and the lack of information has to be fulfilled. The master data management has to be done both for the internal and the external users.

After the master data has been properly maintained and the data is consistent, the development of user rights management processes can begin. This includes role mining, defining work and organizational roles, sorting the information systems and their system roles used in the organization, defining the owners of the systems and otherwise collecting data and preparing the organization to function in a way determined in the authority rights management policy. The collected information should be entered to the IAM system.

Typically developing the user rights management process will be done during the implementation of the IAM system. After this the most critical target systems should be integrated to the IAM system. When prioritizing the target systems the highest priorities are the information systems of higher operational, financial or juridical risks. (33, p.6.)

If the organization does not have an access management team, it should be defined and deployed. The access management team consists of system administrators and the team coordinates all the access management processes in future.

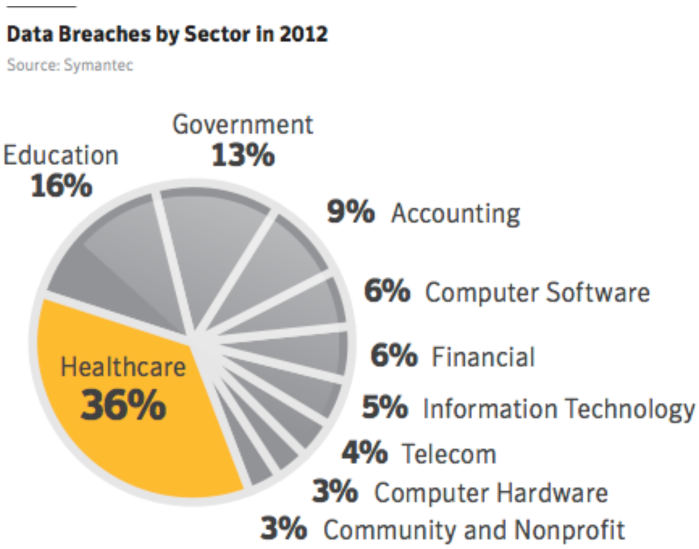
The next step is to have a proof of concept in one organizational unit. This will highlight possible issues within the process. It will also be a good practice for system administrators of the new operations model. After this a full implementation of the IAM system and a user training of the system can be started organization-wide.

After the IAM system has been implemented throughout the whole organization, the integration work still continues. More target systems have to be integrated and there may be a need for acquiring an eSSO system. Also other services such as federation can be implemented. In addition reconciliation and role-mining are continuous processes to be done every once in a while.

2 IDENTITY AND ACCESS MANAGEMENT IN HEALTH CARE

2.1 Drivers for using identity and access management in health care

U.S. Department of Defense (The IP Commission) estimated that the losses as a result of an international intellectual property theft amount are $300 billion annually in the United States only. (1). According to Gartner the size of global IT market was $3,7 trillion in 2013 (2) and $67,2 billion of that has been spent on information security globally (3). According to Remes (4) in context of illness, cybercrime is already costing economically more than U.S. wars and almost as much as drug trafficking annually. In addition, according to Symantec's analysts, there were 1,1 billion stolen identities in 2011. Health care industry has 36% of disclosed data breaches by industry (5) as shown in the Figure 2. These examples demonstrate how important it is to have security policies and processes updated in real time by investing in security.


Data Breaches by Sector in 2012

Source: Symantec

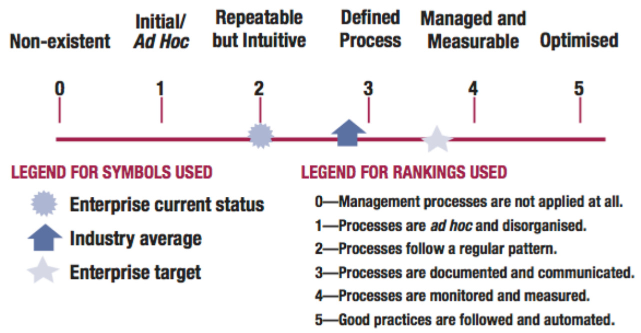
FIGURE 2. Data Breaches by Sector in 2012 (5, p. 18)

To gain from a functional identity and access management in an organization, the deployment project has to have a full support from the corporate management. Ministry of Finance has published several principles and guides, for example Vahti 9/2006 document "Käyttövaltuushallinnon periaatteet ja hyvät käytännöt" (6). This document can be used as a baseline for authority rights management policy. Authority rights management processes stand for all functionalities concerning user management, user rights management and maintenance of authority rights. An organization has to have authority rights management policy that covers both principles and methods for authority rights management. This document is a part of organization's security policy, which also has to be utilized within the organization. (7.)

The identity and access management system can simplify the access management processes in health care in many ways. It will bring predictability and up-to-date information to the processes. As mentioned before, systemizing identity management processes by using an IAM system can decrease the costs of access management, control risks in identity management and make access rights processes less time-consuming. The time used for restoring forgotten user credentials will decrease with the help of self-service user interfaces. Due to the master data, the same user information will be stored only in one place and the IAM system will take care of synchronizing the data with other systems. This reduces the workload needed for maintaining the user data. Using the IAM system can also open up new possibilities for developing business models. Using the IAM system enables to centralize the access management administration. This will reduce the workload in the organization units. (26, p.7-8) Also, organizational changes will be easier to deploy in information systems because the organizational structure will be maintained in the master data system.

2.2 Identity and Access Management project

An IAM project typically begins by analyzing the present state. The present state has to be clarified and audited and the arising issues need to be sorted out. There needs to be a clear vision for the future state, which can be used for defining the preliminary roadmap. In each of the steps the progress needs to be observed from the method of administration and policies, processes and organizational habits, architecture, systems and information model point of views. Because the progress is so profound dealing with many aspects of the information management and the organizational management, some maturity tests can be done to define the maturity level. For example COBIT Process Assessment Model (Figure 3) has some sections concerning identity and access management.



0—Management processes are not applied at all.
1—Processes are *ad hoc* and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

FIGURE 3. Graphic Representation of Maturity Models (8, p. 18.)

Identity management is a comprehensive progress with the need to develop many sectors at the same time. The identity and access management system can be seen as a common service provided to all information systems and software, but also to other systems such as passage control or meal payments. Integrating the IAM system demands lots of technical and administrative work but also good communication skills. There will be many interest groups and none of them can be forgotten. The IAM process itself penetrates through the entire organization and all organizational units. To implement this new process successfully, the employers of the organization have to have enough knowledge of the IAM process. This means the IAM responsibilities have to be known – not only in HR and ICT units but all around the whole organization. This can be done via a good IAM education during the IAM project rollout. Typically, this kind of development program lasts from three to five years, which itself causes challenges. The best way to gain good results is to focus on big and easy wins instead of sticking into small exceptions. (9.)

2.3 Authoritative drivers for using IAM in health care

The patient data is considered as confidential, sensitive information. The mere information of an individual being a patient is considered secret. Health care professionals or other persons working in a health care unit are not allowed to give patient information to outsiders without a patient's written consent. The secrecy obligation remains in force even when the employment relationship is over. (10, 13.)

Identity and access management has a big role in the security and confidentiality of health care systems. The Decree of the Ministry of Social Affairs and Health on patient records claims that each individual employed in health care and each user of an electronic patient record has to have access rights that are being defined according to the current role of the individual. According to the decree each user has to have only the access rights that are needed for the job. As mentioned in Kanta Auditing requirements, access rights have to be maintained for example with an access management system. (13,12.) The decree also claims that all the users of the patient information systems need to be identified and recognized in a way that users are verified unambiguously. In other terms it is a necessity to use digital certificates in Population Register Centre's (later referred as PRC) smart cards for health care when using any patient information. (11.)

At the moment smart cards for health care should be used in a Finnish health care organization at least by the health care professionals who will use the information available in Kanta Patient Records Archive. It would be convenient to use smart cards even more widely. At the moment the Population Register Centre provides smart cards for every employee working in a health care organization. This is the case in Northern Ostrobothnia Hospital District where smart cards have been given to all employees. Using smart cards for authentication when logging in the organization's domain will save time and increase the security of the process. The PRC also offers Fujitsu Oy's mPollux DigiSign Clients free of charge to health care organizations and to all the users who have a certificate issued by the PRC. DigiSign Client is a card reader software that can be used with Windows, Linux and Mac OS X. (12.)

Using smart cards together with an enterprise Single Sign-On (eSSO) system will reduce the memory load needed from the user. With eSSO it is not necessary for the user to remember user credential information any more. The smart card certificate with the user's pin code will be the only things the user needs to use in health care information systems, e.g. an electronic patient record EPR. It is justified to develop the technological environment in health care to fully support the use of smart cards.

Kanta Patient Records Archive auditing requirements claim the management of user rights in a health care information system concerning electronic prescription data has to be done with an external system. Also, all the user rights and changes done to the user rights have to be logged. (13, 12.)

All these qualifications and claims mentioned above have to be considered and required in the process of developing identity and access management system in health care. The amount of different health care information systems is huge. For example, in Oulu University Hospital there are almost 150 different information systems. All of them have separate user databases including user accounts, user roles and passwords although some federation occurs. The vast amount of computer systems is about the same in every health care organization, small health care centres being the exceptions.

2.4 Identity management challenges in health care

As mentioned earlier, in a health care organization identity management is widely spread. In some cases this is the case because of the need to secure the core task in health care – taking care of and nursing patients. The patient work cannot be endangered in any situation, the least because an employee does not have the user rights for the information system needed. In some cases identity and access management is spread because of the lack of access governance and policies. In rare cases this is due to the lack of information in the organization.

In a health care organization there are many users, many different roles, partners, customers and vendors that need to be taken care of. Alone in Oulu University Hospital there are 6,800 employees, of which there are 4,600 full-timers, part-timers, fixed term employees and inside substitutes. In addition, there are students, apprentices, civil servants, temporary workers, researchers and other externals. Each of these groups has to be observed thoroughly to find out specific criteria, characteristics, patterns and possible links in them.

Identity and access management in health care also covers several different target systems and archives: portals, local area networks, e-mail system, remote accesses, as well as operative systems and services for outside customers. There are also different operational environments analyzed by a user directory or a technical platform. In addition to the network infrastructure some of the browser or client-server-based systems leverage organization's AD directory. Some systems can leverage the AD directory and also their own internal structure for user authorization. Some browser-based and client-server-based software use only system's own internal user accounts and access management as data structure. (14, p.5.)

As mentioned in FINeID, there are several types of health care smart cards: a smart card for regulated health care professionals, a smart card for non-regulated health care workers, a smart card for non-clinical health care sector staff and a replacement card for health care sector staff

(15). To attach the PCR's health care smart cards to Active Directory to enable network and domain login using health care certificates, the Finnish Population Register Centre's root certificates have to be installed in the trusted CA's (root certificates) list. In addition, the certificate on the smart card has to be linked to Active Directory. This can be done linking the user's User Principal Name (UPN) attribute with the UPN suffix and the Valvira ID number mentioned in the certificate. The UPN is a unique ID that could be handy to use when identifying users and identities in the IAM system as well as in other information systems. In NOHD an Active Perso Manager software (APM) is used for linking the UPN during the card delivery process in the Registration Authority (RA) Office. The RA officer inserts the smart card into a card reader for the APM to read the contents of the certificate and link them to the AD. However, this task could be convenient to do with the IAM system if the IAM system has the ability to read a certificate content from a smart card.

Peculiar to health care substance there can also be many roles or even electronic identities for one individual. The same person can be a normal employee during the day, a practicing student during the evening and occasionally a private practitioner. The same individual can also appear several times in different user registries and databases. These different roles and also short employment periods make the health care environment challenging for identity management.
All the information gathered in health care information systems is confidential, but apart from that there is also information categorized as secret and specially protected. For example, information created in medical genetics department is secret to other health care departments. The same goes with psychiatric information. This specially protected, secret information has to be restricted to only specific users.

In health care operating environment there is also functional need for switching users rapidly when using workstations. This is even more significant in intensive care units and emergency units. In many places a rapid user switching is resolved using different virtualization techniques. IAM vendors should have understanding of the virtualization platform used in the organization. For example, in NOHD the virtualization is implemented using a Citrix platform in two ways: many software applications are virtualized using Citrix, and virtualized Citrix desktops are facilitating the use of workstations in a patient ward.

Finnish legislation requires that all the user rights in health care has to be maintained role based either within the health care systems or within an identity and access management system. A proper auditing of the health care information systems requires that a full reconciliation has to be possible and an audit trail is available. There also has to be a solid revision history of the events in user rights information. Using IAM systems makes identity management processes more efficient in all areas of the process: requesting the user rights, and also approving, rejecting and implementing or executing them. Using an enterprise-wide single sign-on system decreases the amount of remembering different user logins and passwords. In other words an identity management system project is one of the few projects in health care that actually reduces the amount of time the medical staff have to spend at the computers.

3 BASICS OF IDENTITY AND ACCESS MANAGEMENT

Identity management is an organization wide process. It includes controlling, modifying, accepting, declining and implementing all identity and user data. It also handles with self-service functions, work queues and maintenance services. One of the most important parts of identity and access management system functionality is to get a life-cycle management for all identities.

An identity is created to represent a person, an object or an entity that requires access to organizational assets. Assets can be information, technology or facilities and services. Managing these different identities in an organization requires that the persons, objects and entities are identified, registered and profiled. According to the CERT Resilience Management Model, an organization also has to establish a baseline identity community, from where to perform all the activities that are related to identity. This can also be called the master data system or database. Identity management process addresses the life cycle of identities for objects and entities and for persons who need some level of trusted access to assets. Identities are created so that they are made known to the organization. (16, p. 5.)

According to the CERT Resilience Management Model, there are two specific goals for identity and access management: to establish identities and to manage them. Establishing identities consists of three practices: creating identities, establishing identity community and assigning roles to identities. Managing identities consists of monitoring and managing identity changes, reviewing and maintaining identities periodically, correcting inconsistencies and de-provisioning identities. (16, p 107-108.)

Identity life cycle management is typically one of the key aspects of the identity and access management process. According to Buecker, Filip, Palacios & Parker (22, p.16) in addition to creating and deleting the user account there will be also changes to the account due to transfers, promotions, leaves of absence or management assignments. This is illustrated in Figure 4. However, a full-deletion of accounts in health care is often un-appropriate due to auditing requirements and legislation. This will be discussed later in section 3.7. Verifying the user account's compliancy with security and governance policies should be done routinely. The verifying policy should be mentioned in organization's authority rights management policy.

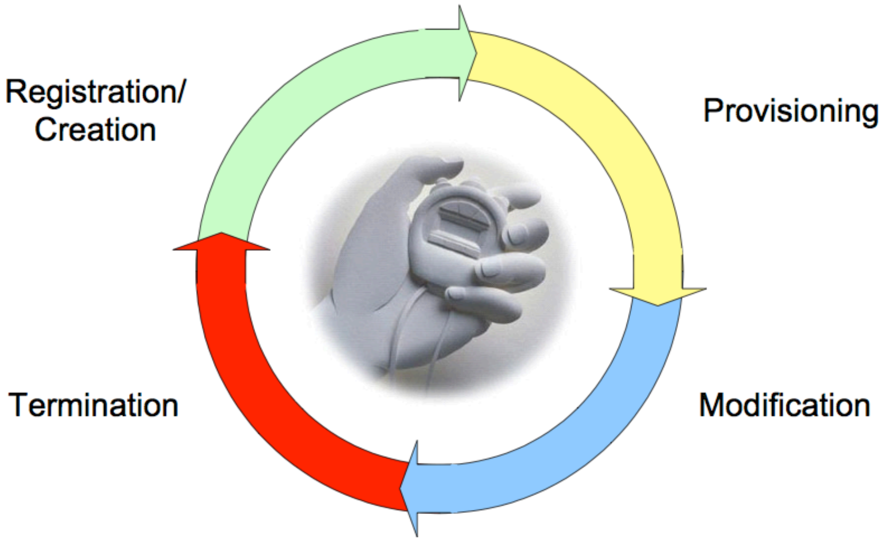


FIGURE 4. Life cycle management (22, p.17)

The IAM system should be a centralized user and access rights database integrated to many different target systems. In health care the variety of target systems is wide, and integrating e.g. legacy systems can be quite tricky. Typically, integrating is done by IAM system vendor's connectors also known as adapters. Identity and access management system should provide adequate tools for creating identities, managing their life cycles, controlling identity and removing user rights and logging and archiving all this information. The system should have comprehensive features for managing internal and external identities and users. Moreover the IAM system has to have automatic user rights provisioning system within. On the other hand the IAM system also has to support a manual provisioning of user and access rights when adapters or integration is not available. (14, p.8.)

When starting to develop IAM processes, many aspects need to be considered. At first a user environment has to be defined: what kinds of users are using the information? How different types of users get user and access rights to the systems? Also, it would be illustrative to measure the delivery cycle in different access rights processes. The appropriate approval of user rights has to be ensured. Characteristic to many organizations using IAM processes the removal of user rights is often neglected. User rights have to be removed or at least inactivated after the contract-based relationship to the organization has ended or the job responsibilities have changed. Also, documentation is needed to describe what kinds of user rights each role and individual has to have to be able to work in that role. (9, part 3.)

Four different identity and access management basic processes have been acknowledged:

1. Information systems' user rights definitions and their life cycles have to be managed.
2. Organization operative structure and organization job roles involved have to be up to date. There has to be a way to maintain and manage the organization structure all the times.
3. Identities and user and access rights have to be managed.
4. Identity management processes have to be reported and audited. (9, part 3.)

Identity management can be roughly divided into user rights management, access management and provisioning. The best practice for user rights management is a role based access control. Each user has organizational roles depending on the organization the user is part of. The user also has business roles or work roles depending on the tasks the user is performing daily. The user can also have dynamic roles, e.g. "superior" or "super user." Most of the tasks concerning user rights management automation can be done based on these rules. However, also additional attributes are usually used. Digital identity involves all these rules, attributes and other user information.

3.1 Master Data Management

Identity and access management cannot function without a comprehensive master data management. Master data is the place where the identity of the person is officially created and maintained. In a hospital the identity management master data consists of the personnel's, customers', students' and vendors' basic data. It can be data collected from HR systems but is often scattered in different information systems. Master data is typically constant information, such as name and address data, location, department, direct supervisor information, a unique identifier for the identity and information concerning the organization structure. It can be used for example in ERP systems. Master data has to be integrated to the target systems with e.g. identity and access management system. Master data helps restricting the access of the employee only to the information that he / she needs.

Different identities must be registered and profiled to become part of the organizational community. The information that defines an identity is called the identity's DNA. A registration process occurs when a new employee is hired to the organization. This process includes defining employee's role and job responsibilities based on business requirements. A registration process can also occur when an existing employee's job responsibilities change. Because the organizational environment is changing all the time, the registration is continuous. (16, p.137-138.)

Registration procedures ensure that user's level of required authentication is consistent with the levels of access available to the user. The task of identifying and registering users include the accurate capture of a user's identity, professional credentials and job title and the assignment of an unambiguous user identifier. (32, p.36-37.)

Master data can be divided into two different categories: internal master data and external master data as shown in Figure 5. Internal master data is based on the fact that a person is employee in the organization. The employee has signed a contract of employment with the organization. The contract defines the title of the employee and the organizational unit the employee works in. The employment can be part-timed, fixed-term or permanent. When working in a matrix organization or in a different project, the person can have several managers. External master data is based on the fact that the organization has some kind of agreement or contract of the service provided between these two organizations. (16, p.138.)

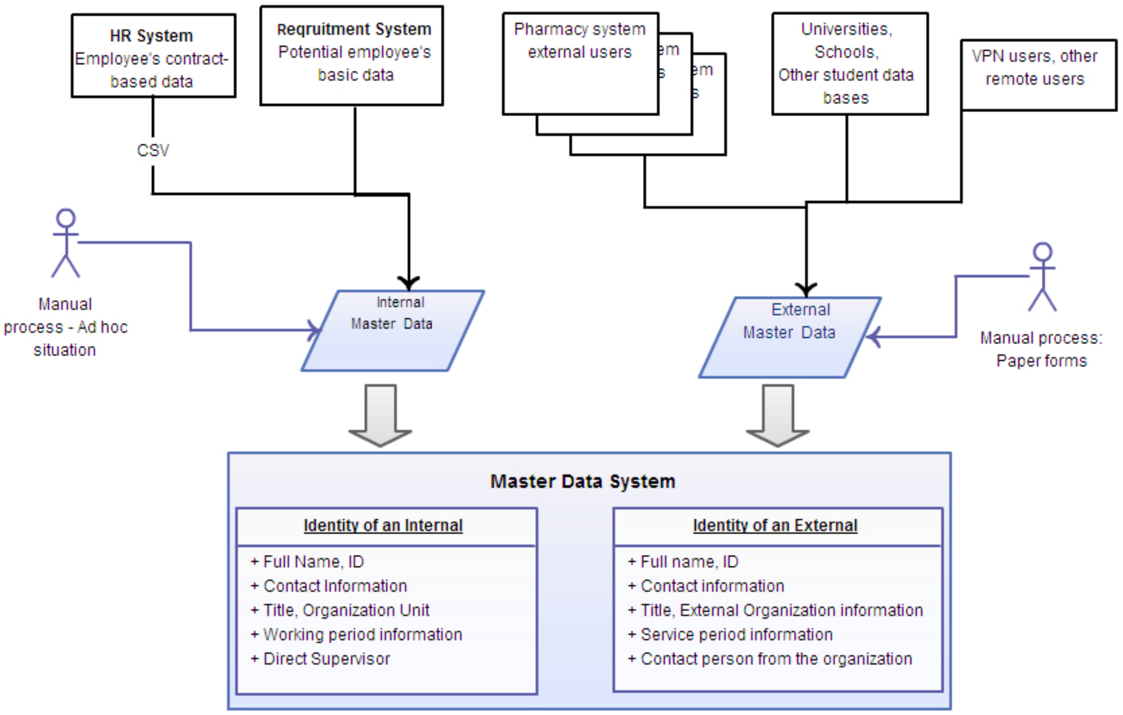

HR System
Employee's contract-based data
CSV
Reqruitment System
Potential employee's basic data
Pharmacy system external users
Universities, Schools, Other student data bases
VPN users, other remote users
Manual process - Ad hoc situation
Internal Master Data
External Master Data
Manual process: Paper forms
Master Data System
Identity of an Internal
+ Full Name, ID
+ Contact Information
+ Title, Organization Unit
+ Working period information
+ Direct Supervisor
Identity of an External
+ Full name, ID
+ Contact information
+ Title, External Organization information
+ Service period information
+ Contact person from the organization

FIGURE 5. Master Data.(Virkkunen, Sanna, 2014)

In a health care organization internal master data can be found in HR systems, recruitment systems, radiology information systems, other information systems and in some paper forms. Also, the health care certificates provided by the PRC contain master data. Depending on the organization, the internal master data can be found in a single database or information system or in several places. External master data is even more widely spread, e.g. in pharmacy systems, material management systems, in schools and universities for medicine and health care students and in different paper forms. In NOHD the master data has been gathered in a master data system.

Some health care organizations have a strictly centralized model for hiring and making contracts with the employees. This makes the master data track easy to follow. For example, in Kajaani Central Hospital the recruitment office is always involved when the organization unit is recruiting a new employee. In Oulu University Hospital the case is not always so simple because an employee can directly contact the head nurse who then personally hires the person. In this case it is possible, that the contract is created to the HR system even after the working period has finished. When this is the case, provisioning and other identity and access management automation is complicated. Every exception in the establishment of an identity creates a complexity to the IAM process. (17.)

The Master data system has to be integrated to other systems. The information coming from HR and other source information systems typically form a CSV file that will be read into master data system. The Master data system then stores the data. The Master data system can provide this information to other systems, too, e.g. identity and access management system. The crucial step is to trust only the information coming from master data. The route of the information is then cascade modelled, as seen in Figure 6. If the data in the master data system is biased, the whole identity process will be biased.

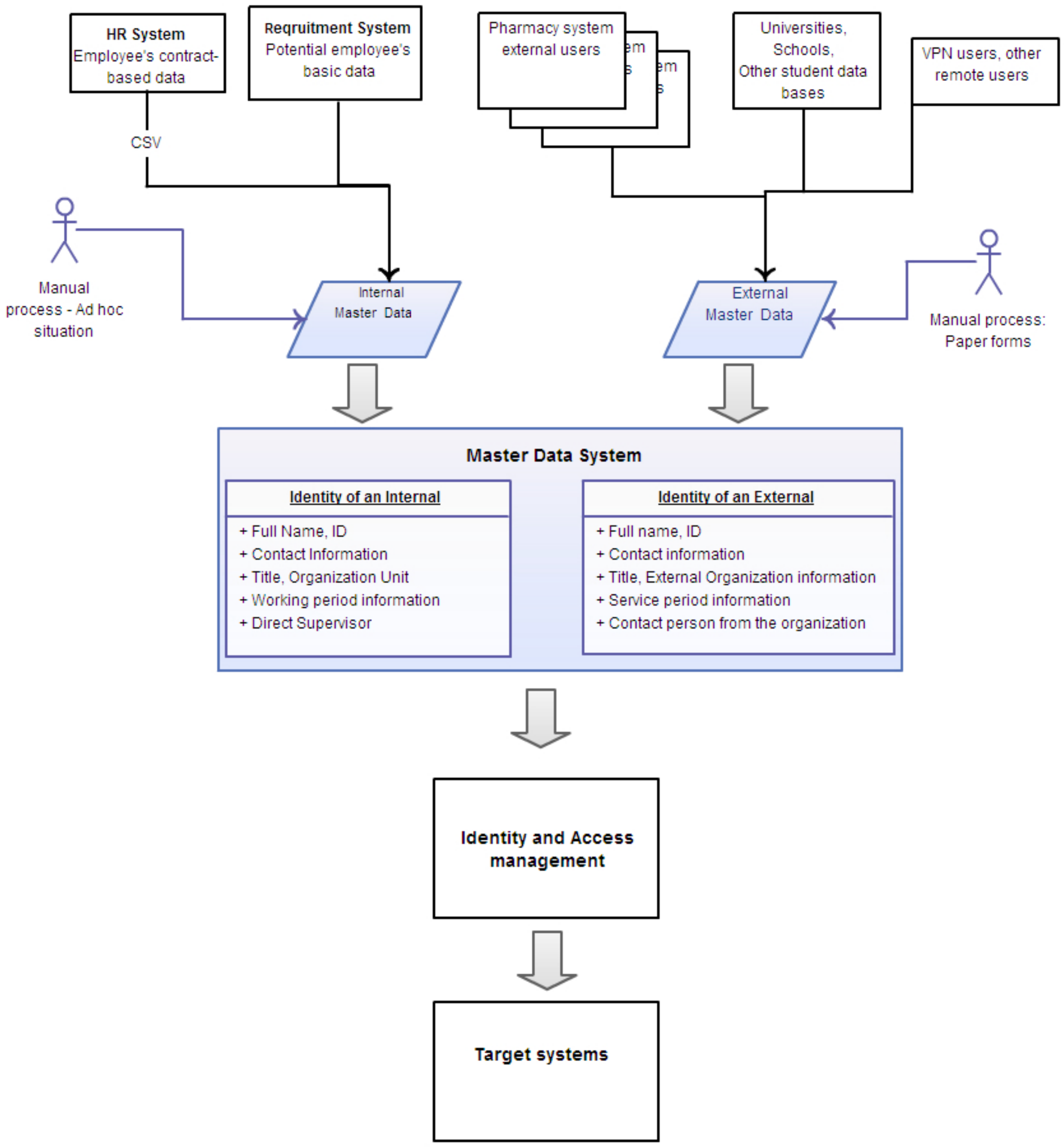

HR System
Employee's contract-based data
CSV
Reqruitment System
Potential employee's basic data
Pharmacy system
external users
Universities, Schools, Other student data bases
VPN users, other remote users
Manual process - Ad hoc situation
Internal Master Data
External Master Data
Manual process: Paper forms
Master Data System
Identity of an Internal
+ Full Name, ID
+ Contact Information
+ Title, Organization Unit
+ Working period information
+ Direct Supervisor
Identity of an External
+ Full name, ID
+ Contact information
+ Title, External Organization information
+ Service period information
+ Contact person from the organization
Identity and Access management
Target systems

FIGURE 6. Master data flow.(Virkkunen, Sanna, 2014)

3.2 User rights management

User rights management answers to questions like “Who am I?” “What rights do I have?” “What is the basis for my rights?” “Who has accepted my rights?” To gain a full functionality of user rights management, properly maintained and gathered master data is needed. User rights management means managing and controlling the internal and external personnel’s information and work assignment life cycles.

Some of the user rights have been pre-defined and automated according to organizational and business or work roles. These rights need to be verified and managed appropriately. Designing organization's roles is in fact the most time consuming task of the whole identity management project. The organization role is based on the fact that the employee works in an organization unit. Because of that, the employee is guaranteed to have some basic rights, for example a right to have a user account and e-mail in the organization, keys to the doors of the department and a nametag with the organization logo on it. Organization roles can also be even more sophisticated in correspondence with the system roles.

Work roles are based on employee's title and tasks in the organization. It is notable that the titles may vary even though the user rights based on the job description are the same. In a health care organization nurses may have access to different information than doctors. They also use different software in their work. The same goes with other occupational group, too. Physicists use calculation and analysis software that no other occupational groups do. In addition to organizational and work roles, there can also be dynamic roles to enhance the user rights. For example, some nurses have drug permissions that give them access to organization's medicine chest. Managing this situation can be done with dynamic roles. The same goes with a dynamic role "supervisor" that gives the user rights for approval and to use specific software. These predefined roles are illustrated in Figure 7. To discover the work roles, organizational roles and dynamic roles, role mining has to be done. More of this will be discussed later in section 3.8.

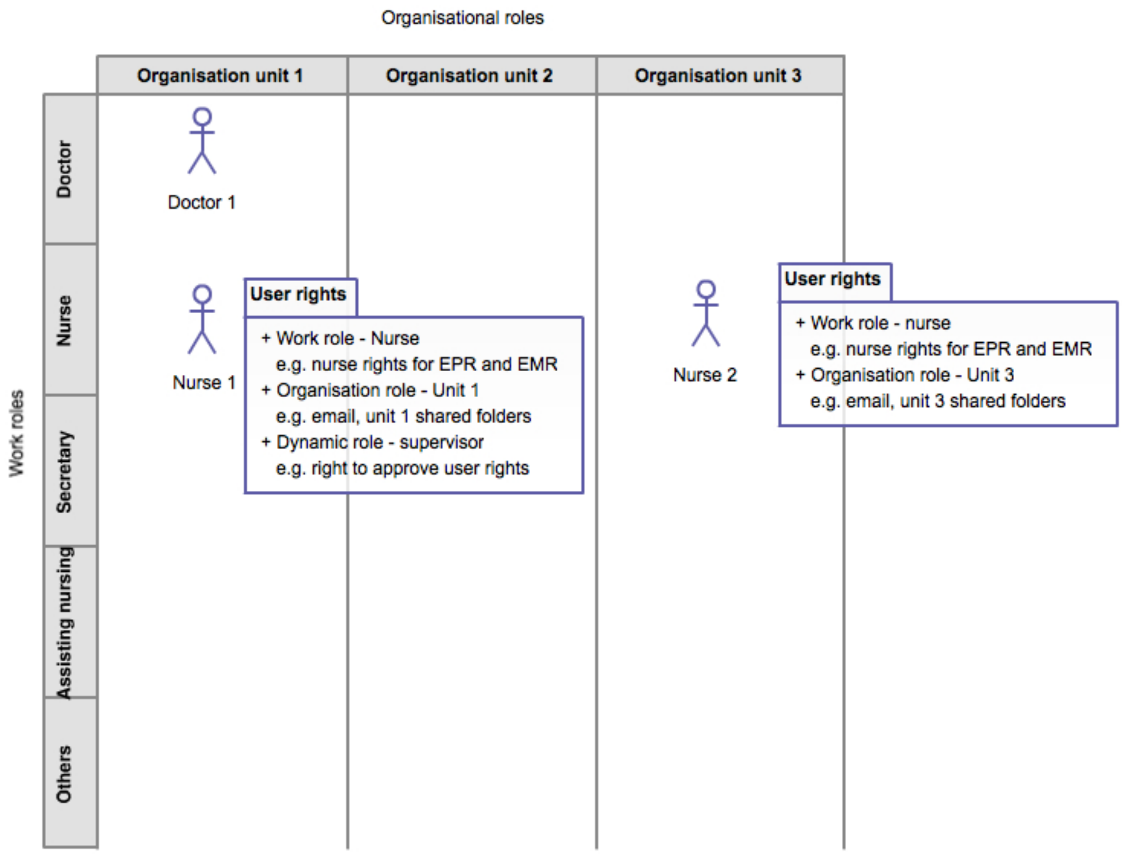

Organisational roles
Organisation unit 1
Organisation unit 2
Organisation unit 3
Work roles
Doctor
Nurse
Secretary
Assisting nursing
Others
Doctor 1
Nurse 1
Nurse 2
User rights
+ Work role - Nurse
e.g. nurse rights for EPR and EMR
+ Organisation role - Unit 1
e.g. email, unit 1 shared folders
+ Dynamic role - supervisor
e.g. right to approve user rights
User rights
+ Work role - nurse
e.g. nurse rights for EPR and EMR
+ Organisation role - Unit 3
e.g. email, unit 3 shared folders

FIGURE 7. Organizational and work roles. (Virkkunen, Sanna, 2014)

In addition to role based user rights there will be need for user rights that are applied separately as described in Figure 8. In Figure 8 the process is simplified. The figure does not take a stand on whether the process itself is manual or automated. In some cases the process can be both.

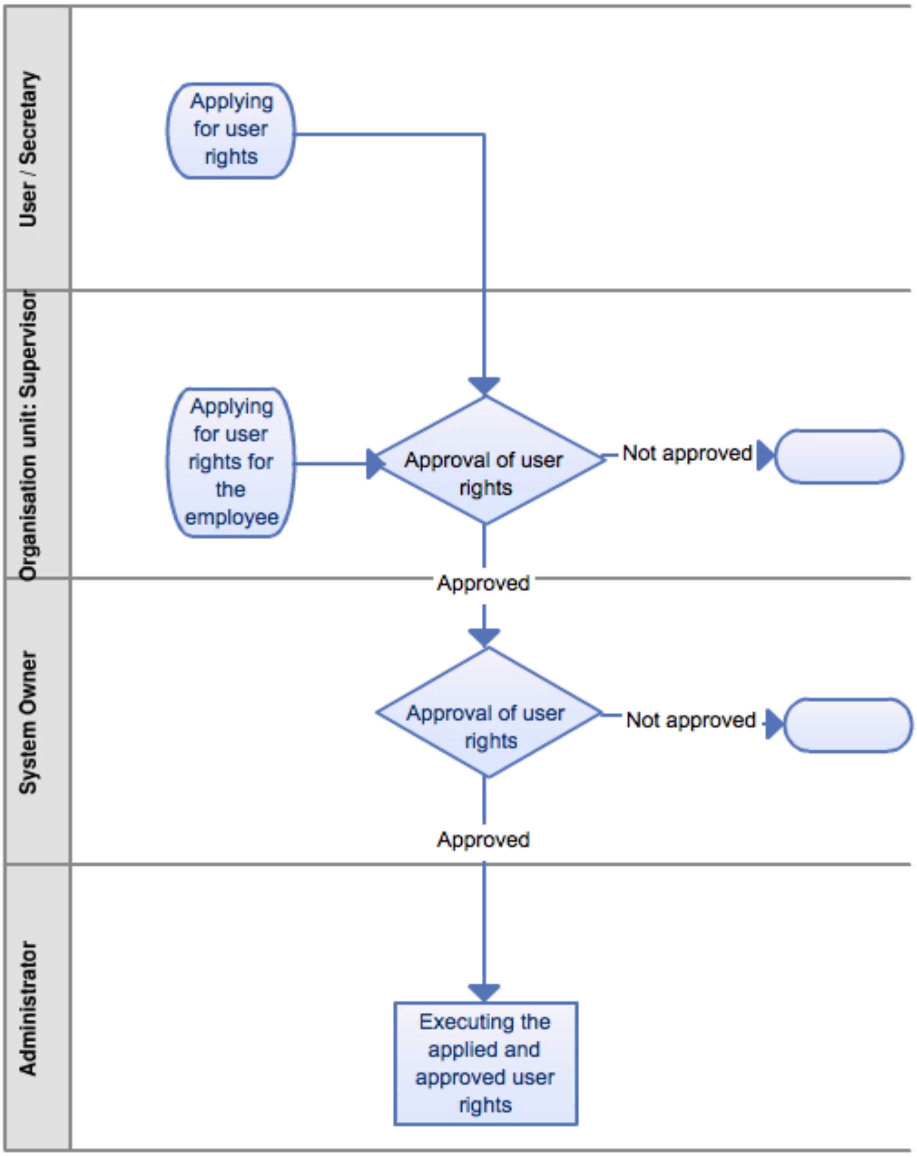


FIGURE 8. Applying for user rights (Virkkunen, Sanna, 2014)

There are some basic processes that need to be designed and implemented for these separately applied user rights. Who has the right to order or apply for user rights? Is it the employee himself / herself or someone else e.g. a secretary on behalf of him / her? Is there a need for classification of users – permanent employees can order their own user rights but fixed-term or temporary employees can not? The most important thing is to create an electronic ordering process so that every action is logged and found in the IAM system.

User rights approval process has to be carefully planned, too. For some of the user rights it may be enough that the direct supervisor accepts the applied user rights. On the other hand with some high-security information systems user rights need to have multiple-stage acceptance protocol. In this case for example the direct supervisor and the system owner have to accept the applied user rights.

Furthermore, the execution of the user rights has to be carefully considered since this is a time-consuming process. According to Huhta (18) it takes about 10 minutes to create one basic AD user account. If any exception occurs, e.g. there happens to be a namesake, more manual work is needed. In an ideal model all of the applied and approved user rights would be executed automatically by the identity management system. However, in real world there will always be some exceptions that need to be taken care of with manual processes. When planning the IAM project, it would be best to focus on easy winnings, big masses and frequent use cases.

In health care it is common that the employee’s organization or title will change. This affects the employee’s access rights. These changes of employment should be processed similarly as for employees who are leaving the organization. All organizations processing patient information will terminate the user access privileges with respect to patient data for any departing permanent or temporary employee as soon as possible. The termination process of user rights should be carefully planned especially for students, interns and other temporary staff with a short-term access to patient data. (32, p.28.)

3.3 Access management

Access management is about authentication, accountability and authorization. It answers questions like “How do we control who is using our systems?” “In what manners our systems are being used?” “How can we make sure the user is the individual he/she claims to be?” The functionality of access management can be implemented using technologies such as repositories, meta-directories, databases, LDAPs and other directory services. (19.)

Access controls are different mechanisms working together protecting the assets of the organization. It means allowing only authorized users, programs or other information systems to observe, modify or take possession of the resources of a computer system. Access control is also a mechanism to limit the use of some resources to authorized users only. (23,p.3.)

One of the most fundamental principles of access control is the principle of the least privilege. It means the user or the process is given no more access privilege than necessary to access only resources and tools necessary to perform assigned functions. (23, p.15.) In health care this means deploying exactly the claim of the decree on patient records that each individual employed in health care and each user of an electronic patient record has to have access rights that are being defined according to the current role of the individual. (11, 4.)

3.3.1 Mandatory Access Control MAC

Mandatory access controls are based on organization policy and determined by the system. MAC requires the system itself to manage access controls in accordance with the organization's governance. Typically MACs are used for highly sensitive systems. MAC is based on interaction between the system and the information owner. The system decides and controls the access and the owner provides the need-to-know control. Only those who have a need to know and who clear the system's access control will be provided the information. (23, p.116-117.)

Access permissions apply to an object based on the level of authority given to a subject. Access capabilities and access permissions can be as mentioned in Table 1 and Table 2. Users can be assigned to different groups, and access capabilities can be assigned to these groups differently. When combining these two tables and adding users to it we get access control list (ACL). (23, p.116-117.)

TABLE 1. Access capabilities

No access	No access permission
Read (R)	Permission to read but not to make any changes
Write (W)	Permission to write to file, includes also the capability to change.
Execute (X)	Permission to execute a program
Delete (D)	Permission to delete a file
Change (C)	Permission to read, write, execute and delete a file but not to change file permission.
List (L)	List the files in a directory
Full Control (FC)	All abilities, including changing access control permissions.

TABLE 2. Access permissions

Public	R – L
Group	R – X
Owner	R – W – X – D
Admins	FC
System	FC

Mandatory access control was developed for the US Army. Creating a complete deployment using MAC in practice has turned out to be tricky. However, MAC is a significant theoretical model for access control. (26, p.33.)

3.3.2 Discretionary Access Control DAC

The data owner places discretionary access controls on data. The owner determines who has access to the data and what privileges they have. DACs are widely used to allow users manage their own data and the security of that information. (23, p.116.)

3.3.3 Role Based Access Control RBAC

A role-based access control RBAC is based on the roles or functions the user is assigned within the organization. Access control decisions are based on work roles and organizational roles.

Each role has its own access capabilities. There are no restrictions how many roles can be assigned to a user, or which permissions can be assigned to a role. This is described in Figure 9.

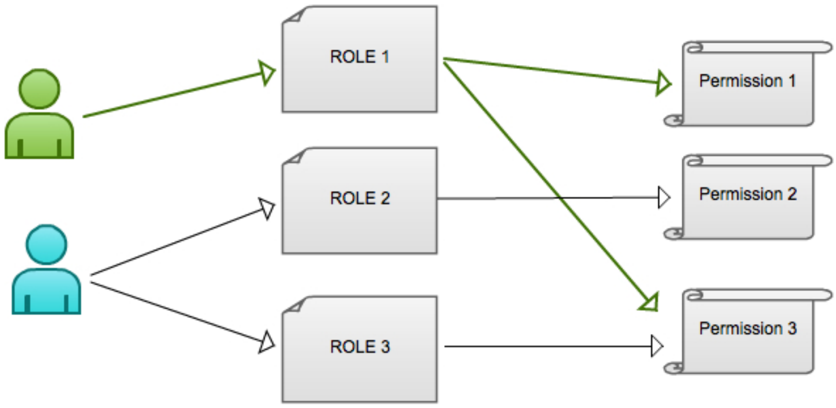


FIGURE 9. Roles assigned (Virkkunen, Sanna, 2014)

Objects associated with a role inherit privileges assigned to that role. As seen in Figure 10, there are many approaches to RBAC.

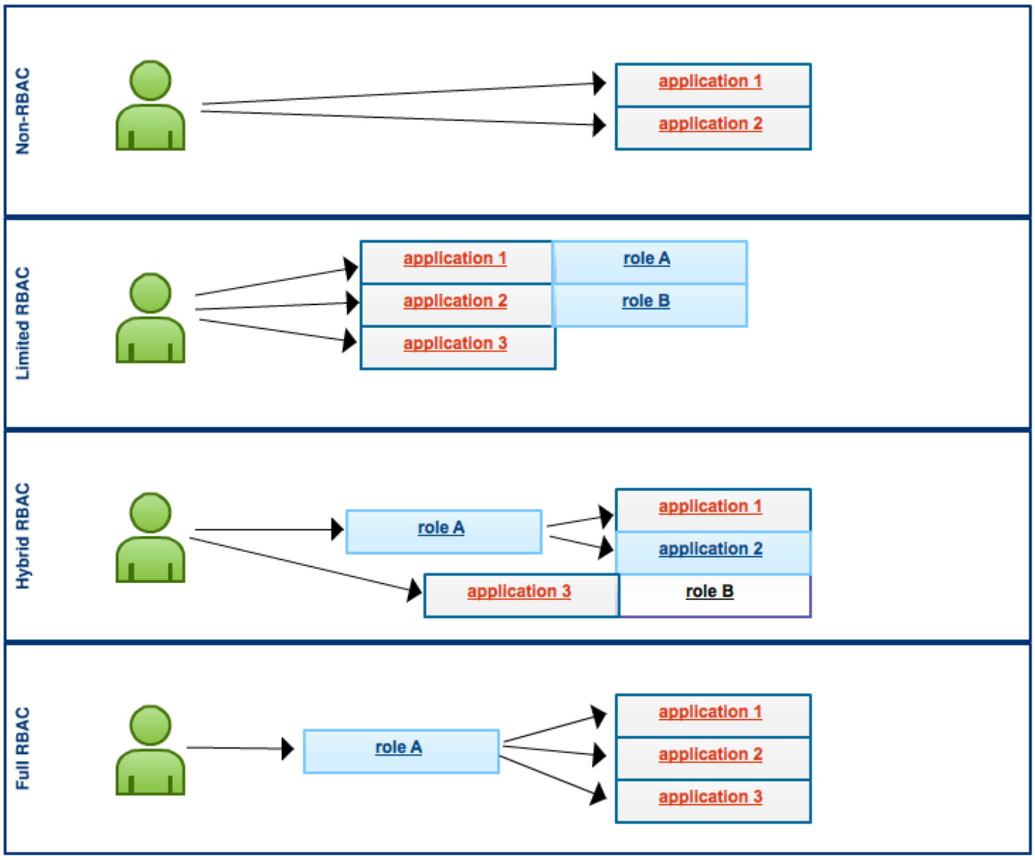


FIGURE 10. Role-based access control models (Virkkunen, Sanna, 2014)

A non-RBAC means granting access to an application by traditional mapping, using e.g. ACLs. There are no roles used. A limited RBAC means that users are mapped to system roles but there is no organization-wide role structure. Users can also be mapped to applications that do not have a role-based access at all. In a hybrid RBAC there are organization-wide roles used, but it does not exclude the use of applications that use system roles. A full RBAC means that information systems and applications are controlled by roles that have been defined by the organization's governance and policies. There are no users mapped to single applications. Possible system roles are defined according to the organizational roles. (23, p.120-121.)

IAM systems support the RBAC model. To develop the maturity level of the organization, role mining to target systems is needed to find out the system roles and their suitability to the organizational and work role structure.

3.3.4 Attribute Based Access Control ABAC

An attribute based access control (ABAC) is an extension of RBAC. ABAC was developed due to the vast amount of effort for engineering roles in the RBAC model. With ABAC the access control can be based on any attribute of user, service, operation or system. The attribute can also be a name of a role. However, in that case it is not possible for the ABAC to contain roles and their permissions. With ABAC the engineering roles is not needed if role names are not used as attributes. Changing attributes e.g. the time of day and organization unit dynamically gives more room for variety. It can also make things more difficult with too many options. To provide an access control, labelled objects and user attributes are used in ABAC instead of permissions. (27.)

With ABAC auditing becomes a laborious task. Instead of only reviewing users and their roles, the auditor has to enumerate user's attributes and then the corresponding attributes of the available protected objects. Also because the attributes can change dynamically, it requires instantiating rules with all possible attribute values while the user is active. (27.)

3.4 Provisioning

Provisioning can be an automated or a manual process. However, with a manual handling of user data the possibility of gaining all the needed log data and reconciliation decreases. With a manual system there is usually also huge amount of manual work to be done with lost and forgotten passwords. Typically provisioning is done distributed in health care. This way there has always been some person close by to create user accounts for new, sudden employees in emergency situations.

Provisioning means a pre-defined process where the employee or external user is provided the possibility to use organization's ICT services according to the identity and user information stored in different systems. In other words, the user information and user rights are forwarded to service systems, which is illustrated in Figure 11. This leads to the basic dilemma of keeping all this information in different systems up to date in all times. The IAM system can be configured to create user objects automatically to several ICT systems according to the master data. In real life there will be some exceptions when the information in a target system is updated without the IAM system knowing it. Also, these situations have to be handled. Usually, this is done by reconciliation.

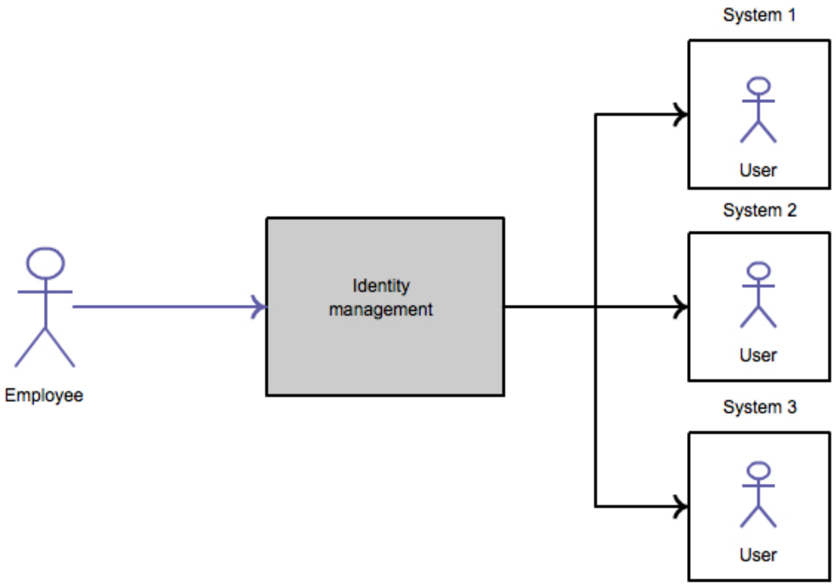


FIGURE 11. Provisioning (Virkkunen, Sanna, 2014)

It is possible to start a provisioning process development from many different points of view. One of the perspectives is to approach provisioning from the used platform. In some cases it may be a good idea to proceed with technical aspects first: to focus on directories, databases and portals, global services and centralized service platforms. Another point of view is to achieve quick winnings first. This can be done focusing on widely used systems: domain login, Sharepoint or email. What should always be considered is whether the cost of automation meets the benefits. (9, part 5.)

When choosing the way of provisioning, it is a good idea to clarify the implementation model of the vendors' provisioning techniques and choose the ones that fit best to the organizational needs. Provisioning can be done using several techniques. Scripting can be used in point to point provisioning. Scripting is made so that identity information is being transferred with scheduled runs in between user information databases. It is also possible to schedule scripts to change rule-based information content e.g. role or group memberships. (9, part 5.)

A backlog based system or service management system is also a way to implement provisioning. With a service management system the provisioning is based on service and change requests. A team of administrators processes requests manually. The service requests and reminders will be sent via email and with the system it is possible to follow the completion of requests. However, auditing and reporting is difficult using only service management system. (9, part 5.)

Using integration services (an enterprise service bus, ESB) is de facto of integration. It is used in a service-oriented architecture (SOA) for implementing communication between software applications that are interacting mutually. It is mostly used and it is optimized for business intelligence (BI) data. If BI data is needed in identity management, it might be appropriate to consider using ESB as a provisioning technique platform, too. If there is no IAM system available, ESB can be used for basic provisioning. However, ESB is way more complex way of provisioning than the IAM systems that are optimized for synchronizing identity information. Ready-made interfaces to common HR systems are a clear advantage of using the IAM system for provisioning. The IAM systems have ready-made database interfaces, also all the filters and data modification are optimized for identity-based information. (9, part 5.)

3.5 Federation

Federation gives identity and access management a more user-oriented point of view. The most of the IAM use cases consist of the user working inside the organization and using only information systems provided by the organization. However, in real life there are many services the user needs, also outside the organization. This is described in Figure 12. In some cases even in health care, it is reasonable to trust the authentication mechanism of a third party. This is called federation. Federation provides an integrating access management to internal directory services and identity management. Managing user rights requires provisioning user accounts to the federated target systems manually or automatically using e.g. SAML2. (9, part 5. Slide 28.)

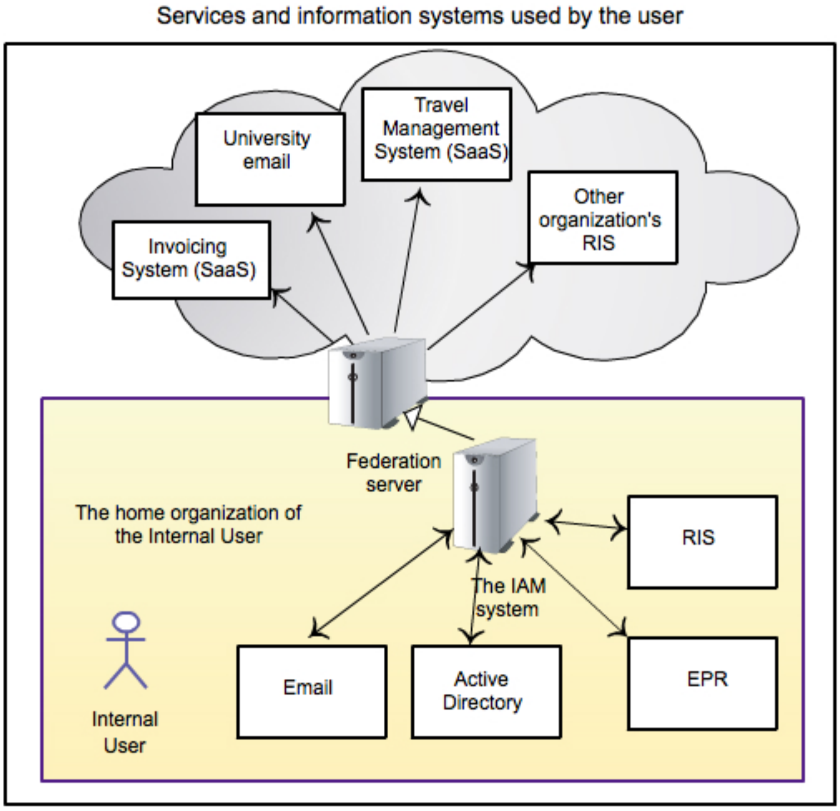


FIGURE 12. Federation.(Virkkunen, Sanna, 2014)

A great example of federation is the commonly used Haka-system in Finnish universities. In Haka web of trust the home university maintains student’s basic data or master data and authenticates the user e.g. with password. The home university then assigns the user data to a service provider who then decides depending on the master data, what kind of view the user sees in the service. Haka is mainly built on Shibboleth open source software (20.)

In order to use federation for example with other organizations electronic patient record, the home organization would have to trust the way different user rights, roles and accounts have been given in another organization to that information system. Typically, this would require agreeing with the governance policies the other organization has made. It would also require all parties to understand the governance policies of the other organization.

3.6 Single Sign-On

Ideally the authentication of hospital's information systems would be based only on certificates. However, often this is not the case due to a varied amount of system platforms and login techniques used in a health care organization. Enterprise single sign-on (eSSO) can provide an agile solution for this. For enabling the eSSO, the identity management system has to store users' system specific user logins and passwords centralized using strong encryption methods for securing the data.

Single sign-on is often mentioned with identity and access management. The enterprise single sign-on system usually consists of a central server, which stores each user's logins and passwords for multiple systems as illustrated in Figure 13. Depending on the implementation of a single sign-on system, there usually is either an integrated single sign-on agent running on each computer, sniffing if there is a login window opened or script-based programs which have login data programmed inside the script.

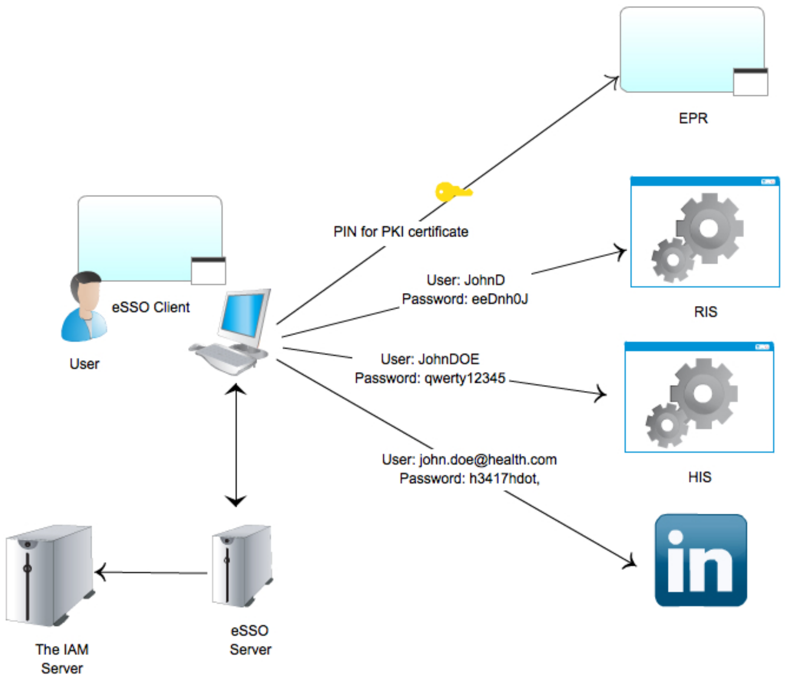


FIGURE 13. Single Sign-On.(Virkkunen, Sanna, 2014)

When using single sign-on the user does not need to remember any account information: single sign-on does this for the user. Using single sign-on with Population Register Centre's smart cards reduces the time needed to log in to different systems. Only actual thing to remember is then the PIN code for the smart card. In an elaborate system environment the enterprise single sign-on system fills in all the login data needed.

Using the eSSO makes the logon process efficient because the users are interrupted less when performing their job. There are no long need for multiple passwords – the introduction of a SSO system translates into a single-use credential. To the user there is only one master SSO password that is replaced by using the smart card. Using the eSSO also makes it easier to enforce standards across the entire system, e.g. inactivity time-outs. The eSSO manages the enforcement across all applications. (23, p.106-107.)

3.7 Auditing and reporting

A complete audit trail of system activities is a necessity to assure that the system is functioning properly, even if there are no apparent signs of system failure or unauthorized access. The system should provide a complete record of all access control activity, like authentication requests, data access attempts and changes to privilege levels. The record should contain both successful and failed activities. (23. p. 28-29.)

A proper auditing makes it possible to view an integrated life cycle of each identity. Auditing means that it is possible to run different reports from the IAM system. The reports supplement the data available in log files. The IAM system should provide full reports to auditing users and interest groups, e.g. data protection officers and supervisors. The reports should be provided and delivered automatically in different formats. Viewing the reports should be possible by conditions and time periods the user has chosen. It should be possible to see precise rights, restrictions, roles and information an identity has had on each information system on a given date.

In health care one of the significant report types is dangerous work combinations. Dangerous work combination in health care happens for example when the same person has rights to order, approve of and use a heavy medication. Another example is that if a single user is performing both system backup and restore procedures, he / she would have the ability to change information, destroy valuable resources or manipulate and destroy the backup data to cover up unauthorized activity unnoticed. (23,p.13.) Dangerous combinations typically consist of administrators, super users and persons who have the right to approve of rights. The IAM system should provide monitoring processes for dangerous combinations.

The IAM system should also provide other versatile reports. There should be available lists of all the users with different prerequisites, such as users with a specific work role or users of a specific target system. There should be listings of added, removed and inactive users, listings of unprocessed user right requests, listings of rejected user rights and separate, selected listings for supervisors and data protection officers. For the IAM administrator the system should also provide provisioning reports of failed and succeeded cases.

Log files are typically created and maintained in each target system separately. It is necessary to review the logs periodically. System logs are high in volume, which makes it difficult to isolate and identify a given event for identification and investigation. (23, p.43) Some IAM systems have an option to provide a centralized log storage with intelligent log analyzing tools.

Apart from centralized logging, every critical target systems' user rights management actions have to generate a complete user-specific log and change history. Also, using log files have to be logged. All the logged information has to be easily provided in different kinds of auditing and analysing situations. Log files have to be available for indisputable user rights auditing. No one can have a right to change or remove log files. (14, p.11-12.) Typically a log can include user IDs, dates and times of log-on and log-off, system identities (IP-addresses, host names etc.) and both successful and rejected authentication and access attempts. (23. p.42.)

The changes made to the IAM system have to generate a log file that is available for administrators. Also, user actions have to be logged real-time. The archiving obligation for log files is the time the person is working for the organization + 12 years. Log files need to be archived 12 years after their emergence. After the time limit, the log files have to be erased appropriately. (14, p. 11-12.)

According to ISO 27799, patient information systems should create a secure audit record each time a user accesses, creates, updates or archives patient data. The audit log should uniquely identify the user, the data subject, the function performed by the user and note the date and time when the function was performed. (32, p.34)

A health care service provider has to keep a register of all use of patient data. The information on used patient data, information on the user, the purpose of use and the time of use has to be logged. The patient has the right to receive information from the health care provider, on who has used the information concerning the patient. The information has to be based on log files. If the patient thinks the information concerning him / her have been used without a sufficient ground, a request can be written to the health care provider to provide a report of the grounds of the use. (24.)

3.8 Role mining

It is necessary to do role mining to discover the organizational and work roles in the organization. Role mining can be done by collecting data from organization units to find out employee’s work tasks and titles and their correspondence to the used information systems. The titles and their relationship to the tasks need to be clarified, since it is typical in health care that the same tasks are repeated with different titles. It is important to start bundling task-based titles to work roles in order to proceed with the IAM project. Discovering the system roles from the information systems used in health care systems and matching them with work roles is the next step.

Some system vendors provide role mining tools to discover system roles or user attributes within each system. Of course, this challenging task can be done with excel sheets but analyzing the collected material manually will take plenty of time. As mentioned earlier, finding out the organizational and work roles is one of the most time-consuming tasks in the IAM project. It requires intense planning. It is a great challenge to keep the amount of the work roles to minimum in health care. It is good to keep in mind it is easier to manage fewer roles. Even when the IAM system is fully deployed, role mining is recommended to be done every once in a while to stay up to date in the alteration of the role structure.

3.9 Reconciliation

Reconciling means comparing and synchronizing the target systems' user information with the initial identity material gathered in the IAM system. This is called a bottom-up point of view. The process of gathering identity material from the master data system is called a trusted reconciliation. The IAM system trusts fully all the user data the master data system provides. This data is the initial identity material. Reconciliation also means the top-down point of view: how the work roles, organizational roles and dynamic roles will be managed and then later provisioned to the target systems. Reconciliation helps synchronizing the user information between the IAM system and the target system before deployment. Reconciliation is illustrated in Figure 14.

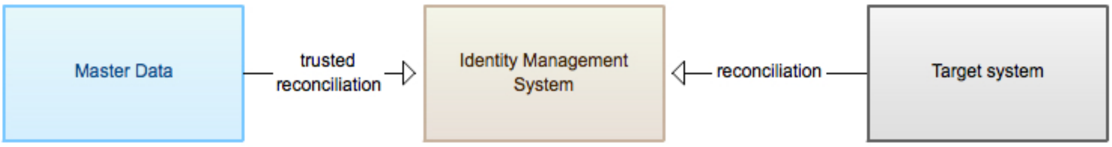


FIGURE 14. Reconciliation.(Virkkunen, Sanna, 2014)

Reconciliation is a process to be done also after the deployment of the IAM system. In some cases there will be changes in user accounts and user rights that have been made outside the IAM system. These unwanted changes (e.g. removal of user rights, exceptions etc.) may cause mix-ups with identity information. Typically reconciliation can detect new and deleted accounts, changes in account attribute values, correlate accounts with IAM users and detect accounts not associated with IAM users. (29.) There should be automatic processes to repair these mismatches, but also manual linking with the information should be possible. The ways to handle the workflow after reconciliation alter with different IAM systems.

3.10 Identity and Access Management Challenges

There are several challenges that have to be overcome before deploying identity and access management system full in health care. It is common that there is a limited number of system administrators to process user rights requests. Their requests for access rights can be backlogged and as a result they are delayed or held until enough requests are pending for a system administrator to process them. This can lead to halting the employee's productivity and in the worst cases to prevent the core task – patient care. (23, p.94.)

One common challenge is that the user rights request forms are not fully completed, causing delay in processing. This can be mitigated with a proper education. Sometimes the number of employees across the organization is growing. This leads to a situation where the number of user rights requests is increasing stealthily causing a chronic shortage in the organization's system administrators. At the same time there are dormant user profiles or departed employees. Removing unnecessary accesses is just as important as granting them in the first place. Many organizations forget to regularly review existing accesses to determine which ones are unnecessary. (23, p.95.)

With or without an identity and access management system, there is always the weakest link. Some people in the organization often bypass defined processes and protocols in an attempt to get their requests implemented more quickly. This can be done by calling a helpful friend in IT rather than going through the standard IAM process. (23, p.95.) In such a sensitive operating environment as health care, there has to be back doors for speeding up the access rights process in some cases. However there has to be a way to control these back doors, too.

Until recently, it has been common for health care information systems that they are not compatible. To solve this issue, several integrations have been made, using both tailored and standardised interfaces. For example a minimum context management (aka desktop integration) has been used in health care as a way to transfer e.g. active user and patient information from one application to another. This way the user does not have to login again when using the same patient's data in another application. The minimum context management is defined by HL7

Finland ry and it is based on a CCOW-standard. The purpose of the desktop integration was to ease the use of separate clinical systems on one workstation. One could say a desktop integration is a way to utilize single sign-on in health care. The advantage of a desktop integration is that it includes the patient's identifying data to the integration. This way switching the patient entry in one system switches the patient data also in other systems the user has been logged in. (28, p.6.)

However, using the minimum context management, the role of the user is not included in the transferred data. This makes the integration very vulnerable from the IAM point of view. For example, the user can have role-based user rights in the EPR system but the user rights defined in the target system depend entirely on the abilities of the target system. The login name can be similar to match the users in these two systems but the roles differ. When deploying the IAM system and role structure to these integrated target systems, it is necessary to do role mining for them, too.

4 HEALTH CARE WORKING PERIODS

In health care the working periods are managed strictly with different working period types and contracts. In NOHD there are seven different working period types being used. An employment relationship typically consists of several working periods that can be overlapping.

A permanent employment contract does not have a predefined end-date. It is valid until further notice. The pre-defined user rights should come into effect on the inception date of the permanent contract according to the organizational and work roles. If the person needs more rights, they need to be applied separately.

A fixed term change contract is a contract type used when a person is working in two or more organization units. A fixed term change can be valid only if the person's basic contract is a permanent one. The contract can also be part-timed and there can be several contracts valid at the same time, e.g. three 33% contracts. A fixed term change means that the person may have two or more direct supervisors. The person will have extensive user rights based on the pre-defined extended organizational and work roles.

A released from one's own post contract type can be valid only for permanent employees for a fixed term. If the contract is made for full-time, the permanent employment contract goes inactive during this time. In this case the employee's old user rights should inactivate during the contract time.

A released from one's own post during an annual leave contract is a contract type for some permanent employees to substitute someone during his / her annual leave. This contract type is valid only for a fixed term with an effective date and an ending date. During this period the employee's own user rights should inactivate and the employee gets the same user rights as the employee on the annual leave.

An employee can also be hired as a substitute. A substitute contract is always fixed term with an inception and ending dates. However, the contract has to be longer than 12 days. There can also be holders of open positions and other temporary employees hired for longer than 12 days. If the contract is made for less than 13 days, the contract type will be timework. (14, p.6.)

The contract types listed above make it possible for an HR unit to manage all the employment cases in a health care organization. The same should go with externals. All the actions made within a health care organization or its information systems should be based on some contract. Furthermore, each person using health care information has to be registered and identified uniquely. (21.)

From the organization's IAM point of view the electronic identity of a person is born when the person's information is added to the HR, master data or IAM system. The identity can remain inactive until the contract's effective date. This is illustrated in Figure 15. This can trigger a user information provisioning to the target systems. On the effective date the identity activates as well as the user rights attached to the identity. In case of a fixed-term contract, the identity and the user rights should inactivate on the ending date. If identity or work period information changes, the IAM system should update the user rights accordingly. A valid user right always requires a valid work, apprentice, research or other contract with the organization.

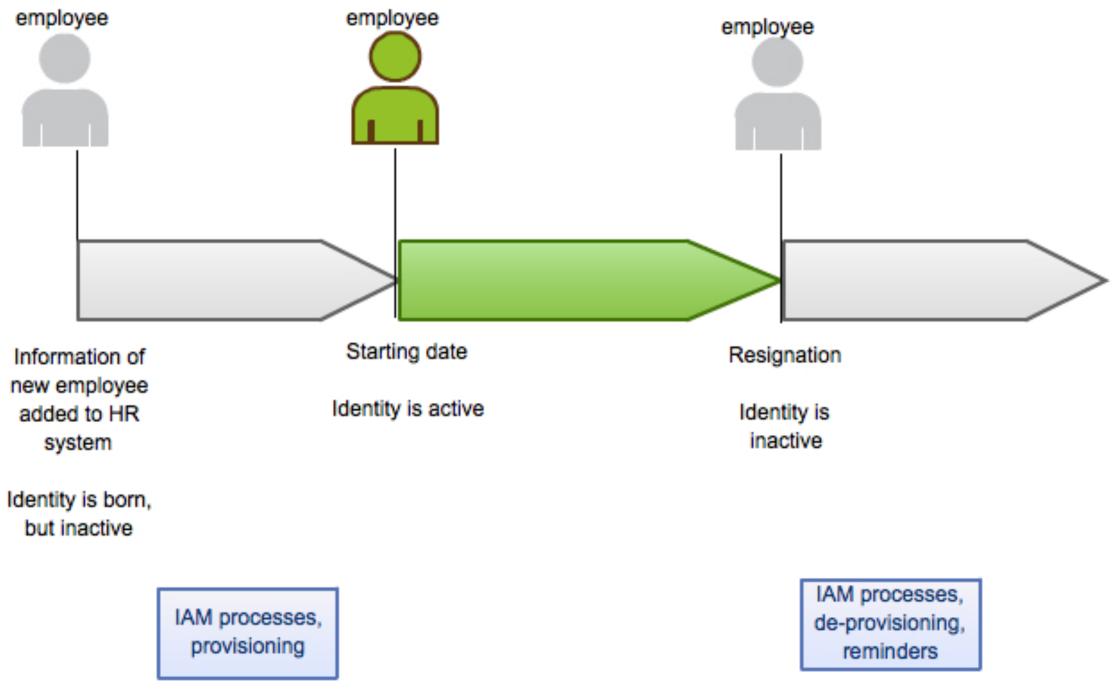

employee
employee
employee
Information of new employee added to HR system
Identity is born, but inactive
Starting date
Identity is active
Resignation
Identity is inactive
IAM processes, provisioning
IAM processes, de-provisioning, reminders

FIGURE 15. Active and inactive identity. (Virkkunen, Sanna, 2014)

5 IAM USE CASES IN HEALTH CARE

The IAM system has to support all basic use cases in the health care organization. The use cases have to be defined so that they are suitable for the organization's working culture especially with human resources management. The goal has to be an entirely electronic user rights management process including an electronic applying for user rights, an automatic user right creation and changing to target systems. If the IAM system offered is not equivalent to the required use cases, the vendor may be allowed to present an alternative way to fulfil the basic need. The use cases listed below imitate the use cases outlined in NOHD.

5.1 An internal employee

5.1.1 A new post or a continuous employment contract

Hiring a new employee

A supervisor or a corresponding secretary enters the employee's information to the HR system and supplements the employee's information to the data master system.

The IAM system reads the new employee's information from the data master system and processes it.

The IAM system creates the user's identity and then creates automatically user rights according to pre-defined rules to defined key target systems e.g. Active Directory, Passage Control system, Electronic Patient Record (EPR), Hospital Information System (HIS) and to workshift list planning system.

User accounts and the AD user account are inactive until the contract of employment comes into effect.

If there is a plan for the organization to start using the eSSO system sometimes in near future, the IAM system should provision the user information also to the eSSO system.

The IAM system sends a service request to system administrators to execute the needed user and access right management actions by the due date. The system administrators create pre-defined user accounts and user rights to manually provisioned target systems. Further system administrators attach each user's system-specific login and password information to the eSSO system to prevent the user for doing this time-consuming task.

The system administrator enters the information to the IAM system.

The IAM system sends an email concerning the new user to the corresponding secretary, supervisor and to Registration Authority (RA).

When the contract of employment comes into effect, an AD user account will be activated.

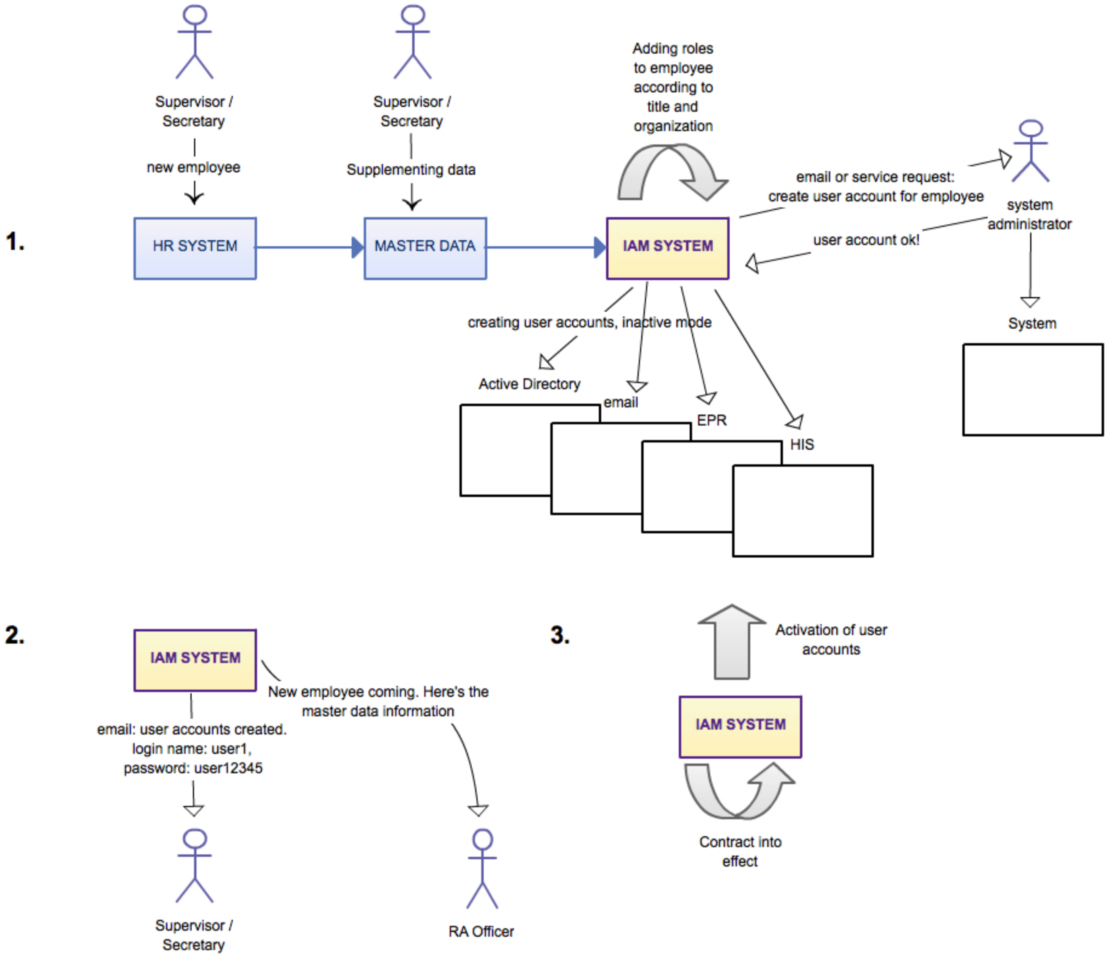

1.
Supervisor / Secretary
new employee
HR SYSTEM
Supervisor / Secretary
Supplementing data
MASTER DATA
Adding roles to employee according to title and organization
IAM SYSTEM
email or service request: create user account for employee
system administrator
user account ok!
System
creating user accounts, inactive mode
Active Directory
email
EPR
HIS
2.
IAM SYSTEM
New employee coming. Here's the master data information
email: user accounts created. login name: user1, password: user12345
Supervisor / Secretary
RA Officer
3.
Activation of user accounts
IAM SYSTEM
Contract into effect

FIGURE 16. Hiring a new employee (Virkkunen, Sanna, 2014)

A new employee in the RA

A secretary schedules an appointment for the employee to the RA.

The employee is photographed for an identity card and a PCR smart card.

If the employee does not have a smart card provided by the PCR, an RA officer orders a primary health care smart card for the employee and gives a temporary smart card and a PIN-code to the employee. The RA officer enters the deeds of transference to the IAM system.

If the employee has the health care smart card, the RA officer then attaches the certificate on the card to the AD user account using a UPN attribute.

The RA officer hands over the electronic key to the employee and attaches the key to the user using passage management system. The user receives automatically pre-defined rights to the doors of the organization. The RA officer enters the deed of transference to the IAM system.

The RA officer hands over the rest of the keys related to the work tasks to the employee, and enters the action to the IAM system.

A New Employee – the first time use

The employee logs in to a domain using the smart card's authentication key.

The rules for using the organization's information systems and access rights contract open for the user in a separate window.

The domain login asks the user to approve the rules for using the information systems.

The user accepts the rules by signing the contract using a non-repudiation certificate on the smart card.

The IAM system allows the user to access the user's virtual desktop and to login to the organization's workstation.

The IAM system creates a report of the user rights contract and archives it.

The user uses information systems according to the given user rights.

The user, a corresponding secretary or a supervisor requests for additional user rights for the user if needed using the IAM system's separate ordering view.

If the user or the secretary requests the additional user rights, the user's supervisor has to approve or reject them.

The owner of each information system accepts or rejects the request if needed but it is not mandatory for every system that the system owner approves the requested rights. In most cases the requests are transmitted directly to the system administrators to be executed.

The requested user rights are provisioned automatically or a manual service request is sent to the system administrators to be executed.

An executed user rights request is entered to the IAM system with a status “completed”.

A post process

The user logs in to the IAM system and is able to view current user rights and user rights requests concerning the user with relevant status information.

The user requests more user rights using the IAM system.

The user's supervisor (or a person authorized by the supervisor) approves or rejects the requests using the IAM system, the IAM portal or an email link sent by the IAM system.

The supervisor is able to view the user rights he or she has approved of or rejected.

The user is able to view the rejected user rights requests in the IAM system.

The user can renew the user rights requesting a process in case the reasons differ from the previous request.

The system owner approves of or rejects the requested user rights in the IAM system by using the IAM system, an IAM portal or an email link sent by the IAM system.

The user and the supervisor are able to view the user requests rejected by the system owner.

The employee gets an announcement of an arrived smart card and fetches the card from the RA. Then the employee returns the temporary smart card and the RA officer attaches the UPN information of the new certificate to user's AD user account and removes the temporary card.

Notes:

The supervisor has the obligation to read through the rules concerning the organization's information systems and access rights contract. It is the manager's responsibility to familiarize the new employee with the practices concerning the organization's information systems. Using the information systems requires the user's digital signature.

5.1.2 The termination of a post or an employment

When the information concerning the termination of employment is acknowledged, the corresponding secretary enters the information to the HR system. The information transfers to the IAM system through the possible master data system.

A month before the termination date of the employment, the IAM system sends a service request to the supervisor, corresponding secretary and the employee via email.

If the supervisor or corresponding secretary does not acknowledge the service request to the IAM system, the IAM system will send a new service request one week before and again one day before the termination date of the employment. If the service request is acknowledged, new requests will not be sent.

The IAM system inactivates the employee’s AD user account after a waiting period e.g. 2 business days after the termination date.

The IAM system disables user rights automatically from the automatic provisioning systems. The IAM system sends an email service request to the system administrators concerning the manual provisioning to disable the employee’s user accounts.

The system administrators execute the task and enter the information to the IAM system as a completed task.

The user returns the smart card (if it has an organization certificate), ID card and keys to the RA officer.

If the user does not return the items, the IAM system sends a reminder to the RA officer who then acts according to given orders.

5.1.3 The organization unit changes

The corresponding secretary of the new organization unit or another authorized person enters the new working period to the HR or the master data system beforehand. At the same time the corresponding secretary arranges the situation with the authorized person of the previous unit and the date of termination is set for the previous employment contract.

The IAM system recognizes a change in the user’s working period information and sends an email concerning the change to the employee and to the supervisors and corresponding secretaries of the old and new organization units.

The IAM system provisions the user rights according to the new organizational roles automatically or using manual service requests to be executed on the exact due date.

The previous organizational role based user rights (also passage rights and keys) are removed when the previous working period ends.

The previous separately requested user rights are removed or the new supervisor approves of them if needed.

The user, corresponding secretary or supervisor requests for additional user rights if needed with the IAM system’s ordering view.

If the user requests the additional user rights, the user’s supervisor has to approve of or reject them.

The owner of each information system accepts or rejects the request if needed but it is not mandatory for every system that the system owner approves of the requested rights.

The requested user rights are provisioned automatically or a manual service request is sent to the system administrators to be executed.

The executed user rights request is entered to the IAM system with a status “completed.”

The employee starts working in the new organization unit and is allowed to use the information systems according to the user rights defined by the new unit.

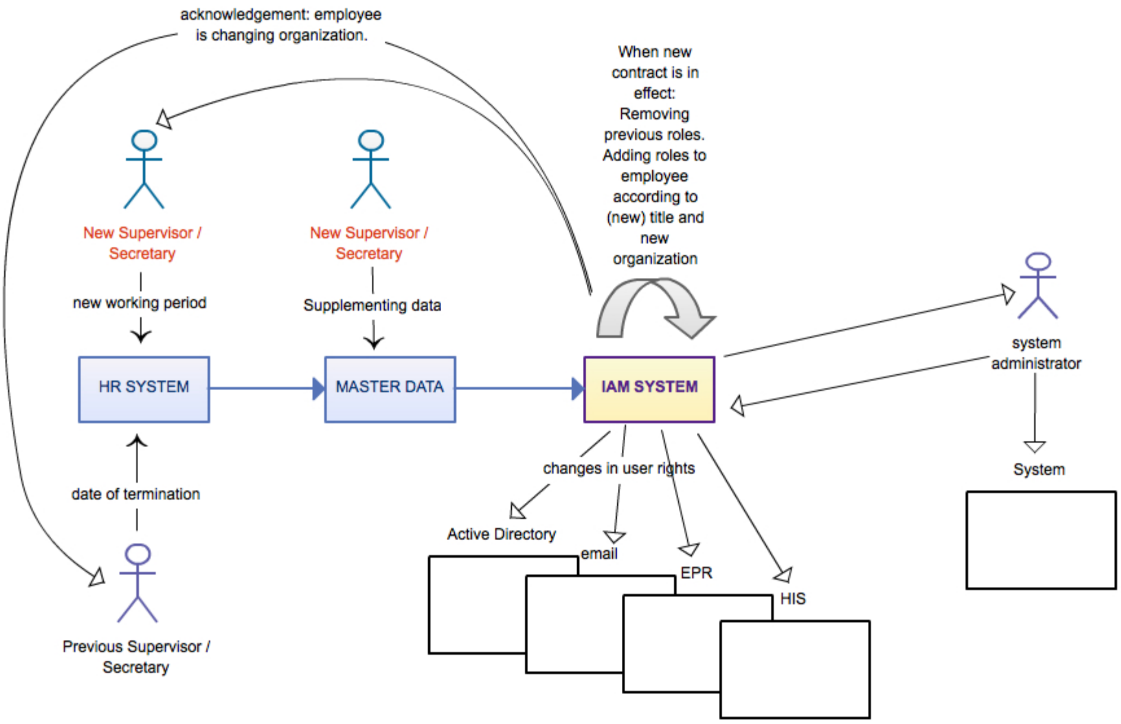

acknowledgement: employee is changing organization.
When new contract is in effect: Removing previous roles. Adding roles to employee according to (new) title and new organization
New Supervisor / Secretary
New Supervisor / Secretary
new working period
Supplementing data
HR SYSTEM
MASTER DATA
IAM SYSTEM
system administrator
System
date of termination
changes in user rights
Active Directory
email
EPR
HIS
Previous Supervisor / Secretary

FIGURE 17. The Organization Unit Changes (Virkkunen, Sanna, 2014)

5.2 External employees

5.2.1 A new external employee

In this chapter the word external can stand for any external employee, a student, researcher, civil servant etc. There is always a contract-based process with an external organization. When it comes to private individuals, the issue at stake is typically a virtual instance of an organization, e.g. a university or other health care organization. The organization unit makes an agreement with the person or the organization concerning the service. The agreement is always temporary.

The corresponding secretary, the RA officer or another authorized person enters the external employee's working / service period information to the external master data system and defines the external organization for the person.

The corresponding secretary, the RA officer or another authorized person enters the information concerning the organization: the unit responsible for the external, the person responsible for the external and the task for the external employee.

The IAM system recognizes the external person from the data master and processes it.

The IAM system creates the user's identity and then creates automatically user rights according to pre-defined rules to Active Directory and Passage Control system.

The AD user account is inactive until the contract of service comes into effect.

The IAM system sends a service request to the user access management administrators to execute the needed pre-defined user and access right management actions by the due date. The user access management administrators create pre-defined user accounts and user rights to manually provisioned target systems.

The access management administrators enter the information to the IAM system.

The IAM system sends an email concerning the new user to the corresponding secretary, supervisor or the person responsible for the external employee and to the Registration Authority (RA).

When the contract of service comes into effect, the AD user account will be activated.

The process in the RA is similar to the internal employee. The RA officer gives the external a smart card and a PIN code. The smart card is attached to the external employee's AD user account using a UPN.

The first time use is also similar to the internal employee's one.

The corresponding secretary, supervisor or the person responsible for the external employee requests for additional user rights if needed from the IAM system's ordering view.

The owner of each information system accepts or rejects the request if needed

The requested user rights are provisioned automatically or a manual service request is sent to the system administrators to be executed.

The executed user rights request is entered to the IAM system with a status "completed".

A post process

The external user logs into the IAM system and is allowed to view the user rights and requests concerning him / her.

The external user is not allowed to request user rights directly.

5.2.2 Re-certificating the external user and the renewal of the contract

The contractual relationship has to be renewed every six months concerning the user information. A month before the due date of the renewal the IAM system sends a service request to the corresponding secretary or the external employee's contact person.

If the corresponding secretary or the person in charge of the external does not acknowledge the service request to the IAM system, the IAM system sends a new service request one week before and again one day before the due date of the contract. If the service request is acknowledged, new requests will not be sent.

If the external employee is still in the service of the organization unit, the corresponding secretary or contact person approves of the renewal. At the same time the external organization information will be checked. If the external employee is no longer working for the organization unit, the renewal is rejected.

Unless renewed, after the recertification date or due date of the contract, the IAM system inactivates the external user's AD user account.

The IAM system disables the external user's other user rights automatically after a period of time.

The IAM system sends an email service request to the system administrators concerning the manual provisioning to disable the employee's user accounts.

The system administrators execute the task and enter the information to the IAM system as a completed task.

The external user returns the smart card (if it has an organization certificate), ID card and keys to the RA officer.

If the user does not return the items, the IAM system sends a reminder to the RA officer who then acts according to given orders.

The information of inactivation is also archived in the external master data system.

5.2.3 The termination of the contract with an external user or an organization

When the information concerning the termination of contract is acknowledged, the corresponding secretary enters the information to the external master data system. It is possible that the termination date has already been entered to the external master data system. The information transfers to the IAM system.

A month before the due date of the contract, the IAM system sends a service request to the supervisor, corresponding secretary or the contact person and the external user via email.

If the supervisor, corresponding secretary or the contact person does not acknowledge the service request to the IAM system, the IAM system sends a new service request one week before and again one day before the due date of the contract. If the service request is acknowledged, new requests will not be sent.

The IAM system inactivates the external employee’s AD user account after a waiting period, e.g. 2 business days after the termination date.

The IAM system disables user rights automatically from the automatic provisioning systems. The IAM system sends an email service request to system administrators concerning the manual provisioning to disable the external employee’s user accounts.

The system administrators execute the task and enter the information to the IAM system as a completed task.

The user returns the smart card, ID card and keys to the RA officer.

If the user does not return the items, the IAM system sends a reminder to the RA officer who then acts according to given orders.

The information is also archived to the external data master system.

5.2.4 An external user’s organization unit changes

If the external employee arranges a transfer to another organization unit, there is always a contract-based process with an external organization or person. The secretary or the contact person of the new unit enters the new working / service period information to the external master data system beforehand. At the same time the corresponding secretary or the contact person arranges the situation with the authorized person of the previous unit and the date of termination is set for the previous working / service period.

The IAM system recognizes a change in the working period information of the eternal employee and sends an email concerning the change to the external user and to the supervisors and corresponding secretaries of the old and new organization units.

Otherwise the IAM system functions are similar to the internal user.

5.2.5 Multiple roles

E.g. an internal physician working as an external researcher at the same time or an internal nurse who is working on a practical training period at the same time.

If a physician does research funded by an external company or foundation, he / she has to be defined as an external employee for the research work in addition to the internal employment. When doing the research the physician uses a different user account and organization card for domain login. This way he / she gets only the user rights needed for the research. A research agreement, as well as any other agreements with external employees has to be re-certified from time to time.

The organization unit makes an agreement with the physician for working as a researcher in the organization.

Corresponding secretary enters the researcher's working / service period information to the external master data system and defines the external organization for the person.

The corresponding secretary enters the information concerning the organization: the unit responsible for the researcher, the person responsible for the external and the task for the researcher.

The IAM system recognizes the external person from the external data master, recognizes the person as an insider as well and processes it.

The IAM system creates an external user for the research work and then creates automatically user rights according to pre-defined rules to the Active Directory and Passage Control system.

The AD user account is inactive until the agreement of research comes into effect.

The IAM system sends a service request to the user access management administrators to execute the needed pre-defined user and access right management actions by the due date. The user access management administrators create pre-defined user account and user rights to the manually provisioned target systems.

The access management administrators enter the information to the IAM system.

The IAM system sends an email concerning the new user to the corresponding secretary, supervisor or contact person and to the Registration Authority (RA).

When the contract of service comes into effect, the AD user account will be activated.

The process in the RA is similar to the internal employee's one. The RA officer gives a smart card and a PIN code to be used in the research work. The smart card is attached to the researcher's AD user account using UPN.

The first time use is similar to the internal employee's one.

The corresponding secretary, supervisor or the contact person for the researcher requests for additional user rights if needed from the IAM system's ordering view.

The owner of each information system accepts or rejects the request if needed.

The requested user rights are provisioned automatically or a manual service request is sent to the system administrators to be executed.

The executed user rights request is entered to the IAM system with a status "completed".

A post process

The researcher logs into the IAM system and is allowed to view the user rights and requests concerning the user.

The researcher is not allowed to request user rights directly. The contact person or supervisor always requests additional user rights for the researcher.

5.3 Fixed-term employees

5.3.1 A new fixed-term employee

The supervisor or corresponding secretary enters the information of the employee to the HR system and supplements the employee information to the master data system.

The IAM system reads the new employee information from the master data system and processes it.

The IAM system creates the user identity and then creates automatically user rights according to pre-defined rules to defined key target systems e.g. Active Directory, Electronic Patient Record (EPR), Hospital Information System (HIS) and to workshift list planning system, but not to the passage control system.

User accounts and the AD user account are inactive until the contract of employment comes into effect.

If there is a plan for the organization to start using the eSSO system sometimes in near future, the IAM system should also provision the user information to the eSSO system.

The IAM system sends a service request to the user access management administrators to execute the needed user and access right management actions by the due date. The system administrators create pre-defined user accounts and user rights to the manually provisioned target systems. Further system administrators attach user's system-specific login and password information to the eSSO system to prevent the user from doing this time-consuming task.

The system administrators enter the information to the IAM system.

The IAM system sends an email concerning the new user to the corresponding secretary, supervisor and to the Registration Authority (RA).

When the contract of employment comes into effect, the AD user account will be activated.

A new fixed-term employee in the RA

Secretary schedules an appointment for the employee to the RA.

The employee is photographed for an identity card and a PCR smart card.

If the employee does not have a smart card provided by the PCR, the RA officer orders a primary health care smart card for the employee and gives a temporary smart card and a PIN-code to the employee. The RA officer enters the deeds of transference to the IAM system.

If the employee has the health care smart card, The RA officer then attaches the certificate on the card to the AD user account using a UPN attribute.

The RA officer hands over the electronic key to the employee and attaches the key to the user using a passage management system. The user receives automatically pre-defined rights to the doors of the organization. The RA officer enters the information to the IAM system.

The RA officer hands over the rest of the keys related to the work tasks of the employee and enters the information to the IAM system.

A new employee – the first time use

The employee logs in to the domain using the smart card's authentication key.

The rules for using the organization's information systems and access rights contract open for the user in a separate window.

The domain login asks the user to approve of the rules for using the information systems.

The user accepts the rules by signing the contract using non-repudiation certificate on the smart card.

The IAM system allows the user to access the user’s virtual desktop and to login to the organization’s workstation.

The IAM system creates a report of the user rights contract and archives it.

The user uses the information systems according to the given user rights.

The corresponding secretary or supervisor requests for additional user rights if needed with the IAM system separate ordering view.

If the secretary requests the additional user rights, the user’s supervisor has to approve of or reject them.

The owner of each information system accepts or rejects the request if needed.

The requested user rights are provisioned automatically or a manual service request is sent to the system administrators to be executed.

The executed user rights request is entered to the IAM system with a status “completed”.

A post process

The user logs in to the IAM system and is able to the view current user rights and user rights requests concerning the user with the relevant status information.

The user requests more user rights using the IAM system.

The user’s supervisor (or a person authorized by the supervisor) approves of or rejects the requests using the IAM system, an IAM portal or an email link sent by the IAM system.

The supervisor is able to view the user rights he or she has approved or rejected.

The user is able to view rejected user rights requests in the IAM system.

The user can renew the user rights requesting process in case the reasons differ from the previous request.

The system owner approves of or rejects the requested user rights in the IAM system by using the IAM system, an IAM portal or using an email link sent by the IAM system.

The user and the supervisor are able to view the user requests rejected by the system owner.

The employee gets an announcement of an arrived smart card and fetches the card from the RA.

The employee returns the temporary smart card. The RA officer attaches the UPN information of the new certificate to user’s AD user account and removes the temporary card.

5.3.2 A new fixed-term employee (less than 12 days)

If the employment contract is less than 12 days, the employee information is not entered to the HR system in the beginning. Work period information is entered directly to the master data system instead. A fixed-term, less than 12 days lasting employment contract can arise when a substitute is quickly called to work in a night shift. In this case the employee already has the PCR smart card for health care professionals. If the employee does not have a PCR smart card for regulated health care professionals, the employee has to get a card for non-regulated health care workers.

The supervisor, other authorized employee or corresponding secretary enters the employee's information to the data master system. If the employee already exists in the data master system, the employee's information will be activated and the new work period will be added to the system. During the night the supervisor or another authorized employee attaches the employee's smart card to the master data information. If the employee does not have a smart card, the employee will get a replacement card.

The IAM system reads the new employee's information from the data master system and processes it.

The IAM system creates the user identity and then creates automatically user rights according to pre-defined rules to the defined key target systems e.g. Active Directory, Electronic Patient Record (EPR), Hospital Information System (HIS).

The IAM system activates the Active Directory user account.

The IAM system sends an email concerning the new user to the corresponding secretary, supervisor and RA.

The employee logs in to domain using the smart card's authentication key.

The rules for using the organization's information systems and access rights contract open for the user in a separate window.

The domain login asks the user to approve the rules for using information systems.

The user accepts the rules by signing the contract using a non-repudiation certificate on the smart card.

The IAM system allows the user to access the user's virtual desktop and to login to the organization's workstation.

The IAM system creates a report of the user rights contract and archives it.

The user uses information systems according to the given user rights.

The supervisor, other authorized employee or corresponding secretary requests for additional user rights if needed with the IAM system separate ordering view.

The owner of each information system accepts or rejects the request if needed. The requested user rights are provisioned automatically or a manual service request is sent to the system administrators to be executed.

The executed user rights request is entered to the IAM system with a status “completed”.

A post process

On the next morning the IAM system sends the supervisor or corresponding secretary a report of every added user and changed user right the authorized employee has done. The supervisor or corresponding secretary checks that the information added or changed is correct.

The user logs in to the IAM system and is able to view the current user rights and user rights requests concerning the user with relevant status information.

The user requests more user rights using the IAM system.

The user’s supervisor (or a person authorized by the supervisor) approves of or rejects the requests using the IAM system, an IAM portal or an email link sent by the IAM system.

The supervisor is able to view the user rights he or she has approved of or rejected.

The user is able to view the rejected user rights requests in the IAM system.

The user can renew the user rights requesting process in case the reasons differ from the previous request.

The system owner approves of or rejects the requested user rights in the IAM system by using the IAM system, an IAM portal or using an email link sent by the IAM system.

The user and the supervisor are able to view the user requests rejected by the system owner.

5.3.3 Termination of a fixed-term employment

A month before the termination date of the employment, the IAM system sends a service request to the supervisor, corresponding secretary and the employee via email.

If the supervisor or corresponding secretary does not acknowledge the service request to the IAM system, the IAM system sends a new service request one week before and again one day before the termination date of the employment. If the service request is acknowledged, new requests will not be sent.

The IAM system inactivates the employee's AD user account after a waiting period e.g. 2 business days after the termination date of the employment.

The IAM system disables user rights automatically from the automatic provisioning systems. The IAM system sends an email service request to the system administrators concerning the manual provisioning to disable the employee's user accounts.

The system administrators execute the task and enter the information to the IAM system as a completed task.

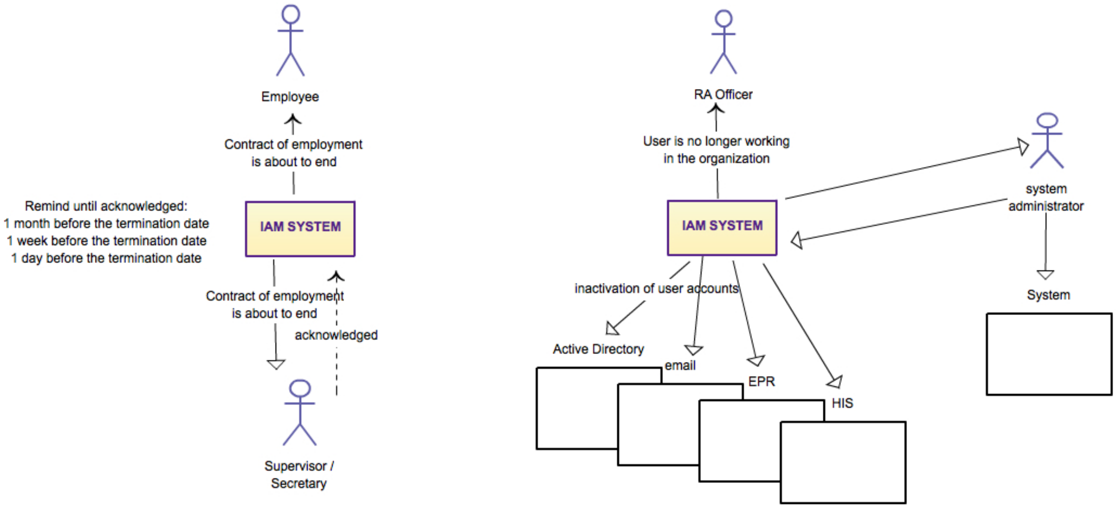

Employee
Contract of employment is about to end
Remind until acknowledged:
1 month before the termination date
1 week before the termination date
1 day before the termination date
IAM SYSTEM
Contract of employment is about to end
acknowledged
Supervisor / Secretary
RA Officer
User is no longer working in the organization
system administrator
IAM SYSTEM
inactivation of user accounts
System
Active Directory
email
EPR
HIS

FIGURE 18. Termination of fixed-term employment (Virkkunen, Sanna, 2014)

The user returns the smart card, ID card and keys to the RA officer.

If the user does not return the items, the IAM system sends a reminder to the RA officer who then acts according to given orders.

After a fixed-term (less than 12 days) employment the IAM system sends a reminder to the corresponding secretary to enter the employee data to the HR system for paying the salary.

5.3.4 A fixed-term employee's organization unit changes

The employee arranges the transfer to another organization unit. The corresponding secretary of the new unit enters the new working period to the HR system beforehand. The information is transferred to the master data system. At the same time the corresponding secretary or the contact person arranges the situation with the previous unit is corresponding secretary and the date of termination is set for the previous working period.

The IAM system recognizes a change in the working period information and sends an email concerning the change to the user and to the supervisors and corresponding secretaries of the old and new organization units.

Otherwise the IAM system functions are similar to permanent employee’s ones.

A removal of old user rights should be done so that they are active for a month after the date of change to enable a transitional period.

5.3.5 A fixed-term employment relationship continues

An employee is called back to work after the employment has ended or the employment relationship has broken accidentally.

The supervisor or corresponding secretary enters the information of the employee’s work period to the HR system and supplements the employee information to the master data system if needed.

The IAM system reads the employee’s information from the master data system and processes it.

The IAM system creates the user identity and then creates automatically user rights according to pre-defined rules to the defined key target systems e.g. Active Directory, Passage Control system, Electronic Patient Record (EPR), Hospital Information System (HIS) and to workshift list planning system. If the user accounts already exist, they will be activated.

User accounts and the AD user account are inactive until the contract of employment comes into effect.

The IAM system sends a service request to system administrators to execute the needed user and access right management actions by the due date. The system administrators create pre-defined user accounts and user rights to the manually provisioned target systems. If the user account already exists, it will be activated.

The system administrators enter the information to the IAM system.

The IAM system sends an email concerning the returning user to the corresponding secretary, supervisor and to the Registration Authority (RA).

When the contract of employment comes into effect, the AD user account will be activated.

A returning employee in the RA

The secretary schedules an appointment for the employee to the RA.

The RA officer gives the employee the ID card.

If the employee does not have a smart card provided by the PCR anymore, the RA officer orders a primary health care smart card for the employee and gives a replacement smart card and a PIN-code to the employee. The RA officer enters the information to the IAM system.

If the employee has the health care smart card, the RA officer then attaches the certificate on the card to the AD user account using a UPN attribute.

The RA officer hands over the electronic key to the employee and attaches the key to the user using a passage management system. The user receives automatically pre-defined rights to the doors of the organization. The RA officer enters the information to the IAM system.

The RA officer hands over all the rest of the keys related to the work tasks of the employee and enters the deed of transference to the IAM system.

A returning employee – the first time use

The employee logs in to domain using a smart card's authentication key.

The rules for using the organization's information systems and access rights contract open for the user in a separate window.

The domain login asks the user to approve the rules for using the information systems.

The user accepts the rules by signing the contract using a non-repudiation certificate on the smart card.

The IAM system allows the user to access the user's virtual desktop and to login to the organization's workstation.

The IAM system creates a report of the user rights contract and archives it.

The user uses information systems according to the given user rights.

The user, corresponding secretary or supervisor requests for additional user rights if needed with the IAM system's separate ordering view.

If the user or the secretary requests the additional user rights, the supervisor of the user has to approve of or reject them.

The owner of each information system accepts or rejects the request if needed. It is not mandatory for every system that the system owner approves the requested rights. In most cases the requests are transmitted directly to the system administrators for execution.

The requested user rights are provisioned automatically or a manual service request is sent to the system administrators to be executed.

The executed user rights request is entered to the IAM system with a status “completed”.

A post process

The user logs in to the IAM system and is able to view the current user rights and user rights requests concerning the user with relevant status information.

The user requests more user rights using the IAM system.

The user’s supervisor (or a person authorized by the supervisor) approves of or rejects the requests using the IAM system, an IAM portal or an email link sent by the IAM system.

The supervisor is able to view the user rights he or she has approved of or rejected.

The user is able to view the rejected user rights requests in the IAM system.

The user can renew the user rights requesting process in case the reasons differ from the previous request.

The system owner approves of or rejects the requested user rights in the IAM system by using the IAM system, an IAM portal or using an email link sent by the IAM system.

The user and the supervisor are able to view the user requests rejected by the system owner.

The employee gets an announcement of an arrived smart card and fetches the card from the RA.

The employee returns the temporary smart card. The RA officer attaches the UPN information of the new certificate to user’s AD user account and removes the temporary card.

5.3.6 A new internal substitute

The employee can be hired as an internal substitute. In the beginning of the employment it will be defined, which organization units the employee will work in. Pre-defined user rights include all the shared folders of the organization units and all the HIS and EPR user rights according to organizational roles. The work organization unit can be named as an “internal substitute organization” in the HR system or one of the organization units (a so called home organization) the employee is working in. However, all the employee’s organization units have to be entered in the master data system. Internal substitutes have extended user rights. The supervisors of each organization unit the employee is working in will request the user rights for the internal substitute.

The HR or master data system contains all personnel, working period and internal substitute information.

The IAM system reads the employee's information from the data master system and processes it.

The IAM system creates the user identity according to the home organization information and then creates automatically user rights according to pre-defined rules to defined key target systems e.g. Active Directory, Passage Control system, Electronic Patient Record (EPR), Hospital Information System (HIS) and to workshift list planning system. If the user accounts already exist, they will be activated.

User accounts and the AD user account are inactive until the contract of employment comes into effect.

The IAM system sends a service request to system administrators to execute the needed user and access right management actions by the due date. The system administrators create pre-defined user accounts and user rights to manually provisioned target systems. If the user account already exists, it will be activated.

The system administrators enter the information to the IAM system.

The IAM system sends an email concerning the returning user to the corresponding secretary, supervisors and to Registration Authority (RA).

When the contract of employment comes into effect, AD user account will be activated.

The process in the RA is similar to other internal employees' one.

The first time use process is similar to other internal employees' one.

A post process is similar to other internal employees' one.

5.4 A long-term absence

When the information concerning a long-term absence is acknowledged, the corresponding secretary enters the information to the HR and / or master data system.

The IAM system reads the information and inactivates all the user rights and accesses for the user.

In cases of research or training leave the defined researcher use case allows the employee to use organization's systems.

The smart card for regulated health care professionals is personal, not to be returned to the RA.

5.5 VPN users

5.5.1 A new VPN user (VPN client or VPN between organizations)

There is always a contract-based process with the organization.

The organization unit makes an agreement with the organization for providing a VPN client to an external individual.

The ICT management enters information of the external to the external master data system and defines the external organization for the person. The ICT Management classifies the user as a VPN user.

The ICT Management enters the information concerning the organization: the unit responsible for the external, the person responsible for the external and the task for the external.

The IAM system recognizes the external person from the data master and processes it.

The IAM system creates the user identity and then creates automatically user rights according to pre-defined rules to Active Directory.

The AD user account is inactive until the contract comes into effect.

The IAM system sends a service request to the system administrators and to network specialists to execute the needed pre-defined user and access right management actions by the due date.

The system administrators create pre-defined user accounts and user rights to manually provisioned target systems.

The system administrators enter the information to the IAM system.

The IAM system sends an email concerning the new user to contact person, supervisor and the person responsible for the external employee and to the Registration Authority (RA).

When the contract of service comes into effect, the AD user account will be activated.

The process in the RA is similar to the internal employee's one. The RA officer gives the external employee a smart card and a PIN code. The smart card is attached to the external employee's AD user account using a UPN.

The first time use is also similar to the internal employee's one. A VPN connection is used for the first time login.

The contact person requests for additional user rights if needed with the IAM system's ordering view.

The owner of each information system accepts or rejects the request if needed

The requested user rights are provisioned automatically or a manual service request is sent to the system administrators to be executed.

The executed user rights request is entered to the IAM system with a status “completed”.

A post process

The external user logs into the IAM system and is allowed to view the user rights and requests concerning him / her.

The external user is not allowed to request user rights directly.

5.5.2 A VPN user: re-certificating an external user and a renewal of the contract

The contractual relationship has to be renewed every six months concerning the user information.

A month before the due date of the renewal, the IAM system send a service request to the corresponding secretary or the external employee’s contact person.

If the corresponding secretary or the person in charge of the external does not acknowledge the service request to the IAM system, the IAM system sends a new service request one week before and again one day before the due date of the contract. If the service request is acknowledged, new requests will not be sent.

If the external employee is still in the service of the organization unit, the corresponding secretary or contact person approves of the renewal. At the same time the external organization information will be checked. If the external employee is no longer working for the organization unit, the renewal is rejected.

Unless renewed, after the recertification date or due date of the contract the IAM system inactivates external user’s AD user account.

The IAM system disables external user’s other user rights automatically after a period of time.

The IAM system sends an email service request to system administrators concerning manual provisioning to disable the employee’s user accounts.

The system administrators execute the task and enter the information to the IAM system as a completed task.

The external user returns the smart card to RA.

If the user does not return the items, the IAM system send a reminder to the RA officer who then acts according to given orders.

The information of inactivation is also archived in the external master data system.

5.5.3 A VPN user: the termination of the contract with an external user or an organization

When the information concerning the termination of contract is acknowledged, the corresponding secretary enters the information to the external master data system. It is possible that the termination date has already been entered to the external master data system. The information transfers to the IAM system.

A month before the due date of the contract, the IAM system sends a service request to the supervisor, corresponding secretary or the contact person and the external user via email.

If the supervisor, corresponding secretary or the contact person does not acknowledge the service request to the IAM system, the IAM system sends a new service request one week before and again one day before the due date of the contract. If the service request is acknowledged, new requests will not be sent.

The IAM system inactivates the external employee’s AD user account after a waiting period e.g. 2 business days after the termination date.

The IAM system disables user rights automatically from the automatic provisioning systems. The IAM system sends an email service request to system administrators concerning manual provisioning to disable the external’s user accounts.

The system administrators execute the task and enter the information to the IAM system as a completed task.

The user returns the smart card, ID card and keys to the RA officer.

If the user does not return the items, the IAM system sends a reminder to the RA officer who then acts according to given orders.

The information is also archived to external master data system.

6 TECHNICAL CHALLENGES AND REQUIREMENTS

It is very important to integrate infrastructure services to the IAM system because they represent big masses of users. For example, in NOHD network services, Active Directory, disk allocation services, a telephone center system, passage control systems and a remote access service should be integrated to the IAM in some time span. Characteristic to health care information systems, they have been programmed with different techniques for almost three decades. This means the IAM system has to support at least Windows client programs, character-based systems, Java Applet based and web-based software.

The IAM system has to be scalable yet agile. It has to be possible to build new interfaces to the system for transferring identity information to a target system. As mentioned before, integration and building adapters has to be considered carefully since scripting and building them tend to be expensive. It might be a good idea to ask vendors for interface descriptions and training for building adapters.

When provisioning the identity and user account information to the target system, it should be possible for the integration adapter or equivalent interface to add a new user to the system, to update the user's information, to define the ending date of the user account validity, to change the ending date, to remove a person, to inactivate a user account and to activate the user account. There should also be a possibility to reset password for the user and to define the password for the user. When adding a new user account, there should be a checking functionality available to check whether or not the user already exists. If the user already exists with the same unique identifier, the old inactive user account should be activated. If the user already exists with another unique identifier, the IAM system has to suggest a new user name according to the rules defined by each target system.

6.1 HR and master data system

When planning the IAM system deployment project it is important to decide from where to begin. At first the IAM system has to be integrated to the master data e.g. the HR system or master data system. For the integration there are some details that need to be decided: how often the HR / master data system will update the identity information to the IAM system? What triggers the updating process? This depends on the technologies used for the integration. For example, when using an integration platform with an ability for a scheduled batch processing, it might be convenient to use hourly update messages for identity and work period information.

Using a separate integration platform enables a more secure logging that helps debugging if transfer issues arise. Typically it is complicated to build up an interface directly to the HR system. Master data systems on the other hand provide different interfaces for the IAM systems, using e.g. a webservice, JDBC, JSON, REST or using SOAP, CSV-files and an XML-interface.

6.2 An Active Directory and Email

Another integration task will be integrating Active Directory and email, e.g. Exchange. Integrating Active Directory and Exchange to the IAM systems is a common task for vendors. It can be said every IAM system has ready-made adapters for these basic systems.

In order to integrate Active Directory, it should be consolidated and its contents should be cleaned up if the data quality is incoherent. There should be at least one unique attribute for each user account and especially in health care, the same user login name should not be re-used to fulfill auditing requirements. This check-up has to be made with every IAM provisioned user account creation. If there are any organizational structures or access management features created with AD user groups, it should be reconsidered, whether it is the AD or IAM doing the ruling and roling. AD will be the first target system where system roles and IAM roles need to be reconciled.

6.3 An Electronic Patient Record and Hospital Information System

Being one of the key systems in the health care organization, an electronic patient record (EPR) should be integrated to the IAM system. The whole medical staff uses the EPR as the primary source of patient information. The EPR has all the patients' medical data in a viewable form, including medication, allergies, laboratory information, radiological images and information etc. The information shown in the EPR can be a collectable view from other sub-systems, such as a radiology information system RIS.

As mentioned before, according to Kanta auditing requirements the user should use the PCR's certificates to log in the EPR to use national Kanta services. All the EPR system roles have to be reconciled to the IAM system to fulfill the auditing and legislative requirements. EPR system roles should be created according to organizational and work roles so that every employee is provided only the information needed in their daily work. As mentioned before, the classified information such as psychiatric and genetic information is available in the EPR only for specific employees. These EPR role definitions have to be synchronized with IAM role definitions.

The same requirements also concern hospital information system (HIS). The medical staff uses HIS for managing the operational aspects of patient care e.g. handling appointments. HIS is modularly connected to all aspects of hospital management.

Common to EPR and HIS users is that the user history has to be audited. Therefore, the log data and the transaction file have to be archived for 12 years from the creation of the data entry. In addition, if the user is under a suspect of misuse of the patient information during the employment, the information has to be held until the end of the process.

6.4 Other Health Care Systems

There are also many other health care systems that need to be integrated to the IAM system. The systems processing patient information have a different authentication method, auditing and logging requirements than the systems that are supporting the patient care other ways. For example, there are systems for planning workshift lists for nurses and physicians, systems for managing medical appliances and therapy services, systems for dictation, and different systems for clinical usage.

Nowadays one of the challenging access management tasks in health care comes from the use of tablets and own laptops. Sophisticated identity and access management systems have also implementations for an 802.1x authentication. The IAM system should provide an authentication interface for using a role based network access (vlan 802.1x).

6.5 Commissioning, Maintenance and Management of the IAM System

6.5.1 Commissioning

When commissioning the IAM system, the vendor should describe the process of reconciling the target systems' user information with the initial identity material gathered from the master data. On the other hand the vendor should also be able to describe the top-down point of view mentioned in chapter 3.9. The vendor should describe how the reconciliation will be done after the deployment of the IAM system. If the vendor offers role mining tools they should be described. Again the used techniques for role -mining may be top-down, bottom-up or hybrid of these two.

The IAM system vendor has to commit good information management practices, and the system should have a centralized maintenance and system management. All the possible fault situations should be fixed centralized using a remote access. Another good tool for evaluating different IAM vendors is to ask them to describe typical problems and issues within the system and the repair mechanisms for them. The system vendor should also commit to document all the issues and their fixes real-time. Naturally, the user interface of the IAM system should be Finnish in Finland. However, the administrator's user interface could be in Finnish or in English.

6.5.2 Documentation

A documentation is one of the key sources for the organization to manage the deployment project and also after the rollout, during the use. It is typical that the quality of the documentation is poor or the documentation is not up to date. In some cases the vendor has claimed the documentation can be made as a separate project, billed separately. However, the documentation should be created during the project to keep the vendor and the customer up to date concerning the situation of the software development and the project.

The vendor should provide a graphical description of the system, a configuration of the system, a guideline for setting up the system, work guides, user manuals for the IAM system administrators and ordinary users and an education material to be used during the roll-out. These documents create the documentation. In addition, the system vendor has to document all installations and changes done to the system in real time. The documentation is a real-time process, and this makes the documentation provided to the customer always up to date.

6.5.3 Architecture

The system should be deployed in a production environment, a test environment and an educational environment. In some rare cases the test environment can be used as an educational environment. The functionality of the IAM system is tested thoroughly in the test environment. During the test vulnerability, usability, integration and requirements mentioned in the requirements analysis will be tested. The testing protocol covers the system, integration and acceptance testing as well as performance tests and system security testing.

6.5.4 Safety and redundancy

Identity and access management should be as invisible as possible for the user. The user should not be waiting no longer than 10 seconds for the system to process the given task. This has to be observed when defining the system hardware specification. The system performance of the system may not be adversely affected, even if there would be hundreds of simultaneous users. The user interface has to be informative and it should inform the user if some operation is delayed or an error occurs. The IAM system has to be able to inform users before a forthcoming planned outage. The IAM system also has to be able to inform the users during the outages. All system databases have to be secured and in cases of need recovered. The vendor has to ensure that none of the IAM information is lost.

After taking the IAM system into production, an individual outage duration can be 15 minutes maximum during 7am – 7pm and 1 hour maximum during other times. This will not be the case with the scheduled outages. Each organization should describe the redundancy requirements and related sanctions suitable for their own needs.

The vendor should describe how the IAM system handles the situation with provisioning, reporting, inactivation of rights and other IAM processes, when the target system is out of use, the IAM integration interface to target system is out of use or the IAM system is out of use.

6.5.5 A Method of Procuring the IAM System

When procuring the IAM system as an investment, the system software is installed to the organization’s hardware unless the hardware is included to the price of the offer. The initial investment is relatively high if compared to Software as a Service (SaaS) model and the organization has to pay for the licenses, usually according to active users. In a SaaS model the organization pays only for the software leases as a tenant. The model is often justified using the argument of reducing the costs in hardware. However, the costs reallocate paying for the services and the hardware of the SaaS vendor as a lease. In a SaaS model the IAM system is deployed as a hosted service that can be accessed over the Internet. (30.)

In health care procuring the IAM system as a SaaS model is not problem-free. The IAM system contains sensitive information, e.g. social security numbers, Valvira IDs, home addresses and other attributes in addition to user names and passwords. When the IAM system is deployed in a SaaS model and the other applications of the organization are on-premise, the data will be transferred via the Internet. It is an information security risk to run SaaS services through the Internet as it makes services susceptible for man in the middle attack or similar techniques. (31.)

A health care organization is always responsible for the availability, usability and reliability of the data regardless of the chosen method of procurement. This is the case during the contract period but also in the possible event of bankruptcy of the vendor. With a SaaS model it will be laborious to change the vendor or the platform once all the data has been installed and adapters made for the specific environment. Changing the SaaS vendor can also cause problems to the archiving, auditing and reporting requirements discussed earlier in this document.

If the chosen type of procurement is investment, a technical operating environment should be carefully documented. In the case of investment the system has to function in the workstation and server environment of the organization. The domain structure has to be documented, as well as the used group policies. The workstations used in the organization have to be defined for the vendor to avoid a dysfunctional system. Also, used database technologies and techniques used for virtualization have to be explained for the vendors.

7 CONCLUSIONS AND POSSIBILITIES OF FURTHER DEVELOPMENT

Writing requirements specification for an IAM system requires a deep understanding of organization's identity processes. The knowledge of identities can not be found in the ICT department of the organization, it is the silent wisdom of the HR department that needs to be found out instead. However, it is the know-how of the ICT department that will make controlling the identities easier. When planning an identity and access management project, it is essential to have these two departments to combine their super-powers.

Developing the IAM process and supportive processes in NOHD was essential for the organization to gain a sufficient maturity level to deploy the IAM system. For example, creating the PKI environment and the procedure for attaching the PCR's smart card to a user account in Active Directory was a prerequisite to merge users, identities and smart cards.

The IAM system is one of the largest information systems in a health care organization. It will be integrated to almost all other applications used in the organization. Needless to say, the IAM system and adapters have to be robust and safe to use. This work describes a base line for defining a system safety and redundancy. However, each organization has to modify this base to suit their needs.

The Use cases described in this work have been created for the needs of NOHD. Some of the use cases are universal and can be used in every organization. It is still needed that the organization's IAM project immerses in the basic needs and functionalities of the identity and access functionalities in practice to really understand the tiny details that actually could become big obstacles unless defined.

What is notable is that the master data has to be coherent. All water runs downwards, also dirty water. If the quality of the master data is poor, all the rest of the processes will be defective. Luckily, in a health care organization the master data is created based on strict working and service periods. These periods are the true beacons for managing identities and accesses. Having such a firm way of handling periods helped to realize that the identity can be born at any moment the information of the person comes to the organization. Yet the born identity does not dictate to the date when the identity, user and access rights will be active. The information written in the contract of employment is the determining factor for activating identity and access rights. Contracts and agreements define the starting and terminating dates for active periods. After the termination date the identity is still present but not active. Honoring this principle is a key factor for using RBAC in health care master data. It is in fact this matter that enabled the possibility to consider multi-role identities to be manageable. Using smart cards for authenticating the person and the working or service periods to determine roles with each active identity period make managing multi-role identities easier. Previously managing multi-roles has been very problematic.

The IAM is a never-ending process. After the critical and key systems have been integrated to the IAM system, there will always be yet another integration to build. New information systems will be deployed and they need to be integrated to the IAM system. The legislation changes all the time, and the organization structures changes. All these affect the IAM processes and the IAM system. However, handling and controlling these significant changes will be easier when there is one process motor to be configured. There will also be changes to target systems outside the IAM process. Reconciliation has to be made regularly to find out the changed user information, attributes and deleted users. Reconciling the systems with the IAM system requires planning the workflow for reconciliation: how to manage the differences in each case? Will it be a manual process or does the IAM system have tools for automation? The same goes with role mining. The roles will change in process of time so they have to be updated in specified periods.

Many clinical systems have been integrated to the EPR system using the desktop integration. When the basic, most critical information systems have been integrated to the IAM system, it is also necessary to integrate these clinical systems to it. However maintaining the role information in these systems is not straightforward. Within the desktop integration a user and patient context is included. The transfer does not include role information. It can be possible that these systems don’t have any system role abilities at all and restricting access rights according to the organizational and work roles may not be possible. These cases have to be recorded as exceptions of information security policy.

Choosing the best business model for the organization when procuring the IAM system is also a subject of consideration. If the organization does not have its own data centre, it is reasonable to contemplate the SaaS model, too. Regardless of the chosen business model, the health care organization is always responsible for the data. However, when settling on the SaaS model the contract has to be done extremely carefully taking every aspect of management and maintenance of the system into account.

REFERENCES

1. Garamone, J. 2010. Cybercom Chief Details Cyberspace Defense. U.S. Department of Defense. 23.9.2010. Date of retrieval 6.1.2014.
http://www.defense.gov/news/newsarticle.aspx?id=60987.

2. Pettey, C. & Goasduff, L. 2013. Gartner Says Worldwide IT Spending Forecast to Reach $3.7 Trillion in 2013. Date of retrieval 31.12.2013
http://www.gartner.com/newsroom/id/2292815.

3. Rivera, J & van der Meulen R. 2013. Gartner Says Worldwide Security Market to Grow 8.7 Percent in 2013. Date of retrieval 31.12.2013
http://www.gartner.com/newsroom/id/2512215.

4. Remes, J. 2013. Dise käyttäjäpäivät Opening lecture 30.10.2013.

5. Symantec Corporation. 2013. Internet Security Threat Report 2013. Volume 18. Date of retrieval 2.1.2014
http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf.

6. Ministry of Finance 2006. Käyttövaltuushallinnon periaatteet ja hyvät käytännöt VAHTI 9/2006. Date of retrieval 4.12.2013.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061122Kaeyttoe/vahti_9_06.pdf

7. Ministry of Finance, Vahti-ylläpito, 2009. Hyvän käyttövaltuushallinnon edellytysten luominen. Date of retrieval 4.12.2013.
https://www.vahtiohje.fi/web/guest/hyvan-kayttovaltuushallinnon-edellytysten-luominen.

8. Cobit 4.1. 2007. IT Governance Institute.

9. Kunnas, J. 2013. IDM Master education material.

10. Act on the status and rights of patients 785/1992.

11. Decree on the creation and storage of patient records and other health care data 298/2009

12. FINeID. mPollux DigiSign Client card reader software. Date of retrieval 28.12.2013.
http://fineid.fi/default.aspx?id=494

13. Ministry of Social Affairs and Health, 2013. Kansalliset auditointivaatimukset terveydenhuollon organisaatioille versio 2.0.

14. Pohjois-Pohjanmaan sairaanhoitopiirin kuntayhtymä, 2013. IDM-järjestelmän vaatimusmäärittely, 23.12.2013.

15. FINeID. Smart cards, certificates and services. Date of retrieval 28.12.2013.
http://www.fineid.fi/default.aspx?id=638

16. Caralli, R. A., Allen, J.H. & Curtis, P. D. et al. 2010. CERT Resilience Management Model, Version 1.0, May 2010.

17. Korhonen, E. & Lamminen L. 2013. Kainuun keskussairaala. Interview 14.11.2013.

18. Huhta, M. 2013. Email. ADn käyttäjäobjektien käsittelyaika-arvioita käyttöoikeuslomakkeiden ja sähköpostitilausten perusteella… 30.10.2013.

19. Balasubramaniam, S. & Lewis, G. A. 2009. Identity Management and its Impact on Federation in a System-of-Systems Context. March 2009.

20. Linden, M. 2008. CSC. Ajankohtaista identiteetinhallinnassa. October 2008.

21. Karhunen, P. 2013. Interview. 8.10.2013.

22. Buecker, A., Filip, W., Palacios, J. M. & Parker, A. 2009. Identity Management Design Guide with IBM Tivoli Identity manager. Fourth Edition. November 2009. Date of Retrieval 31.1.2014
http://www.redbooks.ibm.com/redbooks/pdfs/sg246996.pdf

23. Tipton, H. F. 2010. Official (ISC)2 guide to the CISSP CBK 2nd ed. Boca Raton, FL:Taylor & Francis Group, LLC, Auerbach Publications

24. Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007.

25. Personal Data Act 523/1999

26. Linden, M. 2012. Identiteetin- ja pääsynhallinta luentomoniste. 9.1.2012. Date of retrieval 5.1.2013.
http://www.cs.tut.fi/~linden/iam-pruju.pdf.

27. Coyne, E. Weil, T. R. 2013. ABAC and RBAC: Scalable, Flexible and Auditable Access Management. Publications of the IEEE Computer Society. May/June 2013. Date of retrieval 5.1.2013.
http://csrc.nist.gov/groups/SNS/rbac/documents/coyne-weil-13.pdf.

28. Minimikontekstinhallinnan määrittely. Versio 3.0. 2006. HL7 Finland ry.

29. Sun Identity Manager Deployment Guide. 2010. Oracle. Date of retrieval 8.1.2014.
http://docs.oracle.com/cd/E19225-01/820-5820/ahucl/index.html

30. Chong, F. & Carraro, G. 2006. Architecture Strategies for Catching the Long Tail. April 2006. Date of retrieval 8.1.2014.
http://msdn.microsoft.com/en-us/architecture/aa479069.aspx.

31. Identity Management as a ServiceDeploying IAM in a SaaS Model. 2011. Hitachi ID Systems, Inc. 2011. Date of retrieval 8.1.2014.

http://www.slideshare.net/HitachiID/identity-management-as-a-service-deploying-iam-in-a-saas-model.

32. ISO 27799:2008. International Standard. Health Informatics – Information security management in health using ISO/IEC 27002. ISO 2008.

33. Kunnas, J. 2012. OYS – Käyttövaltuuksien hallinnan esiselvitys, etenemissuunnitelma versio 0.7. 20.1.2012.