**Aalto University
School of Electrical
Engineering**

Lauri Laitinen

Case study on identity and access management in an EU level pharmaceutical company

Thesis for Master of Science degree has been submitted for approval in

Espoo, on 23rd May 2016.

Supervisor: Professor Jukka Manner
Advisor: MSc Antti Väänänen

Author Lauri Laitinen

Title of thesis Case study on identity and access management in an EU level pharmaceutical company

Degree programme Communications engineering

Major/minor Data networks   **Code** S3022

Thesis supervisor Prof. Jukka Manner

Thesis advisor(s) MSc Antti Väänänen

Date 23.05.2016   **Number of pages** 10+58   **Language** English

Abstract

Today, the world becomes ever more computerized and a growing number of users possess an increasing amount of different identities in this digitalizing world. Nevertheless, users have to be able to run these computerized systems smoothly in this changing environment. In order to do so, digital identities and their access rights have to be properly managed and controlled along the various stages of their life cycle. This so called identity and access management is useful or even essential especially for large organizations with hundreds or thousands of internal and external users.

The goal of this thesis was to investigate the possibilities to standardize the identity and access management of a large European company that works closely with pharmaceutical business. The aim was also to get an overview of the level of identity and access management within the member countries of this organization.

Carried out as a case study, the research in this work is based on a survey sent to the member countries of this company. The survey was answered by leading experts and decision-makers in these corresponding states. The possibilities for standardization were then analyzed according to the results of the survey.

The contents of the diploma work are divided into theory and research parts. The theory part provides fundamental information on identity and access management and gives a glance at the future trends of the field. In addition, readers are briefly introduced to international regulations, which guide not only pharmaceutical business in general, but also the implementation and maintenance of computer systems in this business.

The research part explores the identity and access management of the company under study. First, some general information is provided about the target company and the research procedures. After this, the actual results will be presented and analyzed. The questions are divided into several categories, depending on the ways how the results are analyzed. Finally, the conclusions and possible further actions will be summarized.

Keywords IAM, IDM, identity, life-cycle, identity management, access management, pharmaceutical

Tekijä Lauri Laitinen

Työn nimi Tapaustutkimus tunnusten- ja pääsynhallinnasta EU-tasoisessa lääketieteellisessä yrityksessä

Koulutusohjelma Tietoliikennetekniikan koulutusohjelma

Pää-/sivuaine Tietoverkot   **Koodi** S3022

Työn valvoja Prof. Jukka Manner

Työn ohjaaja(t) DI Antti Väänänen

Päivämäärä 23.05.2016   **Sivumäärä** 10+58   **Kieli** englanti

Tiivistelmä

Nykyään maailma teknistyy kasvavassa määrin ja yhä useammalla käyttäjällä on yhä useampia eri identiteettejä tässä digitaalisessa maailmassa. Jotta käyttäjät pystyvät käyttämään eri järjestelmiä sujuvasti, täytyy näitä digitaalisia identiteettejä ja identiteettien pääsyoikeuksia pystyä hallinnoimaan ja valvomaan niiden elinkaaren eri vaiheissa. Tällaiseen identiteetin- ja pääsynhallintaan on tarve etenkin isoilla organisaatioilla, joissa on satoja tai tuhansia sisäisiä ja ulkoisia käyttäjiä.

Tavoitteena tässä lopputyössä oli tutkia mahdollisuuksia yhtenäistää ison lääketieteellistä toimialaa sivuavan eurooppalaisen yrityksen identiteetinhallintaa sekä saada yleiskuva sen tasosta yrityksen eri jäsenmaissa. Tämän tapaustutkimuksena suoritetun tutkimuksen varsinaisena pohjana oli jäsenmaihin lähetetty kysely, johon maiden asiantuntijat ja päättäjät saivat vastata. Tutkimuksen tulosten pohjalta työssä analysoidaan edellytyksiä yhtenäistämiselle ja pohditaan myös mahdollisia jatkotoimenpiteitä.

Lopputyö jakautuu sisällöltään teoria- sekä tutkimusosiin. Teoriaosuudessa annetaan aluksi pohjatiedot identiteetin- ja pääsynhallinnasta sekä tulevaisuudennäkymistä. Lisäksi lukija tutustutetaan lyhyesti lääketeollisuutta ohjaaviin kansainvälisiin säädöksiin, jotka ohjaavat myös tietojärjestelmien toteutusta ja ylläpitoa.

Tutkimusosuudessa syvennytään tutkimuksen kohteena olevan yrityksen identiteetin- ja pääsynhallintaan. Ensin kerrotaan yleistä tietoa kohdeyrityksestä ja tutkimuksen toteutuksesta, minkä jälkeen siirrytään tulosten esittämiseen ja analysointiin. Kysymykset on jaettu eri kategorioihin, joiden mukaan tulokset vastaavasti analysoidaan. Viimeisenä käydään vielä läpi työn lopputulokset ja jatkotoimenpiteet.

Avainsanat IAM, IDM, identiteetti, elinkaari, tunnustenhallinta, pääsynhallinta, lääketieteellinen.

Forewords

Accomplishing this master's thesis has been a long and a hard task, like a marathon run. However, a very rewarding one. I want to give special thanks to my mother Maija who always encouraged and supported me in my studies. Thank you Kalevi, my father, for supporting in many ways. Thank you Saila for believing in me.

The steady progress of this work was made possible with the dedicated support from my advisor Mr. Antti Väänänen. Thank you! Moreover, big thanks to my supervisor Professor Jukka Manner for giving constructive feedback always when I asked for it.

Finally, this diploma work would have been extremely hard to carry out without the strong support from Corporation X. Equally, the support from managers of Company Z and Corporation X was vital. Thank you!

In Espoo, on 23rd May 2016

Lauri Laitinen

Table of contents

Concepts

Access	In information technology, a way or a permission to get to a system.
Access Token	An indication to inform that the user has been granted access to a system.
Attribute	Attributes are used to describe the properties of entities.
Authentication	The process of demonstrating the truth about entity's claims of its identity.
Authorization	The process of determining access rights of entities to resources.
Availability	The degree to which a property is accessible and usable.
Centralized Identity Management	Identity management model where identities are provided by a central identity management system provider.
Confidentiality	Information is confidential if it can be accessed by only authorized entities.
Credentials	A piece of information, such as a document, a password or a biological property, to prove the identity of an entity.
Deprovisioning	The process of breaking off the link between an identity and its attributes. This is the last phase in the life-cycle of an identity.
Digital identity	The way the entity is defined in the digital world.
Electronic identity	Close to the concept of *digital identity*, but refers to electronic identification of a person.
Entity	Something that has an existence and an objective. In this thesis, by an entity is meant that in addition to humans, identities can be associated to computers and programs as well.
Federated Identity Management	In contrast to centralized identity management, in this model, identities are provided by multiple identity management system providers.
Identifier	A label that is associated with an identity.
Identity	Identity comprises of a set of attributes that describe an entity in a specific context. More tangibly, an identity can be associated with identifiers, credentials and attributes.
Identity assurance	The ability to determine with some level of confidence that the identity belongs to an entity.
Integrity	Assurance that the information being accessed, is complete, accurate and is being maintained with good quality without access by unauthorized entities.

OAuth	Open protocol to allow secure authorization from applications running on different platforms.
OpenID	A protocol to enables users to sign in to services using only a single existing OpenID account.
Propagation	The integration of an identity in other systems than the original.
Provisioning	The first phase in the life-cycle of an identity where the identity is linked with certain attributes.
Single Sign-On	A method of sharing authentication data. Single sign-on enables user to access multiple systems with only single login.
Subject	In identity and access management, an entity, whose identity is managed.
Virtual identity	Online or online gaming identity.

Abbreviations

API	Application Programming Interface
BYOD	Bring-Your-Own-Device
CIO	Chief Information Officer
DAP	Directory Access Protocol
ESSO	Enterprise Single Sign-On
ETSI	The European Telecommunications Standards Institute
FDA	The United States Food and Drug Administration
GCP	Good Clinical Practice
GDP	Good Distribution Practice
GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
GxP	Abbreviation to describe a "good practice" in any field
HTTP	Hypertext Transfer Protocol
IAF	Identity Assurance Framework
IaM	Identity and Access Management
IAWG	Identity Assurance Work Group of Kantara Iniative
IDaaS	Identity as a Service
IdM	Identity Management
IMA	Identity Management Application
IMS	Identity Management System
IoT	Internet of Things
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
LDAP	Lightweight Directory Access Protocol
LSC	Local Security Coordinator
NIST	The United States National Institute of Standards and Technology
OP	OpenID Identity Provider
PET	Privacy Enhancing Technologies
PKI	Public Key Infrastructure
PKI	Public key infrastructure
RP	OpenID Relying Party
SAML	Security Assertion Markup Language
SSO	Single Sign-On
URI	Uniform Resource Identifier
WHO	World Health Organization

1 Introduction

As we all know, computing has spread over almost every field of business or work, and continues to spread. Computerized systems are guided by humans or other computerized systems. They, whether they are humans or computers, have an identity by which they interact with each other. And the more the world is computerized, the more identities there will be. It is not unusual, on the contrary, it is more a rule than an exception that every one of us has multiple identities, especially in the digital world. When you have a growing number of identities, of which some are referring to the same user, you need some kind of management in order to cope with the chaos.

Computerized systems are an essential part of modern logistics and pharmaceutical companies as well. One company of this kind is Corporation X, one of the largest European pharmaceutical wholesalers. While planning and carrying out an identity and management project in a large company is an effort itself, how difficult it is when you consider it for a multinational corporation that is bound to comply with national and European Union pharmaceutical regulations? First step to figure this out would be to try to explore technical possibilities and the interest to even start to think a project like that. Specifically, that is what this work tries to achieve. Only after the initial mapping one has time to explore details and possible technologies. And this is a whole other story.

The research topic of this thesis was to find out the possibilities to standardize identity and access management in the target company and also to get information about the level of identity and access management within member companies of Corporation X. The answers to these questions in this case study were sought with the aid of a survey sent to experts throughout Corporation X. In search of possible barriers against standardization, regulatory issues in country and European Union level were examined. Additionally, respondents of the survey were asked about interest in standardization and possible regulatory or other obstacles. In addition to the actual research topic concerning Corporation X, this thesis introduces readers to the fundamentals and trends of identity and access management, and regulation on pharmaceutical business. After all, only by understanding these topics, it is possible to see the whole picture and comprehend the task of planning a common identity and access management environment or similar processes to use within same corporation.

This diploma work is divided in five chapters. First, basics of identity and access management are covered. This chapter deals with fundamentals first: the essence and definition of identity, characteristics and information that identities possess, stakeholders that have some kind of role with identities and last, but not least, life-cycle of identities. Next, after introduction to basics, different identity management models and fundamental identity and access management technologies are presented. Last section of this chapter discusses current trends that could shape the future of identity and access management.

Next, one of the topics of this thesis, regulatory framework, is left as its own chapter. This is deliberately done so, because firstly, it doesn't belong to any other subjects and secondly, to emphasize that the importance of following regulations in pharmaceutical business. As said before, computing systems are a vital part of pharmaceutical companies

nowadays, too. Therefore, when changes are made to computer systems, one has to take into account the effects on the whole production chain so that the regulations framed by officials and decision makers, will be met.

The third chapter, first of the two that deal with the case study, introduces the goals and the research method of the case study to the reader. The chapter gives an overview of the subject company, the Corporation X, as well.

After the presentation of the case study and the subject company, next chapter goes into the very essential part of the work – results. Before the actual results, a few paragraphs are said about the general information regarding the results. The results are divided in different categories based on the types of the questions and are presented by tables and charts. The results are then analyzed in sections by these categories. The last sections sums up the analysis and makes further conclusions about them.

Fifth and last chapter, naturally, focuses on the outcome of the case study and diploma work. It is also considered here, whether there is any demand or interest for further actions regarding identity and access management in corporation level.

2 Identity Management

In this chapter, the fundamentals of identity management will be explained. Before going in to the details of identity management models and fundamental technologies, it is good to have a thorough view of what identity is, what kind of identities there are, what kind of information are associated with them and who are the players in the field of identity management. Deeply thought, identity is a very multi-dimensional and abstract concept. It has to be mentioned here that when identity and access management is talked about, in practice it means specifically *digital* identity and access management since identities in modern information systems have a very strong digital dimension.

In the same way as living creatures, identities have "a life". Regarding the management of identities, it is important to see that identities have a lifespan. First, they are born e.g. when a user account is created. Before the "death" of the identity, besides the usage of the identity, it can be modified or maintained.

After the basic concepts, requirements of *identity management systems* (IMS) are covered briefly and identity management models from a certain perspective in sections after that. Identities can be managed with different principles, depending on the purpose of usage. Thus, different kind of management models can be distinguished.

The seventh section of this chapter is more about access management rather than identity management. This section tells about some key technologies and protocols that are fundamental concerning access and authentication of digital identities.

In the next section some present trends and future concerning identity and access management are covered. As we know, the Internet has grown to a massive network of billions of users and this has multiplied the number of interacting identities. This section tells for example about the Internet of Things (IoT) which will further revolutionize the digital world and identity management.

Lastly, a few words about cyber security and IaM are shared. Cyber security is a hot topic nowadays and cyber security is also very much about the access and security of identities.

2.1 About identities

Before discussing what identity management is all about and how identities are managed, it is important to define what the word identity actually stands for. In everyday life, people understand *identity* to mean how a person describes oneself or another person. However, identity can be viewed from many perspectives. Further, what is essential to modern world and this work, identity is not limited to human aspects, but can have artificial attributes from the digital world attached to it.

2.1.1 What is identity?

Identity is a word that describes "the fact of being who or what a person or thing is" [1]. To English language, the word identity has derived from Latin word *idem*, meaning *same* in English. Identity carries in itself the meaning of sameness, having the same characteristics as another identity. Further, as the definition says, identity can also refer to identity of things rather than just persons.

More philosophically speaking, identity can be viewed from two different angles:

- **A structural perspective** – Identity as a representation: Identity is seen as a set of attributes characterizing or referring to a person or an entity.
- **A process perspective** – Identity for identification: Identity is considered according to a set of processes relating to disclosure of information about a person and usage of this information. [2]

And by further analyzing these points of view, the concept of identity can be observed:

- **Mentally** or **procedurally** (ipse vs idem). The ipse identity ("I") is a perspective that is affected by interactions between the individual and the environment and refers to the representation of the person who he really is. The idem identity ("Me"), on the other hand, emphasizes the role of social, economic, governmental or other processes and needs.
- **Implicitly** or **explicitly**. Identity can also be seen from the perspectives of
  o I. How the person perceives the environment from first perspective?
  o Implicit me. What is the person's view of herself?
  o Explicit me. How the person is seen by the environment?
- **By the view of identity control**. Additionally, identity can be categorized more tangibly according to the view of control over (digital) identity:
  o Tier 1, true ("My") identity or *medentity* [3]. Tier 1 identity means the identity that is wholly controlled by the person herself.
  o Tier 2, assigned ("Our") identity or *ourdentity* [3]. Assigned identities are identities that corporations and governmental institutions assign to people. These identities include social security number, credit card number, customer number, cell phone number, job title etc.
  o Tier 3, abstracted ("Their") identity or *theirdentity* [3]. Abstracted identities don't refer to any single persons, but to statistical categorization or a profile of certain group of people. This categorization can deal with for example profiling through socio-economic demographics of a person to marketing purposes. [2]
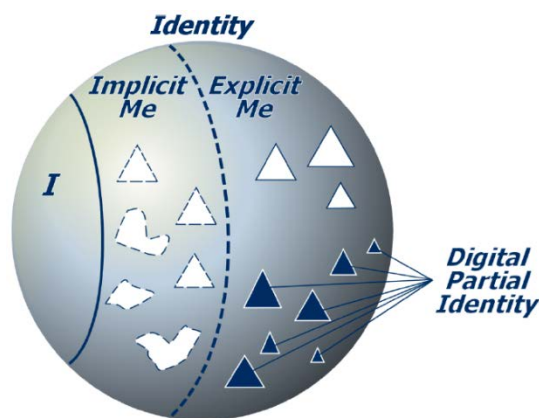

Fig. 1 Structure of identity and relations between different perspectives of identity [4].

So identities are usually not about complete identities, but *partial identities* that define the person in a certain context [2]:

> "*Partial identities* are subsets of attributes of a complete identity. Each identity of a person comprises many partial identities of which each represents the person in a specific context or role."

To clarify the definition of identity, the definition of identity depends on the context where one wants to define it. As [5] comprehensively summarizes it:

> "An identity of an individual person may comprise many partial identities of which each represents the person in a specific context or role. A partial identity is a subset of attribute values of a complete identity, where a complete identity is the union of all attribute values of all identities of this person."

However, a remark to these two definitions has to be made. Namely, when speaking especially of (digital) identities in computerized systems, the entity behind an identity is not always a living person. It could be an artificial entity that is used to control for example a collaborative system account. Therefore, the word entity is used from now on in this thesis instead of person.

2.1.2 Digital identity

The focus of this thesis is the management of identities and especially digital identities. As specified in last the chapter, the definition of identity depends on the context and the attributes that are associated to the identity. Thus, the definition of *digital identity* can be defined as follows [2]:

> "*Digital identity* refers to the representation of the identity of a person in digital environments, in particular in terms of the representation of the characteristics (attributes and properties) of the person."

From now on in this thesis, I will use the term identity or digital identity to refer to person's digital partial identity. There is also some usage of terms *electronic identity* and *virtual identity*. Although very closely related, electronic identity is about electronic identification and authentication of a person and in particular European Union's *eID* strategy to advance digital economy [6]. *Virtual identity*, on the other hand, is used mainly to refer to online identity or online game identity [5].

In today's world, where the old-fashioned physical world and the modern ever more computerizing digital world are getting more and more mixed, the difference between traditional identity and digital identity is getting more vague.

2.2 Identity information

The fundamental problem in digital interaction is to know for sure with whom one is interacting. Currently, it is impossible to get a complete assurance about counterpart's identity. Thus, digital interaction is very much about level of trust and authorization to various systems. This means also securing the integrity of the identity. Therefore, managing identities in present day information society means always managing *information security*.

Identity management systems can always be said to be part of Information Security Management Systems (ISMS). In ISMS information security is defined by three aspects:

- **Confidentiality**: property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Availability**: property of being accessible and usable upon demand by an authorized entity.
- **Integrity**: property of accuracy and completeness. [7]

2.2.1 Identifiers, credentials and attributes

Various pieces of information are associated with identities. That information can be grouped in *identifiers*, *credentials* and *attributes*.

Identifiers are labels of identities that represent identities. These labels may comprise of various letter and number combinations or plain language words. Identifiers can be composed of types such as [8]:

- user ID
- account name
- telephone number
- email address
- pseudonym
- IP address
- URI.

Identifiers can also have special characteristics such as limited scope so that they may be unique only within a group (e.g. account name on a web site), or the identifiers may be globally unique (e.g. URI). They can also have a property of expiration so that an identifier may be valid only a certain amount of time. [8]

Attributes are used to describe entities e.g. by IP address, domain, address, telephone number and they can be categorized in following types [3]:

- Legal documents based such as name, passport number or social security number.
- Demographic attributes like name, birth place or age.
- Financial based like bank account or credit card number.
- Biometric such as fingerprints or iris.
- Transactional attributes which for example characterize subject's interactions in the internet.

Attributes are important in defining the level of assurance of identities. Thus, it is necessary to be able to define the management and provisioning of attributes in a correct manner. [8]

Pattern is a special type of an attribute and describes the behavior of an entity. Pattern information is assigned by identity management systems based on reputation and past interactions, not by the entity itself. The information can be for example an IP address, location information, usage time or systems used. [8]

The use of credentials is a method of *authenticating* an entity. When the entity is authenticated, it has proven to be what it claims to be. Therefore it has the right to access the resources what it requires. Or shortly, the entity is *authorized*. Nowadays, the most common type of credentials is password. Other credentials include:

- security hints
- digital certificates
- Kerberos tickets
- SAML assertions
- biometrics such as fingerprints
- PKI information like keys, certificates and cryptographic information
- tokens and smart cards. [3] [8]

As is the case with attributes, credentials have to be managed and maintained properly to ensure the effectiveness of IdM. The management process consists of creating, issuing and managing information used to authenticate identity.

2.3 Stakeholders in IdM

In identity management systems there are many parties that deal with identities and information related to them. Each of the parties has its own role in the system. Basically, the parties can be classified to entities that use identities and entities that provide them.

However, stakeholders can be further categorized in four groups: subjects, identity providers, relying parties and control parties. [3]

2.3.1 Subjects

Subjects are entities whose digitally recorded attributes are used for transactions or other purposes. Typically subjects are ordinary individuals, whose attributes are categorised using different kinds of classifications as previously listed in 2.2.1.

2.3.2 Identity providers

The function of identity providers is to *provision* identities to subjects. Provisioning is a process of:

1. Creating and assigning identity attributes to a subject.
2. Binding an identity attribute of a subject to other identity attributes of a subject.
3. Create assertions (i.e. claims) about attributes.
4. Provision credentials recording identity attributes and identity assertions. [3]

Additionally, one has to take into account that the values of identity attributes of identity provider can be bound by attribute values of other identity providers. For example, social security number provided by Social Security administration can be bound by person's first name and surname or other important credentials. However, one has to observe that identity providers need to trust on credentials issued by other identity providers. In order

to reach a sufficient level of confidence, so called *identity assurance processes* need to be established. [3]

2.3.3 Relying parties

If some sort of a service or an access to resources is needed by users (or agents of them), relying parties are needed. Relying parties are parties that require the submission of proper credentials. It depends on services or resources to access, how high a level of assurance or verification is needed. However, there has to be at least some kind of an assurance process in place. [3]

2.3.4 Control parties

Control parties are parties that need to access identity information, such as transactions of identity information or forensic information. These control parties are typically government officials or regulatory bodies [3]. They could be for example a police investigating a crime or social security officials controlling admitted benefits.

2.4 Identity life-cycle

Fundamentally, identity life-cycle management has always the same idea. First, the identity is created. Then, it is be used and some changes might be made for example to the identity's attributes. After the "life" of the identity is over, it is removed from use. Depending on author's point of view or identity management system being managed, these phases can be further divided into many subphases. Further, depending on identity, some of these phases can be re-applied to the identity several times. According to [9], the identity life-cycle consists of *provisioning*, *propagating*, *using*, *maintenance* and *deprovisioning* (see Fig. 2).

2.4.1 Provisioning

Provisioning is a process where a new identity record is created and associated with certain attributes such as name and email. Provisioning can be done by administrator or one can do it by self-service, such as creating a user account to a web site. [9]

When the identity is created, the attributes are usually first proofed, depending on the importance of the identity. For example if a person wants to create an account to a local video rental store, person's age and address information will be checked. After successful proofing, credentials are issued and the identity is formed and ready to use. [3]

2.4.2 Propagation

If the identity needs to be integrated in other systems during its life-cycle, there needs to be a phase of propagation. This means that original system and the system where the identity propagates to, will be linked together. Propagation must happen every time when there is a change in identity record and should be done reliably in order to ensure the mutual functionality of two systems. [9]

2.4.3 Using

This is naturally the most obvious step and the phase where all identity management aims at – reliable and fluent usage of identities.

2.4.4 Maintenance

Maintaining identities, including their attributes and credentials, is vital to keep the IMS functional and in control. Whether it is an agent such as a network printer whose IP address has changed or a person who has changed her name, the integrity of attributes must be intact at all times. Moreover, people may want to change their passwords or digital certificates of non-person agents expire so the credentials of them need to be updated.

2.4.5 Deprovisioning

Having a proper protocol for deprovisioning of identities should be considered as important as provisioning. As in maintenance, in order to preserve the identity management system clean of old and invalid accounts, the identities should be deprovisioned, removed from use, immediately after there is no need for them anymore. If there are still old, but active accounts left in the system, they could pose a security threat. Firstly, a clever hacker could abuse them or, secondly, a former employee might still have access to company's information after leaving from the firm. [9]
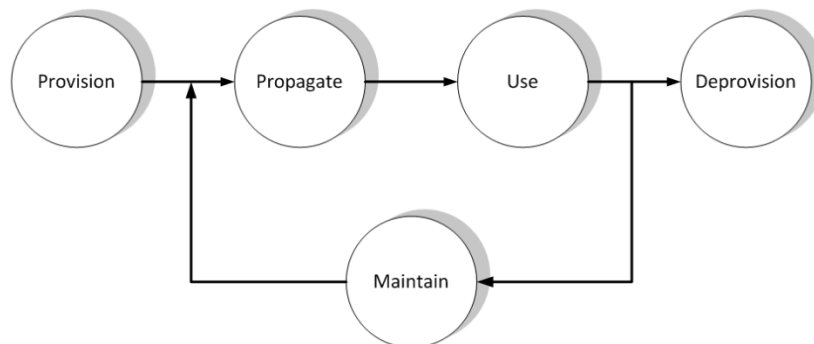
Fig. 2 Digital identity management life-cycle.

2.5 Requirements of Identity Management Systems

Now when we have some basic knowledge about the fundamentals of identities and how they are managed, it is time to get more acquainted with the practical part. In the following chapter, the essential models of identity management will be introduced. Before that, however, it is good to get a picture of the characteristics that are common to most IMS and what their requirements are.

In order to ensure proper functionality and operability of an IMS, *the Identity Management Applications* (IMA) should fulfil certain requirements. Identity Management Applications can be considered as an application layer on top of infrastructure layer which is formed by the Identity Management System. The eight requirements and their characteristics to fulfil, comprise of following areas: [4]

- **Functionality.** An IMS is functional when the identities are administered and maintained well. This also means functional communication between all stakeholders in IMS.
  - o Identity administration. Provisioning, maintenance and deprovisioning of different kinds of pseudonyms for users.
  - o Gateway. IMA can serve as a tool to communicate between parties.
  - o Notice and control. The control of pseudonyms should enable them to be durable for different kind of actions and addressable by organization. It should also be possible to use real name and re-use a pseudonym.
- **Usability**. It is very important that an IMS should be usable to everyone. This means that basic usability is guaranteed for normal users. In case of more advanced users, the system might be more complex.
- **Security**. This is an area which shouldn't be undervalued. A lot of personal, private attributes can be linked to person's identity which cannot be compromised such as credit card numbers, phone numbers and social security numbers. Further, in case of identity management systems, there are usually loads of identities stored in the same place. Therefore, integrity, availability and confidentiality of IMS must be protected against attacks.
- **Privacy**. The laws and regulations regarding privacy must be respected and this must be implemented in the IMA. Even though a particular piece of information doesn't seem to be of great value to a person, this might be very valuable for an organization that is profiling users. Despite the fact that pure technology can't fully protect one's privacy and also regulation is needed for that, it may still help on doing that. In this case we are talking about Privacy-Enhancing Technologies (PET). The purpose of PET technologies is to eliminate or reduce or prevent unnecessary or undesired processing of personal data – and at the same time maintaining the functionality of the data system.
- **Law Enforcement**. Protecting one's privacy and collecting information on one's life is a difficult question not just to individuals, but to lawmakers as well. Law enforcement agencies typically would like to have all personal data available for many years. There are also laws that oblige person's privacy to be protected. This makes it sometimes very complicated to implement identity management systems that comply with "both sides" of the law.
- **Trustworthiness**. It is important for people to be able to trust to the IMA where they have their valuable data stored. At this point, having a good reputation in the market as an IMA vendor helps a lot.
- **Affordability**. In order to have success for an IMA, the cost-gain ratio shouldn't be too big. Organizations might invest to an IMS even if the cost is high, assuming that they get other benefits such as more efficient and time saving identity control.

- **Interoperability**. Being able to integrate with existing systems is one of the most important aspects of IMA requirements. This isn't restricted to just corporation's systems such as Enterprise Resource Planning (ERP) or Human Resources Management Systems (HRMS). IMAs should also be compatible with international standards and other players in the IMA markets. [4]

2.6 Identity management models

Depending on source, a number of identity management models can be distinguished. Mostly, the principle of classification is based on authentication and relationships between identities and identity providers. On a very general level, two main classes of identity management can be identified: *centralized* and *federated* [4]. However, when this issue is looked at more precisely, one can recognize four different types of identity management [10]. In the following sections, these types, and their pros and cons, will be further explained.

2.6.1 Local identity

If identities are stored locally and the authentication happens also by using a locally maintained registry, the identity is called *local identity*. Local identities are managed centrally using a flat namespace so that every added identity has to be unique compared to other existing identities. As local identities are controlled centrally, they always use a single IMS provider. Using local identities has following advantages (+) and disadvantages (-):

+ Simplicity. New identities are easily provisioned by comparing the credential to credentials of existing identities. Flat namespace makes the structure simple, too.
+ Maintenance. When the identities are controlled centrally, the registry is easier to maintain.
+ Security. If credentials get in wrong hands, only the local host is compromised.
- Scalability. Although centrally controlled identities are easier to maintain, scalability will become an issue as the population of users and subsystems using the registry grows. If the system grows to unmanageable proportions, enterprise-wide provisioning tools might be a solution for that.
- Password authentication. Because in this scenario, identities are local, they are only valid in one system. In order to use same passwords in other systems, password synchronization or Single Sign-On could be used.
- Security. When user information is stored in single place, it always sets big responsibility to IMS provider to take care of the confidentiality of data. If password synchronization or single sign-on is used, an attacking hacker might also be able to breach to other systems as well. [10] [4]

2.6.2 **Network identity**

To counter the drawbacks of local identities, *network identities* can be used. These are becoming more and more common as computing is becoming more distributed. Network identities are valid within an enterprise network or a domain formed by many enterprise networks. Network identities possess the following pros and cons of:

- \+ Scope. The identity has access to all nodes in the network where it has authentication, not just to one as in the case of local identity.
- \- Security. A malicious user has now access to all nodes of the network where authentication applies. [10]

2.6.3 **Federated identity**

In contrast to centralized identity management is *federated identity management* (FIdM). In today's world where users need to be connected to many different types of systems using the same credentials, there is a demand for more flexible management of identities. In FIdM, there is not a single, central IMS provider. Identities are established in home organization and the attributes of them are then exchanged to connected foreign organizations, so there is no need for the user to register to anywhere else but to home organization. In case that the attributes, which are required by the foreign organization, are missing, they can be provided by for instance a third-party organization. [10] [4]

The federated model of IdM is fundamentally based on trust between organizations. The topology of how the attributes of entities are established and shared may vary, but three different profiling schemes can be recognized [10]:

- \- **Local profiling**. In this model, the attributes of an identity are only known and managed by the local home organization. The foreign organizations are unaware of the local profiling process. However, if access is needed across boundaries, the attributes may be exchanged to foreign organizations as well.
- \- **Distributed profiling**. In this scheme, profiles are distributed across home and foreign organizations. This also means that the definitions of identity attributes may be duplicated and this may become a maintenance issue.
- \- **Profiling by a third party**. There is also the possibility of outsourcing the profiling to a third party. By this method, the member organizations are relieved from the task of maintaining and exchanging attributes of entities. However, there may be problems with scalability if too many members are jamming the third party.[10]

These drawbacks and benefits can be found out in federated identity management model:

- \+ Flexibility. Using FIdM allows entities to operate dynamically across wider scale of systems and organizations than with other models.
- \- Trust. Cross-organizational trust is needed in order to securely interact within multi-organizational environment.
- \- Duplicate attributes. When distributed profiling is used, there may be a problem with synchronizing attributes.

- Scalability. When having a third party controlling the identity management, the IMS might not scale well if the number of member organizations grows too high.

Federated identity management is further discussed on subsection 2.7.2.

2.6.4 Global Web identity

By a *Global Web Identity* is meant an identity which is recognizable throughout the Internet in the same way as *Uniform Resource Identifier* (URI) identifies a physical Internet resource uniquely.

In order for Web identity to work universally, it should make use of existing identity management mechanisms which are based either on local or network identity registers. Web identities should then be mapped to these already existing registers. A couple of technologies providing basis for global Web identity exists today; *metadirectories* and *virtual directories*. Although the Internet has exploded to a massive network of over 3 billion users [11], the use of global identities hasn't spread worldwide among users (excluding URI). The reasons for that may be following:

- Need. There hasn't been a need to identify oneself globally, yet.
- Scalability. In order to have a global identity management system, there should also be a system where the register for all identities are maintained. [10]

2.7 Fundamental technologies

2.7.1 Credentials

Entity credentials are used to authenticate identity. Entity credential management deals with activities to create, issue, and manage information used to authenticate identity claims. The effectiveness of identity management depends on the credential management processes, procedures and capabilities. [8]

A credential is typically a set of attributes and assertions about a certain subject issued by an identity provider, called as *credential issuer*. Concerning the validity of credential, it is related to the assurance level of the credential that is the level of confidence that the subject is who he/she claims to be. [3]

Based on validity, credentials can be divided into three classes [12]:

1. **Raw Credentials**. Credentials specified by either the user himself or by any other party without any guarantee as to their validity.
2. **Authenticated Credentials**. Credentials that are digitally authenticated, either by the user himself or by a credential issuer, without prior verification of their validity.
3. **Validated Credentials**. Credentials that are digitally authenticated by a credential issuer only after the validity of the credential has been verified.

Another way of classifying credentials is by the way these credentials are created and used [13]:

1. **Primary identity credentials**. This class includes credentials that are derived from significant life events such as birth, death, marriage, graduation or various social occasions.

2. **Secondary identity credentials**, on the other hand, are admitted in response to a request for authorization to perform an action (such as driving license to drive a car), or demonstrate proof of affiliation (e.g. passport to prove claimed nationality). When requesting secondary identity credentials, the verification process relies mostly on primary and other secondary credentials.

3. **Tertiary identity credentials** include limited purpose credentials which are issued by authorities or organizations. These are for example employee identification cards, membership cards and loyalty program cards. The identity verification and proofing requirements may be very variable. Some of them like loyalty cards don't require almost anything unlike employee identification cards that may be very close to secondary identity credentials. [13]

2.7.1.1 Public Key Cryptography

The foundations of *public key cryptography* reach in the 1970's, and are based on the paper of Whitfield Diffie and Martin Hellman. The suggestion of Diffie and Hellman was the encryption keys to come in related pairs – private and public. The private key is and must remain concealed whereas the public key may be freely distributed. [10]

Public key cryptography is also known as *asymmetric cryptography* in contrast to traditional *symmetric cryptography*. In symmetric cryptosystems, or secret key cryptosystems, Alice and Bob share the same key. In some symmetric cryptosystems the key might be different, but easily computed from the other. In public key cryptosystems, the key to encrypt the *plaintext* differs from the key that it used to decrypt the encrypted plaintext, i.e. *ciphertext*. One of the most used cryptosystems is the RSA cryptosystem. [14]
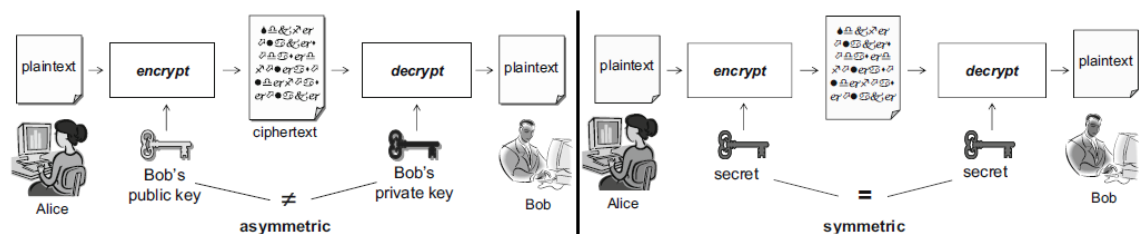
Fig. 3 Difference between asymmetric and symmetric encryption [14].

Using asymmetric ciphering solves the problem of key distribution and management in secret key cryptography. However, asymmetric cryptography doesn't solve all the problems. Essential problem of public key cryptographic is the secure linking of a public key to its true owner. One answer to the problem of public keys is so called Public Key Infrastructures (PKI). In PKI, the parties relying on public keys, base their trust on public key certificates provided by an entity known as Certifying Authority (CA). The CA digitally

signs the user's public key and thus binds it to a certificate. The key pairs can be generated by the user, CA or by a trusted third-party. After verifying the key, the public key can be distributed to public repository and is ready to use. The usage always requires the verification of the integrity and the validity (e.g. possible expiration or revocation) of the certificate. In the Internet, the structure and distribution methods for PKI are founded on International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard X.509. [10] [3]

2.7.2 Federated identity management

2.7.2.1 Oasis Security Assertion Markup Language (SAML)

The Security Assertion Markup Language is an XML-based framework for managing identities based on federated identity. SAML allows (business) entities to assert the identity, attributes and entitlements of a subject to other entities such as other companies or applications. The first version, SAML 1.0, was approved as a standard in 2001. The latest version, SAML 2.0, was adopted as an OASIS standard in 2005. Before SAML, there was no other XML-based standard capable of exchanging security information between a security system and an application trusting to that system. [15]
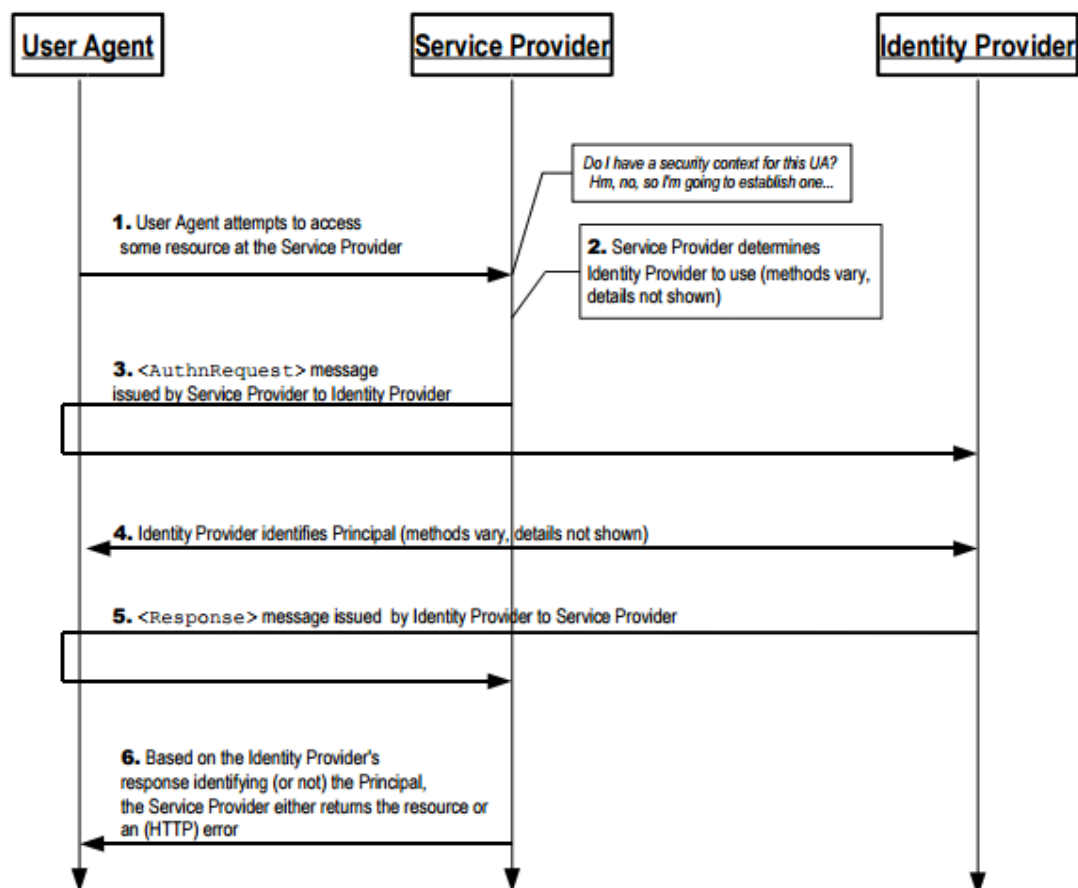

Fig. 4 Basic method for achieving single sign-on in Web Browser SSO Profile [16].

The primary uses of SAML are Web SSO, attribute-based authorization and the securing of web services. The most famous of these is the Web SSO (see Fig. 4). The main components of SAML are assertions, protocols, bindings and profiles:

- **Assertion** is a package of information that supplies statements made by an SAML authority. These statements come in three types: authentication, attribute and authorization decisions.
- A set of **request/response protocols** is defined in SAML in order for service provider, for example, to request/query for assertions, ask for a subject to be authenticated, manage federating identities through linking etc.
- **Bindings** are used to map SAML request-response message exchanges into standard messaging or communications protocols.
- The role of **profiles** is to define constraints or extensions to support the usage of SAML for a certain application. For example, the Web Browser SSO Profile defines how SAML authentication assertions are communicated between an identity provider and service provider to enable *single sign-on* (SSO) for a browser user. [15] [3]

2.7.2.2 OpenID

OpenID, an approach by OpenID Foundation, enables users to sign in to websites using only a single existing OpenID account. This eliminates the need to register to these websites using the same account information. By eliminating the need for multiple registrations, OpenID also relieves webmasters from the responsibility of storing user identity information on servers, thus enhancing user security. This open source community, which is called the OpenID Foundation, developed OpenID in 2005. [16]

The current version, OpenID Connect, is an interoperable authentication protocol and is based on OAuth 2.0. OpenID uses variety of standardized JSON- and HTTP-based message flows of the OAuth 2.0 framework to provide identity services [16]. Regarding protocol sequences, both OpenID and SAML 2.0 WebSSO Profile have similarities. Both of them transmit authentication results between OpenID identity providers (OP) and relying parties (RP) by using HTTP browser redirection mechanism [3]. In short, the operation of OpenID Connect protocol has the following steps [16]:

1. The RP (such as a website) sends a request to the OP (OAuth 2.0 Authentication server).
2. The OP authenticates the End-User and obtains authorization.
3. The OP responds with an ID Token and usually an Access Token.
4. The RP sends a request with the Access Token to the UserInfo Endpoint.
5. The UserInfo Endpoint returns Claims about the End-User.

2.7.2.3 OAuth

OAuth is an open protocol to allow secure authorization with a simple and standard method from web, mobile and desktop applications. The idea of OAuth began on 2006 when a group of people was working on OpenID and Twitter application programming interface (API) authentication. It was figured out that there was no open standard for API access delegation and a group was established to come up with a solution for that. On October 2007, OAuth Core 1.0 was released. [17]

OAuth allows the user, to grant access to user's private resources on a (web) site (service provider), to another site (consumer). The principle of OAuth differs from OpenID in that it is used to grant access to person's private data without sharing identity and OpenID is used to sign in to many sites using single identity [17]. To further clarify, OpenID is more about authentication and OAuth more about authorization.

OAuth is designed to be used only with HTTP and usage over any other protocol is "out of scope". The purpose of OAuth is to solve following security problems and limitations present in traditional client-server model:

- storing resource owner's (end-user) password in clear text,
- requirement of supporting password authentication in servers despite weaknesses in passwords,
- third-party application's extensive access to resource owner's resources,
- compromising third-party application compromises resource owners' resources and passwords as well. [18]

The introduction of authorization layer and separation of the role of the client and resource owner addresses these issues in OAuth. The current version of OAuth is OAuth 2.0 and the protocol flow is following:

1. The client sends authorization request to resource owner.
2. The client receives authorization grant, a credential representing the resource owner's authorization.
3. The client sends a request for an access token by authenticating with the authorization server, using the authorization grant.
4. The authorization server authenticates the client and validates the authorization grant. If the grant is valid, an access token is issued.
5. The client sends a request for the protected resource on the resource server and authenticates by presenting the access token.
6. The resource server validates the access token and serves the request, if the token is valid.[18]

2.7.3 Single Sign-On

Basically, single sign-on is a method of sharing authentication data. SSO enables user to login once and then use the same login name to connect to multiple systems without having to login to each of them again. In local-identity model, SSO functions as an advanced method compared to password synchronization. [3] [10]

Although single sign-on provides a way to access multiple services with one authentication, this doesn't necessarily mean that the login information itself is unified across all the systems. Instead, the SSO system uses mapping of the subject login onto local accounts or transmits authentication information which is accepted by all the systems within the realm of the SSO. [3]

There are different types of single sign-on in use. Enterprise SSO (ESSO) makes it possible to use same login name within all the systems of an enterprise. Multidomain SSO, enables single sign-on between multiple enterprises. Web-based SSO is even capable of

allowing users to connect via web browsers with web applications. Of these SSO types, ESSO is the most common. [3]

The single sign-on architecture is supported by standard interfaces and frameworks which provide tools for security, authentication and operation in different kinds of environments. These standard solutions include: The Generic Security Service Application Program Interface (GSS-API), Open Software Foundation's (OSF) Distributed Computing Environment (DCE) and The Pluggable Authentication Modules (PAM). [19]

In addition to general solutions that support the building of actual single sign-on architecture, there are a few models that provide various implementations to SSO. These are:

- **Broker-based**. These kinds of solutions are based on servers which handle the authentication and account management of users. The most common way to implement broker-based SSO is by using Kerberos. In Kerberos, a trusted server acts as a broker. The broker authenticates users and in exchange of credentials, gives them a digital identity which is used to request tickets for different services. A European counterpart for this MIT based protocol was Secure European System for Applications in a Multi-vendor Environment (SESAME).
- **Agent-based**. In agent-based solutions, an agent program is used to recognize the user with the help of lists or cryptographic keys. This agent may be located on client or server side. Example of this type of method is SSH Agent.
- **Reverse Proxy-based or gateway-based**. This approach uses the gateway or proxy server between client and trusted network behind the gateway, in the so-called demilitarized zone (DMZ). The proxy server allows only access from users with valid credentials and redirects others to server that allows clients to get registered. [19] [3]

2.7.3.1 Kerberos

In Greek mythology, Cerberus (Greek: Kerberos) is a three-headed dog of Hades, guarding the entrance to the underworld. [20]

In computer technology, Kerberos is a distributed authentication service which allows a client, running on behalf of a user, to prove its identity to a verifier (authentication server) without sending data across the network which might allow an attacker or the verifier to subsequently impersonate the user. [21]

Respectively, Kerberos has three "heads" – the client, the authentication server and the desired target server. Kerberos uses symmetric encryption and the authentication process has basically three steps (see Fig. 5):

1. Client proves his/her identity and requests a ticket to gain access to a desired server.
2. Client receives ticket.
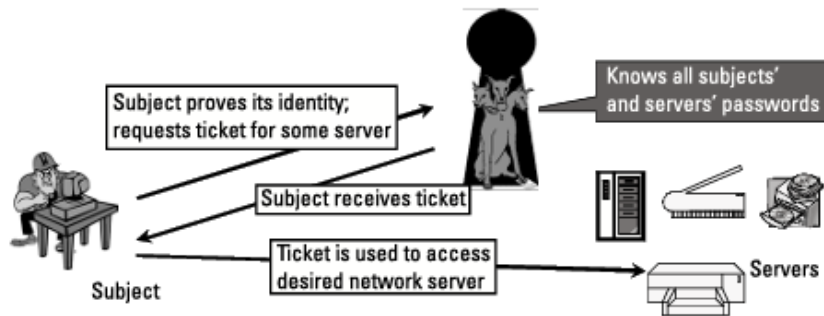3. Client uses the ticket to access the server.

Fig. 5 The simplified authentication process of Kerberos [3].

2.7.3.2 Reverse proxy based SSO

A reverse proxy server is a type of proxy server which is located usually behind a firewall (e.g. in DMZ area) in a private network directing client requests to the appropriate back-end server [22]. An SSO reverse proxy is a reverse proxy running SSO software inspecting SSO requests. Only requests with valid credentials are passed through to private network. These requests might be for example valid Kerberos tickets or SAML authentication assertions. If the request is not valid (e.g. the user has typed wrong credentials, or some entity is using false credentials), the user is redirected to an authentication server. The authentication server may be located either in the private network or elsewhere in the Internet. Reverse proxies typically support HTTP protocol, but FTP and SSL and other communication protocols are common as well. [3]

2.7.4 Directory services

Directories are special type of databases that are optimized for data searches and reads. Although directories can be seen as databases, they differ from traditional databases in many ways. Directories usually contain static information that doesn't change very often such as contact information about users. Therefore, they are not suitable for storing data that changes rapidly. Further, directory services don't support similar access methods as general-purpose databases such as Structured Query Language, but simpler access protocols. [23]

Many of the modern directory services solutions are based on the X.500 protocol standardized by the International Organization for Standardization (ISO) and ITU-T in 1988. In X.500, a protocol called *Directory Access Protocol* (DAP) was used in communication between the directory client and directory server. However, being too heavy and resource-intensive, a lighter version called *Lightweight Directory Access Protocol* (LDAP) was developed. [23]

2.7.4.1 LDAP

Entries in an LDAP system are arranged in a tree-like structure called *Directory Information Tree* (DIT). LDAP entries are organized within the directory based on their *Distinguished Name* (DN). Each DN consists of sequence of *Relative Distinguished Names* (RDN). Every RDN in a DN corresponds to a branch in the DIT starting from the root of the DIT to the directory entry. [23]

The interaction between a client and a server happens with TCP/IP protocol and consists of four steps [23]:

1. **Binding:** Session establishment between client and a server.
2. **Authentication:** The client provides a user name and a password or authenticates anonymously.
3. **Operations:** The client performs LDAP operations (search, modify, delete) on the directory.
4. **Unbinding:** The session is closed.

Nowadays, there are various directory services in use. The most common of them is Microsoft Active Directory (or AD in short). Others include NetIQ eDirectory (used to be Novell eDirectory), Sun Java System Directory Server, Red Hat Directory Server (formerly Netscape's solution) and other. Common factor for all the directory services is that they all support LDAP. [24]

2.8 IaM trends and the future

Former Finnish prime minister said once in Finnish that "prediction is very difficult, especially about the future". He was right about that. No one could have imagined computer networks, which we have today, to exist in 2015. However, a number of clear trends in information and communications technology (ICT) seem to be in sight. Because identity and access management is an inseparable and important part of ICT in many ways, developments and trends in the Internet inevitably affect IAM as well. Some of the trends have been continuing for years, and some of them aren't yet here, but they are expected to change the Internet one way or the other. In the following chapters we will take a look at some of the hottest topics of identity and access management right now.

2.8.1 IaM and IoT

Today, the Internet of Things (IoT) is seen as one of the megatrends of the future. In the traditional present-day internet, people are communicating with each other via devices over global network. In the near future, however, experts and futurologists believe that the IoT will bring implications of two kinds. Main implication will be that the number of devices connected to the internet will increase rapidly. Furthermore, the Internet will evolve more and more to the direction where these machines are communicating with other machines, being connected to the Internet at the same time. This is also called Machine-to-Machine (M2M) communication and is not considered being synonymous entirely to the IoT, but being actually a subset of the IoT, anyhow [25].

According to market research company Gartner, the IoT will change IaM in several ways. First of all, IaM will be divided more clearly into identity management and access management. Identity management will take more the role of relationship management and access management the role of relationship execution, replacing authentication policy and authorization enforcement. Secondly, because of the growing number of Internet-connected devices and M2M relations, the traditional authentication and authorization methods will include more requirements to devices and M2M communication. The expanded concept of IaM will spread more to embedded software and systems, as well. [26]

Table 1 Internet of Things Units Installed Base by Category (Millions of Units). [27]

Category	2014	2015	2016	2020
Consumer	2277	3023	4024	13509
Business: Cross-Industry	632	815	1092	4408
Business: Vertical-Specific	898	1065	1276	2880
TOTAL	3807	4902	6392	20797

2.8.2 Enterprise Mobility Management

According to [28], Enterprise Mobility Management (EMM) is about securing and enabling employee's use of smartphones and tablets. EMM typically consists of Mobile Device Management (MDM), Mobile Application Management (MAM) and Mobile Information Management (MIM).

Gartner predicts that by the year 2017, integrating EMM with IAM will be a critical requirement for 40 % of buyers [26]. Motivation behind that is explained to be that organizations want to provide a convenient and secure access to services by using a wide variety of devices [26]. It is clear that organizations need firm management in constantly changing IT environment where phenomena such as bring-your-own-device (BYOD) are creating challenges for IT managers.

This kind of development might be realistic for large organizations which are using IAM solutions and have EMM disciplines in use. Having bundled IAM and EMM solution may simplify identity and device management of a company and help them improve security as well. However, small or medium sized companies might not get advantage from this and platform differences between traditional Windows-based PC environment and mobile environment may slow development.

2.8.3 IDaaS

Cloud services have been one of the greatest success stories of ICT in recent years. No matter what subject is named, it most probably has some applications or connections to cloud services. Especially Software as a Service model or SaaS has been an integral part of the breakthrough of this "everything as a service" model or XaaS.

One of these models that have emerged as a by-product of this hype is Identity and Access Management as a Service or IDaaS. IDaaS systems are used to support the management processes of customers' identities and access privileges in their premises and in the cloud. IDaaS providers can be divided in two types: web-centric and full-featured. Web-centric vendors concentrate on providing IAM functionality for Web-architected applications. Full-featured providers, on the other hand, aim to provide deeper functionality, especially for identity governance and administration. [29]

Although there are signals that the hype of IDaaS is slowing down, IDaaS will continue to gain ground in IAM markets. According to, 25 % of purchased IAM solutions will use IDaaS in 2019 compared to 10 % in 2014. [30]
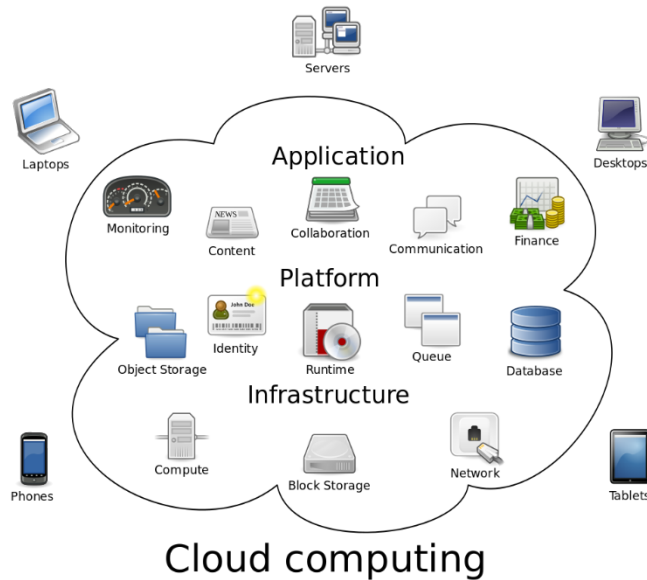
Fig. 6 Representation of cloud computing [32].

2.9 Cyber security

Cyber security is becoming an increasingly important topic nowadays. The more there are identities created every day, the more there are identities to be maintained and deprovisioned. This not only makes managing identities more challenging, but also provides even more opportunities for abuse of identities. And the more digital the world is coming, the more there will be misuse of identities. One of the most serious threats for identities is identity theft. Therefore, in order to trust to an identity, it is vital to have at least a sufficient level of confidence on the identity of a subject. This subject will be discussed in the next section.

Fig. 7 The importance of cyber security cannot be undermined anymore.

2.9.1 Identity assurance

In identity management, it is crucial to have confidence that someone or something is what she/it claims to be. However, in the "real world", it is usually good enough that one has only a certain level of confidence on the identity of an entity.

The Identity Assurance Framework (IAF) published by the Kantara Initiative Identity Assurance Work Group (IAWG) attempts to address this. Kantara Iniative, established in 2009, is a collaborative group of tens of global communities dealing with identity and Internet [31]. The IAF defines a set of guidelines and criteria for Credential Service Providers (CSP), relying parties and operators of federated identity networks to trust each other's credentials at known levels of assurance. The IAF is composed of these components:

1. **Assurance Levels**. Assurance levels (see Table 2) describe the degree from low to very high, how much relying parties can trust on the identity information provided by a CSP. The structure and idea of assurance levels in IAF is influenced by the guidance of U.S. National Institute of Standards and Technology (NIST).

2. **Glossary**. Glossary presents a summary of commonly used terms in IAF.

3. **Assurance Assessment Scheme** (AAS).AAS defines how to create criteria for certification and accreditation, focusing mostly on CSPs. The aim of these criteria is to facilitate intra- and inter-federation transactions based upon a range of identity credentials, across a number of levels of assurance so that relying parties can trust that credentials having the Kantara Initiative Mark are worthy of their trust.

4. **Service Assessment Criteria** (SAC). SAC specifies basic criteria for organizational conformity, identity-proofing services, credential strength, and credential management services against which all CSPs will be evaluated. The criteria qualify the requirements that identity services and their CSPs must meet at each assurance level within the IAF.

5. **Assessor Qualifications and Requirements**. This document defines the requirements which applicant assessors must fulfil in order to become Kantara-Accredited Assessors.

6. **Associated Profiles**. In addition to the IAF components depicted above, particular implementation of the IAF may require further specifications, relating to, for example, jurisdictional privacy principles or operational conditions.[32] [33] [34]

Table 2. Assurance levels defined in Identity Assurance Framework

Assur-ance Level	Example	Assessment Criteria – Organization	Assessment Criteria – Identity Proofing	Assessment Criteria – Credential Management
AL1	Registration to a news website	Minimal Organizational criteria	Minimal criteria - Self assertion	PIN and Password
AL2	Change of address of record by beneficiary	Moderate organizational criteria	Moderate criteria - Attestation of Govt. ID	Single factor; Prove control of token through authentication protocol
AL3	Access to an online brokerage account	Stringent organizational criteria	Stringent criteria – stronger attestation and verification of records	Multi-factor auth; Cryptographic protocol; "soft", "hard", or "OTP" tokens
AL4	Dispensation of a controlled drug or $1mm bank wire	Stringent organizational criteria	More stringent criteria – stronger attestation and verification	Multi-factor auth w/hard tokens only; crypto protocol w/keys bound to auth process

2.10 Conclusion

Identity management, the activity of managing identities, is about defining the identity, which is affected by the context where the identity is being operated in, and managing the life-cycle of the identity in a proper way in all the phases of its life-cycle. As [2] phrases it:

> "Identity Management are the organizational and IT processes for handling (partial-) identities and their changes, taking into consideration the identity life cycle and the context an identity is acting in (e.g., governmental, enterprise, or private)."

Identities, whether they are digital or not, can be associated with various pieces of information. Identifiers link the identity with a label. Attributes, on the other hand, depict the identity with characteristics that are specific to the identity. And finally, credentials are used to prove that the identity is what it claims to be.

3 Case study Corporation X

The principal focus of this chapter is the introduction of the case study and the research method. In addition, challenges and goals of the study will be introduced to provide motives why this study was taken. First, some background information of the challenges that the Corporation X is facing, are provided. This multinational company is not just a homogenous large corporation, but more like a group of companies that try to co-operate with each other.

The primary goal of the study was to explore possibilities to have common IaM processes throughout the Corporation X organizations. Secondly, in order to achieve a good overview of the situation, it was important to get to know better about the IaM status in organizations. More on this on section 2.

On the next section, introduction to the chosen research method will be given with detailed information about the respondents. Research method was chosen to be an online survey which was organized internally in company network. Target group consisted of top experts of Corporation X in each country.

The fourth section is about the survey as well. The aim of this section is to clarify each of the survey questions group by group. The questions were divided in four groups in order to simplify the analysis of the results. For each question, the answering options and the grounds for asking this question will be presented.

Next, a short introduction of the target company, Corporation X is in place. Due to the publicity requirement from the university and privacy requirement by Corporation X, the real names of Corporation X and Company Z are hidden in this work.

The last section provides a look at the regulatory framework guiding the operators in the pharmaceutical field. History of the pharmaceutical regulation and present day good practices will be described.

3.1 Current challenges

The history of the Corporation X is relatively young. The corporation was established as late as in 1994. The expansion of this company to be a major player in pharmaceutical business in Europe has been rapid. With dozens of acquisitions of pharmacies and wholesalers, the company has increased from a big German company to a large European corporation in just over twenty years.

On the contrary, many of the companies that the Corporation X has acquired, such as Company Z from Finland, has long history – dating even back to the 19th century. These companies have been doing their business in their own markets for decades before these mergers.

Furthermore, as we are speaking of European countries, these are countries with different cultures ranging all the way from the Mediterranean to the Baltic Sea. Even companies in the same country may have very diverse company cultures. And when these companies have origins from all around the continent, this must have some kind of an effect on the

way things are managed. Nonetheless, regarding computer systems, the corporation has already started the process of linking all the networks of member companies.

Uniting companies with tens of years of history from different cultures may not be an easy task. Nevertheless, this is not the only challenge in the middle of today's rapidly changing world. Technological revolution in information and communications technology (ICT) and in software development has increased the use of computers and applications exponentially. This revolution has grown, and will grow, the number of digital identities and their access rights throughout the digital world. And so is the case with Corporation X. Having a functional IaM strategy now, is not just a necessity for the present, but an investment for the future.

3.2 Goals

The main goal of the case study was to find out whether there are possibilities to standardize identity and access management in an EU level pharmaceutical company, e.g. Corporation X. The secondary goal was to get a good overview of the level of identity and access management within Corporation X. The secondary goal gives not only information about the technical level in countries, but gives also answers for the primary goal, the possibility of standardization.

The information about both the status of Corporation X IaM and possible obstacles (such as legal or financial) against standardization, together with knowledge of motivation towards standardization, give a good grasp on the possibilities to consider common group wide processes or solutions.

3.3 Introduction to the research method

The research method was chosen to be internal online survey. Moreover, there was also a possibility to perform an interview study. However, survey's sufficient response ratio affected to the decision to limit the research to online survey. The survey was created with Microsoft SharePoint to the company's internal SharePoint portal. Another option was to use a 3rd party online survey tool. In the end, SharePoint was chosen in order to get use of existing company software and because of security reasons (availability only in company network).

The target group was selected to be all the Local Security Coordinators (LSC) and certain Chief Information Officers (CIO) throughout the company. An email, with a description of the study, a link to the survey and incentives of product awards, was sent to this target group. A bonus to reveal the results to all the respondents after the survey was promised as well. Although the respondents were promised the results of the survey, they were also promised confidentiality of the survey and for this reason the names will not be published. The number of persons in the target group was 30.

The survey was carried out as a multiple choice questionnaire with a couple of questions allowing free text answers. The total number of different questions in the survey was 19. One of the questions had a branching logic, so the possible amount of answered questions could be either 17 or 18. There could have easily been more questions in the survey.

However, increasing the quantity of questions could have affected the quality of answers or motivation to answer negatively.

All the multiple choice questions were set "required to answer" and free text answers not compulsory. No deadline for taking the survey was given, but a reminder was sent to rest of the group, who weren't yet answered, 3 weeks after the first invitation. The questions can be categorized into four different topics:

- IaM status in member countries (7 questions)
- Motivation and interest in IaM (5)
- Authentication (3)
- Obstacles, such as legal requirements or regulations (2)

In addition to these subjects, two questions for comments and contact details were asked in the end. The survey questionnaire for Corporation X experts can be found on Appendix I: Internal Survey on Identity and Access Management. The questions of the survey with comments on the reasons why exactly these questions were asked, will be described in the next section.

3.4 Description of the survey questions

This section opens up the questions of the case study. Question by question, the reasons for asking each particular question will be explained. The answering options are provided along with the questions. The selection of these questions was largely based on the knowledge and opinions of the writer. However, I also took influence on some similar surveys in the Internet.

3.4.1 IaM status in member countries

When investigating the possibilities to standardize identity management in this multinational company, it is important to get a good overview of the existing processes and status of identity and access management in each of the responding countries. The next 7 questions were asked about the status of IaM in Corporation X countries.

1. How many systems or applications do you have in your organization that require different login name (including Microsoft AD or other directory services)?

- o 1-3
- o 4-6
- o 7-9
- o 10-19
- o 20+

This was an important question to find out how many different user account domains each country has. The more there are applications, the more there are identity spaces to be managed. It was already known that some countries might easily have over ten applications. Therefore, the scale could have been even wider.

2. Do you have IaM (Identity and Access Management) software in use at your organization?

- o Yes [2a]

o No, but we are interested in acquiring one [2b]

o No, and we are not interested in acquiring one [3]

o I'm not sure [3]

The question was asked to know if a Corporation X organization already had IaM software in use. If there were already IaM software in place, this would also tell that there is interest in identity management in that organization. If there were not, two other choices asked if there were interest in acquiring one. This question was a branching question that would lead the respondent to question 2a, 2b or 3.

2a. Which vendor's software are you using in your organization?

☐ IBM

☐ Sailpoint

☐ Oracle

☐ EMC (RSA)

☐ Courion

☐ NetIQ (former Novell)

☐ CA Technologies

☐ [Specify your own value]

Some major identity and access management vendors were selected for questions 2a and 2b. These questions were only asked if the respondent answered "Yes" or "No, but we are interested in acquiring one" to the question 2. If there were already IaM software acquired in organizations, it would have been interesting to know which software. Question 2a is categorized to status questions.

3. How centralized is the identity management (provisioning) process of INTERNAL users in your organization?

o Not centralized at all. We have to manually add or remove user access rights to each application.

o A little bit. Some of the applications use shared profile data or some of the provisioning processes have been automated.

o Quite a bit. We have a single process for provisioning.

o Fully. We have a single process for provisioning including an application to do this.

o [Specify your own value]

Question 3 was also an important one since the answer tells the level of provisioning process of internal users. This tells quite a lot about the identity management status of the organization. These questions also might give some hint about the difficulty of the possible standardization of processes. The more centralized and organized the processes are, the easier it is to build common solutions. External users must not be undermined, but because probably most of the systems are used by internal users and it is about the company's own employees, the internal provisioning process is more important than external.

4. How centralized is the identity management (provisioning) process of EXTERNAL (partners, customers etc) users in your organization?

o Not centralized at all. We have to manually add or remove user access rights to each application.

o We have to manually add or remove user access rights to each application.

o A little bit. Some of the applications use shared profile data or some of the provisioning processes have been automated.

o Quite a bit. We have a single process for provisioning.

o Fully. We have a single process for provisioning including an application to do this.

o [Specify your own value]

Questions 3 and 4 were separated to ask about internal and external users, because there might have been different processes for each of them.

5. Are the processes for managing internal and external identities the one and same process?

o Yes, if an identity is provisioned, changed or deprovisioned, it goes through the same process.

o No, they are separate processes.

o [Specify your own value]

Although question 5 is a bit overlapping with 3 and 4, questions 3 and 4 asked about the level of centralization in provisioning. There could have been a situation that the internal and external provisioning processes were not very centralized, yet they still went through the same process.

6. Is your provisioning process connected in any way to HR department?

o No, not at all. When a person is employed or leaves the company, the HR isn't involved in the process.

o A little bit. The HR informs the IT about the status changes of the employee.

o Quite a bit. The HR informs the IT what kind of access changes have to be made.

o Fully. The HR department takes care of the whole provisioning process.

The last question in this category asks if the provisioning is connected with the human resources department. The connection to HR department is considered very important in IaM solutions. Because HR department controls persons entering and leaving the organization, they can efficiently control the identity lifecycle at the same time.

3.4.2 **Authentication**

The questions in this category were access-oriented. Because thesis subject was about identity and *access* management, there had to be even some questions regarding access management. These questions also relate to the status questions in that they try to find out how sophisticated authentication methods there are available in Corporation X organizations. They don't necessarily give an answer whether the standardization would be easier or not, but they do tell something about the level of access technology. The following 3 questions were asked about authentication.

7. In your organization, is it possible for users to access multiple applications by providing their user id and password only once? (Single sign-on)

o Yes, we can access all applications with SSO.

o Yes, some applications have this feature.

o No, not at all.

o [Specify your own value]

Today, single sign-on is a very popular authentication technology which makes users' life a lot easier.

8. In your organization, is it possible for users to access multiple applications by using the same password? (Password synchronization)

- o Yes, we can access all applications with password synchronization.
- o Yes, some applications have this feature.
- o No, not at all.
- o [Specify your own value]

Although this technology is quite similar to single sign-on, it is completely different technology and easier to implement than SSO.

9. Which other authentication methods do you have in use in your organization other than username/password?

- □ Biometric
- □ Certificates
- □ Smart cards
- □ Tokens (e.g. one-time passwords delivered by SMS, token devices,…)
- □ None
- □ [Specify your own value]

The last question asked about different kind of methods of authentication. This is also irrelevant to identity management, but can give good information regarding to access management.

3.4.3 Motivation and interest in IaM

Ultimately, the 5 questions about motivation and interest in identity and access management, and especially the standardization of it in Corporation X, were the most important questions of the survey. Even if the responding organization had good prerequisites to apply common solutions, they might not have any interest in doing so for a reason or another.

2b. Which vendor's software are you interested in acquiring to our organization?

- □ IBM
- □ Sailpoint
- □ Oracle
- □ EMC (RSA)
- □ Courion
- □ NetIQ (former Novell)
- □ CA Technologies
- □ [Specify your own value]

This question was presented if the respondent answered not to have IaM software, but were still interested to get one. Therefore it is categorized in Motivation and interest category.

11. In a scale from 1 to 10 (highest), how interested is your organization in following IaM software solutions:

1. IaM software in general.
2. Password synchronization.
3. Single sign-on (SSO).
4. Federated identity management.
5. User provisioning.
6. Directory services (other than Microsoft AD or the current you are using?).
7. IaM solutions (solution covering some or all above mentioned areas).
8. IaM cloud solutions (solution
9. Covering some or all above mentioned areas).

The purpose of the question 11 was to explore the interest in various IaM solutions and technologies. This was a multiple choice question with answer values ranging from 1 to 10. The question was also important, because it straightforwardly asked e.g. motivation in IaM software in general.

12. In a scale from 1 to 10 (highest), how interested would your organization be in:

1. Using more cloud services (SaaS, Software as a Service)?
2. Providing better IaM (such as SSO, better provisioning) for EXTERNAL users?
3. Providing better IaM (such as SSO, better provisioning) for INTERNAL users?
4. Knowing about IaM processes or solutions in other Corporation X countries?
5. Acquiring a common Corporation X-wide IaM solution?
6. Standardizing or creating common Corporation X-wide processes for identity management?

The next question was also a multiple choice question with 1 to 10 scale. This also asked about interest in a common solution or processes, but also about motivation to provide better IaM to users.

14. For how large an IaM solution is there need in your organization? Define the scope:

□ Internal
□ Partners
□ Customers
□ [Specify your own value]

The question 14 aimed to discover which would be the target groups for IaM solution in respondent organization. This was a question with one or many answer possibilities.

15. What would be the main motivator for centralized IaM solution?

o Governance, Risk management, Compliance (GRC)
o Operational excellence
o Business agility
o [Specify your own value]

The last question in this category sought the primary motivator for common IaM solution. One of the answering options was Governance, Risk management and Compliance (GRC), defined by [44] as:

"GRC is neither a project nor a technology, but a corporate objective for improving governance through more-effective compliance and a better understanding of the impact of risk on business performance. Governance, risk management and compliance have many valid definitions. The following definitions illustrate the relationship of the three terms and serve for Gartner's GRC research:

- **Governance** — The process by which policy is set and decision making is executed.
- **Risk Management** —The process for preventing an unacceptable level of uncertainty in business objectives with a balance of avoidance through reconsideration of objectives, mitigation through the application of controls, transfer through insurance and acceptance through governance mechanisms. It is also the process to ensure that important business processes and behaviors remain within the tolerances associated with policies and decisions set through the governance process.
- **Compliance** — The process of adherence to policies and decisions. Policies can be derived from internal directives, procedures and requirements, or external laws, regulations, standards and agreements."

To sum up, the last question searched for the reason for interest, as other questions of the category asked more for the level of interest.

3.4.4 Obstacles, such as legal requirements or regulations

Lastly, the background for the questions in fourth category was to gather some verbal feedback of the survey. The answers to these 2 questions were optional and open-ended unlike the case in other questions in the survey. These were also sort of questions which would have been difficult to implement as multiple choice or interval types. Moreover, allowing the opportunity to free speech, provides a chance to patch up possible defects elsewhere in the survey. Some questions may have accidentally been left outside and, as said, the length of the survey had to be kept as compact as possible.

10. Please specify regulations or laws by authorities or European Union regarding identity and access management that you have to comply with (e.g. laws related to personal privacy or directives related to EU Good Distribution/Manufacturing Practices)

   o [multi line textfield]

Considering the fact that one of the aspects of this thesis is the pharmaceutical dimension, it was important to probe the possible knowledge of regulations or laws from the experts. If there were regulations that strongly affected the function of the organizations, the respondents should have known about this.

13. In your opinion, are there any issues or obstacles (such as legal) against a common and standardized Corporation X-wide IaM solution?

   o [multi line textfield]

The last question was a very general one and enquired about other possible restrictions regarding common solution.

3.5 Introduction to Corporation X

Corporation X is a leading integrated healthcare provider in Europe with operation in over 20 countries. It was formed in the 1990's when five regionally active wholesalers merged as one large group. The family-owned company employs nearly 30 000 persons and produced revenue of billions of euros in fiscal year 2014/2015. In addition to home country Corporation X has a strong market position in Northern and Eastern Europe and is a market leader in 11 countries. [47]

Fig. 8 Corporation X has wholesale and retail operations in 25 European countries.

While the primary focus of Corporation X is acting as a leading pharmaceutical wholesaler with well over a hundred distribution centers all over Europe, Corporation X works also in retail business, owning hundreds of pharmacies in many corporation countries. Additionally, Corporation X offers pharmaceutical services to patients and the whole supply chain in co-operation with pharmaceutical manufacturers and pharmacies. Therefore Corporation X can be thought to be an interface between pharmaceutical industry and both retailers and patients (see Fig. 9). [47]

Fig. 9 Different roles of Corporation X in the supply chain.

Although majority of Corporation X countries operate in similar market environments, some of the markets have small distinctions with each other. For example minority of European Union countries (Finland and Sweden) enforce single-channel systems where a wholesaler has an exclusive right to distribute medicines of a certain manufacturer. Unlike in single-channel countries, in multi-channel countries the competition is tough and they don't have so much market dominance as in single-channel markets. In addition, some of the corporation countries are not members of the European Union. [48]

3.5.1 Computer systems

The table below represents the number of applications from each Corporation X country. Although it can be seen that the quantity varies a lot depending of country, there are tens of applications per country.

Table 3 Number of applications in Corporation X countries. BMS = Bulgaria, Former Yugoslavian Republic of Macedonia, Serbia. DACH = Germany, Austria, Switzerland. FISEBALT = Finland, Sweden, Estonia, Latvia, Lithuania.

Country	# of apps
BMS	44
Bulgaria	10
Croatia	9
DACH	34
Denmark	18
FISEBALT	52
Hungary	29
Italy	23
The Netherlands	67
Norway	48
Slovakia	60
UK	38
TOTAL	432

Corporation X uses also a variety of cloud services. According to the Corporation X cloud survey, there are a total of 59 cloud services used by the member countries. Majority of them are considered good or excellent.

Table 4 Distribution of Corporation X cloud services by purpose. Source: Corporation X cloud survey.

Main business process	%
Customer Relationship	12
Facility Management	3
Finance Management	10
Human Resources	26
Infrastructure Service	26
Order Management	2
Payroll Management	2
Project Management	5
Retail	7
Travel Management	3
Warehouse Management	2
Others	2
TOTAL	100

3.6 Regulations and good practices in pharmaceutical industry

There are multiple bodies and organizations that regulate or provide guidelines for manufacturing and distributing medical supplies in the world. On a global level, actors such as European Union (EU), United States Food and Drug Administration (FDA or USFDA) and the World Health Organization of the United Nations (WHO). On a national level, regulations and laws mostly follow the regulations of these larger organizations. National organizations then advise pharmaceutical companies to act according to these principles or laws.

Negative events have greatly influenced to the evolving of pharmaceutical regulation. One of the first accidents was the diethylene glycol poisoning in the USA in 1937. This led to the introduction of The Federal Food, Drug and Cosmetic Act which gave a lot more control to the FDA, founded in 1906 [35]. Another, far more worse event, was the thalidomide disaster. Thalidomide was a sedative medicine which resulted in over 10 000 babies being born with phocomelia or other deformities. [36]

The influence of thalidomide catastrophe cannot be underestimated. As a result, the pharmaceutical regulatory system was reshaped in the United Kingdom. Further, in the USA, the Drug Amendments Act of 1962 was passed by demanding FDA to approve all new drug applications. Of the same importance, the FDA was authorized to require compliance with Good Manufacturing Practices (GMP) to officially register drug establishments and implement other requirements. In the European Community, the thalidomide event led to the introduction of the first [37] European pharmaceutical directive, Directive 65/65/EEC. [36]

3.6.1 **GxP**

The implications resulting in pharmaceutical regulation in Europe, the USA, Japan and other western countries led to the introduction of the so called Good Practices. Good Practice guidelines are used to control processes in various fields of expertise from agriculture to engineering. In the fields of pharmaceutics and medicine, Good Practices are a fundamental part of controlling the Quality Assurance (QA) of medicines.

3.6.1.1 GMP and GDP

The most important and well-known set of guidelines of medicinal quality control is defined by Good Manufacturing Practices (GMP). As the name implies, defined by the European Union, GMP determines the principles and guidelines to ensure that [38]:

> *"…products are consistently produced and controlled to the quality standards appropriate to their intended use and as required by the Marketing Authorization, Clinical Trial Authorization or product specification manufacture medicinal products with good quality."*

Each regulatory organization has defined GMP's of its own. In 1969, WHO recommended the first version of guidelines which were introduced in resolution WHA22.50 [39]. These guidelines have been updated in later resolutions. The FDA's GMP is based on Code of Federal Regulations Title 21 (parts 210 and 211). And European Unions above mentioned Directive 65/65/EEC has evolved to the so called GMP Directive of 2003/94/EC.

In short, basic requirements (in the EU) of GMP are [38]:

- Manufacturing processes are clearly defined and validated.
- All necessary facilities are provided.
- Instructions of the procedures are written clearly and the procedures are carried out by trained personnel.
- Records are made of the manufacturing, or deviations in it, and they are maintained appropriately to enable tracing of full history of batches.
- The risks of distribution are minimized and distribution takes account of Good Distribution Practices (GDP).
- A system is available to recall any batch of product and complaints of products are investigated carefully.

According to previous list of requirements, one part of GMP is GDP. However, from the point of view of a pharmaceutical wholesaler, GDP is considered as a set of guidelines of its own. To generalize, it is up to pharmaceutical manufacturers to fulfil the requirements of GMP and up to wholesalers to take care that GDP guidelines are complied.

There are not very many differences between GMP and GDP except that the other concentrates on manufacturing and the other on distribution. GDP guidelines, however, make additions to requirements of warehouses and transportation or products and mention the role of a Responsible Person (RP) as well. [40]

Other important Good Practices in the field of pharmaceutical regulations are Good Clinical Practices (GCP) for clinical trials of drug products and Good Laboratory Practices (GLP) for associated laboratory operations.

3.6.1.2 GxP and computerized systems

In any given field, telecommunications and computer systems have revolutionized the practices and ways how we work. Although the aim of computerization is to get more efficient results with better quality, from the point of view of officials, this means more monitoring and validation.

As one might assume, the developments in the field of regulation and in the field of ICT don't go hand in hand. The first requirements in EU were defined in Annex 11 in 1993 and they are still applied within EU. Also other countries such as Australia and Canada have adopted Annex 11. [41]

The Annex 11 is essentially a general checklist of things that help officials determine whether requirements have been fulfilled, not a detailed set of rules. However, it is important to notice that although Annex 11 is not a regulation itself, it is a fundamental part of EU GMP guidelines and key to complying with EU Directives. [42]

Despite being a list of general guidance, Annex 11 mentions an important principle [43]:

> *"Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process."*

3.7 Conclusion

Corporation X is a large European pharmaceutical company that operates mainly in the pharmaceutical wholesale business. Due to the short history of the company and expansion by company acquisitions, the corporation structure is quite loose and non-centralized. Every organization uses numerous applications, which have different user registries to be maintained. In the middle of this technological change, these numbers are probably going to increase. Nevertheless, Corporation X is willing to proceed uniting computer systems of the countries. Eventually, this also means having more advanced identity and access management processes. To accomplish standardized IaM processes, the before mentioned challenges and regulatory issues have to be solved.

In order to get answers to the possibility of standardization of IaM processes, a case study with an online survey was organized. The study had two goals. Primary goal was to find out whether there are possibilities to standardize IaM processes in this kind of a company. Secondly, it was important to explore the technological level in the countries, especially concerning IaM processes. In the survey, a total of 19 questions were asked from the specialists in those countries. The results of the survey questions will be handled in the next chapter.

4 Results

The fourth chapter is about presenting and analyzing the results of the survey. As previously explained, the questions were divided in four different categories. The results will be gone through category by category with visualizing charts and tables.

First, some general information of respondents will be presented. This section describes the countries that responded or didn't and some statistics about response ratio. The analysis method and the structure of the analysis will be explained as well.

The second section begins the actual analysis of the results by showing the results of the questions that belong to the Status category. Followed by that, are the results from the Motivation category. Although all the questions were important, these two categories are the essential ones that help determine the answers to the objectives of the case study.

Section 4 tries to bring out the access part of identity and access management by representing results from the Authentication category. Although it is important as well, the weight is a little bit more on identity management.

Two questions gave the respondents the opportunity to answer with free speech and they are located in the Obstacles category. Therefore, this section doesn't contain any charts, but the results are displayed in text-form.

Finally, in the last section further analysis is made based on the results. The results from the Status and the Motivation categories are combined together and each answer is given a value based on the answer. These values are then used to form charts that display overall results of these two categories country by country.

4.1 General on results

A total of 15 responses were received during the time the survey was open for answering. Because LSC's were responsible of multiple countries, the exact number of countries is troublesome to count. If this "little contradiction" is left aside, the total of all countries included in this study rises to 17 out of all 23 countries (otherwise to 13) to which the invitation was sent. In any case, the response ratio is 74% or well over 50% anyway. 6 countries didn't answer at all. These two blocks, where one LSC was responsible of each, were DACH (Germany (**DE**), Austria (**AT**), Switzerland (**CH**)) and BALTICS (Estonia, Latvia, Lithuania). One country, Finland, was the only country that had three respondents. Results from Finland were mostly identical compared with each other. Basically, only the answers to motivation questions had differences in Finnish answers. Table 5 lists both participants and non-participants of the survey.

Table 5 List of participants and non-participants in the survey.

Respondents	Non-respondents
BALTICS (Estonia)	Bosnia and Herzegovina
BALTICS (Latvia)	Bulgaria
BALTICS (Lithuania)	France
Croatia	Poland
Czech Republic	Serbia
DACH (Austria)	United Kingdom
DACH (Germany)	
DACH (Switzerland)	
Denmark	
Finland	
Hungary	
Italy	
Macedonia	
The Netherlands	
Norway	
Slovakia	
Sweden	
Count: 17 (13)	Count: 6

What comes to the geographical distribution, there is not any clear and common factor there - the responding countries are located pretty much all over Europe. However, the Nordic and Baltic countries were very well represented. From the large countries, France, the United Kingdom and Poland didn't respond. Of the 15 respondents, 8 are CIO's and correspond quite well the ratio of CIO's in the target group, 18 out of 30, to whom the survey link was sent.

Because most of the answers, namely all the multiple choice answers, were obligatory to answer, the answer ratio is very good with all the respondents. Regarding free text answers, roughly half of the answers have enough text to be able to use it in analysis.

The results will be analyzed in the following sections categorically, based on the before mentioned (3.3 Introduction to the research method) subjects of the questions: status, motivation, authentication and obstacles. Additionally, further analysis is made by calculating the values and averages of the answers to status and motivation questions, and then combining the results to get an overall picture.

Regarding the before mentioned contradiction, it is dealt with so that factual responses, namely all the IaM status answers, are analyzed country wise. Other, more opinion oriented questions, will be handled by respondent.

In order to help yourself understanding the results in the charts and tables, please refer to the Appendix I where the corresponding questions are listed.

4.2 IaM status in Corporation X member countries

Total of 7 questions covered the topic of IaM status in Corporation X countries. These were questions from 1 to 6, including 2a, marked by green color on Appendix I and will be handled by country. Question number 1 was about the number of systems that users need to log in. The average amount of systems in that case seems to be quite high. As can be seen from Fig. 10, there were five choices to choose from and nobody chose the option "1-3". 38 percent of countries answered 7-9 which is quite high. Half of the respondents, total of 50% answered that they need different login credentials to 10 or more systems which is a considerably high figure.
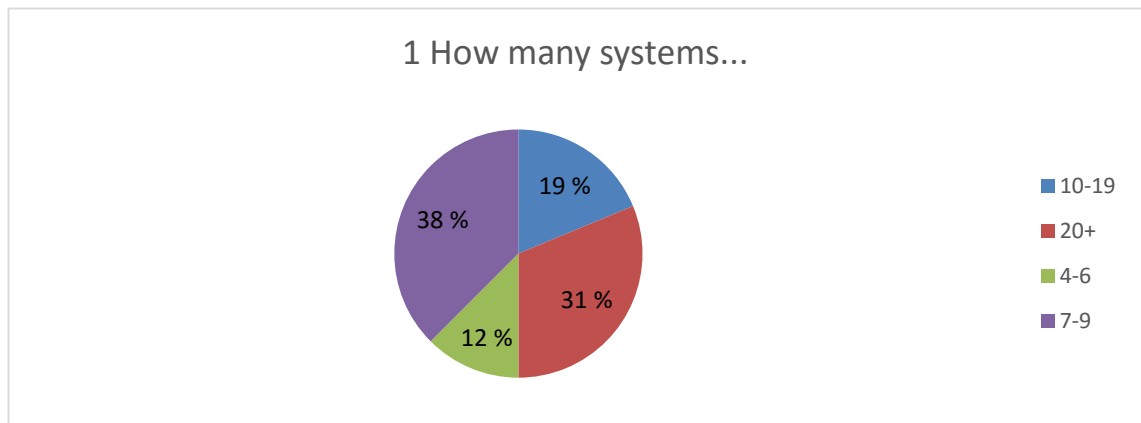

Fig. 10 Question 1. How many systems or applications do you have in your organization that require differ-ent login name (including Microsoft AD or other directory services)?

The next question was an important one and was about existing IaM software in respondent company. Only one person answered to have IaM software and 3 persons weren't sure. What is noteworthy here is that the majority of countries, 56 percent, stated that although they don't have IaM software, they are interested to have one.
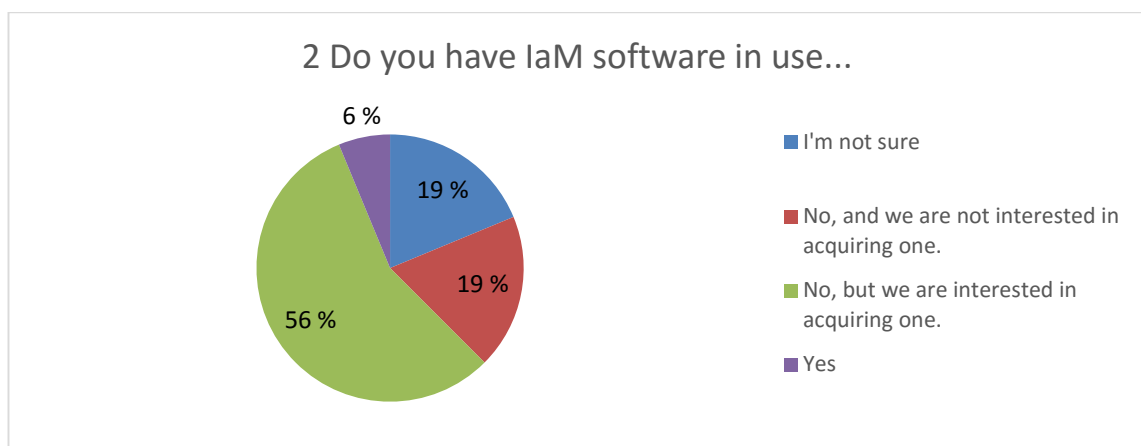

Fig. 11 Question 2. Do you have IaM (Identity and Access Management) software in use at your organization?

Regarding provisioning processes in questions 3 to 5, both internal and external identity provisioning processes are only slightly centralized, if even that. However, results of question 5 tell that in half of the countries these processes are actually the same. One of

the key issues in implementing proper identity management is considered to be a tight bond with company's HR department. In the final question of IaM status question, a majority of countries, 87 %, answered that the provisioning process is at least a little bit connected to HR department.
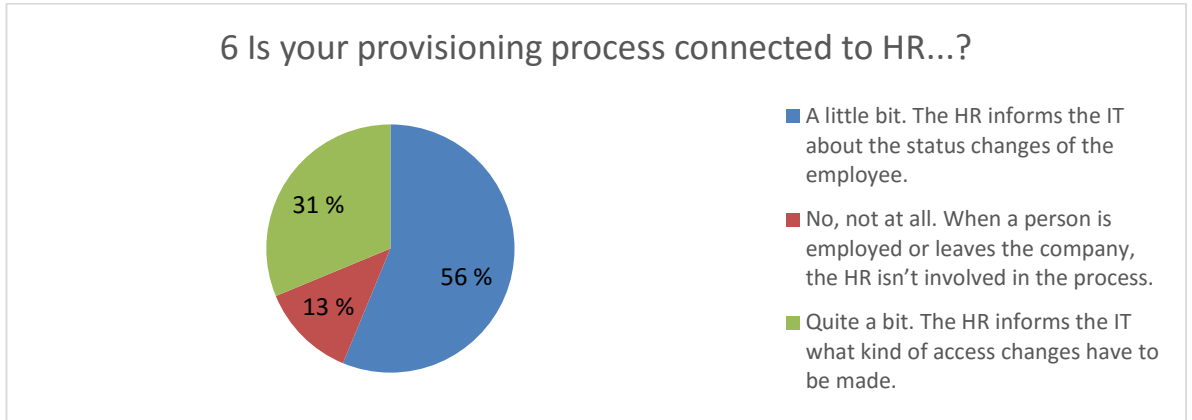

Fig. 12 Question 6. Is your provisioning process connected in any way to HR department?

To summarize the status of identity management in Corporation X, there are many countries with lots of systems with separate management for identities and unorganized processes for identity provisioning. However, there seems to be interest in improving things. In the next chapter, the motivation for improvement will be further examined.

4.3 Motivation and interest

Lack of IaM solutions, high number of software with separate identity management and decentralized provisioning processes speak for the need of strong improvement of identity management. But how about the motivation? There were a total of five questions (11, 12, 14, 15 and the branched question 2b) that tried to find out how much interest there is in IaM technologies or solutions. These questions are marked by blue color in Appendix I. The results of these questions are more or less opinions, so they will be handled by respondent.

Table 6 Question 11. In a scale from 1 to 10 (highest), how interested is your organization in following IaM software solutions…?

Qst./Cntry	DACH	HR	CZ	DK	BALTIC	FI	FI	FI	HU	IT	MK	NL	NO	SK	SE	AVG	STDEV
11.1	5	10	1	10	7	8	8	9	5	7	7	8	10	1	4	6,67	2,84
11.2	5	10	2	10	N/A	9	10	9	7	9	8	7	4	2	6	7,00	2,73
11.3	10	10	5	10	8	9	10	10	7	9	8	9	10	2	6	8,20	2,26
11.4	7	7	1	7	N/A	9	8	9	5	N/A	7	5	4	2	5	5,85	2,38
11.5	10	8	1	7	8	6	6	8	5	8	7	6	9	3	4	6,40	2,30
11.6	2	7	4	1	8	1	1	5	6	N/A	5	4	2	2	2	3,57	2,26
11.7	5	8	2	9	7	9	5	10	5	8	7	9	10	2	4	6,67	2,60
11.8	1	6	1	9	7	8	5	10	4	1	8	9	10	1	1	5,40	3,50
	5,63	8,25	2,13	7,88	7,50	7,38	6,63	8,75	5,50	7,00	7,13	7,13	7,38	1,88	4,00	AVG	
	3,08	1,48	1,45	2,85	0,50	2,60	2,83	1,56	1,00	2,77	0,93	1,83	3,20	0,60	1,66	STDEV	

Answers to questions 11 and 12 maybe easiest to interpret by calculating the average and standard deviation of the values. This way we can see, for example in Table 6 that the most interesting IaM technology seems to be single sign-on (Qst. 11.3). Or that Slovakia and Czech Republic seem to be quite critical about IaM overall. Other interesting IaM

topics seem to be password synchronization (Qst. 11.2) and IaM software or solutions in general (Qst 11.1). Clearly, the least interesting IaM solution was using directory services (Qst. 11.6). And although the question 2 doesn't strictly speaking belong to this category, over half of respondents (56%) mentioned to be interested in acquiring IaM software.
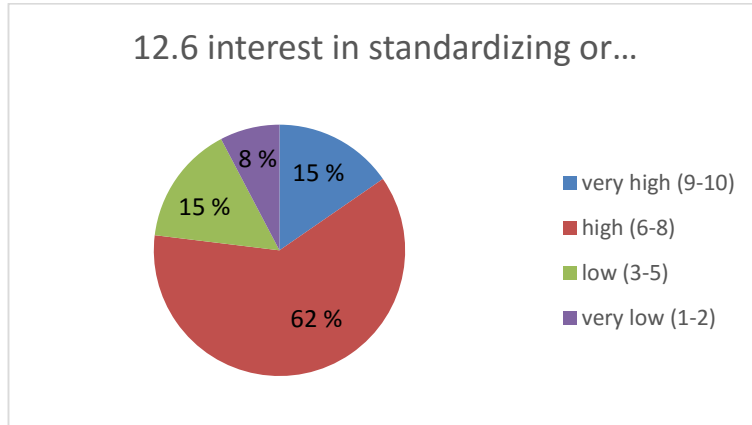

Fig. 13 Question 12.6. In a scale from 1 to 10 (highest), how interested would your organization be in standardizing or creating common Corporation X-wide processes for identity management?

Furthermore, as in Table 7, it can be seen that there is huge deviation among some answers such as the answer to question 12.1 about the interest on using more cloud services. One question, where answers have the least deviation and the respondents are most unanimous with, is 12.5, about acquiring a common Corporation X-wide IaM solution. The answers to question 12.6 about common Corporation X IaM processes gained similar results than to 12.5. Majority of people were in favor of that (some of them strongly, three values of 10) and only four people under value 6. Respondents are also very much in favor of providing better IaM solutions for both internal and external customers (Qst. 12.2 and 12.3).

Table 7 Question 12. In a scale from 1 to 10 (highest), how interested would your organization be in…?

Qst./Cntry	DACH	HR	CZ	DK	BALTI	FI	FI	FI	HU	IT	MK	NL	NO	SK	SE	AVG	STDEV
12.1	1	3	1	9	N/A	9	5	9	4	8	8	10	10	1	1	5,64	3,58
12.2	6	5	4	10	6	10	10	10	5	9	6	10	8	4	6	7,27	2,29
12.3	8	5	3	10	7	9	8	10	5	9	6	10	10	5	6	7,40	2,22
12.4	8	7	2	1	7	8	10	3	6	9	4	9	8	5	8	6,33	2,65
12.5	8	6	4	10	6	8	8	7	6	8	7	10	5	4	4	6,73	1,91
12.6	8	8	6	10	6	8	10	4	6	7	8	10	1	3	4	6,60	2,60
	6,50	5,67	3,33	8,33	6,40	8,67	8,50	7,17	5,33	8,33	6,50	9,83	7,00	3,67	4,83	AVG	
	2,57	1,60	1,60	3,30	0,49	0,75	1,80	2,79	0,75	0,75	1,38	0,37	3,16	1,37	2,19	STDEV	

Regarding the scope of IaM, nearly everyone answered Internal and 60 percent (9 of 15) thought that customers shouldn't be forgotten either. Only about third of respondents considered that there is a need for partners and 3rd parties to be in IaM scope.
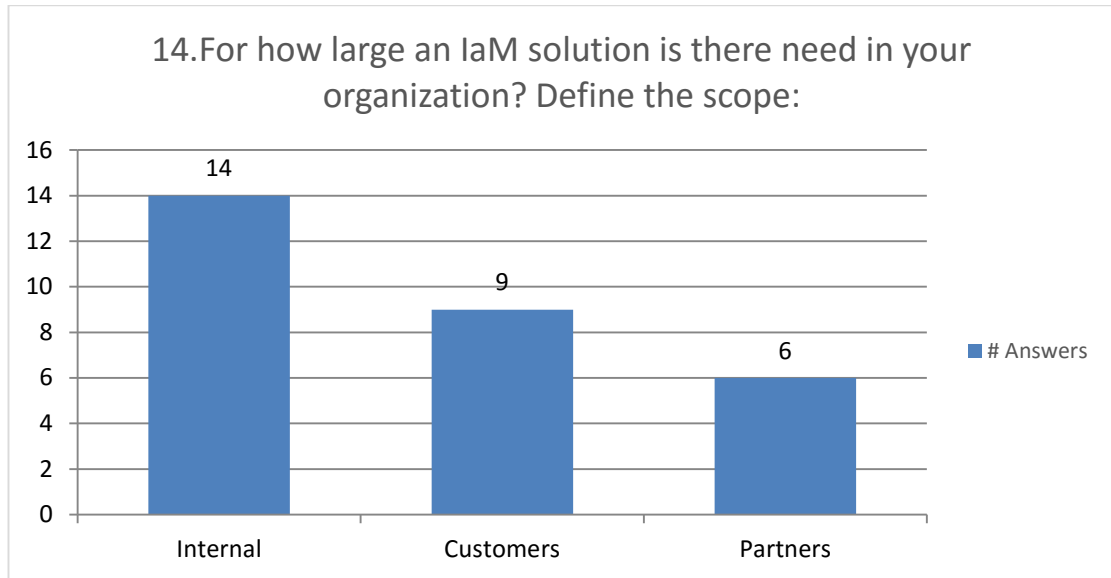
14.For how large an IaM solution is there need in your organization? Define the scope:

Fig. 14 Question 14. For how large an IaM solution is there need in your organization? Define the scope.

In the 15th question, experts were asked to name the main motivator from three choices or a specified own value. The results to this question were very evenly divided, but business agility seems to be biggest priority of most respondents.
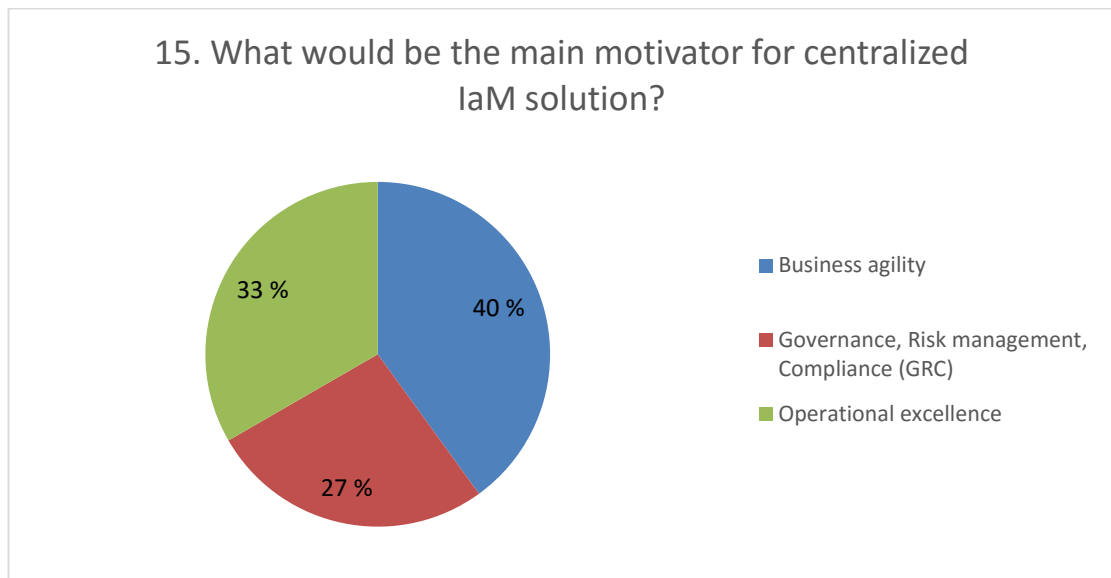
15. What would be the main motivator for centralized IaM solution?

Business agility 40 %
Governance, Risk management, Compliance (GRC) 27 %
Operational excellence 33 %

Fig. 15 Question 15. What would be the main motivator for centralized IaM solution?

The most interesting topic in IaM solutions was single sign-on. In addition, respondents had a very positive attitude towards IaM solutions in general. However, there were big differences of motivation between countries. Regarding both questions 11 and 12, majority of respondents (12 in both questions) answered above average of 5. 3 respondents, the same in both questions, got an average below five.

4.4 Authentication

Regarding authentication and access management, three questions were asked. The first was about single sign-on (Qst 7), the second about password synchronization and the last

about other authentication methods than the traditional username/password combination. Questions 7 and 8 are handled here by country and questions 9 by respondent.

Majority of respondents answered that at least some of their applications make use of either single sign-on (77 percent, see Fig 15) or password synchronization (61 percent, see Fig. 16). None of respondents told that all of their applications use these technologies.
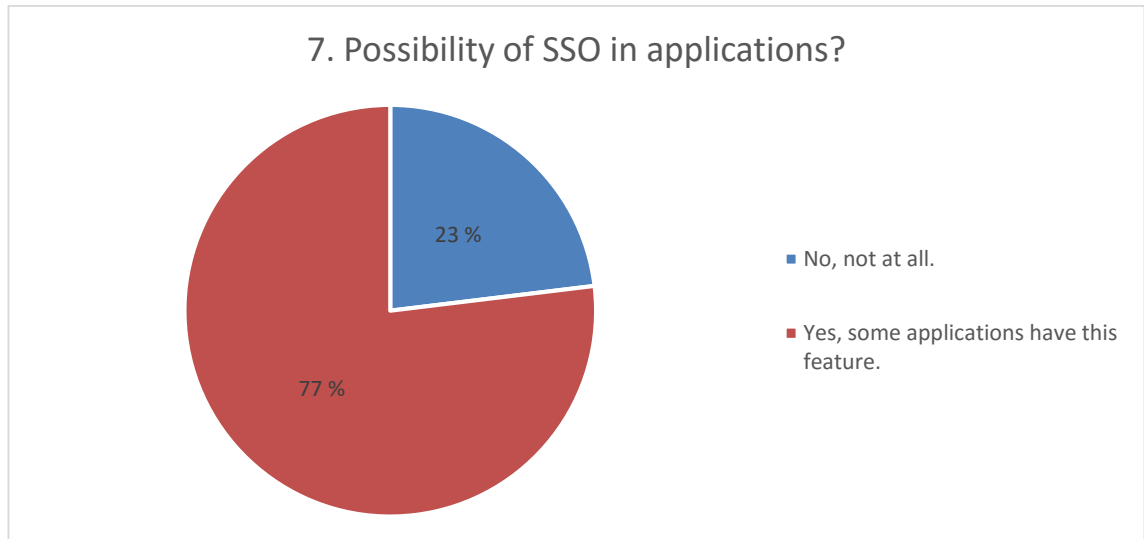

Fig. 16 Question 7. In your organization, is it possible for users to access multiple applications by providing their user id and password only once? (Single sign-on)
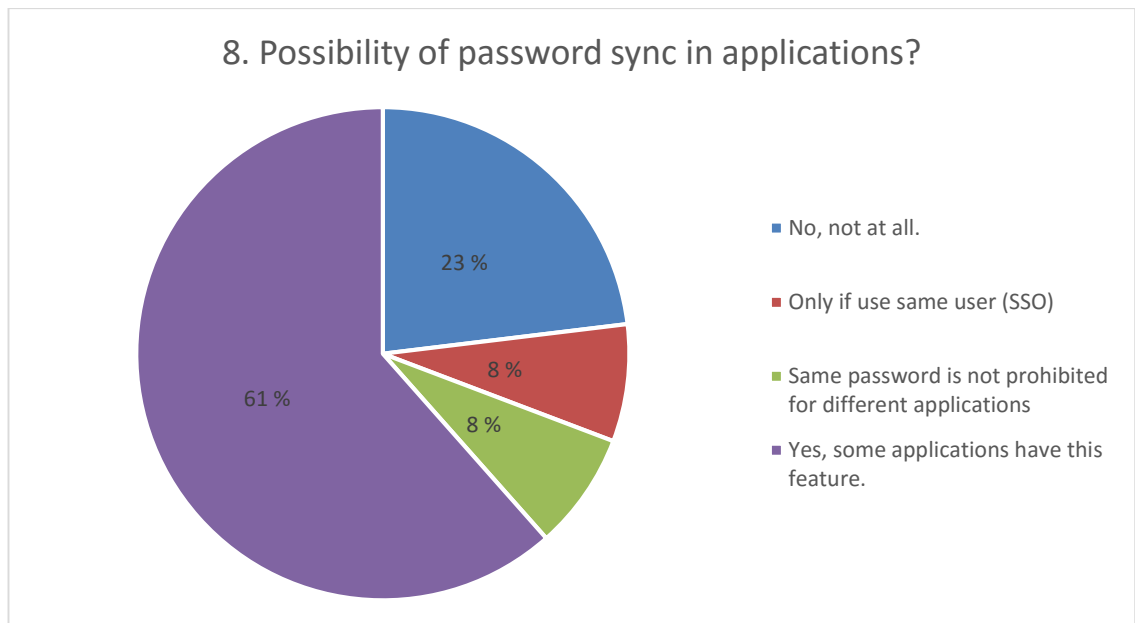

Fig. 17 Question 8. In your organization, is it possible for users to access multiple applications by using the same password? (Password synchronization)

Other authentication methods than username/password seem to be quite rare. The most common of other methods is the use of certificates. Most of the other methods are either the use of certificates or tokens.
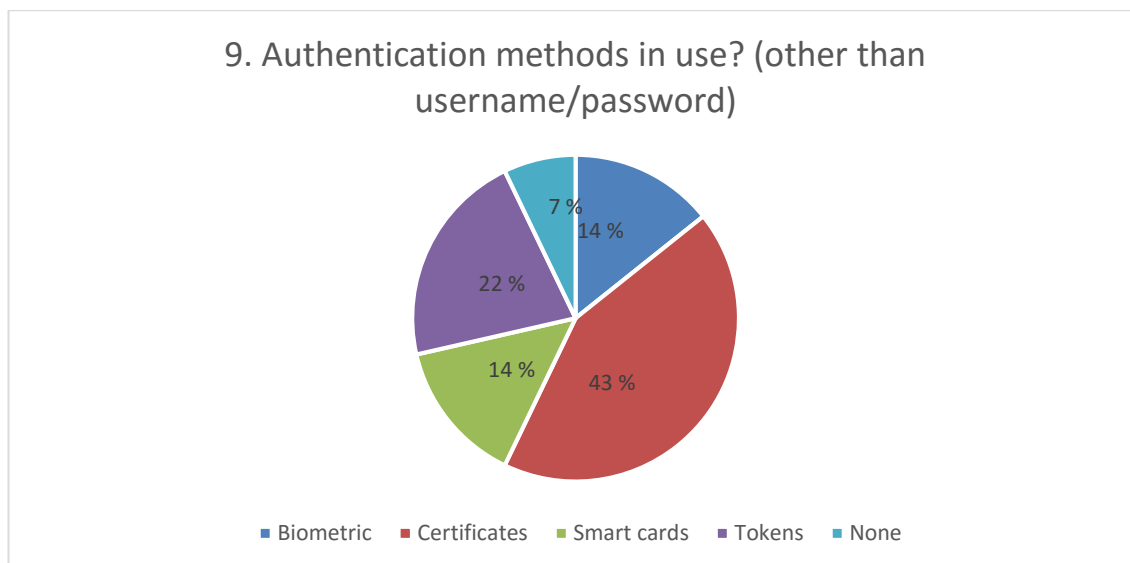
9. Authentication methods in use? (other than username/password)

Fig. 18 Question 9. Which other authentication methods do you have in use in your organization other than username/password?

General picture of authentication in Corporation X seems to be that in most of the countries, users can log in to at least some of the applications by using SSO or password synchronization. However, there are still many countries where these methods are not used at all. Other authentication methods than username/password are not very widely used either.

4.5 Obstacles

Concerning obstacles, two questions were asked. The first one, as a matter of fact, wasn't directly about obstacles but instead about regulations or laws that countries have to comply with. Second one asked if there are any obstacles against a common Corporation X-wide solution. These questions were not obligatory to answer. Fortunately, most of respondents gave at least a short answer. Some of the answers to the questions will be listed in the following paragraphs.

- 10. Please specify regulations or laws by authorities or European Union regarding identity and access management that you have to comply with (e.g. laws related to personal privacy or directives related to EU Good Distribution/Manufacturing Practices):
    o *"laws related to personal privacy"*
    o *"Hungarian Data Protection law, Hungarian labor law, GDP guidelines"*
    o *"Italian Legislative decree 196/2003 (privacy), Italian legislative decree 231/2001 (company responsibility)"*
    o *"GxP"*
    o *"None really - it's quite liberal in DK"*
    o *"Code of Conduct section 1.2 summarize applicable legislation. Section 5 describe the requirements together with the specific Fact sheet. Fact sheet 14 describes Access management:*

> *https://ehelse.no/Documents/Normen/fact-sheet-14-access-control.pdf"*
> - *"Laws covering GDP/GMP critical activities."*
> - *"GDP, GMP (only in one function, repacking, due some special regulatory). Wholesale-permit, ISO 9001 (Quality), ISO 14001 (Environment)"*
> - *"Bundesdatenschutzgesetz"* (remark: this is German Federal Data Protection Act)
> - 13. In your opinion, are there any issues or obstacles (such as legal) against a common and standardized Corporation X-wide IaM solution?
>   - *"We do not see any local legal issue against a group-wide solution."*
>   - *"Not sure, more 'no' than yes'."*
>   - *"Not in general but due to the decree 231 the Italian company should remain in control of the process, furthermore the complexity and costs could depend from the wide range of different application in use (may the scope should cover only core applications)"*
>   - *"A common solutions has to allow each country to implement it's own IaM processes and policies."*
>   - *"As we are facing issues with deploying local IaM solutions we see Corporation X-wide IaM solution would have challenges in order to be flexible enough to meet local requirements. Local requirements for IaM are very detailed and complex."*
>   - *"We are restrective regarding cloud-services and not open to transfering data to the cloud."*
>   - *"time and costs"*
>   - *"No"* (remark: 6 answers)

On question 10 about regulations, most people told that GDP or GMP guidelines are the ones to comply with. Personal privacy and data protection laws were mentioned as well.

Question 13 tried to find out whether anyone had anything against a common company-wide solution. An overwhelming majority wrote that they have nothing against a common IaM solution. However, there were also some criticism towards a Corporation X-wide IaM. Some said "time and costs" and another brought up issues deploying local IaM. One respondent was also very pessimistic on cloud solutions.

Although some critical opinions towards a common IaM solution were presented, responses were generally quite favorable. Any insurmountable issues were not stated either although some local regulations were brought up.

4.6 Further analysis

Now that we have gone through both the level of identity management and the motivation to improve it in Corporation X countries, it is good to combine and analyze these results. Both in the second and the third part of this chapter, a lot of charts and tables were shown

to visualize the results of individual questions. This may not have given a clear, big picture of the results. However, being individual, different kind of questions, this was necessary.

Next, conclusions of status of IaM, motivation to improve it and both of them combined will be shown. Because only the motivation-related questions 11 and 12 had numerical answers between 1 and 10, the IaM status answers, which were non-numerical, had to be converted to values. On question 2, a minus point was given if particular country wasn't even interested in acquiring IaM software. The importance of questions is taken into account by using coefficient 0,5 to 1,5.

Table 8 below, shows how countries rank based on the total of points gained from questions 2 to 8 whose purpose was to measure the level of IaM. The red line in the middle of the rows of depicts the average of all answers, 6,73.

Table 8 Level of IaM. Data is based on weighted values from questions 2 to 8.

Country	Q2	Q3	Q4	Q5	Q6	Q7	Q8	SUM
DACH	2	1	1	0	2	1	1	10
Italy	1	0	0	1	0	1	1	9,5
Finland	0	1	0	0	2	1	0	8,5
Norway	-1	2	2	1	1	1	1	8
Denmark	1	2	2	0	2	1	0	7,5
Macedonia	1	1	1	1	1	0	1	7,5
Czech Republic	0	1	0	1	0	0	1	7
Hungary	1	1	0	1	1	1	1	6
Sweden	0	1	1	1	1	1	0	6
BALTICS	-1	0	0	1	2	0	0	5,5
The Netherlands	-1	2	1	1	2	1	1	5
Slovakia	1	1	1	0	1	1	0	4
Croatia	1	1	1	0	1	1	1	3
coefficient	*1,5*	*1,5*	*0,5*	*1,5*	*1,5*	*1*	*1*	**AVG(6,73)**

Although it may be overemphasizing to make far-reaching conclusions about the calculated answers to these questions, the values may still give some indications about interest and state of IaM in the respondent countries. For example, as shown in Table 9, DACH-countries are *probably* more motivated on building better IaM processes than Croatia, Slovakia or the Netherlands, but one has to bear in mind that these answers are opinions of individual persons in these countries, not opinions of the whole companies in those countries.

Table 9 shows the averaged values from questions 11 and 12. The purpose of these questions was to gather data about interest in IaM related issues. The red line shows again the location of the average of all countries.

Table 9 Motivation of improving Corporation X IaM. Data is based on averaged values from questions 11 and 12.

Country	Q11	Q12	AVG (Q11, Q12)
The Netherlands	7,13	9,83	8,29
Denmark	7,88	8,33	8,07
Finland	7,58	8,11	7,81
Italy	7,00	8,33	7,67
Norway	7,38	7,00	7,21
Croatia	8,25	5,67	7,14
BALTICS	7,50	6,40	7,00
Macedonia	7,13	6,50	6,86
DACH	5,63	6,50	6,00
Hungary	5,50	5,33	5,43
Sweden	4,00	4,83	4,36
Czech Republic	2,13	3,33	2,64
Slovakia	1,88	3,67	2,64
			AVG(6,24)

In the chart below, Fig. 19, the results on motivation and status categories are combined to get a good overall picture. This chart illustrates three variables in one chart. The horizontal position is determined by the status of IaM, vertical position depends on the level of motivation and the size of a bubble is based on the number of applications in that country. It can be clearly seen that the countries seem to get divide in three groups. However, as said before, it is quite questionable whether countries can be classified based on the values of the answers.
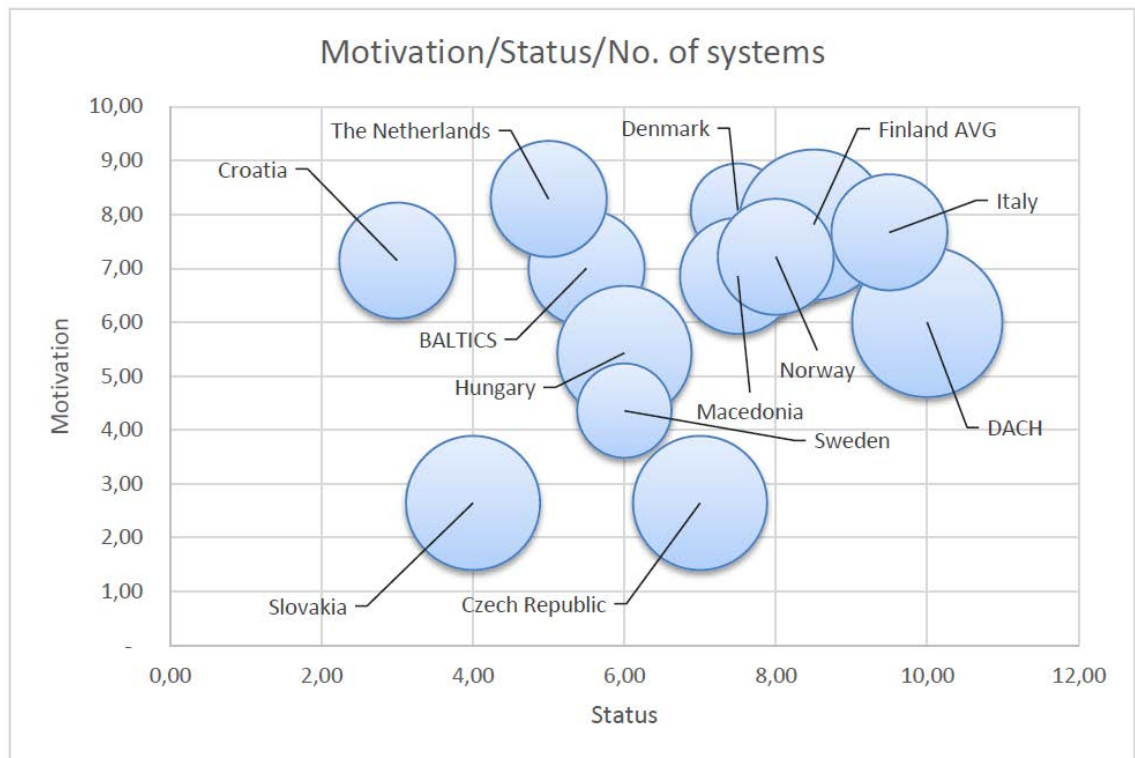

Fig. 19 Combined chart on motivation (Y axis), status (X axis) and number of systems (size).

5 Conclusions

In today's growingly IT-oriented world, people, and machines, have increasingly more different kinds of identities in use. This huge technological development has affected industry after industry, including pharmaceutical and logistic businesses. In order to maintain efficiency in computing and control of who is accessing where, some guidance is required. This is where identity and access management steps in.

This thesis was not only done for the Aalto University, but also for Corporation X which offered, along with Company Z, a great deal of support and help in writing this work. There were two objectives in the work. First of all, it was important to get a good view of the status of identity and access management in Corporation X countries. Secondly, and more importantly, the main goal was to find out if there are possibilities – or interest – to standardize identity and access management in Corporation X. In order to get answers to the main goal, a good conception of the level of IaM in fellow countries was needed.

Roughly put, the structure of the work follows the basic elements of a diploma work: theory part, case study and conclusions. In theory part, an introduction to basic methods and processes of identity and access management is provided. Moreover, a short glance to the trends and the future of IaM is made. At the end of the theory part, some regulatory framework guiding the pharmaceutical industry is presented. After that, it is time to move to case study part. In addition to actual results, an overview to the research method and the Corporation X is introduced. In the last part, we will focus further on the outcome of the study and possible implications.

The case study was sent to 30 people in 23 countries. Out of these 30 people, 15 persons, belonging to 13 countries or regions, responded. That might sound like a small number. However, for example the DACH region is a large and important part of Corporation X and Europe. The only negative setback in the scope was that other large countries, the United Kingdom, France and Poland didn't respond. Basically, it can be said that the scope was large enough to use it as a framework on the scale of the whole Corporation X.

Regarding the status in IaM countries, the bottom line seems to be that most of the countries have quite a lot of applications with different logins, having to deal with non-centralized and non- HR-connected provisioning processes. Only one of the countries said to have IaM software in use. Therefore, it appears that the standardization of processes and systems has some challenges if the environment is so heterogeneous. However, there is a lot in common in many countries. Most importantly, each and every country in Corporation X belongs to the same directory service domain. Furthermore, several countries and regions have same applications in use, such as the Nordic countries and Baltics, or the DACH countries.

The results on the motivation category of the case study suggest that there is mostly quite high interest on finding common IaM solutions. Some of the respondents were even thrilled about IaM. There were, however, some persons who didn't care at all about it. Primary scope of IaM was internal users, according to the results. These results imply

that there is interest in Corporation X countries, at least in most of them, to investigate possible common processes.

The authentication methods in Corporation X countries are mostly modern and up-to-date. Only a minority of countries didn't have single sign-on in use at all. Other than username and password combination is used in almost every country.

One of the aspects in this thesis was to investigate if there are any legal or regulatory challenges from the European Union or national legislation. The fourth category of survey questions dealt with this and other possible obstacles as well. Based on small background research of myself and the answers in the case study, there seems to be no major regulatory challenges except that some people highlighted national privacy laws in their answers.

Finally, the results from status and motivation categories were put together and analyzed further. The combined results may give some indication of countries capable and willing to implement common IaM solutions and countries that are not. However, it may be over-analyzing to make far-reaching conclusions based on this fairly limited set of results.

What next? Are there reasons to look into common IaM solutions? In my opinion, yes. And there are several motives for that. Firstly, many of the countries have countless numbers of applications with an identity system and management processes of their own. When summed up to Corporation X level, this means hundreds of processes. The interest for development of them was generally quite high as well. It shouldn't be forgotten either, that Corporation X ICT systems have been developed and integrated for years now and this would be a logical step in this path. Finally, the mere observation and studying of possible standardized processes or solutions don't have to mean committing to them yet.

References

[1]   O. Dictionaries, "oxforddictionaries.com," 2015. [Online]. Available: http://www.oxforddictionaries.com/definition/english/identity.

[2]   D. Royer, Enterprise Identity Management, Springer, 2013, p. 219.

[3]   E. Bertino and K. Takahashi, Identity Management: Concepts, Technologies and Systems, Artech House, 2011, p. 198.

[4]   M. Hansen, H. Krasemann, C. Krause ja M. Rost, Identity management systems (IMS): Identification and Comparison Study, Independent Centre for Privacy Protection; Studio Notarile Genghini, 2003, p. 327.

[5]   P. Andreas ja H. Marit, A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, TU Dresden; ULD, 2010, p. 98.

[6]   N. N. G. d. Andrade, Electronic identity, Springer, 2014, p. 90.

[7]   ISO27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary, 3rd toim., the International Organization for Standardization, 2016, p. 34.

[8]   ITU-T, Rec. ITU-T Y.2720, International Telecommunication Union, 2009, p. 34.

[9]   P. J. Windley, Digital Identity, O'Reilly Media, Inc, 2005, p. 256.

[10]   M. Benantar, Access control systems : security, identity management and trust models, New York: Springer Science; Business Media, 2006, p. 261.

[11]   www.internetlivestats.com, "internetlivestats.com," 2015. [Online]. Available: http://www.internetlivestats.com/internet-users/.

[12]   S. Brands and F. Légaré, Digital Identity Management based on Digital Credentials, Credentica Inc., 2002, p. 7.

[13]   W. MacGregor, W. Dutcher and K. Jamil, An Ontology of Identity Credentials, National Institute of Standards and Technology, 2006, p. 70.

[14]   J. A. Buchmann, E. Karatsiolis and A. Wiesmaie, Introduction to Public Key Infrastructures, Springer, 2013, p. 206.

[15]   Oasis, "OASIS Security Services TC - FAQ," 2006. [Online]. Available: https://www.oasis-open.org/committees/security/faq.php.

[16]   Oasis, "Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0," 2005.

[17] OpenID Foundation, "OpenID Connect FAQ and Q&As," 2015. [Online]. Available: http://openid.net/connect/faq/.

[18] The OAuth community, "Introduction," 2007. [Online]. Available: http://oauth.net/about/.

[19] IETF, "tools.ietf.org/html/rfc6749," 2012. [Online]. Available: http://tools.ietf.org/html/rfc6749.

[20] J. Hursti, "Single Sign-On," 1997. [Online]. Available: http://www.tml.tkk.fi/Opinnot/Tik-110.501/1997/single_sign-on.html.

[21] Merriam-Webster, 2015. [Online]. Available: http://www.merriam-webster.com/dictionary/cerberus.

[22] B. C. Neuman and T. Ts'o, "Kerberos: An Authentication Service for Computer Networks," vol. 32, no. 9, September 1994.

[23] NGINX Inc, "nginx.com," 2015. [Online]. Available: https://www.nginx.com/resources/glossary/reverse-proxy-server/.

[24] S. Tuttle, A. Ehlenberger, R. Gorthi, J. Leiserson, R. Macbeth, N. Owen, S. Ranahandola, M. Storrs and C. Yang, Understanding LDAP Design and Implementation, 2nd edition ed., IBM Redbooks, 2004, p. 774.

[25] For Dummies, 2016. [Online]. Available: http://www.dummies.com/how-to/content/defining-terms-what-is-a-directory-service.html.

[26] Telefónica, "What is the difference between M2M and IoT?," 2013. [Online]. Available: https://m2m.telefonica.com/blog/what-is-the-difference-between-m2m-and-iot.

[27] Gartner, "Predicts 2015: Identity and Access Management," Gartner, 2014.

[28] Gartner, "Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015," November 2015. [Online]. Available: http://www.gartner.com/newsroom/id/3165317.

[29] TechTarget, 2014. [Online]. Available: http://searchmobilecomputing.techtarget.com/definition/enterprise-mobility-management-EMM.

[30] Gartner, "Hype Cycle for Identity and Access Management Technologies, 2015," Gartner, 2015.

[31] Gartner, "Magic Quadrant for Identity and Access Management as a Service, Worldwide," Gartner, 2015.

[32] S. Johnston, Wikimedia Commons, 2009.

[33] Kantara Initiative, "Kantara Initiative Reshapes Global Identity Landscape Based on Industry-Wide Collaboration, Announces Initial Focus Areas," 2009. [Online]. Available: https://kantarainitiative.org/kantara-initiative-reshapes-global-identity-landscape-based-on-industry-wide-collaboration-announces-initial-focus-areas/.

[34] Kantara Initiative, "Identity Assurance Framework: Overview," 2010.

[35] Kantara Initiative, "Identity Assurance Framework: Assurance Levels," Kantara Initiative, 2009.

[36] Kantara Iniative, "Identity Assurance Framework: Assurance Assessment Scheme," Kantara Iniative, 2009.

[37] U.S. Food and Drug Administration, "Significant Dates in U.S. Food and Drug Law History," 2014. [Online]. Available: http://www.fda.gov/AboutFDA/WhatWeDo/History/Milestones/ucm128305.htm.

[38] L. Rägo and B. Santoso, "Drug Regulation: History, Present and Future," 2008. [Online]. Available: http://www.who.int/medicines/technical_briefing/tbs/Drug_Regulation_History_Present_Future.pdf.

[39] T. Vander Beken, The European Pharmaceutical Sector and Crime Vulnerabilities, Maklu, 2007, p. 218.

[40] European Comission, "Volume 4 Good manufacturing practice (GMP) Guidelines, Introduction," 2013. [Online]. Available: http://ec.europa.eu/health/files/eudralex/vol-4/2011_intro_en.pdf.

[41] World Health Organization, "WHO Good Manufacturing Practices for Pharmaceutical Products: Main Principles. WHO Technical Report Series, No. 986, 2014, Annex 2," WHO, 2014.

[42] Inspired Pharma Training, "The Main Differences between GDP and GMP," 2014. [Online]. Available: http://inspiredpharma.com/2014/11/12/the-main-differences-between-gdp-and-gmp/.

[43] G. Wingate, Pharmaceutical Computer Systems Validation: Quality Assurance, Risk Management and Regulatory Compliance, CRC Press, 2010, p. 798.

[44] O. Pearce, "The Beginners Guide to Eudralex Vol. 4 Annex 11," 2015. [Online]. Available: http://blog.montrium.com/blog/the-beginners-guide-to-eudralex-vol-4-annex-11.

[45] European Comission, "Good Manufacturing Practice, Medicinal Products for Human and Veterinary Use. Annex 11: Computerised Systems," European Comission: Health and Consumers Directorate - General, 2011.

[46] Gartner, "Why I Hate the Term GRC," 2013. [Online]. Available: http://blogs.gartner.com/paul-proctor/2013/05/13/why-i-hate-the-term-grc/.

[47] Corporation X, "Corporation X: At a glance 2015," 2015.

[48] P. Kanavos, W. Schurer and S. Vogler, The pharmaceutical distribution chain in the European Union: structure and impact on pharmaceutical prices, The London School of Economics and Political Science, 2011, p. 121.

Appendix I: Internal Survey on Identity and Access Management

Categorization

- Status (7)
- Motivation and interest (5)
- Authentication (3)
- Obstacles (2)
- Other (2)

Symbols

Symbol	description
○	radio button, single choice per question
□	check box, multiple choices per question
*	required field.
[]	field where the choice can be explained in respondent's own words or multi line textbox for free writing
[2a]	question with branching logic to next question

1. How many systems or applications do you have in your organization that require different login name (including Microsoft AD or other directory services)?*

- ○ 1-3
- ○ 4-6
- ○ 7-9
- ○ 10-19
- ○ 20+

2. Do you have IaM (Identity and Access Management) software in use at your organization?*

- ○ Yes [2a]
- ○ No, but we are interested in acquiring one [2b]
- ○ No, and we are not interested in acquiring one [3]
- ○ I'm not sure [3]

2a. Which vendor's software are you using in your organization?*

- □ IBM
- □ Sailpoint
- □ Oracle
- □ EMC (RSA)
- □ Courion
- □ NetIQ (former Novell)
- □ CA Technologies
- □ [Specify your own value]

2b. Which vendor's software are you interested in acquiring to our organization?*

- □ IBM
- □ Sailpoint
- □ Oracle
- □ EMC (RSA)
- □ Courion
- □ NetIQ (former Novell)
- □ CA Technologies
- □ [Specify your own value]

3. How centralized is the identity management (provisioning) process of INTERNAL users in your organization?*

- o Not centralized at all. We have to manually add or remove user access rights to each application.
- o A little bit. Some of the applications use shared profile data or some of the provisioning processes have been automated.
- o Quite a bit. We have a single process for provisioning.
- o Fully. We have a single process for provisioning including an application to do this.
- o [Specify your own value]

4. How centralized is the identity management (provisioning) process of EXTERNAL (partners, customers etc) users in your organization?*

- o Not centralized at all. We have to manually add or remove user access rights to each application.
- o We have to manually add or remove user access rights to each application.
- o A little bit. Some of the applications use shared profile data or some of the provisioning processes have been automated.
- o Quite a bit. We have a single process for provisioning.
- o Fully. We have a single process for provisioning including an application to do this.
- o [Specify your own value]

5. Are the processes for managing internal and external identities the one and same process?*

- o Yes, if an identity is provisioned, changed or deprovisioned, it goes through the same process.
- o No, they are separate processes.
- o [Specify your own value]

6. Is your provisioning process connected in any way to HR department?*

- o No, not at all. When a person is employed or leaves the company, the HR isn't involved in the process.
- o A little bit. The HR informs the IT about the status changes of the employee.
- o Quite a bit. The HR informs the IT what kind of access changes have to be made.
- o Fully. The HR department takes care of the whole provisioning process.

7. In your organization, is it possible for users to access multiple applications by providing their user id and password only once? (Single sign-on)*

- o Yes, we can access all applications with SSO.

o Yes, some applications have this feature.
o No, not at all.
o [Specify your own value]

8. In your organization, is it possible for users to access multiple applications by using the same password? (password synchronization)*

o Yes, we can access all applications with password synchronization.
o Yes, some applications have this feature.
o No, not at all.
o [Specify your own value]

9. Which other authentication methods do you have in use in your organization other than username/password?*

□ Biometric
□ Certificates
□ Smart cards
□ Tokens (e.g. one-time passwords delivered by SMS, token devices,…)
□ None
□ [Specify your own value]

10. Please specify regulations or laws by authorities or European Union regarding identity and access management that you have to comply with (e.g. laws related to personal privacy or directives related to EU Good Distribution/Manufacturing Practices)

o [multi line textfield]

11. In a scale from 1 to 10 (highest), how interested is your organization in following IaM software solutions:*

o IaM software in general.
o Password synchronization.
o Single sign-on (SSO).
o Federated identity management.
o User provisioning.
o Directory services (other than Microsoft AD or the current you are using?).
o IaM solutions (solution covering some or all above mentioned areas).
o IaM cloud solutions (solution covering some or all above mentioned areas).

12. In a scale from 1 to 10 (highest), how interested would your organization be in:*

1.
2. Standardizing or creating common Corporation X-wide processes for identity management?
3. Acquiring a common Corporation X -wide IaM solution?
4. Knowing about IaM processes or solutions in other Corporation X countries?
5. Providing better IaM (such as SSO, better provisioning) for INTERNAL users?
6. Providing better IaM (such as SSO, better provisioning) for EXTERNAL users?
7. Using more cloud services (SaaS, Software as a Service)?

13. In your opinion, are there any issues or obstacles (such as legal) against a common and standardized Corporation X -wide IaM solution?

8. [multi line textfield]

14. For how large an IaM solution is there need in your organization? Define the scope:*

9. Internal
10. Partners
11. Customers
12. [Specify your own value]

15. What would be the main motivator for centralized IaM solution?*

13. Governance, Risk management, Compliance (GRC)
14. Operational excellence
15. Business agility
16. [Specify your own value]

16. Are there any comments that you would like to say regarding this survey or possible centralization of Corporation X IaM?

17. [multi line textfield]

17. Please enter your contact details (Name/Organization/Postal address/Phone/Email)*

o [multi line textfield]