Linnæus University
School of Computer Science, Physics and Mathematics

Degree project

Single Sign-On

Risks and Opportunities of Using SSO (Single Sign-On) in a Complex System Environment with Focus on Overall Security Aspects

Author: Ece Cakir
Date: 2013-02-15
Subject: Software Technology
Level: Master
Course code: 5DV00E

Abstract

Main concern of this thesis is to help design a secure and reliable network system which keeps growing in complexity due to the interfaces with multiple logging sub-systems and to ensure the safety of the network environment for everyone involved. The parties somewhat involved in network systems are always in need of developing new solutions to security problems and striving to have a secure access into a network so as to fulfil their job in safe computing environments. Implementation and use of SSO (Single Sign-On) offering secure and reliable network in complex systems has been specifically defined for the overall security aspects of enterprises.

The information to be used within and out of organization was structured layer by layer according to the organizational needs to define the sub-systems. The users in the enterprise were defined according to their role based profiles. Structuring the information layer by layer was shown to improve the level of security by providing multiple authentication mechanisms. Before implementing SSO system necessary requirements are identified. Thereafter, user identity management and different authentication mechanisms were defined together with the network protocols and standards to insure a safe exchange of information within and outside the organization. A marketing research was conducted in line of the SSO solutions. Threat and risk analysis was conducted according to ISO/IEC 27003:2010 standard. The degree of threat and risk were evaluated by considering their consequences and possibilities. These evaluations were processed by risk treatments.

MoDAF (Ministry of Defence Architecture Framework) used to show what kind of resources, applications and the other system related information are needed and exchanged in the network. In essence some suggestions were made concerning the ideas of implementing SSO solutions presented in the discussion and analysis chapter.

Keywords: SSO, information security, authentication, federated identity, multi-factor authentication, MoDAF framework, SAML, LDAP, certificate authority, kerberos, shibboleth, SSO architectures, risk evaluation.

Acknowledgement

I would like to thank Ola Flygt, my supervisor for his encouragement and support; he has provided me throughout my MSc study which could not have been finalized without his assistance.

My special thanks goes to Fredrik Ruuda, ISMP Information Security Management Professional and the owner of the Ruuda Consulting AB who has been guiding me with his valuable knowledge and experiences in network security systems.

I also would like to extend my thanks to my mother Dr. Sen Cakir, my father Prof. Ahmet Cakir and Carina Öster for their help and assistance throughout my work.

Lastly, it is my pleasure to thank Bergström's family and David Öster for their hospitality and friendship during my thesis work.

Content

Table of figures

Abbreviations and acronyms

API Application Programming Interface
AS Authentication Server
ASP Authentication Service Provider
CA Certificate Authority
COI Community of Interest
CRL Certificate Revocation List
DAS Directory Access Protocol
DS Discovery Service
EAP Extensible Authentication Protocol
Eduroam Educational Roaming
HTTP Hyper Text Transfer Protocol
IdMs Identity Management System
IdP Identity Provider
IPSec Internet Protocol Security
ISP Internet Service Provider
IT Information Technologies
KDC Key Distribution Centre
LAN Local Area Network
LDAP Lightweight Directory Access Protocol
MoD Ministry of Defence
MoDAF Ministry of Defence Architecture Framework
NAS Network Access Server
NEC Network Enabled Capability
OSI Open System Interconnection
OTP One Time Password
OV Operational Viewpoints
PAM Pluggable Authentication Module
PGP Pretty Good Privacy
PKI Public Key Infrastructure
RADIUS Remote Authentication Dial-In User Service
SAML Security Assertion Markup Language
SESAME Secure European System for Applications in a Multivendor Environment
SLA Service Level Agreement
SMS Short Message Service
SMTP Simple Mail Transfer Protocol
SP Service Provider
SSL Secure Sockets Layer
SSO Single Sign-On
TGS Ticket Granting Server
UAS Universal Authentication Server
VPN Virtual Private Network

1 Introduction

Objects of this study are introduced in this chapter. Problem definitions in lines of the objects are given together with some ideas to be used. A simple network draft in conformity with the layout of the project is designed to show how SSO is applied to improve the security and reliability in network environments. Methodology to be studied and limitations concerning security, technology and architecture are briefly introduced. Finally, the structure of the thesis is given.

1.1 Need of SSO

In today's growing technology, risks are more challenging and sophisticated. It is therefore complex to acquire good solutions in any technological field. This project is inspired from business processes, clients and system managers who are facing rapidly complex interfaces with multiple login subsystems to fulfil the job functionalities. **The demand is to have those interfaces secure and easy to manage so that users can login to multiple systems securely.** For that SSO is a good solution to implement. Especially in IT (Information Technologies) systems, computer based storing of information grows rapidly. In according with that, number of services used during the day is increasing. It is harder to handle the use of information inside the network against the external factors like internet worms, service attacks, viruses and other intrusions (Hussein S. H., 2010). Those systems in IT must meet the needs and support all services and applications in the enterprise to reach the goal. To have a better performance and reliability, those services and applications need to be distributed in several different machines in the enterprise network. As a result, authorities involved in enterprise must come up with developed solutions for the needs of their secure network. User and customer contentment is also as important as the network security. The aim is to make them satisfied and feel secure while they are supplying the important information available in the network. The users must authenticate those machines distributed in the network in order to access the services and applications hosted by them. It is possible to prevent the user not to enter the authentication information, like username and password, several times or once for each network application by having wide authentication architecture in the network. If no system has the wide authentication architecture, then the user may be forced to access in at least one for each network zones by entering authentication information multiple times (Bui, S., 2005). So for that reason, multiple authentications can cause a loss of productivity and generates much more effort and time in order to control the services to make sure that they are under control by the security policy. This is where SSO steps in to become a part of this work, which can be labelled as a solution to achieve a secure access into a network. On the other hand, SSO can be defined as a way to access multiple, related, but independent software system in such a way that user logs in to a system and gains the access to all the system without being prompted to re-login in each application (Tiwari and Joshi, 2009). At the same time it increases the productivity of the company without having multiple logins for each application.

The main issue in a big network environment is the importance to distribute the specific individual or group roles to prepare the enterprise for security, and then organize the security by resource and domains, identify the security technologies and complete the requirements to understand how those requirements interacts with the network (Byrnes F.C. and Kutnick D., 2002). Finally, come up with some risk and threat analysis based on the requirements.

1.2 Research problem and goals

This project describes the risks and opportunities of using SSO in a complex system environment focusing on the overall security aspects and finding an optimal solution about usage of SSO. On the other hand, it also concerns building a centralized network in a big environment.

The goal of this thesis is to design a technical solution consisting of products, protocols and standards, which enable single sign-on users and management feel that implementation of SSO is easy, provide with high security and comfortable within a complex system environment.

Results for this project will be presented by using a model based approach with the possibility of an application on the other environments, and see if it will be widely accepted by them. This approach is developed to support defence planning and changed management activities. This is used to support system engineering and also to develop the complex system of systems, set of principles, rules and standards.

During the process of the project, some questions are going to be posed and answered and accordingly some suggestions are to be made by myself concerning the following criteria, which will be handled and evaluated in chapter 7;

- Information security analysis before implementing SSO,
- Definition of SSO,
- SSO benefits,
- Functionalities of SSO,
- Architectural guidelines for SSO,
- Protocols and directories used to provide security assertion token to the enterprise,
- Critical functionalities that SSO-service would need to work proper,
- Descriptions about technical risks with SSO from an architectural layout.

1.3 Background

Every organization has a certain way of communication and security based on the network infrastructure. That might support all systems within one physical network containing wireless access, servers, firewalls, access controls, certificates, internal and external devices which enables different subsystems to communicate.

Figure 1.1 is taken from Ruuda Consulting AB. It indicates a draft of a network that shows the basis for the project. As seen in Figure 1.1, there are a few entry points for the network. Each subsystem is secured by an access control. The SSO would be a solution for the clients running on the client-server and accessing to the subsystems so that they could be able to reach the information at all locations. Identification and authentication is performed via username and a password. First clients have to pass through an SSL (Secure Sockets Layer) tunnel between the client and the firewall. The only access allowed for the clients is from the access control. After passing through the access control and the firewall, clients are distributed from this point by using SSO to reach different subsystems trough a client-server. Each subsystem is classed into the same security level, but separated due to the risk of corrupt data or malfunctions within the subsystem. Each subsystem with the equipment in itself provides and consumes information within the same security class. A SLA (Service Level Agreement) is arranged for all systems connected to the infrastructure to be able to control the policies, to identify potential areas for improvement and also to support the use of security measures against the unknown or illegal activity. Concepts concerning security strategies would be mentioned in the following chapters. Outer clients who got an access to mobile phones or Internet use voice, text and data by using external SP's (Service Provider). All information sent through the email service between subsystems has to be encrypted. For the

military information systems, without a configured firewall between the zones, it is not possible to have an access to Internet or ISP (Internet Service Provider). Any sensitive information that is sent through the email service has to be encrypted with military standard encryption solution. Support and management desk is ready to command the systems and the infrastructure. Moreover, it is permitted to prevent the network from having an unsecure environment. To prevent a data loss from shutting down servers or links, security measures power backup is supplied by the electrical power supply.

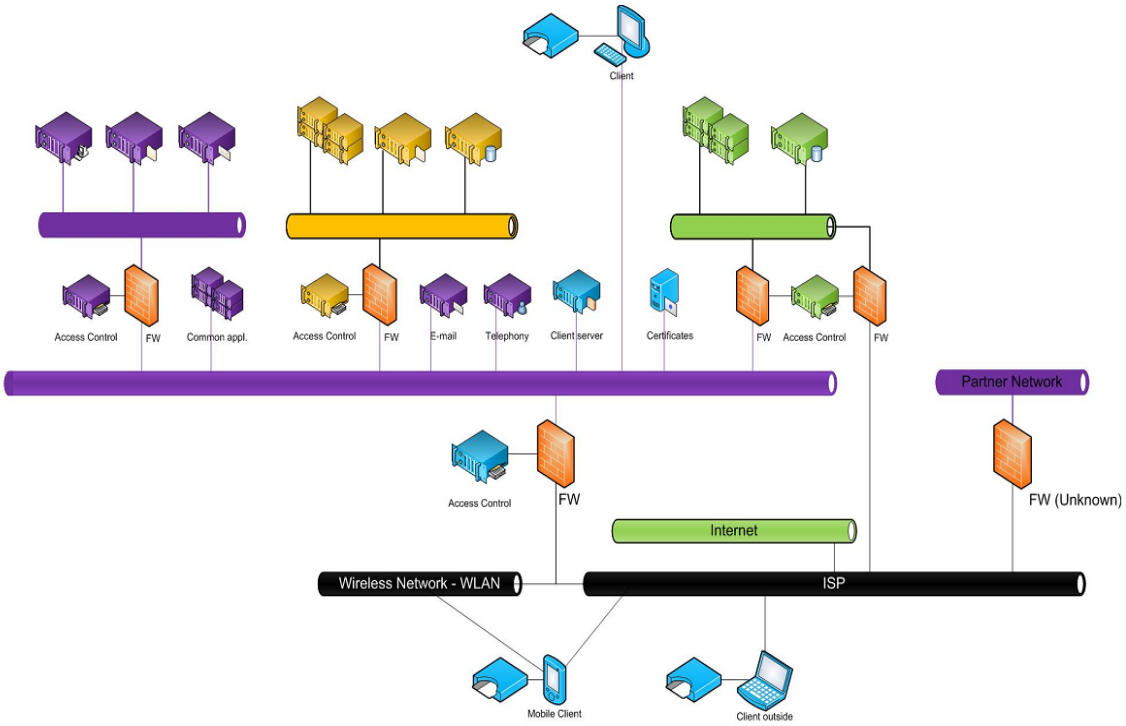

Figure 1.1 High level operational concept graphic

After explaining Figure 1.1, SSO is an environment of access control for multiple related but independent software systems. With this property a user logs in once and given access to all systems without login multiple times in each subsystem. So the clients are using one type of identification to reach the information. Additionally, multiple authentication systems are used to identify the users. The architecture of the layout is designed by using commercial standards to have a scalable and flexible infrastructure for the modifications in the hardware. Those standards are mostly used on the market.

1.4 Limitations

This project contains a research about different possible implementations of SSO, such as how secure they are with each other? Also it considers how a company is working with the selected SSO solution. After investigating and comparing the substantial solutions of SSO, new solution is expected to emerge. Some aspects concerning about SSO like cost, complexity, user friendly...etc is going to be described. Unfortunately all solutions for SSO could not be described in this study.

Various protocols are used in different levels, from the physical level up to the application level. The thesis will discuss various protocols and standards, but many of them are not going to be described in details. Only protocol and services, which are directly connected to SSO, will be mentioned. SSO scheme could be designed by combining the different models. Possible ones are going be selected and put in use. Problems concerning security, technology,

methods and architecture that are included in the contents would be discussed from a different point of application level.

1.5 Methodology

The flow of this thesis is based on searching literature studies, which includes similar studies about SSO. Following the literature survey, an empirical study is done. Firstly it is based on general security concepts and secondly focused on security analysis regarding to the requirements. Furthermore, this work is planned to use a model based approach MoDAF (Ministry of Defence Architecture Framework). This framework is mentioned as a model based approach for this infrastructure of the work. It is used for organizing the structure and the views. There are several types of views to comprise business components and relationships between them. According to The Ministry of Defence organization, MoDAF is an internationally recognised enterprise architecture framework developed by the MoD (Ministry of Defence) to support defence planning and change management activities. It is done by enabling the capture and presentation of information in a rigorous, coherent and comprehensive way that helps to understand the complex issues.

1.6 Thesis structure

The idea of the whole entire report is structured in eight chapters for the people who would like to learn and implement the SSO. Specific answers are given based on the implementation of SSO.

In chapter two, security is defined for the information. Definition is followed by the three main goals to achieve the security of information together with the security layers based on the organization structure. COI (Community of Interest) is defined according to the business and the need of information to full fill the work. After that, risks are explained briefly based on the information security. Subject of interest is focused on SSO definition in the third chapter. This is supported with the advantages and the disadvantages of SSO. According to the definition, common SSO requirements are explained for the solution. Following this, basic SSO technologies are handled in different ways to implement the SSO. After that, as an example different combinations of basic technologies are given with using MoDAF framework. Chapter five is about risk and threat analysis which is done for only one system used in this project. As a result, the analysis which is based on requirements for supporting SSO capabilities is presented in the sixth chapter. Those requirements are supported with the different technologies based on the advantages and disadvantages with the other solutions.

Finally, the discussions concerning the risk analysis and the ideas involved in SSO solutions were presented in the last chapter.

2 Information security

General information regarding the network security in terms of data protection and environmental safety is briefly introduced. The steps to be taken for a secure network environment such as information classifications and security levels are explained. Some fundamental security principles like limitation, diversity, simplicity of the system and the risks to the system are discussed for building a secure working environment.

2.1 Information security requirements

Security in our life has an important role in many areas for protection and defence. Security is defined as part of physical or information point of view. From a management perspective, the main role of security is to complete duties sufficient enough to protect the enterprise (Peltier Thomas R., 2005). However, in this thesis security is defined from the same perspective but more on the network systems for data protection, safety of hardware and software components, internal and external threats based on SSO solutions. Additionally security is defined as a freedom to be preserved against from a danger or a risk (Ciampa M., 2007). It is important to establish and maintain security requirements to protect the system. But even if it is assumed to be a safe state, it is not guaranteed that a system would never be attacked. The role of a security is to prevent information leakage and protect the information from intruders. Moreover, information security is responsible for defending and protecting the information as it is transmitted or stored on personal devices through a network or an intranet. Here come three important goals in order to achieve the information security requirements (Ciampa M., 2007).

Firstly, information security assumes that protective measures are properly implemented in the network. Secondly, information security needs to protect the data in the system. And thirdly, classification for the information priority has to be done. Implemented protective measures are not guaranteed that the system secured. But at least it gives the user safety to rely on. In secure systems there are several levels to protect the information in different priorities for users and organizations (Ruuda Consulting AB). Those levels for the system, where the case for this thesis have been developed, defined from the lowest priority to the highest by defining as unclassified, open classed, restricted, confidential, secret and top-secret. In the first level, unclassified information is not classed to any security level. Therefore, the information in this level cannot be published and found in the Internet. This level of information is defined as work material. The only data that can be published is open classed material or higher. Because unclassified information is something a person does not know what harm it will give for the organization if it is published. It is only allowed to publish in the own work group or, as a working material but it should not be published as an open document on the Internet. Next step is a decision step to decide if this information is to be kept as private or an open document. Moreover, open classed level is also one of the lower level priorities. Everyone in the system can read that information on this level. For instance, bigger networks divided in different number of sub-networks. Those sub-networks can be called as private clouds and those clouds are classed as open. One future step is that those clouds are defined as secret clouds so that no one could reach the secure ones. If the information is classed as open, then the company should stand for it and say that they are taking the responsibility of the information that they are sending is open within their knowledge. After that, it is possible to publish it. Restricted and confidential levels can be considered as same security level. Both level have no open access to Internet. If any information is wanted to have shared through the network or Internet then encryption devices need to meet the standards for the organization or with the owner of the information. Only difference is that any information at restricted level could be classed one level up at

confidential level with higher priority. But none of those information that belongs to the confidential level could be classed one level down from the higher level as soon as when they are classified as substantial information. Confidentiality makes sure that only the authorized users are able to view the information. That means, this information should not be revealed to anyone else. When the information is public, then it is readable from everybody. That is the common form of the security that is used, specially related to the military systems. **Together with the information classification, information confidentiality, integrity and availability is as important as to achieve the information security requirements.** In some cases based on the classification, confidentiality of the information is not important. It is allowed to classify as public information. But of course it is very essential that no one can go in and change the information. So the integrity has much higher security demand for that type of information than the confidentiality. In some cases the availability of the information is not important to get it immediately. Each type of information is classified according to those three terms. Secret and top-secret levels are the last and the most secure ones. Higher priority information is forbidden to share with other users. All users have their own private and secret data so sharing those data could give grave damage to the organization like, national securities, militaries and government. At top-secret level, such material is convenient to cause "exceptionally" grave damage to organizations, if they are publicly available. However it is possible to discuss the data with other users without publishing, but not explicitly. Information in the system is stored in computer hardware and software. Also used as communication resources. According to that, information priority is classified under organizational, personnel and physical layers. Those classification layers are for the last achievement of information security requirements.

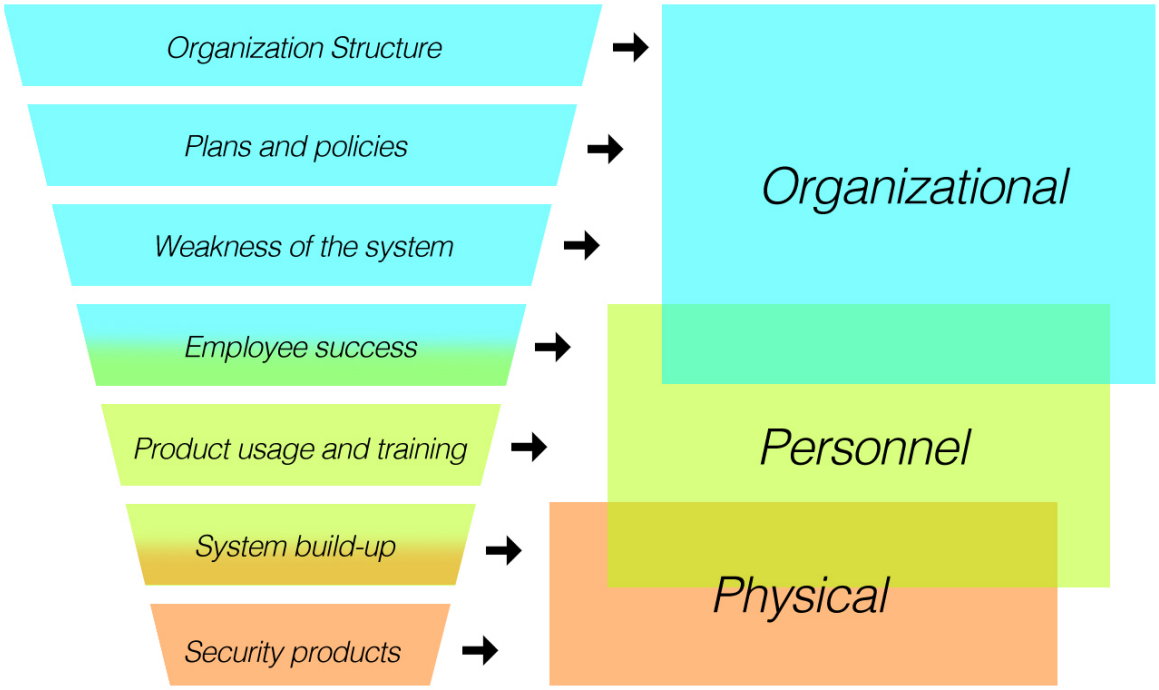

Figure 2.1 Security layers

In Figure 2.1 security layers are shown from the organizational, personnel and physical point of views (Ciampa M, 2007). It is easy to understand that; these three entities are related to cooperate together. Physical layer consists of basic security products, like firewalls, proxy servers, access controls, antivirus software, intrusion detection systems, alarms and power supplies. And personnel in the organization mainly use those products. The organization layer

contains how the structure is working, how users and employees are good enough to use those products. Data is more secured by using and establishing those products properly. The last layer reserves the plans and policies about the company. According to those plans, organization trains the users to make sure that they can correctly use the products.

Information security is also being built on the COI (Community of Interest). COI is the area that is related with a business, or the information is needed to fulfil the work to share with other users (Ruuda Consulting AB). Compartment is another word to call the COI. Cloud networking is a good example to use for all the information that is needed in one group or in one COI. And that is called a private cloud. Interests are defined as resources of the cloud. Those interests can be divided into different sub-systems like technically, physically or logically. When you combine the information you will get the COI. For instance, COI of an organization would be the same as an employee working in a security department. As a COI, employees might share some needed information or they might need the same type of information. According to that, they can tag and say that this is the shared information from the security department. Another way is if they want some specific information, they have to be sure that they requested all the information about security into one domain or in one cloud. That will be their COI. Now it is known that everyone working with the same goal or in the same area shares the same information. If it is decided to create those systems in an organization structure, they will actually end up with requesting a lot of information from different systems, databases or libraries and that will end that information up in one COI. Now it will have a lot of communication to keep the information secure in all systems. On the other hand, building up a system of systems, like private cloud or COI, it is better to use only one network resource to perform on the work. It is easy to keep the data secure with their own resources in the cloud. Then it is advantages to introduce a user to all users according to their roles. Sharing the same goal or wanting to share the same information could be defined as COI. Furthermore to have a COI, one should need to have the same mass of information to be able to collaborate on a work. Sometimes users need to take part with more than one COI according to needs. So that user can pull information from different COI's and put them together in another COI cloud in personal. It becomes a larger community or sum of all the information having a common interest. After classifying and assigning the COI's, the further step is the security clearance should be determined for the users. Some users could have access to the top-secret level of information but that does not mean that they could look at all the top-secret information in another COI related to that level. So it is possible to break down the information according to different COI and users could only get classification for certain COI. Moreover, sometimes COI's might have sub-COI. According to that, some users could have clearance for that sub-COI and some could have access to entire COI. So COI together with the classification is needed to break down the information and to be able to point exactly what each user should be allowed to access. This refers on confidentiality in information security. Those accessed information might have highest classed in integrity, which means that no one can change it except one special person. But at the same time it might be public in confidentiality, so that information does not have to be secret in that regard. In some cases security of the information is more important than the integrity. The integrity of the information is also important but in this case it is more important to have the information secure from the outside. That might not be a lack of integrity. It is just the security could have an impact on trying to keep the information up to date and keeping it traceable inside the network. If the information is moving from one COI to another COI that could be a lost in that solution and it might keep the integrity undeveloped.

2.2 Risks

In information security there are some aspects used to find out the risk possibilities and solve them according to their needs. Main threatening risks for the secure systems or networks are threat agents that are called as internal or external aspects. According to those threats, weaknesses have to be known by an organization. Otherwise it can cause a loose of information, competitive advantage, missed deadlines or suffer embarrassment (Peltier Thomas R., 2005). Those kind of weak points allow a threat agent to pass the security bridge. Thus, information security must pay attention with intrusion detection systems in the network software like firewalls and other security products, which are not allowing unexpected or unauthorized user to have an access to a network without identification. So it is good to have some restrictions, boundaries, according to a user role in a system. Also that provides a process that allows an organization to see the risks, threats, concerns and a solution to lower the risks to an acceptable level. From an access control, each login can be checked if they have rights to pass through a security bridge. In a worst-case scenario, if threats find a gap or defenceless point to hack in to the network, they will try to exploit that security weakness.

In large scale public networks consume much information and there are many possibilities for attackers to perform different type of attacks. It is not easy to have control of the information. Working with the public networks might cause security issues. But even in private networks security is not guaranteed. It is good to be aware of any kind of possibilities that is possible to crash your computer or a work place network. Nevertheless, information security attacks are mostly events or actions that have an important impact on information. Therefore organizations have a big role on to plan and prepare for every possible risk that might happen. Those risks are information theft, loss of credentials and listening to network which is transmitting data. For instance, attackers often check the emailing service in a network if it is scanning the files against the viruses. According to that they might send infected emails to get in. A theft of information in security can cause a loss of data or a delay in information being transmitted. Phishing attack is another example for threats. They also work with fake emails which might direct user to a false link to enter the credentials. That causes information theft. Mostly happens in online shopping, social networks and IT administrators. There are also outer threats like natural disasters which can destroy the network equipment causing important and costly damages. First of all it is good for each organization to start asking “How much risk can we take up and tolerate?” According to that they can build up the organization chart for the company. In this chart it should be pointed out the employee roles and restrictions. Employees who work for the company or need to have access to the network should be authorized with using smart cards or ID’s with passwords. They should be well trained about security products to be able to produce and accomplish the important roles. Secondly, operating system, software applications and hardware equipment like databases; servers need to be reviewed for controlling the security and completing the needs. It is good to keep track of the equipment by printing them out including the damages of functionality reports maybe every month. Thirdly, organization needs to reconstruct the policies and procedures to create a well working environment. They have to be documented to review, including employee recruitment or termination, employee responsibilities, installing or updating the software products. And it is also important to have documentations about a data back up and security policies. Lastly as a conclusion, after containing those needs it is good to make a recovery plan and a backup procedure for the network according to unexpected failures.

There are three options to deal with risks, one is accepting the risk, second one is to diminish the risk and third one is to transfer the risk. Here are some examples about dealing with the risks. It is good to know the possible risks that might happen to equipments in the network. For instance, it is possible to have a fire on one of the servers and it is known that

can cause a loss of information. Building a backup server makes the cost less than expected. And that is accepting the fire risk that might happen in any time. According to Ciampa M. (2007), has claimed that for the information security, it is good to diminish the risk. It is good to begin with educating employees and creating a strong security boundary area. Every failure coming after a risk has a cost to pay back. This loss of information is reported to show results in a financial penalty or the loss of good will or a reputation. So by diminishing a risk is to stop it before actually being performed. If there is no solution to accept or diminish a risk, then it is good to transfer it before that risk cause a big cost and a loss for the organization. So actually organization transfers the security of the important information to the insurance company by taking insurance for the network equipment.

Another way to build a secure system is to implement fundamental security principles, about protecting systems by layering, limiting, diversity, obscurity, and simplicity to stay strong against the attacks (Ciampa M., 2005). In many of the cases a single security product is not sufficient to prevent from external attacks. A layered security approach is needed to generate strong defensive mechanisms. In any cases, if one layer breaks by chance than the other layers are strong enough to penetrate. In information security this is important to provide it for the important data. To have only firewalls and antivirus programs would not be sufficient to protect personal computers or a network. To build a resistant protection wall, layers need to have a coordinate relation. Every layer should be stronger than the previous one to possess every kind of attack. This is explained in 2 figures.

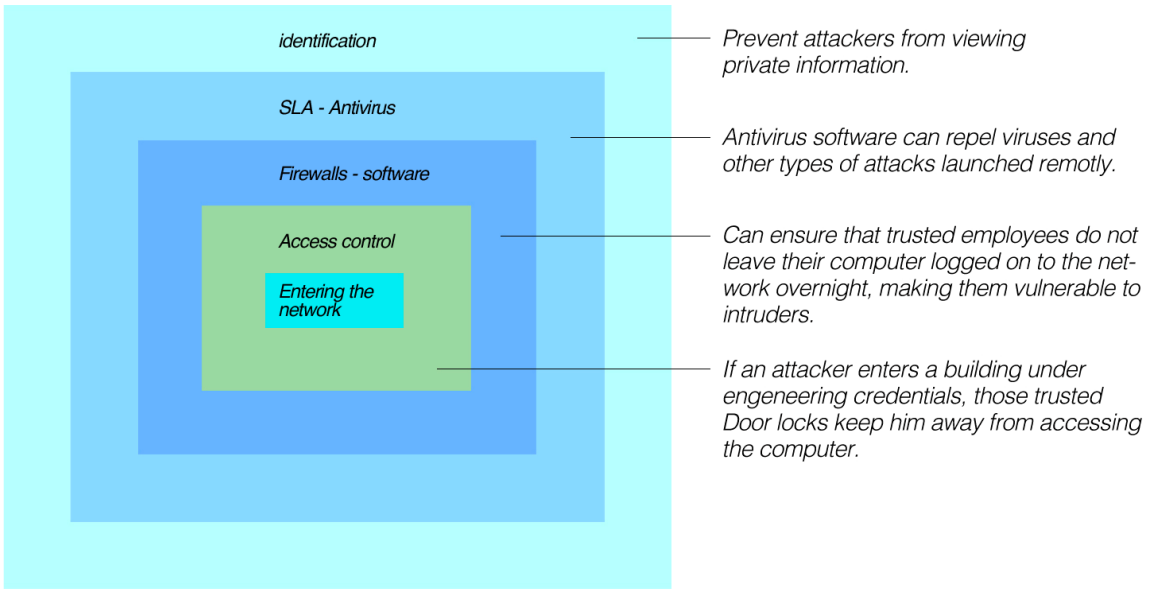

Figure 2.2 First entries to the network

Figure 2.2 points out the layers for the entry of the network. A network that is using the SSO technology, every user has expected to have one type of identification to enter the network. High secured users are equipped with extra devices to ensure the service. This is the beginning to reach the information. To support the security in each system, SLA must be created for the connection to the infrastructure to be able to control the policies and also to identify and take actions against unwanted, illegal data or activity. Firewalls and antivirus software ensures that only allowed traffic and wanted, safe data will pass through. Access control is allowing only permitted accesses to the network and to the other sub networks. Access control mechanism is implemented to protect the information from an unauthorized access, to catch the modifications from foreign interventions to determine and implement. This mechanism is capable of detecting, logging and reporting actions to breach the security

of the information (Peltier, T. R., 2005). **This is important for the limiting protection system. Minimum access is needed to protect and minimize the attacks against it.** Only permitted users should be allowed to reach the information. Every user has different limited access to perform only the job needs to do or reach the information needs to know. Especially organization databases are important to have a limited permission for users. Users who are taking the backup of the database are not allowed to display the data anywhere.

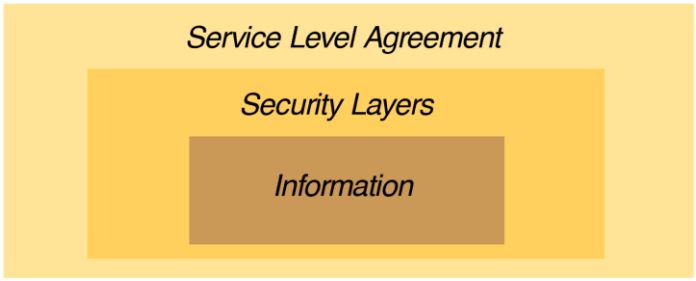

Figure 2.3 Accesses to the network

After gaining an access to the network, those layers in Figure 2.3 show the distribution for the sub-networks. Like in Figure 2.2, to protect the network and the information SLA is used to support the use of security measures like firewalls and antivirus programs against the unknown or illegal activity. Access control is used to decide a user place at the security layer for the sub-networks. Also link encryption ensures that the information transportation is protected. User authentication ensures that only listed users are able to reach the information and services that they have the right to see. The separation of information enhances the credibility of the information through limited access. Additionally for the layering security, diversity is related with this mechanism. One layer represents one level of security. Since there are several layers, security increases as going deeper in the network. So of course the total security of the first two layers is stronger than the first layer. Each layer has different level of security. The more layers in the system give strong security. The strength could be different under the roles of each layer, so that if an attack occurs on one layer, the second layer cannot be attacked similarly together with the previous layer. Another way of protecting the network or an organization is to hide the techniques (Ciampa M., 2005). These information are related to what is it inside a system or a network, how the system behaves and what security plans they have in the system. Those are the kind of information that an attacker is likely to use for hacking. Those techniques are protected by passwords. Every user must be trained to change passwords as required. According to Ciampa M., this mechanism should be used with additionally with diverse layers to get strong security of defence. Sometimes in complex networks it is hard to figure out the attacks in which forms they will pass through the network. It is good to make it simple for the users but complex for the attackers. That is the point in this project. Access servers are separated together with the firewalls for each sub-network. Each firewall is programmed by different actions to perform. Users are trained to know about their interactions between the networks. This is an advantage for a user to fix a problem when it occurs in the network. And also the design of the network is not known from outside attackers. That makes it hard to guess the behaviour and the architecture of the network. To stay strong and defensive against threats, security requirements are explained in the following chapter three.

3 Single sign-on

Definitions of SSO technology, it is advantage and disadvantages are introduced in this chapter. For the classification of SSO products some criteria of the system regarding to SSO requirements such as availability, scalability etc. has been described. Following the discussion of SSO requirements, different authentication techniques that are possible are also explained together with different SSO characteristics and multi-factor authentication techniques.

3.1 SSO and its benefits

SSO technology is a system that is used in different networks to provide safety and easy access for all multiple sub-systems after being authenticated one time. It forms authentication to a user including user credentials and access permissions. That provides user to get access for all permitted applications. After permitted to have an access for one application, all other applications occur that user already has authenticated to one application. That authentication is **reusable** for all other permitted applications without entering a username and a password (Bhosale, S.K., 2008). There are other applications and services needed to be accessed remotely by other users. Those applications are transferred and managed from remote distributed systems with different characteristics and access control methods (David, B.M., Nascimento, A.C.A and Tonicelli, R., 2011). Some applications are placed in one domain and some others are placed in multiple domains. So SSO solution is coping with user credentials across those domains (Alphonso, M. and Lane, M., 2010). From the architectural perspective (Grundmann, M. and Pointl, E., 2008) there are three types of SSO. They are Pseudo SSO systems, Centralized SSO systems and Federated SSO systems. Those types are placed and used on different customer demands. And they are discussed in the SSO application chapter. SSO serves on different purposes (Msdn, 2012). It serves communication between applications within the network, it enables communication to applications which are located in the internet by using web resources and it gives integration between different domains with different set of credentials located all over the world. The aim for using **SSO is to improve the communication and security during the user authentication and access permission verification and also to decrease the management cost.** Access control provides easy management to control and monitor user's policies, rights and traffics. More detailed information is given about access control and other requirement hardware's in the SSO requirement section.

There are different advantages and disadvantages in using or not using SSO. First of all, **availability gets higher** if SSO is used. But integrity gets lower because it depends on the security solution. It is good to have SSO if the dimension of security is extended. The difference between using and not using SSO is, if there are more sub-systems, extra mechanisms or extra functionalities within the current system that can break down, there can be some errors or adjustment problems. Secondly, while availability gets higher by adding SSO mechanisms, troubleshooting gets lower, because every mechanism that is added in the system needs to be checked for the errors and the failures or needs to be mapped for the services (Ruuda Consulting AB). As an example, in local networks it is easier to map, sniff or to see the communication between the mechanisms. But if it is a large network separated over the world then it might be hard to troubleshoot where the fault is. Such as communication between the sides, transmission problems, delays, service availability problems on the sides where miss mapped the communication between the services or DNS. Those problems are depending on the kind of the used network like a small network, isolated local network or a large network. All these networks need to have their own security dimensions, policies implemented on the system. According to that you can decide to have or not to have the SSO in the system.

More about the advantages of the SSO is that, implementing this technology helps to **improve the productivity** for users by not having them authenticate every application separately (Sandhu, S.S., 2004). It is **easy to manage user's credentials and security** for applications. It is convenient to adapt the SSO for new software or to new application programming. And this is convenient for security and the functionality of services not to be rebuilt from the beginning for each new application in the network. One disadvantage to have SSO implemented in a company might give the intruder an opportunity to reach all applications and servers in the network. For instance, almost all banks are providing internet banking service for their customers. This allows the customers to reach every service on their private profile to complete their business. Unfortunately, this might become a nightmare for customers if a hacker gets their credentials to get access to their profiles. This is called a single point of failure. Another disadvantage might be using the authentication tickets to get the access by sending it to SP's or applications (David, B.M., Nascimento, A.C.A and Tonicelli, R., 2011). This requires secure online transportation while sending and receiving messages or tickets. And this increases the network traffic, requires large bandwidth and processing loads.

In SSO feature, organizations are expecting high security to generate trust in their customers. They are doing it by securely identifying users and hosting different user authentication methods like, passwords, biometrics, hardware tokens like smart cards, certificates, digital signatures and using network standards like Kerberos, SAML...etc. Those methods are used to support the requirements of the SSO. In the upcoming chapters those requirements are explained step by step in order to understand how SSO is working and also to give a possible solution in support of SSO for the network. First of all this chapter will continue listing the requirements for the SSO.

3.2 Single Sign-On requirements

SSO requirements are availability, compatibility, deployment, maintenance, usability, performance, privacy, scalability and security, which are explained in the following subchapters. They are used to compromise a few criteria of the system to classify the SSO products. Authentication mechanism products are explained in this chapter.

3.2.1 Availability

Availability reduces the time and increases the efficiency of production by letting the information available in the network. As it stated in the second chapter SLA is created for the system security support. Creating SLA for the system security is directly connected with the availability also. For instance, downtime and the availability of the system are decided in SLA together with the SP and the system itself. So online and offline time of the system availability is known before the maintenance. Maintaining the system might decrease the availability and productivity of the organization. So it is better to finish the maintenance on agreed time. Furthermore, availability is required to merge systems or databases if new sub-system or certificate is needed inside the current system. SSO should be able to get updated with that additional information for the system. This is also connected with the scalability of the system.

3.2.2 Compatibility

For the compatibility, there are different SSO solutions that are building on different types of standards. They also building different products so these products need to be combined in order to build an entire SSO solution. Therefore compatibility is dealing with different aspects. Those are a combination of different standards. Those standards might be communication components like VPN tunnels and authentication mechanisms like smart

cards. They are two different standards to serve on different purposes. But are they working properly together or do they have conflicts. This is one aspect of compatibility. Another aspect is products that are used in the current system. In the future new products would be available to replace or exchange the current ones, and also extending the system by adding more products. Those changes should be compatible with other known solutions to follow known standards or all ingoing mechanisms. For example like the login technology and the tunnelling...etc. are standardized to be able to replace or complete the whole full system logout with the parallel SSO mechanisms. From the login point of view, while entering the network, the first firewall is meeting the user to give access directly to the environment or redirect the user to another environment. Between those environments there should not be any conflicts if this user profile is not known by the SSO environment. The profile is not thrown away; it is redirected to another environment inside the network. This is the compatibility when it comes to SSO. SSO has some functionality for sharing rights at the first point of defence. The first firewall set the information to show that the user profile is correct or not correct to have the access. If it is not correct, the user will redirected to the other applications that has permission to work. After entering to a specific application, for tracking the user behaviours, here **honeypot is given as an example to detect and deflect the unauthorized information systems.** Honeypot is discussed in detail in the discussion and analysis chapter. Also SSO should be compatible (Sandhu, S.S., 2004) for diverse sub-networks on clients and servers running on different applications, hardware and operating systems.

3.2.3 Deployment

The deployment is discussed on how to implement SSO into the system and how to start building up a system. After some guidelines for that implementation, the first mechanism or the initial mechanism is adding up on the current system or on a new system. That is happening just to prove the whole concept is right or not for the SSO solution. And then one or two systems are added in the small scale just to see if the ways of integrating mechanisms are correct or not. That helps to start up the system for the new environment. This helps to continue building up and try to verify the functionality for the SSO. So that would be the first step of the deployment to verify the SSO to the real life.

3.2.4 Maintenance

To maintain the SSO system, firstly cost measurements are considered. For instance management costs are considered to know if the SSO system is working or giving a deep knowledge to a user to run the system correctly. It is not enough to have knowledge about the sub-systems or the security measurements that protects the information. Users should be given an appropriate education, substantiated with a right certificate to the users how to maintain the SSO system. Those certificates are given according to user's job functionalities inside the system. An SSO technology must be reliable and provide maintenance to a fail-over arrangement (Sandhu, S.S., 2004). By adding a new feature like SSO, it is actually equal to adding a potential weakness in to the system. During the adjustment, if a hole is left unsecured then the cost of repairing the damaged sub-systems might be high. The cost is not only due to damages, it is due to keeping the environment up to the same level from hardware to software. Same level means the security and the updates of the equipment inside the SSO system. It is also important to have a configuration control to know that the system is running the versions of the sub-systems. That is to check if that updated sub-system is having an impact on the other sub-systems. To be preventive, it is good to have a reference system (Ruuda Consulting AB). That reference system is used to try new updates on. So the current system will not be updated before seeing the impacts on the entire system. It might not be a feature update for the system. The entire system might stop working so no one can reach the

sub-systems or that update might create weaknesses inside the system. As a result, if the entire network is followed by attackers at the time of uploading the features, it might give attackers a chance to interfere with the system. Finally, costs about the SSO system are depending on the customer and the organization needs.

3.2.5 Usability

Usability defined as a specific product which is used by certain users need to achieve goals with effectiveness, satisfaction and efficiency in order to increase the usability (Linden and Vilpola, 2005). Usability measures the system facility. Different architectural categorization of SSO is specified the usability level, like pseudo SSO, centralized SSO or Federated SSO. To increase the usability one categorization is selected based on to customer demands. These categorizations are defined in pros and cons to decide the best one in the application chapter. To have a high usability in SSO systems, it needs to be able to reach easily to the user detection information, to have fast access for the applications. Increasing the efficiency and the user satisfaction at the same time develops usability of the system application. This usability requirement makes it easier to login or to gain access to the network for the users. Although it should be cooperate together with the security to make work easy and secure. Before giving easy access for users, it is taken into consideration that new ideas may not be secure enough to prevent vulnerabilities. The new ideas should support the security technology to create safe environment for the users, then the usability would be high for the network. Additionally, single sign-off is just as important as single sign-on due to the fact that SSO opens all the systems when a user signs in before signing off. So that it is just as easy to sign off from all subsystems as it is signing in to the system. This could be the fact to increase the usability. Unfortunately, single sign-off on its own is a wide subject to discuss in this work. Another possibility to increase the usability on security applications are by recording, observing and interviewing the applications (Linden and Vilpola, 2005). Desired SSO system is easy to use and manage, reliable, robust, secure and scale to meet the feature needs (Ponnapalli, R., 2004).

3.2.6 Performance

This requirement is responsible from knowing the current performance of the network. This is calculated by considering the total time spent on the login/logout sessions, time to add a new user to the system or deleting a user from the system, supported updates for the system, the response time from a feedback or requested information, time periods for having a backup of the system...etc. All those aspects are to give better performance if the time for login is fast, if the time for adding or deleting a user is fast, if the updates are regularly checked and up-to-date, and if the responding time is short in the network. Also deciding user roles could increase the performance. According to that the user got accessed only for finishing the work that is assigned by the administrator. Many user behaviours are evaluated after a certain activity (Grundmann, M. and Pointl, E., 2008). Performance is related with the scalability. For instance, increasing number of users might not decrease the performance. For that organization tend to have multiple authentication servers to control user activities and identities.

3.2.7 Privacy

Privacy is important to supply for all information and resources kept in the system like personal detail information, users' profiles, addresses, cost documents, certificates and policies related to the company. Those important documents should be safe in a secure environment against the attackers and unwanted users. SSO identities are carrying the personal information of a user. Because of that, in open SSO environments privacy is more

important than the closed environments. As a matter of fact, organizations are looking for SSO identities which are not carrying personal details and supports unlinkability information for those identities while they are transporting inside the network (Pashalidis, A. and Mitchell, C.J., 2003). Based on different SSO architectures some of them support the unlinkability but some cannot because of those carrying identities are SP specific. The traffic between the user and SP should be routed through a proxy. That proxy ensures that user's real network address is replaced with the proxy address. For the closed environments instead of privacy priority, deployment, running and maintenance costs are more important (Pashalidis, A. and Mitchell, C.J., 2003). **Another aspect about privacy is about confidentiality and integrity.** When it comes to confidentiality, it is encryption or different information availability for each user. Also the accessed time and the context of information are important in privacy. And when it comes to integrity, the information that a user is requesting or communicating through a network must be trustworthy. User can only trust the information if it is known who has the access to that information or where that information is coming from. Privacy requirement is in conflict with the amount of user's login in the system. This is defined as, the more user is logged, the less privacy on the information, since it is possible to track user's activities according to the privacy level of the information. For some less private information tracking is not performed.

3.2.8 Scalability

SSO technology must offer scalability to expand the service for meeting the requirements of a large network (Sandhu, S.S., 2004). System might be expanded by registering more users or by adding more applications inside the system. During this growth, the system should scale well and work in the same way as before. After scaling up, the system should not lose any performance and should not lose the possibility to keep the information secure.

3.2.9 Security

At security level the aim is not only to reach the secure identity information. Besides this, it needs to know the user limitations and the way of accessing the information. It might need a single password or might need special certifications. In more centralized SSO, trust is obtained easily because only one company and one security domain is involved (Grundmann, M. and Pointl, E., 2008). In other SSO systems, security relies on strong encryption of the authentication or on trust relationships.

Confidentiality, Integrity and Availability of Information

Confidentiality and integrity are related with security requirements. Both need to protect the information from unauthorized, unwanted, unintentional alteration. Beside confidentiality and integrity, information availability is also important to meet the requirements and to prevent information from theft and losses. At the same time the information usability must be restricted for only particular objectives. There are some general requirements for the security in a system. **They are identification, authentication, encryption, log management for the network activities for identifying the events and actions of the users and security tunnels for transferring the information.** Log management activity is used mostly as a solution for the network to be able to support log analysis for the SSO solution. But it is possible to have it as a security aspect like others mentioned above.

Identification

Layout of the network used in this project has multiple sub-systems from different COI. Different SP's are located and deployed access restriction on their own information. That requires a user to be authenticated and authorized from a SP to perform access to reach the

information. The first important thing is to identify and agree from a common authentication mechanism about the identity (Huntington G, 2006a). According to this, SSO requires authoritative sources to keep the identity. Those authoritative sources need to contain required enterprise identity data and also need to be up to date for new coming processes. Provisioning processes need to be integrated with good business processes that require the normality of a system in the company. There are three main goals for the provisioning processes in the system. First one is, when a user is hired, they should be able to provide the system and the application access in the same day. Second one is, if any user's role is modified, they should make the changes in the same day. The third goal is, if any user is terminated, they should be achieved the terminated user from all network systems and applications in the same day. There are several solutions for SSO to register, to store and to look up the identities from identity repositories in a system. Detailed information is available at the Identity and Registration section. Common functionalities of SSO have two components from an outer layer of the network. One is access control and the other one is SSO API (Application Programming Interface). As stated in the previous chapter, one classic way to handle the authentication is access control which requires username and password from a user. It has a connection with an identity directory to initiate the access to the other applications by sending credentials of the user. At the same time it determines the credentials with an encrypted login cookie (Burroughs, T., 2000, pp.22). This login cookie guaranties that the authentication is already performed with that user credentials. This determined cookie sent through the encrypted SSL tunnel to the user browser. This avoids attackers to listen the network. There is no storing mechanism of cookies. Cookies expire when the login session assigned by the administrator or when the user exits the browser. If the user has an access from a partner sub-system, then the cookie expires when the user logs off from its own explicit logout. SSO technology is supporting the re-authentication for the user, authentication information and user login time outs (Sandhu, S.S., 2004).

Encryption

API is an interface between the applications and the access control in the network. It gets the user credentials from access control together with a permission to give an access for the information. As shown in Figure 1.1, the network layout provides two way of accessing, one from partner applications like other sub networks or the other one is web-based applications that might require different SSO user name and password (Burroughs, T., 2000, pp.23). External partners provide their own access control mechanism different then the local access control. SSO enterprise provides the monitoring that follows the functionalities of SSO and reports on security, performance, costs, in brief the health of the whole network. Partner applications contain SSO API, which allows them to accept the trusted user credentials coming from the access control. Cryptography is also dealing with the security of information, production of certificates, signatures, data and the traffic while it is transmitting or hiding in a secure database (Causton, R. P., 2002). In order to view the information, it requires special codes with keys used by the sender/receiver (Volonino, L. and Robinson, S.R., 2004). Those keys are used to encrypt and decrypt the information, to protect from the attackers. Keys should be kept in secret to transmit the information in a secure way. There are two types of encryption: symmetric and asymmetric. In symmetric encryption, both parties are using the same key to encrypt/decrypt the information. For this type of encryption, key should be kept under secret key cryptography because this key shared by all parties authorized to encrypt/decrypt the sent/received information (Causton, R. P., 2002). During the key exchange amount of data sending/receiving is limited for the attacks (Stallings, W., 2011). If two parties are needed to communicate with the other third party, KDC (Key Distribution Centre) is an option to produce a key to deliver through the encrypted links. This centre

decides which parties are able to communicate with each other. When the communication is permitted then the KDC provides a one-time-session key, which is known as a public key to encrypt the information before transmitting it to another party. KDC is providing keys to SSO system itself and the key for the sub-systems. It depends on the functionality of the systems. Each system might have one KDC or share one with the other sub-systems. Asymmetric encryption is functionally different than the symmetric encryption. The difference is that asymmetric encryption is using public-key encryption to deliver the secret keys. This encryption type is using two different keys; public key and a private key. Other parties could reveal public key but the second key, which is known as a private key, should be kept secret from the other parties. Public key is used to encrypt a message to send to another party to communicate. The only way to decrypt the information is using this private key (Stallings, W., 2011). The main difference between asymmetric and symmetric encryption type is that anyone can send any encrypted information securely, which can only be decrypted with the private key (Causton, R. P., 2002). This private key should only be known by the two parties, it should not be shared with a third party. Moreover, PKI (Public-Key Infrastructure) is based on asymmetric encryption. Detailed information is available about PKI at the authentication mechanisms chapter. KDC and PKI are mostly used as a solution for authenticating the users and distribute keys or distribute trust. SSO solutions are discussed for the systems in the discussion and analysis chapter.

Log Management

Log management is used by organizations to achieve the network convenience and robust. First of all, definition of a log is access requests or network activities of records from events of an organization and a network. They are used for the security needs. It is defined as a stack of logs. Each log contains information related to a specific event and security of a computer. Administrators and operators have separated logs for the security (Ruuda Consulting AB). Those logs are separated to monitor different user authentication and to record possible attacks. Monitoring systems are used to protect the log information. It is important to keep logs self-protected so no one can change or delete the entry. Logs achieve the information from antivirus programs, firewalls, remote access software, and operating systems on servers, centralized workstations and applications. Increasing number of applications, software and hardware equipment in the network require event management. It requires high security to handle events in logs. Log management is not a security system itself. But it is used to support the information security. Log management process is for generating, transmitting, storing, analysing and disposing of computer security log data. It is for troubleshooting, intrusion detection or for the integrity of information security (Ruuda Consulting AB). If there is no log management inside the system, the integrity of the information is not defined. Operating system logs are also identifying or detecting any unwanted activity. Also system applications are keeping logs for activities. They keep the information between user requests and server responses. For instance email servers. They are able to keep the list of each user access and the time that it has been accessed to applications (Kent, K., Souppaya, M., 2006). Also including login and logged out times. As it seems, log management could count as a security requirement for SSO solution. That gives capabilities to collect logs on different systems and to analyse them in order to increase the security of the system. And also clock synchronization is part of the log management, to trace and know the time stamps for logs.

Security Identifying Techniques and Secure Tunnels

There are several types of security identifying software to detect, protect and support the activities. Antivirus software detects the attacks and logins for the events that happens in the files and the systems. It also shows the file quarantines and updates that occurred within the

system (Mell, P., Kent, K., Nusbaum, J., 2005). Intrusion detection systems, detects and records detailed information of distinct actions and attacks. Remote access software is used between every sub-system and external devices to log the login sessions together with the time line used by every user connection and disconnection. It shows the amount of sent and received data for each user session (Kent, K., Souppaya, M., 2006). The VPN (Virtual Private Network) tunnels are open in the network for one tunnel per user. But multiple tunnels are available between the sub-systems inside the network. Those tunnels are not visual. Every communication is isolated inside them. VPN tunnelling is depending on security features like using the SSO to get access for the network. Those tunnels are open only if that user is having a right to enter. Additionally, tunnels are related with the access control mechanism to keep the logs between the network and the external devices. Web proxies are used to keep track of user activities on the web, passes or blocks the authentication of users, and secures web traffic (Slideshare, October 2008). It saves the URL's accessed by each user. Authentication servers, identity directories and SSO servers are saving logs of each user access attempt together with the username, success or failure, date and time. As mentioned before, login cookies are sent through encrypted SSL tunnels to avoid attackers to listen to the traffic. VPN is more to create a secure network connection. VPN and SSL are used for securing the network traffic in different parties. Firewalls are used between every sub-system and every login access from external devices. It enables or disables activities based on the policy. Enables logging for allowed connections, logging for outbound connections and monitors unusual traffic from inside to outside (Slideshare, September 2008).

3.3 Security features for handling the SSO

After discussing SSO requirements, different possible security techniques are defined in this chapter. Those techniques are used to build up a SSO solution supporting together with the SSO requirements.

3.3.1 Identity and registration

From the SSO requirements, directory services are defined for keeping identities of users and network devices. Those services are linked to the different identity directory solutions of how SSO is storing, registering and giving grant permissions to identities. Those solutions are active directories, LDAP (Lightweight Directory Access Protocol), X.500 catalogues, RADIUS (Remote Authentication Dial-In User Service) databases. Otherwise it is hard to authenticate users by confirming individually from each application. With the directories it is easy to control user grant privileges and access permissions for the network. Those directories are discussed according to different SSO solution examples further in the chapters. Short descriptions of those directories are given as followed (Ciampa M., 2005); Active directory is used as a service for Windows. This directory stored on a database and each database stored on Windows servers inside the domain. LDAP directory is in use for a server or a distributed set of servers that contain an information database of users. Server is reported to store the user names, addresses, roles, network addresses and other information about the user (Stallings, W., 1998). Using a virtual directory to an enterprise LDAP directory could link databases, which are used as an authoritative identity sources. Virtual directories could be used to synchronize LDAP directories. X.500 catalogues are not dealing with user information. It is dealing with the structure of how user data is stored. So the system is deciding which information is accessible. This catalogue provides a user protocol named DAS (Directory Access Protocol). LDAP is the simplest version of DAP. DAP requires private networking to access but LDAP is easy to obtain directory of information almost on virtually any computer platform. LDAP uses SSL to provide identity authentication and that is also obtained by using certificates. RADIUS is used for centralized authentication and for access control for remote

connections. Each user request first goes to NAS (network access server). That server is acting as a tunnelling between the user and the internet. After a request sent from NAS, RADIUS searches the user identity in its database. Each user is required to have a unique enterprise identifier in directory services. Those enterprise identifiers need to be mapped to each application used by a user for the security. It is important to keep the user credentials safe in the network. That is also done by the directory services. To keep them safe, some steps have needed to be considered. To determine registered users identity types and check which systems of records are used to justify for an identity, for instance driver license, passport, etc. Make sure which type of identity background (employee, customer, consultant, and contractor) is required to have a safe access to the network.

3.3.2 Authentication mechanisms

The security of information is important to identify and prevent unauthorized activities are done by access control in a network. Authentication is another process needs to be providing to ensure the security of information. When a user claims to have an access to the secure network, identity should be verified. The process of verifying the identity is known as authentication (Ciampa M., 2005). After this process, authorization is taking place for giving limited permission to each authorized user to access the applications inside the network. As it known, username and password is the first oldest solution for authentication, but typically that is not enough to have a secure environment. Today's human authentication ways are in three categories (Jin, A.T.B., Ling, D.N.C. and Goh, A., 2004); first, what a user know, like password or a pin number, second, what a user have, like a smart card and third, what a user is, like biometrics. If a user only uses a password or a pin for an authentication that is called one-factor authentication, which is not secure enough. If password used with both one of the other authentication mechanisms, than it will be two-factor authentication. In addition, to have a strong authentication mechanism, clever combinations needed to come up as a benefit for the system. First of all variety types of authentication mechanisms are presented in the following part to provide strong authentication. Later on, those authentication mechanism combinations are discussed in chapter 3.3.

User authentication

Authentication from a user perspective brings in minds passwords. Passwords might be the first possibility for attackers to penetrate in to a network. To counter measure any action or any device to reduce networks vulnerability, it is possible to create strong passwords together with strong authentication. Meaning of a strong password is the ones that are difficult to break. Here are some bedrock rules for creating strong passwords (Ciampa, M., 2007). Firstly, a password needs to be at least eight characters. Secondly, a password should not be created only from letters. It should be a combination of letters, numbers and special characters. Thirdly, a password needs to be changed within a month or after some number of logons and should not be reused later on. Lastly, the password that created must be unique for SSO system. It should not be a personal email password, a desktop password or even same password with other users (Byrnes, F. C., and Kutnick, D., 2002). Those similarities could be detected by the enterprise.

In this work, ID management technology is used to detect the identification and authentication problems based on user access for multiple accounts. ID management is includes the SSO and password synchronization (Ciampa, M., 2005). The layout of the network contains several sub-systems. There are many users permitted to have an access grant to more than one sub-system after being authenticated once. It would have been time consuming and unfriendly environment to have several authentication ways to get access for those sub-systems. At this point SSO minimize to have multiple identities for the sub-systems

(Byrnes, F. C., and Kutnick, D., 2002). When user makes a request for an application, SSO interferes the user request to authenticate and immediately attaches the identity of the user to the current application (Ciampa, M., 2005). To get access for multiple sub-systems, password synchronization provides the user to get an access to multiple applications by using a single username and a password. From SSO architecture perspective using one password from one single point might bring disadvantages to a user security and privacy. A disadvantages called single point of failure (Grundmann, M. and Pointl, E., 2008). It depends on the SSO solution used for the system. If single point of failure happens in a centralized SSO environment, then the user is not able to reach the service provider. The login system is closed after that failure and user is blocked from the system. But if that happens in distributed SSO environment, user might not reach some systems. But some systems are still able to authenticate the user. Due to a SSO solution one stolen password gives consistent damage to the system. To solve this problem, one option is to store all passwords and credentials into an encrypted file or database that is secured with a master password. Then user needs to memorize one password only. Unfortunately that is not secure enough either. Additionally using other authentication methods with a password makes the system more secure. For instance smart cards and fingerprints are might use to secure the database (Park, B. et al., 2006). That is a two-factor authentication. It should be protected by highest level of security mechanisms. If this database is reachable from every device on that network, then it might be easy for an attacker to track the password. To solve this problem, the SP's could store databases online in secure clouds. Therefore trust is needed to SP's (Grundmann, M. and Pointl, E., 2008). Another possibility of having an access for high restricted states is using special certificates together with a username and a password for the applications. To be able to distinguish the normal state from a high restricted state, web security needs to provide a secure transportation between those states between the users. Another way might occur to transport between different domains, than the system should be provided to recognize those domains. Hence SLA needs to clarify the security levels and rights needed to transport. Tracking the movements within different domains, networks and applications are also important to have a strong authentication.

Alternatively, OTP (One Time Password) is another mechanism for the user authentication. OTP is changing every time when it is used. This increases the complexity of the password. This approach used to build a communication between the user and the applications. Combination of OTP with SSO is explained in Figure 3.1.

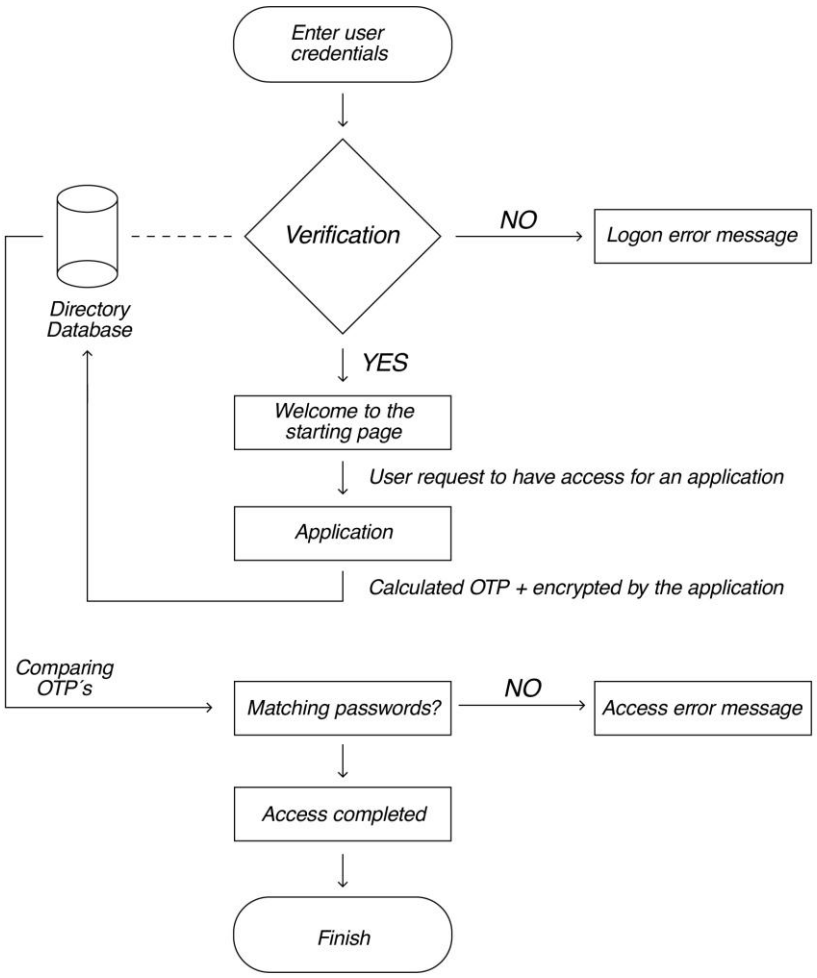

Figure 3.1 Implementation of OTP

Figure 3.1 is inspired from Tiwari and Joshi (2009) and shows the implementation of how OTP is working with the system. First of all, user needs to enter the credentials to get an access. That username and OTP password verified from a directory database. This database contains username, password, number of how many times OTP should be generated for that user, and secret questions for each user. User and the database both have the same list of passwords. User is able to get that generated OTP by using a password token (Pfleeger, C.P. and Pfleeger, S.P., 2007). That token might be a device like mobile phones or remote hand devices which are unpredictably create a password. If the password is correct than the user directed to a starting page including the applications that permitted to get an access. If the password is not correct then a warning message pops up in the screen. Each link on the welcome page sends the user credentials to the application that user clicked. After that, some specific algorithms calculate the OTP and encrypt it before sending back to the database. Here OTP computed again with the same algorithms and encrypted. If two passwords are equal which OTP sent by the user and other OTP computed by the application, then the login accessed securely. If they don't match, then the login is not successfully completed. Each successful login decreases the number of logins in the database. Now the user is directed to the application. The system checks every time the left number to use the OTP, before giving the access to the user. If it is zero, then the user must need to update the password and the secret question. This mechanism makes the tracking of the password nearly impossible. If by chance the password tracked by an attacker (Tiwari and Joshi, 2009), it is useless for the next time and the attacker cannot compute the next password because of the one-way function that

produced the OTP. Disadvantages are if that password token got stolen or lost than an eavesdropper has a change to have that device to use the intercepted password. After some certain time, re-authentication might require depending on the level of the system that user got granted. To solve this problem, the application that user had already granted an access, should be reminded by the identification of that user. From the first session of the logon, SSL servers used for the determination of the current state and also server logs are able to save the duration of the session (Huntington, G., 2006b). Alternative authentication methods like biometrics, token based, certificates, PKI, and other network authentications are given to put in use together with the passwords and are discussed in coming up chapters.

Biometrics authentication

Majority of the people want to combine security with the efficiency for their organization. According to them it is easy to maintain a single password that is not changing for each user. And it is easy to remember. At the same time, to have a stronger authentication is passing through to generate not simple passwords that related with users personal lives. But then it is hard to remember the passwords. As a solution, they write their password on a paper or on their personal computer without having any encryption (Zvetco Biometrics). This increases the risk of tracking the password. Additionally, help desk is engaged with user's passwords problems. Thus, cost time and reduces the efficiency. Therefore, using only a username and password in the enterprise is not feeling secure among the users. It is most commonly used another techniques together with the combination of username and password. One of these techniques is called biometrics. And this serves strong authentication to the users. Biometrics is using people's characteristic behaviours and genetic features for the user authentication (Ciampa, M., 2007). Using biometric features could differentiate one person from another (Byrnes, F.C., and Kutnick, D., 2002). And it provides secure authentication. There are several characteristic features of biometrics used for identification, like fingerprints, voices, iris, signatures, and hands. Those characteristics are used together with certain devices to have an access. If the user wants to connect to a website or a file stored in a database more authentication is required. At this time user needs to use a device to access it. Most popular one is known as fingerprint device. This device can differentiate the fingerprints by loading each finger scan. Differentiating is decided by looking ridges and valleys located on the skin. Ridges are being the upper skin layer segments and valleys the lower segments (Ciampa, M., 2007). The user only needs to touch the scanner with the finger. For voice recognition feature is identifying the user from the voice characteristics. For the authentication some certain questions might asked by the speaker to a user or might ask to repeat after what speaker says. Those set of questions or verbal information (Bishop, M., 2005) is saved to the database to compare that the answers coming from the user are the same as the answers recorded in its database. Authentication by eye feature uses the iris and the retina checking. Iris characteristics are unique for each person and retinal authentication records are based on blood vessels in the retina (Byrnes, F.C., and Kutnick, D., 2002). Those mechanisms might be expensive to purchase. There are different combination of the features, like combining username and password with fingerprint or eye scan. Another feature might be combining the voice and face recognition (Duc, B., Bigun, E., Bigun, J., Maire, G. and Fischer, S., 1997). Adding features with features might have higher degree of authentication but more complex environment.

Token based authentication

Token based authentication provides a cryptographic token to prove the user identity for the authentication server in order to get an access (Bui, S., 2005). A token is a physical device intended to give secure authentication to be used by only one person to get an access to the

system (Volonino, L. and Robinson, S.R., 2004). It has a trusted secret key between the authentication server and the applications that user wants to have an access (Bui, S., 2005). But this mechanism is different than a biometric device. It can be defined as a hardware device provides secrecy of encrypted personal information, until it is in the safe hands. User registration in token based authentication happens by using symmetric cryptography (Bui, S., 2005). And the use of a token device is with a personal identification number or with a pin number in due course (Bishop, M., 2005). Good examples for tokens are smart cards.

Smart card is one of the most secure authentication technologies which contain a secure computer chip. Instead of using only a username and a password, this gives confidentiality to users. Smart cards are famous tokens for storing personal information and cryptographic computation capabilities to protect the authentication data (Erdem, E., et al., 2010). They act as embedded computers that can reserve personal information and dependable on keeping login history from a user access which might be used later to verify speculative logins, login attempts and auditing purposes (Erdem, E., et al., 2010). It has also physical security that won't spread out the information from the card (Causton, R. P., 2002). All those possibilities are held by a chip on the card. One feature for smart cards provides two-factor authentication (Rankl and Effing, 2003). Using a one-factor authentication gives some level of security. But in order to have better security level two-factor authentication is used. Smart card SSO security is more reliable than using a username and password instead of typing user credentials from a keyboard to a browser. That smart card serves authentication to a user by accessing the application with using credentials that embedded inside the chip. This technology allows users to have access only by entering the pin code to activate the smart card. For SSO smart card, entering a pin is one time only. This prevents users to remember several different usernames and passwords to have an access (Erdem, E., et al., 2010). Figure 3.2 shows a smart card. On the figure it shows only the interface of a smart chip. When the chip is in physical interaction with the card reader, circuitry that embedded inside it contacts with electrical connectors for transferring data to and from the card (Gemalto). This card has a capability of storing encrypted keys, which used for key exchange, identification or digital signatures. It is also possible to encrypt messages with the key or the information on the chip itself (Causton, R. P., 2002). The keys are the information that carried by the chip.

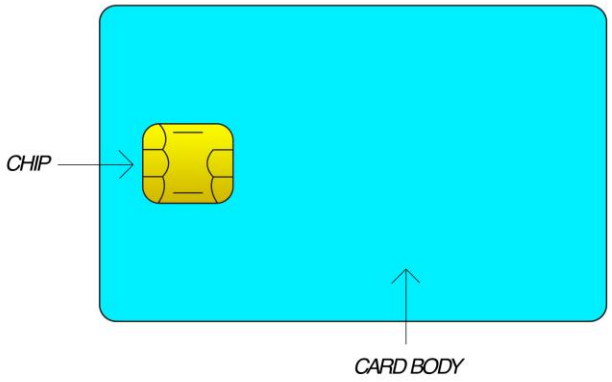

Figure 3.2 A smart card

Beginning of the work the layout that described for the network is an alternative SSO solution to use smart card feature. One objective is to integrate this solution for this system and using two-factor authentication. Second objective is to install it easily and make it convenient for users. Another feature solution might be for this device is, after activating the

smart card with users private pin code, that device might send back the OTP of the user to have access for the private networks. And those passwords can be created randomly and expires in a certain time. So that password will not be used for the next session.

Out of band

Out of band authentication is using two different ways of communication which makes user to use two factor of authentication. Computer has a network connection to a server. That is ordinary way of communicating. Between the computer and the server, authentication message is sent and received. Using out of band means one part of it is using other way of communication. It might be mobile communication. One part of the information is sent by the network and the other part is sent through the mobile. For instance, nowadays internet banking is popular for the customers. That security requires the user to identify him/her two times. A computer is login in to the bank over the internet. And then to verify the user it is receiving, for instance OTP on sms. That OTP is needed for to authenticate. So that user deals with two different bands. This way of communication makes it hard to hack in, because the attacker needs to hack in several communications.

Certificates

There are different ways of gaining trust on humans. Those might be provided by voice, face or handwriting. This is easy for the people have known before. For the rest, it needs more techniques to trust with. Each implemented technique need to be improved personally by asking specific questions to trust the other party. It called as a "trust threshold" (Pfleeger, C.P. and Pfleeger, S.P., 2007). It might be a unique form of paper or unique signature of trust. There are two way of having trust to the other parties (Pfleeger, C.P. and Pfleeger, S.P., 2007). One way is to have several people inside the organization, police or another third party who could be a voucher for the both parties. The second way is to apply for exchanging cryptographic keys. Those keys are providing communication between users, like explained before in encryption types. All public keys are attached with each user identity. So that users can trust the communication by knowing with whom they are exchanging the information. This protocol is used in each sub-system in order a demand of communication between different sub-systems. Everybody has a unique signature to communicate. That signature is attached with other user's signatures from higher positions to communicate a person with a higher position inside the same sub-system or another person from a different sub-system. Therefore, users in higher positions are vouchers to prove that the user who wants to communicate is an official employee to trust in that company. This trusted chain including public keys is proved on a letter. However certificates are communicating and identifying users electronically. This protocol is used between different SSO components. The public key and the user identity stored in a certificate and this is called a public key certificate (Stallings, W., 2011). This certificate is proved by a CA (Certificate Authority). Everything is done electronically by creating a hash value of the message and encrypting the public key and identifying those with the hash value using the private key of the CA (Pfleeger, C.P. and Pfleeger, S.P., 2007). CA might be a manager for each sub-network or a project leader in each sub-network, who has the higher position than the other user. Each certificate is signed by a private key and attached with all higher certificates for users in the company. For creating CA is important to know who is behind that public key. It is not that important to know about usage of that certificate. They are used internally, in the public internet, for creating tunnels or for electronic commerce. The purpose is to give trust about the owner of that key. After that policies and roles are declared to carry the information with the certificate between the sub-systems. Figure 3.3 illustrates the parts in a certificate structure.

Figure 3.3 Certificate structure

KDC is described as a trusted third party that is helping to setup the communication between two users by providing a one-time session key. That one-time session key and the user information are only encrypted and decrypted with the private key of the other user who wanted to be communicated with (Kaufman, C., Perlman, R. and Speciner, M., 2002). If a problem occurs in this centre, than it is not possible to use applications or provide a communication in the network. That is called single point of failure. KDC gives access to users by verifying the identities on each server that access is needed. But for the certificates each user is responsible from their private keys and need to be configured by CA with public keys (Kaufman, C., Perlman, R. and Speciner, M., 2002). This configuration gives unique signatures for each certificate. Unlike KDC, certificates are not storing on every server. They are under responsibility of each user. Moreover, if a technical problem occurs in CA that will not stop the communication or access for users. Communication between the SSO components with certificates is secured until public keys are compromised (Ponnapalli, R., 2004). For security, application servers are placed after firewalls to allow the traffic from the SSO components which have certificates to access and deny the rest of the traffic. X.509 and PGP (Pretty Good Privacy) are example standards for certificates used to describe the certificate and certification (Bishop, M., 2005). They have different structures for representing a certificate. X.509 certificates provide a directory service as a database to store the mappings between the user and the network, as well as stores the information about the user (Stallings, W., 2011). An X.509 used as a standard to format the public key certificate and provides a relation between a public key and a set of information about certificate name, issuer name, serial number and validation (Hallam, P., Kaler, C., Monzillo, R. and Nadalin, A., 2004). That given public key might be related with more than one certificate which belongs to the same user. Therefore, the signature of both certificate, make sure that created under an X.509 certificate uniquely and unchangeably. X.509 certificates are used in most network security applications with IP security, SSL, secure electronic transformation, S/MIME or PGP

(Stallings, W., 2011). S/MIME is a standard for electronic email security as like PGP. PGP certificates are used to provide security for the emails sent through the network and is using a certificate public based key for managing users public keys (Bishop, M., 2005). Even if the certificates are convenience to use, they require attention to expiration dates to renew and install the new ones on the servers (Ponnapalli, R., 2004). Otherwise entire applications might be unused until the certificates are up-to-date and installed. Since the certificates are unique for each user, that makes a certificate revocation difficult. With the KDC, it is easy to delete the key from the centre. But for the CA, it is not that simple to delete the certificate from a user. Certificates are valid until the expiration date is over. This might cause serious damages for the company from that user. The solution is overcame by using the similar system for the credit cards (Kaufman, C., Perlman, R. and Speciner, M., 2002). X.509 is determined a format to store invalid certificates. That is CRL (Certificate Revocation List). In this list there are serial numbers of the certificates, expired dates, issuer information and a signature of the issuers (Bishop, M., 2005). By using this list, it is possible to revoke certificates at any time even if the validity time is not yet over. If the expiration date is over then it is not need to put it in CRL.

PKI structure

It is challenging to believe somebody that is not known without trusted third party. PKI used as a trusted communication in ecommerce contacts made over the Internet (Volonino, L. and Robinson, S.R., 2004). How you will know that if it is trusted communication proceeding by a person without any concrete documents? Or how do you know that is that the right public key to encrypt a secure message? A PKI is designed to enable users to create, manage, store, distribute and revoke digital certificates by implementing public key cryptography (Stallings, W., 2011). Additionally it is designed to make trusted communications between users within private or public networks (Volonino, L. and Robinson, S.R., 2004). PKI provides services for identification and access control. Those are such as creating certificates with using public key, distributing certificates, signing certificates within an authenticity, adding validation date to certificates and extracting certificates which private keys are no longer validate or the supplier of the certificate is no longer allowed to have access (Stallings, W., 2011). Created certificates that PKI is using are provide the identity and the integrity by a provider or a vendor. The communication line is created to have a secure interaction between two users and they have their own unique public keys to open massages or files (Volonino, L. and Robinson, S.R., 2004). PKI structure uses asymmetric cryptography for a user registration (Bui, S., 2005). Moreover, PKI structure is the use of the technology to have an open network when the infrastructure is shared. For instance, if there will be a system that has isolated within a security zone, then it is going to need a third party of the PKI structure. That isolated information might be difficult to transfer from one zone to fetch the third party and then go to another zone, even if the firewall needed to be configured over the encrypted mechanism to allow the communication going out. So it is important to check if that third party is reachable from inside of the system when building the PKI structure.

Network authentication

Nowadays e-businesses are compacting through the internet application systems, emailing, conferences, merging several organizations in one large network...etc. Those countable serious communications are operating through the internet. Large numbers of users are online in the systems for their businesses. Those systems are protected by different security standards in the form of web services for the users and each mechanism has different policies and use of authorized certifications. For the identity issues SSO came in for the systems. However it is not enough only to increase the security for the web and has no trusted standard

to provide the communication (Wu kaixing and Yu xiaolin, 2008). SAML is an XML based security standard mechanism for communicating identities between different organizations (Ping Identity, 2002). It provides authentication documentation according to web user's authentication and authorization attributes including authentication event description for the web user between the application and the enterprise security system (Collan, J., 2009). The importance of the SAML is defined in four steps (Ping Identity, 2002). First of all the key point of the SAML maintains the multiple authentication credentials like passwords in the multiple locations. Secondly, it increases the security and decreases the identity theft by not allowing several credentials for the same user. This also decreases identity phishing inside the network by eliminating the number of times the user needs to login. The third one is SAML increases application access, so that users do not need to enter the same form of password to enter the application. All they need is to click on the application link. The last and the fourth one is preventing from duplicate credentials helps to decrease the administration time and also minimize help desk calls for resetting the last passwords. Those steps let the user safely authenticate to the application. Hence SAML builds the communication flow on the SOAP (Simple Object Access Protocol) over HTTP (Hyper Text Transfer Protocol) binding. SMAL standard has a flow of steps including the communication between the SP and the IdP for applications of SAML (Gross, T., 2003). Figure 3.4 shows how SAML is working with the protocol communication to achieve SSO system. This flow of diagram shows the relation between the user, the organization and the SP.

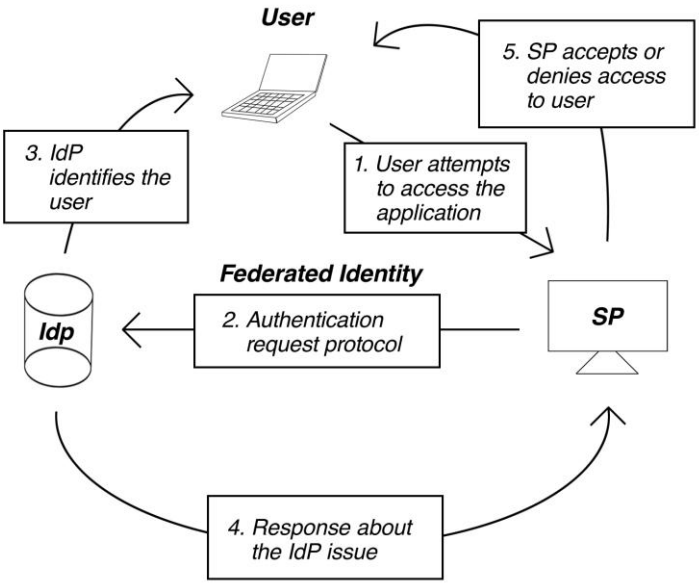

Figure 3.4 Protocol communication

As seen in the Figure 3.4, there is a user, an organization that creates and manages a directory of users and identifies them in IdP (Identity Provider) and another organization called SP hosts the applications (Hughes, J. et al., 2005). User who has a profile in the IdP wants to reach an application. This is done by clicking to a link in a portal or connecting directly to a URL address through a browser. SP has a role to host the user for the requested application. But first of all, SP sends an authentication request to the IdP just to verify if this user has a permission to complete that attempt. If user is authenticated and determined the target application, IdP identifies the user and response about the identity issue back to SP. The respond message includes the user identity encrypted into a SAML assertion (Goode, J.,

2012). Before sending the message, it is signed digitally and extra data is included about the requested application. According to the respond, user gets the acceptance or rejection as a result from the SP. SP creates a session for that known user inside the application and lets the user to get direct access (Ping Identity, 2002). For the message transferences, HTTP Redirect, HTTP POST or HTTP Artifact binding is used. Unfortunately, for the response messages HTTP Redirect binding is not allowed to use because the response would be exceed the URL length permitted by most of the users (Hughes, J. et al., 2005). Advantages of SAML on security, scalability, dependability and deployment are having appreciative impact for an adoption of growing industry (Goode, J., 2012). It is reusable for additional SP and IdP which are SAML enabled. And last it is user oriented to get direct access to the application (Ping Identity, 2002).Federated identity used in SAML provides user access to different applications through several organizations (Collan, J., 2009). Detail information about federated identity management is given in the following chapter. Having federated identity management helps users to get access to services on servers for reaching the applications in a secure and easy way. At this point services are using Kerberos standard and the Shibboleth software packages for the projects. Kerberos provides centralized authentication for users (Stallings, W., 2011). It intended to the software, servers, and user configurations that are allowed to use Kerberos standard to perform secure authentication on an open network (Brennen, V.A., 2004). Kerberos has two versions 4 and 5. Kerberos standard is explained in Figure 3.5.

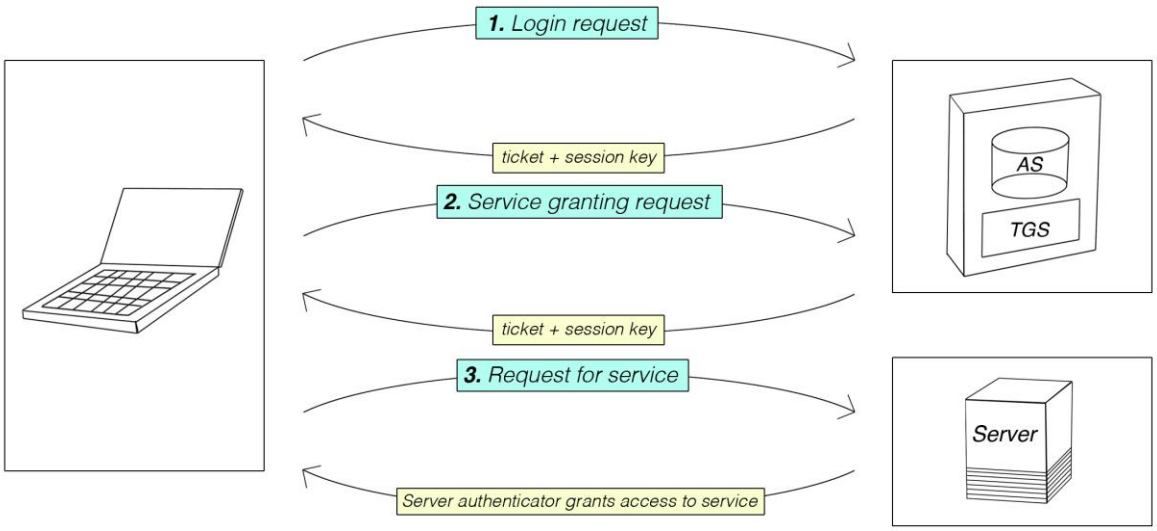

Figure 3.5 Kerberos standard

Kerberos itself uses two servers which are AS (Authentication Server) and TGS (Ticket Granting Server) (Stallings, W., 2011). This standard works for each user login request. It has one session key and one ticket to the AS and for each service request one access ticket and a session key for an authentication to the TGS server. After granting a ticket from TGS, user sends a request to the server which verifies that ticket and the identity are matching to gain an access for the application. User's credentials and the messages coming from the Kerberos are encrypted. The only way to decrypt them is user's password. To use Kerberos the system needs to have KDC and supported applications for it (Stallings, W., 2011). Moreover, it is designed to manage the large number of account databases, and uses encryption technology by sending encrypted tickets. That avoids the password sniffing and stealing information over the wire and gives more secure enterprise for the users.

Shibboleth is a web-based SSO software package (Orawiwattanakul, T. et al., 2010). That controls the identity authentication based on several federated identity standards like SAML and also using Kerberos standard. It provides secure access to applications by using security domains (Klingenstein, N., 2011). Like in SAML, Shibboleth consists of IdP and SP for exchanging attributes. Those attributes are browser profiles or protocols like groups, roles and unique ID's. In Shibboleth communication, IdP checks the SAML assertions depending on the request and SP gets the SAML assertions to decide giving a permission or not to the user like in the SAML. However Shibboleth produces another option to support IdP for identity discovery (Barton, et al., 2006). The difference between the SAML and Shibboleth is accepting a request (Scavo, 2005). SAML browser profile demands a request to IdP but Shibboleth is more SP-first. Additionally Shibboleth provides attribute authority to deal with attribute assertions different then SAML assertions (Barton, et al., 2006). More technical explanation about Shibboleth is that IdP provides information about applications to users, and the SP protects that applications from users by collecting and checking the authenticity of the information. After that the user web browser accesses a protected application, it enlightens the SP about the authentication of the user and at last allows user to login (Klingenstein, N., 2009). Another component DS (Discovery Service) is used for Shibboleth. After using Shibboleth to get access for an application, DS identifies the users own IdP. This can be done automatically or manually (Cantor, S., 2012). After being requested, SP knows which IdP should be connected with the user. That is SP-first for Shibboleth attributes. But there might be several IdP's listed for the user. User should know which IdP's to select and the application knows which IdP's are letting the access complete successfully. This works fine with the large multiple communities (Cantor, S., 2012). Additionally, if DS placed centrally then it can reduce the time of selecting home IdP to get an access for the applications (Cantor, S., 2012). After making a selection, DS links the user to a SP. At this point SP authenticates the user based on the selection. DS is embedded as an interface into a web browser (Cantor, S., 2012). Shibboleth uses different versions of SAML to specify which IdP should connect with a SP. Moreover, the user's web browser directed to an endpoint called "Single Sign-On Service" (Klingenstein, N., 2009). During that process some cookies are created, set and read by the IdP to control the user activities. For instance, logging in and logging out from the system. Before complete a successful access attributes which contains user data passed through an attribute filter (Scavo, T., 2011). That private user data is not shown all the time. It depends on SP and the principles to show it. This also improves the user privacy.

3.3.3 Federated identity management

Federated Identity management is a mechanism which provides identity management and transportation between the enterprises (Collan, J., 2009). It helps to increase the user authentication and user activity by using protocols. Some bests are known as Microsoft Passport, the Liberty Alliance and WS-Federation (Pfitzmann, B. and Waidner, M., 2003). Those open standards for identity management are discussed in the subchapter 3.3 in detail. Although from a security perspective, employees cannot control the user activities done by connecting different devices on the network (Goode, J., 2012). This might cause problems of information security. On the other hand, that brings efficiency, productivity and user motivation. At the same time this requires more responsibility of protecting the identity and the information. At that time security needs to be sure about the right access is done by the right person at the right time (Goode, J., 2012). Here comes the SSO to provide security of identity management for the sub-systems. Identity management provides different services to support the users inside the system. These services are typically servers for users who are trying to get access to resources and services in the network (Stallings, W., 2011). IdP is also in this scenario, like in Kerberos. It defines an identity for each user and associates

authentication information with attributes to get the access for the permitted services. In this scenario, there are administrators to provide roles, attributes and access permission to users, and data consumers to provide the access depending on that user credentials (Stallings, W., 2011). Furthermore, when the services are mounting up outside the network firewall or to another domain which has different IdP system, each requires its own identity management for access and authorization. In this matter, SSO is on the track to decrease the different service application passwords and provide secure, scalable, standard based and cost effective ways (Goode, J., 2012). SAML and Shibboleth are cooperating with open standards for federated identity management like Liberty Alliance, WS-Federation. Nowadays social networking service Facebook is acting like a federated identity management provider. Those federated standards provide secure and friendly environment by sharing the user identities during the data transmissions between different domains, services and applications.

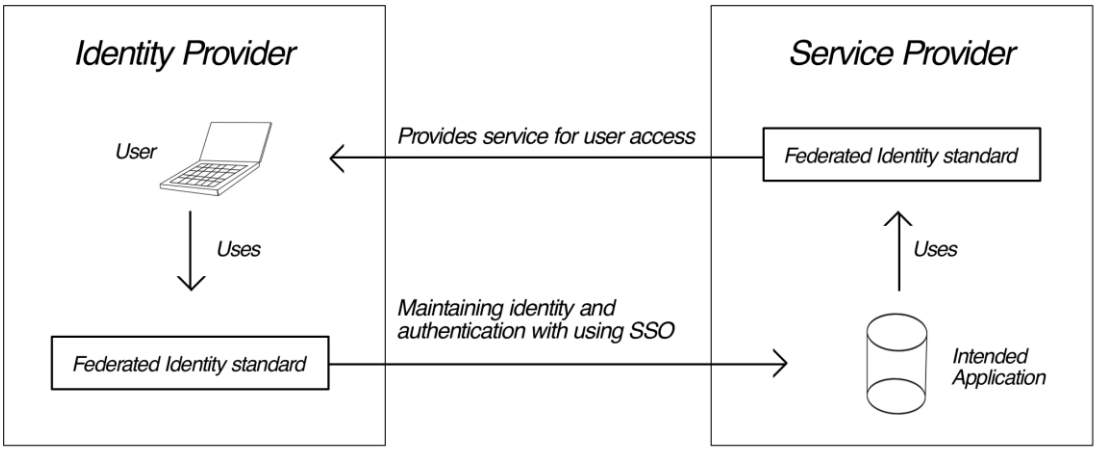

Figure 3.6 Federations in an organization

Figure 3.6 illustrates the transmission of a user access between IdP and SP with using federated identity standards. In the figure, IdP is acting as a host organization, which provides the credentials for a user to gain an access to the intended application with using federated identity standards. SP gets the credentials to provide the access for the service applications.

3.4 Single sign-on application

SSO solutions are implemented in different architecture perspectives. Those perspectives are divided in to two different SSO, simple SSO and complex SSO. As it shown in Figure 3.7, simple and complex SSO are divided in their own right as Pseudo SSO systems, Centralized SSO systems and Federated SSO systems.

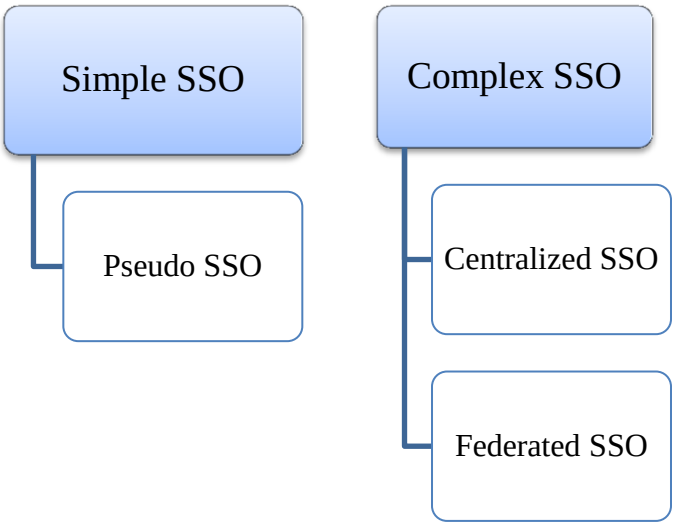

Figure 3.7 SSO Architectures

Pseudo SSO is a single authentication mechanism. Each user's access is depending on a single SP (Pashalidis, A. and Mitchell, C.J., 2003). In other words, each user credentials are SP specific. Additionally, it is possible each user has multiple identities to get an access to more than one SP. And those multiple identities require different authentication mechanisms to get a successful access (Hussein, S. H., 2010). This might be described as one-to-one authentication between the user and the SP. So in pseudo systems user has several identities but only authenticating with one credential for the first system. For other systems user is using other identities to connect. In Pseudo SSO, user first directed to the primary authentication which is the Pseudo mechanism (Pashalidis, A. and Mitchell, C.J., 2003). This authentication might require a single username and a password. Other authentication mechanisms used for the other SP's are protected under a database (Grundmann, M., Pointl, E., 2008). To make it more secure, this database is protected among different authentication mechanisms like biometrics or token based. User should trust the SP to get in the system. There is a communication of trust between the user and the SP's which called ASP (Authentication Service Provider) (Hussein, S. H., 2010).

Complex SSO is divided in to Centralized SSO and Federated SSO systems. In this complex environment it is possible to have more than one domain or company. Centralized SSO has a centralized database and a centralized third party of trust communication in one domain. In centralized systems, user has the same identity for all different systems. More than one domain in one environment is called Federated SSO (Grundmann, M., Pointl, E., 2008). And in federated systems user has the own identity which is trusted by other systems. Token based SSO is one way to authenticate user in the centralized environment. This system is using cryptographic methods to authenticate users (Grundmann, M., Pointl, E., 2008). User authentication is achieved by using symmetric cryptography between the ASP and the SP. SP validates the identity by using secret keys which is passing through the ASP (Grundmann, M., Pointl, E., 2008). PKI based SSO is done with asymmetric cryptography between the user and

the SP by generating a public key through CA. SP is able to verify the user by obtaining that generated public key.

Federated SSO is built for the users who started using services provided by different domains or companies (Linden, M. and Vilpola, I., 2005). This becomes a necessary to have different federations between the domains for securely exchanging information. First of all each SP in different domains should trust each other and know their own hosting IdP's. As it described in Federated Identity Management chapter, Microsoft Passport, the Liberty Alliance and WS-Federation protocols are used together with the security standards like SAML, Shibboleth and Kerberos to provide secure and friendly environment by sharing the user identities during the data transmissions between different domains, services and applications.

Microsoft Passport is offered by Microsoft for web-based SSO services. This solution is mostly integrated with Microsoft products like Windows XP (Mahrt, R., 2003). The functionality of this protocol arises from having the same logic with Kerberos (Pashalidis, A. and Mitchell, C.J., 2003). User communicates with ASP via web browser to request an application. ASP finds if the user is already has been registered a cookie in the browser cookie cache. In this case if user cookie is found in the cache then there is no need to authenticate one more time. However if there is no user cookie found then ASP request the user to authenticate. That cookie is a ticket to get an access inside the service. Only disadvantage of a stolen ticket from a browser cache will work as fine before. In Kerberos there is an authenticator which protects against attacks by generating a session key with encrypted data structure inside (Pashalidis, A. and Mitchell, C.J., 2003). This generated session key is only encrypted and decrypted between the user and ASP. And the communication between the user browser and passport server is secured with the SSL tunnels. Cached cookies reserve users PUID (Password User ID) and other personal information to remember the identification for another request. This request could be done with a mobile device entering the mobile number and a pin. SP's are communicating with users through ASP by registering themselves. User is using one factor authentication for different SP's that means users get the same credentials for every SP. After user identified successfully, browser is connected with the required SP and logs in the user.

The Liberty Alliance standard offers a solution securely transferring the user identity over internet. Many users are in interaction with websites for business shopping or surfing (Mahrt, R., 2003). Many websites are offering this solution to give privacy and security for users to keep their personal information. Liberty Alliance is based on SAML platform for authentication and authorization communication (Pashalidis, A. and Mitchell, C.J., 2003). Users are communicating with IdP's on a specific request. IdP's give trust to the users by specifying the personal information is shared only with trusted SP's. Providers are using X.509 certificates and are establishing public keys for user credentials to have a trust relationship (Mahrt, R., 2003). Web transactions via HTTP requests are utilized with SSL. Access is gained between the IdP and the SP by passing through the user profile for each request and response. Another scenario for gaining access is IdP's and SP's are communicating directly with using web services like SAML and SAOP (Mahrt, R., 2003). Each user has a unique credential for each SP in the system. This is not like in Microsoft Passport.

WS-Federation allows communication in between different standards like Kerberos, X.509 and SAML. It specialize the management trust of trust relationships according to the WS-Policy and WS-Trust (O'Neill, M., et al., 2003). Authentication is done by using SOAP messages between the user and web service. It is using security specifications like public and private keys. Also SSL is used asymmetric encryption to authenticate point to point and used for the confidentiality of web services communications. The difference between using WS-Security and SAML is that SAML is used to determine the security arguments with using

XML format and WS-Security shows the use of SOAP for containing the security information (O'Neill, M., et al., 2003). Authentication is achieved by using those protocols and standards between the IdP's and the SP's. Federated SSO is integrated to use multiple authentication techniques to achieve strong security between the services and users. This might improve the user trust and productivity in order to achieve the best solution for the SSO.

Implementation of SSO is built on an easy way of communication with the services in the system. And it purposes SSO to have a secure communication, transmission and reliability of the user privacy from the SSO itself to the other applications or users As it mentioned before, user is authenticated only once for the permitted services. The access control allows users to perform their activities. Several servers might keep track on the user identities and authorizations for the accesses. Together with them several protocols like Kerberos, PKI, SAML, Shibboleth and SESAME (Secure European System for Applications in a Multivendor Environment) are helping to complete the communication. SESAME enables SSO functionality which protects the authentication information and giving access to the system (Causton, R. P., 2002). SESAME is using both Kerberos and PKI. It is actually created similar to Kerberos but improved to use PKI structure to protect and distribute secret keys (Sandhu, S.S., 2004). Another protocol for the same purpose is RADIUS. That is used between connectionless client and server protocol. This provides users to get access through the VPN tunnels (Alphonso, M. and Lane, M., 2010). To increase the security of the environment, SSO system should be able to easily identify users. For this matter different identity verification methods and concepts are used. As it mentioned in the previous chapters, they are dynamic passwords, biometrics, token based as smart cards, certificates, OTP, public and private key encryption, etc. In several SSO researches, user information and the profile for the data access control is stored centrally inside the SSO mechanism for better security and management (Sandhu, S.S., 2004). Activities are under control by the log management service by adding timestamps for each important activity. Firewalls, VPN's, SSL and IPSec (Internet Protocol Security) are components to achieve the secure transmission and communication between the servers and databases. The communication is not only in one domain. It might be in several domains like different organizations and environments working together. As known in federated identity management there are different federated methods are used to recognize the different domains to create secure communications. SSO system recognizes different clients and servers running on several subsystems, applications, OS, hardware and software which users are signing in (Sandhu, S.S., 2004). Also recognizes the time-outs and give re-authentication for the online users.

Another characteristic feature of SSO is that handles certificate and license based accesses. Certificate based access in SSO is mentioned in the certificate subchapter. About license based access is used to understand how possible is to handle the specific applications in the system. According to this definition it ends up with license based issue to run the system. License based access is a supporter for the system that is giving SSO rights to run the applications. It does not contain any certificates. There is only a license connection between the application and the database or the main application itself. Moreover, to implement the SSO in the local networks come across with critical functionalities in order to run the SSO-service properly. One of the critical functionality about the SSO-service is to have secure access to all applications in the system. According to that, if the system has different sub-systems then it needs to be separated by the different security levels. All those levels are connected to SSO system. Although all security levels in the system might indicate better SSO solution in the end. In the second chapter security layers are mentioned such as unclassed, open classed, restricted, confidential, secret and top-secret. Any information that is under protection is also protecting information that is classed as the highest. The mechanisms of high priorities carrying the important information such as login mechanism, user

information...etc. are needed to be under the same level of protection. For instance, security levels are categorized as1, 2 or 3 from the lowest to highest. So the important information is protected under the security level 3. As an example, active cards could be used to track id for one username and the password to be able to login the system. This shows one security level supporting the security definitions or requirements for the sub-system. Together with this, two-factor security mechanisms are in use to make the system more reliable and secure.

After all those explanations about different SSO architectures, standards, protocols, Federated methods and communication tools, here come to build up all those information to have a good implementation strategy for the SSO. Strategically SSO terminology is divided and showed in two blocks in Figure 3.8.

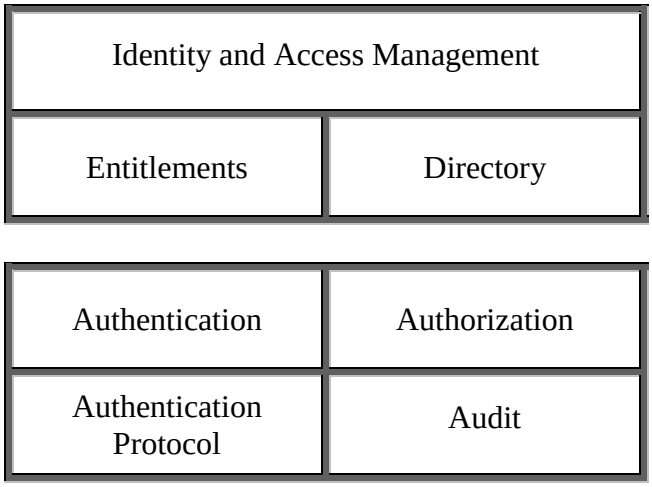

Figure 3.8 SSO Implementation strategies

The first block is related with all users in the network. This is the basic system in the network and they are based on the user profile. Entitlements are determinate user activities about what they can or cannot do. Directory helps SSO to register and store the user identities. The second block is the core system of the network. All are independent and need higher level of security. And this block is in a repeat cycle to check or identify the user rights to enter the system or one system to another. That happens in the future when user entitlements are changed or need to have an entry to the other systems. The change is all depending on the user profile and the level of the system. Only that user profile is used and gave rights to the next system. The system authentication is done to prove the user and the authorization is done to verify if that user is authenticated or not according to the user profile. After being authenticated, user is passing through the protocols and standards to work under safe and secure conditions. Different protocols are used for the authentication in higher system levels. That is depending on how high level is intended to be accessible. And then the same cycle is processing for the authentication and authorization. Auditing is controlling and documenting user's activities in case of attacking and faults.

3.5 Combination of multi-factor authentication

Authentication methods such as passwords, OTP's, biometrics, smart cards, and digital certificates are mentioned before together with the SSO. Additionally, **multi-factor authentication is as important as SSO to build and adapt in to a system.** Today's trends on authentication mechanisms are challenging questions and answers, image or patterns, seals, OpenID, Kerberos and out of bound authentication. Some examples are given in the following paragraphs about those authentication mechanisms. Using at least two of those

authentication methods creates a multi factorial authentication for better security and trust. That leads the system to have less vulnerability (Alphonso, M. and Lane, M., 2010). For instance banks are simple examples the way of showing the multifactor authentication. People are going to banks to take out money or doing other banking issues. In order to be successful, customers need to have a bank card (visa or maestro) and a pin number. This could be an example of using a smart card together with a password (OTP). Implementations of the authentication methods are different in each organization (Osterman Research White Paper, 2009). They are depending on some requirements. Those requirements are listed in Figure 3.9.

Organization Requirements	History Customer Culture
User Authorization	Applications Email Systems File Systems
Government Requirements	Industries or Geographies
Organization Individuals	External users Internal users

Figure 3.9 Authentication requirements

Organizations differ from each other depending on their history, customer requirements, culture and using the SSO system or not. User authentication is depending on the privacy or the organization policies (Osterman Research White Paper, 2009). If it is a private email account or widely social network then it allows users to get more access. But if it is under an organization boundary then it limits the access for the users. Different domains located in different countries or regions are separated in need of the work load or preferences. Moreover, external and internal users are not permitted to have access to the same domain or application. According to those requirements and based on different SSO architectures are used in different SSO solutions. First example is users who have different credentials to get access for more than one sub-system, stored in client-side credential storage or server-side credential storage (Pehrson, B., 2005). As an example Windows Server 2003 and Windows XP are given for client-side storage (De Clercq, J., 2003). Those known operating systems are used to make client-side storage more secure. Second is for the server-side storage. Tivoli Secure Way and ETrust SSO are given as an example. Those examples are for SSO to store credentials to a central data repository for authentication. Server-side storage is using a central repository like LDAP different then the client-side storage (Pehrson, B., 2005). LDAP locates at the server-side. Only access is available to server-side is to have successful access to the LDAP directory. And it is more secure because user credentials are not available on client-side all the time. They are deleting after user terminates the access (De Clercq, J. and Grillenmeier, G. 2007). According to a server failure, there is a copy of credential storage as a backup system for security. With the difference of the client-side, server-side is reachable from the portable devices. There are internal and external users connecting to server-side storage by using portable devices. Third example is for the centralized SSO solution. PKI based and token based SSO are given as an example. As it known, PKI is using public key which is included into a unique digital certificate. That certificate is signed by a private key. Those kinds of certificates are unique for every user. Entrust GetAccess is given as an example for PKI based solution (Pehrson, B., 2005). According to Entrust definition (2012)

"Entrust GetAccess is a high performance, scalable Web access control solution." It is used in centralized SSO for managing authentication through single domain for multiple applications. Additionally, smart cards and USB tokens are used to protect the private keys. Entrust GetAccess has an interoperability with SAML standard together with Liberty Alliance for integrating with other 3rd party organizations for business needs. And all together provides authorization and authentication verification through multiple domains as a federated identity (Entrust, 2012). Token based solution is using Kerberos authentication protocol and Microsoft Passport for federated identity management. Each user is getting a temporary token for requesting to get an access (Pehrson, B., 2005). Web SSO came up after many users started to have several usernames and different passwords (Sun, S., Boshmaf, Y., Hawkey, K. and Beznosov, K., 2010). That caused to get access by typing redundant credentials several times a day. And that expose unproductive user work and luck of motivation. Additionally on web based SSO, Microsoft Passport, Liberty Alliance and WS-Federation standards are given before as an example. They are using valid authentication tickets, SSL for secure transportation between the client and the server, shared secret keys and cookies for keeping track of user activities. Cookies are used to identify user authentication state. And those cookies are passing from one web resource to another. Additional to federated identity standards, SAML is used as a federated protocol like others (Lodha, A. and Sarma, R., 2006). SAML is used to exchange authentication and authorization data between different networks and in one single network (Ping Identity, 2002). In SAML, IdP is responsible to identify users from their usernames and passwords. And also different authentication mechanisms like smart cards and biometrics are included for multifactor authentication. In version of SAML 2.0 contains Liberty Alliance identity federation and Shibboleth (Ping Identity, 2002). Because of this combination SAML become a federated identity protocol. At the same time there are OpenID and InfoCard are used as a web based solutions. However interoperability is required between those solutions and SAML. But those two solutions could not provide enough reliable SP's to the environment. There are many user accounts which are relying on the same SP. But a few of them are reliable third party as we called ASP (Sun, S., Boshmaf, Y., Hawkey, K. and Beznosov, K., 2010). OpenID is a user protocol which identifies the user with a specific URL (Recordon, D. and Fitzpatrick, B., 2007). That URL is for users to rely on a third party ASP to login. User requests to get access with the URL, and IdP conducts the user to enter the password. After verifying the identity, IdP redirects the user to the ASP. Communication is done by HTTP request and response between user and the browser. In OpenID protocol third party is directing the user to the IdP. Typically it is the same with federated identity solutions like WS-Federation and Shibboleth. The difference is that IdP is directing the user to the third party to authenticate (Bellamy-McIntyre, J., Luterroth, C. and Weber, G., 2011). Another difference is that OpenID is directing users via URL but for the Shibbolth and WS-Federation is not directing with OpenID URL. InfoCard is also a user protocol. User selects a card instead of using a username and a password to authenticate (Sun, S., Boshmaf, Y., Hawkey, K. and Beznosov, K., 2010). After the selection, IdP indicates how user can prove the identity. According to the poof, user allowed to get an access by the ASP. Alternative to authentication protocols, authorization protocol OAuth is also used to authenticate but requires different set of steps (Bellamy-McIntyre, J., Luterroth, C. and Weber, G., 2011). It provides to send the private information from one website to another but without showing user login credentials. This authorization protocol is similar with the OpenID protocol technically. This means that OAuth is using as an addition for federated identities and OpenID (Bellamy-McIntyre, J., Luterroth, C. and Weber, G., 2011).

Many techniques, technologies are used with a combination of trust. InfoCard, OpenID, smart cards, biometrics and so on more techniques are used together with a username and a password. That makes the user trust more but it might be a cost effective. One user example

shows that Facebook, a popular wide social network, is offering to people to use Facebook as an identity provider since November 2010 (Constine, S., 2010). If people link in to Facebook then they will get SSO for their solutions. As it known, it allows users to enter their email addresses and passwords once to login. All other Facebook integrated applications then are ready to use without entering any user credentials. It is possible to reach that social network from the mobile applications and internet browsers by login in only once. The application or the internet browser passes the authorization token or the cookie to the other ASP applications which are used inside the social network site. Benefit of using SSO on Facebook is that user's information is kept secretly until they authorize their information to be known. Facebook SSO is allowing the owners to keep track of their integrated application activity which is used by other users (Hijleh, A., 2012). An example to integrated applications is Spotify which is a music platform that allows users to listen music on Facebook. Other examples are games that users can play online, personal websites or mobile applications (Hijleh, A., 2012). The convenience part about it, users are connecting once on Facebook and start using those integrated applications without log in several times.

Another example is from the Linnaeus University in Sweden. Since July 2012 they have been started using Shibboleth as web based and for other network authentication systems. Nowadays Shibboleth is using for Eduroam (Educational Roaming), Ladok and adobe connect in the university. Eduroam is a wireless networking system for students, researchers, teachers and other university stuff to use. In this networking system there are IdMs (Identity Management System) where all the contact information is stored, a RADIUS server which is connected with all IdM's and a wireless LAN (Local Area Network) to connect with the internet (eduroam, 2012). It works with EAP (Extensible Authentication Protocol) for different authentication methods which are username and a password or public X.509 certificates. Ladok is a student profile keeps track of students and courses. Adobe connect is for sharing lecture meetings and lecture slides either live or later from the internet. Students and the university stuff do not need to enter credentials several times to reach their profiles. Moreover, Shibboleth is used as an open standard according to the university boundaries. This allows users to have individual access for the protected university information within authorization manners. This Shibboleth project might extend as a future project by combining windows based SSO with using Kerberos standard. Shibboleth standard can perceive if a user logged into windows by using Kerberos standard. Then Shibboleth can log user automatically in the Internet.

4 Developing and evaluating concepts for SSO by using selected standards

Evaluation of security levels is scrutinised together with the information classification and authentication mechanisms. Also a marketing research conducted for the 2010 and 2011 concerning the different companies providing SSO solutions has been discussed. Finally a brief explanation of MoDAF (Ministry of Defence Architecture Framework) is explained to show how various demands from users are combined with different viewpoints.

4.1 Authentication strategies

Several examples are given for multi-factor authentication based on different SSO solutions. In this chapter, those examples are evaluated with positive and negative sides related to security concerns and users perspectives. Before the evaluation, possible ways of selecting the right authentication strategies are discussed briefly. Organizations need to decide the right strategy to secure the system according to their data types, hardware and software equipment, and customer needs. It is possible that authentication strategies might be changing depending on the specific needs. Certain strategy is also changing by incorporating more services, devices, users and customers in to the system. Selected authentication strategy should adopt itself to the system based on the changes. For the future steps, the solution for the successful adaptation is to use standard based and scalable authentication protocols to make sure the system is in cooperation (Sawyer, J., 2010). For internal user only username and a password might be enough but for external users is not. They need to prove their identities by applying high level authentication mechanisms. In previous chapter, alternative choices about dealing with the risks are explained. According to those choices, company need to decide which option is better for dealing with risks and which part of the system it is going to be used. Those alternative solutions are accepting, diminishing and transferring the risk. Deciding the level of the risk and authentication mechanism to prove the user identity helps the company to evaluate the security of the system, needs, and the future steps. Here are the information protection levels just to remind; unclassified, open classed, restricted, confidential, secret and top-secret. Different authentication examples are evaluated based on those risk levels. In chapter 5 those evaluations are combined with different risks and explained different alternative risk solutions. Figure 4.1 shows the evaluations of security levels.

Level of Security	Information	Authentication	Security Evaluation
Open Classed	Published online and available to reach	No identity verification is required	Simple pin number Knowledge based authentication Image and message replay
Unclassified	Uncertain information Not published Decided ones are published in work environment	No identity verification is required	Simple pin number Knowledge based authentication Image and message replay
Restricted	Available for permitted users No open access to Internet	One-factor authentication	Usernames and Passwords Biometrics Geo Location
Confidential	Available for permitted users No open access to Internet	Multi-factor authentication Cannot class back as a lower level	Username and password Smart card Hardware Device
Secret	Forbidden to share online Private information	Requires one-to-one personal identity verification Cannot class back to a lower level	OTP Tokens OTP List Digital certificates Out of band Biometric
Top Secret	Forbidden to share online Private information	Requires one-to-one personal identity verification	OTP Tokens OTP List Digital certificates

Figure 4.1 Evaluations of security levels

For unclassified information it is right to say no identity verification is required for confidentiality reasons but for traceability and integrity of the information identity verification is needed. According to traceability, the ability to verify the information or to see if a user logged in as his or her profile and also to see the log statistics on when that information found, open or used, is required some kind of authentication of the identity or the role who is accessing the information. Availability of information is also another issue. To have high availability some kind of feature like information back up needed according to information security reasons. This would assure that no one can actually delete or change the information. Together with that logs are provided to show the status of the information. Another possibility to keep the information is in layers like roles or positions. Then each user has unique but the same functionality to treat all the information. That is eliminating the risk of doing wrong things with class of documents, because there is only one possible way to treat for each user. Therefore, for unclassified information has no classification and not protected by a specific sub-system. But that class of information should be treated to be on the higher level of security. So the lowest level is almost the open classed information. It is okay to send and reach unclassified information but it needs to have a control of the limitations for each user. Information classified restricted has also limitations but it's available for permitted users. The information can be changeable from the permitted users. Restricted information needs higher

traceability and for its availability is also limited amount of users. Actually availability of all the information in the system is important but it changes regarding to the importance of the information. If a user has no correct smart card or token to reach the sub-system then the information is not available for that user. Users, who have the permission to get access for the restricted classed documents, have higher availability standard than the open classed documents. Higher security documents are classed as confidential according to the rules. For the secret information it is possible to have it in the internet as long as the files are encrypted and transferred through safe tunnelling. Mostly secret information is decided not to be shared because this class is defined due to what harm can that secret classed information might do to the organization. Top secret classed information might have a great impact on the organization when it is shared.

According to Figure 4.1, online banking for example, Tivoli SecureWay and ETrust SSO examples are classed as confidential. They require multi-factor authentication according to the interoperability with different standards. Client-side storage Windows Server 2003 and XP examples are classes as restricted. Only one username and password is needed to access for the windows based SSO. Secret and top secret information are protected either in centralized SSO or federated. It depends on where the information is located. Using only passwords for the authentication is least expensive but also least effective on security. Regarding on this, passwords are not used for the high restricted levels. Positions require more security for instance banking issues is good to use password or a pin number together with other multiple authentication solutions. This provides confidence (Sawyer, J., 2010). For that solution there might be a risk that an attacker might connect internally to the computers and has a chance to use hardware tokens or digital certificates which are used for the multiple authentications. Digital certificates and PKI are difficult to manage and administrate (Cobb, M., 2011). Those authentication mechanisms including biometrics are used with hardware tokens like smart cards and USB (Universal Serial Bus). Smart cards need a card reader on the devices but for the USB it does not require. Login sessions which accessed with the hardware tokens are terminated as soon as the user removes that token from the device. Out of band authentication requires a mobile phone and a cost for a message (Cobb, M., 2011).

4.4 SSO market research

In SSO business many organization needs are almost focusing to the same area: Reducing complexity, improving customer convenience, managing the growth of user ID's, reducing the costs and giving a secure enterprise. According to a market research, during late 2009 Microsoft sold SSO solutions to Sentillion Company which serves to the healthcare industry (Kreizman, G., 2010). In the market research it expected more sales from Microsoft to Sentillion (Kreizman, G., 2011). But according to another research; Microsoft had limited SSO product sales. Instead of Sentillion and Microsoft integration, other companies like Oracle & Passlogix, NetIQ & Novell and i-Sprint innovations occurred on the 2011 market. Product improvements for SSO solutions have continued from 2010 to 2011 (Kreizman, G., 2011). SSO solution improvements are fulfilled from other known companies like Imprivata, IBM and Evidian. In more technical way, each developed solution or product is adoptable together with the other applications which are supporting Java, Flash, mainframe terminal interfaces and Unix/Linux interfaces before the implementation of SSO. Different technical risks from architectural perspective are explained in this chapter.

Figure 4.2 2010 Market research

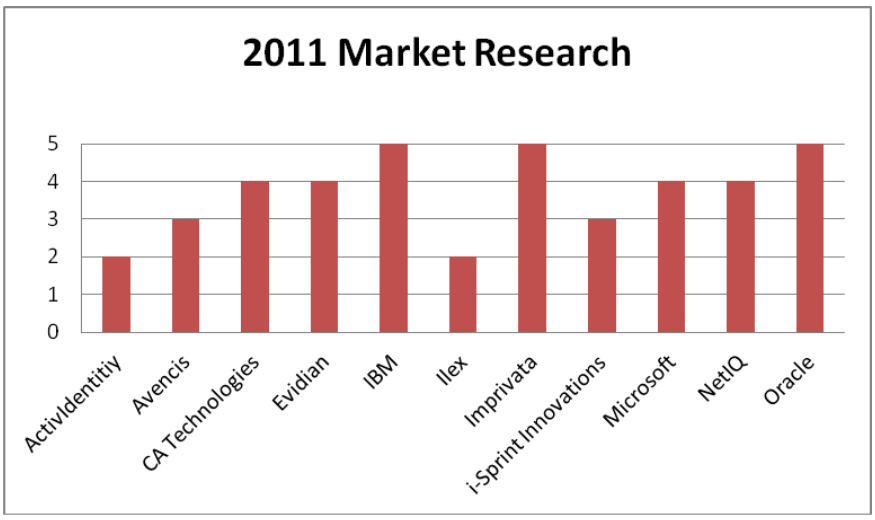

Figure 4.3 2011 Market research

Figure 4.2 and Figure 4.3 show the different market vendors who produced SSO solutions. This two figure shows which companies are in or out from the market (Kreizman, G., 2010 and Kreizman, G., 2011). ActivIdentity decreased in the market ratings, Avencis and CA Technologies increased one step up in the market. Evidian, IBM, Imprivata and i-Sprint Companies are remaining in the market. Additionally, Oracle, NetIQ, Ilex and Microsoft are taking their place in the 2011 SSO market. IBM and Oracle Companies are given as an example in this paper due to their growth and the placement in the market. An internet based research conducted in 2011 market on different companies was done and explained.

ActivIdentity is serving solutions to government, commerce customers and online banking mostly based on strong authentication and smart card solutions (ActiveIdentity, 2012). According to the company's researches, ActiveIdentity offers SSO for strong authentication platforms to provide cost effective, flexible and scalable solutions. It decreases help desk costs and provides easy password management. The solution that they provide is used in centralized SSO. Smart card feature that they support is for deploying and maintaining PKI. It gives opportunity to deploy different combination of authentication devices, smart cards, card

readers, OTP, USB tokens, software and hardware tokens. Moreover, it provides secure identity verification both internally and externally among different organizations.

Imprivata is well known in healthcare environment on clinical, financial and administrative applications by saving time, improving satisfaction and handling medical records. And like in other companies, it is also combining SSO with strong authentication mechanisms. It provides fast availability for the applications and information. It disables multiple logins to sub-systems after one user login to the current system. It gives device based solutions with smart cards, active and passive cards, finger biometrics, OTP and USB tokens. Users are accessing through VPN tunnels or even offline. Access is managed like in centralized SSO by using active directory (Imprivata, 2012).

Avencis created a SSO solution to prevent from complexity of managing users, leak of sensitive data and to decrease workload of technical support. It decreases the workload of password reset and combines smart cards, USB tokens and biometric authentication with passwords to have strong authentication. It provides easy management of users accounts by decreasing the risk of errors and gives a document of activities by tracking user's behaviours and activity times. It is creating solutions for finance, healthcare and manufacturing sectors (Avencis, 2012).

Evidian is using username and password for windows, java and web based environments. It provides mobile SSO to access all web applications. It offers smart cards or biometrics for protecting access to PCs, login with OTP for external access to servers, ID and password to login on standard sub-systems. All those combinations are given for easy access and easy changing password opportunities. It is having a SAML support for accessing to web applications. It works with large organizations, finance, government, telecommunication sectors and manufacturing. Also Evidian enterprise modifies and updates SSO on any type of application in the system. Identity management on this solution is based on LDAP or active directory. For the trust security data is encrypted for all communications. It prepares activity reports of events, administrators regarding to any risk and vulnerability (Evidian, 2012).

Isprint provides SSO solution for strong authentication, good access control and identity management. It produces solutions for global financial services. It indicates that the solution is extendible to integrate with new customers for their current environments. It allows mobile communication access via VPN using multiple authentication mechanisms. Its UAS (Universal Authentication Server) solution provides flexible, secure and efficient access via VPN. It offers SMS (Short Message Service) or SMTP (Simple Mail Transfer Protocol) for delivering OTP. It gives strong encryption during the communication between the user and the host. For internet banking issues, it gives end-to-end password protection to keep data secure. Companies future authentication mechanism is to integrate new authentication methods easily in to PAM (Pluggable Authentication Module) framework to address authentication requirements of the organization (Isprint, 2012).

CA Technologies provides a scalable access management solution that includes SSO for identity management, auditing and administration for web and cloud applications. It supports federated identity to give access for users between different domains. Web SSO in CA Technologies is a centralized solution. It is SAML standard based federation between wide ranges of partner websites. CA Technologies aim is to combine identity federation solution of SSO with the cloud based services. Deployment of those two services is minimizing the management of the system, software of facilities. That leads to a strong business and good experience between end users (CA Technologies, 2012).

NetIQ solution automatically logs in and out the user from the active session in regarding of a card removal or any attempt to get an access. This feature is useful when there are multiple users connecting through the same system or from the same device. Also it makes sure that the previous system is already logged out and ready to use by another user. Typically

like other solutions, NetIQ offers self-service password administration without any expenses and time consuming (NetIQ, 2012).

Ilex is a company which produce for both web SSO, centralized SSO and federated identity. Although Ilex's Sign&go solution for SSO is a new generation which stated as a first Global SSO product for the market. This solution is flexible and adaptable for various architectures. It works with all applications and thin-client environments. Communication and identity verification coming from a third party is put in use of SAML transmitted by Liberty Alliance enterprise. It offers user productivity, reduced costs and increased security. Company provides a comprehensive identity and access management platform including SSO solution (Ilex, 2012).

Microsoft is world distributed company which produce products and services about computing. IdP is based on open standards like WS-Federation and WS-Trust. Microsoft implements these open standards in windows identity foundation. Centralized SSO uses active directory and host systems to map user accounts and activities. This mapping is stored in centralized database using Microsoft SQL server. Inside network communication is integrated with UNIX workstations using active directory. Integration for SAP R/3 is for keeping the activities, information and resources by using Kerberos version five authentication protocol. Communication with cross domains is provided for business-to-consumer and business-to-employee web accesses. Business-to-employee web access and SSO are using X.509 certificates. Business-to-consumer web access and SSO are using Microsoft Passport (Microsoft, 2006).

Oracle has Open Fusion Middleware family products and offers access management, directory services, identity management and security tools for better security, reduced costs, compatibility and deployment (Oracle, 2012a). It provides Oracle OpenSSO solution to handle web access management, federated SSO and web services security for applications. Also offers a control of trusted third party identity sharing between other partner networks (Oracle, 2012b). Oracle Enterprise Single Sign-On Suite Plus solution is to centralized access control for identity verification internally and externally. This solution offers user to communicate and be success in business faster and inexpensively. Although gives improved security, identity control and cost saving. Supporting different type of identities to provide strong network authentication is for improving the security and flexibility. Oracle and Passlogix become successful partners since three years. This constitution aims to adapt new architectures, cloud deployment and newer browsers (Oracle, 2012c).

IBM offers a product named IBM Tivoli Access Manager for centralized SSO together with IBM security services. This helps users for manage password security, user productivity and reduce help desk costs (IBM, 2008). IBM Security Access Manager provides SSO for applications, Citrix servers, web portals and shared kiosks. Security Access Manager V8.2 product offers strong authentication mechanisms like smart cards, biometrics, OTP tokens. And this product contains IBM Tivoli Access Manager to provide an integrated identity and access management solution. Since April 2012, IBM has been supporting Epic Software applications which are for large medical groups, hospitals and healthcare organizations (Epic Software, 2012). This integration offers for the doctors and patients receiving information faster and increasing productivity through SSO. Also IBM provides centralized auditing and documentation for those organizations (IBM, 2008). Another Support from IBM is to educational institutions which are using web portals to get connected with students, courses and meetings. Web portal applications are java based and the service uses Microsoft Active Directory server LDAP compatible. LDAP supports different authentication mechanisms which are Kerberos, SecurID, secure remote password and X.509 for building a configuration between client and the server (Dunne, C., 2003). IBM enables SSO for SiteMinder for having

user authentication by managing web accesses. All web applications on the environment are running on IBM Lotus Domino server. This enables SSO for user authentication.

4.3 MoDAF Framework

Eventually there are many companies offering different SSO solutions for people who have various requirements. Different requirements are listed in this thesis previously. MoDAF architectural framework is used to assemble the requirements in a platform. **MoDAF combines different needs from the users and then map them together with the system requirements.** It provides a means to model, understand, analyse and specify Capabilities, Processes, Systems and Systems of Systems (SoS) to assist in the improvement of military and cost effectiveness across the MoD (MoD Architecture Framework, 2005). MoDAF has various set of rules and patterns which are known as views. Each view is used to represent for different stakeholder interests. This model framework is used for the enterprise architectures that need to specify and control the tasks to create new views. In addition to considering different standards of MoDAF views that has provided. Also it is used to store and manipulate the data elements. By using those views, a graphical and textual visualisation could be able to provide for the business area being investigated.

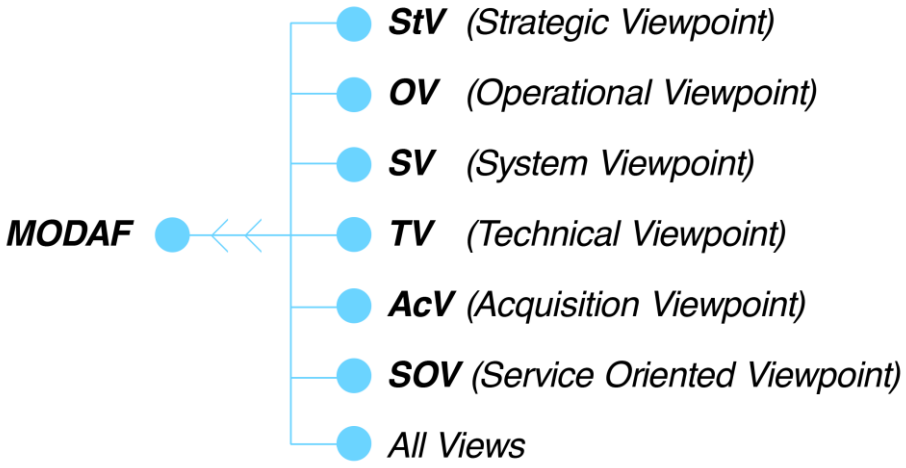

Figure 4.4 MoDAF Viewpoints

As shown in Figure 4.4, MoDAF has seven viewpoints. Each viewpoint represents different modelling views, giving diverse perspectives, to provide clarity of the complex MoD activities. Each user selects one most effective one to specify the business area being investigated. If it can be applied correctly to the infrastructure, then MoDAF will be a successful delivery of NEC (Network Enabled Capability).

Viewpoints that are used to build, analyse and visualize, they work actually together and are related to each other. To start creating a model view by using those viewpoints it is important to describe the relations about the work roles, interaction between the system and the technical viewpoint. This is a good side to use the operational viewpoint. It is easy to see how the system itself has an impact on the work or how the work has an impact on the system. So from the system viewpoint it would always be connected to the operational viewpoint. If we are talking about a subsystem or combined resources we could see from the operational point of view that this subsystem is related to a technical viewpoint. Combination of technical views would build up to system products that build the system. During the progress this system is put into use through the operational viewpoint. For instance, building a SSO application on this system would be a part of technical viewpoint. All mechanisms and

protocols are located in this view. They together are used to build up the SSO from a technical point of view. After constructing SSO, from operational viewpoint it is important to decide, "How this would be used in the system?" or "Where in the system it has to be used?" It is important to stick with one or two level of viewpoint (Ruuda Consulting AB). Which means you could only focus on building up one system with different subsystems or resources. That is good from the system point of view for the security meaning that the decision is made for separating different information resources to make sure that they are not having a conflict or an influence on each other if a fault or an error occurs in the system. Therefore from the operational point of view the system has trustworthy environment to work and make the information more reliable. So MoDAF more or less is a way of showing the relations between the standards that actually provides together with the SSO solution to a user in an architectural framework. The viewpoints are for guiding the user to look at from different aspects when they want to develop a system or to choose a solution. This is combined and given as a conclusion in the result chapter.

5 Risk and threat analysis based on requirements

The components, upon which this study is based, are discussed in terms of risks that can be encountered in security systems. The vulnerability of the network systems imposed by different threats is explained by considering various types of risk scenarios. It is also discussed how grading the possibilities and consequences for possible threats motivates the risk analysis. The use of ISO 27003:2010 Standards is used to treat and analyse the risk scenarios.

5.1 Threats and possibilities caused by SSO

Risk management in continuity of the organization planning is quite important for the future steps. If there is no risk analysis or no treatment for the risks, there won't be a future plan because risks actually fall out in to real actions. **There are many factors that SSO solution offers to discuss about threats and possibilities.** It can be an area of threats of humans, communicational or physical because SSO is implemented in all those environments. Both in data layer, physical layer and machines need a backup to reach SSO. From the architectural point of view one technical risk with SSO is pointing out the system availability. For instance if one service or one certificate holder in a system is not reachable then that is a risk from an architectural perspective. If the PKI server in the network is not reachable or is not redundant then it is one of the weakest parts of the system for the availability. If the stable system is desired in the network all the time running then each part of the key service holder need to be redundant. For example, SSO system solution is needed to have access to all sub-systems, access to different servers or authentication systems in the network. If one part of the system is redundant and the other one is not on the third parties then from the architectural perspective SSO will try to look as symmetrical as possible to make sure that the network has the same level of stability or availability for the solution (Ruuda Consulting AB). Another technical risk is that if SSO solution for Kerberos standard needs to have Windows environment to operate but another environment needs Linux/Unix to live then it is quite hard to have those two environments coexist on the same server. They probably are in need of having two different servers for those two solutions. So from the architectural perspective it is possible to say that there are two possible SSO solutions that divided in to two functions in the network. The organization might end up with one SSO solution for the user but from the architectural point of view there could be more possible different SSO solutions. So as a result if different sub-systems are not cooperating or unreachable that can affect the SSO solution, it will have a null function or time out. That is decreasing the availability. There are more technical threats which make break downs on the systems and other threats may come from user responsibilities. It depends on the password usage, unattended user equipment and unauthorized user access to web servers and services. Some of the users are using the same passwords on many computers, at home or at work. This might have an impact on the SSO solution. If one user has an access all systems in the network and internet with the same password then that's a threat for the whole system. According to that threat, it is easy for someone to get that password and try that on all user ID's on the system. Company can give unique passwords to users, but that is not a solution. Probably users cannot remember and write them to a paper so that will cause a threat. Highest security layers are not only protected by username and password. Because of that the attacker needs higher security authentications to reach important resources. Some users are storing passwords for different applications in a file, unsecured cookies in to their personal computers. If that whole file got corrupted then the attacker will get all possible passwords to have access for different applications. Another threat is hacking passwords and phishing. Phishing attacks are normally directing users in false websites or emails by asking to enter their credentials. So by means of that attackers can

get the user credentials to get in to the network (Collan, J., 2009). About the effects of a risk if it happens is explained in charts covering the probability and the consequences. The consequence, the level of catastrophe would turn the business out of business or it would leave it with just a small disturbance. Probability indicates whether it is happening all the time or almost never happening. Outcome of risks are listed from least affected to high affected for the company. A risk that happens with low consequences and low frequency would be okay for the system. A risk that starts to happen a lot but still with low frequency, that will start disturbing the system and loss of time. A risk that never happens but has high consequences would cause catastrophe for the company. And a risk that is happening a lot with high consequences will be a catastrophe also for the company.

The layout which is taken as a base for this work contains hardware, software, information and communication links protocols, bridges, firewalls, certificates, access controls and servers. To keep a high integrity is important for all those components. Any small brake or weakness may cost for the organization. Those weaknesses are appearing with corruption, leakage and unavailability which might be exposed by those components. Such kinds of vulnerabilities would cause threats and threats bring actions along the attacks. According to the network layout, there are users some are authorized within the network and some are authorized from outside the network. Many of the attacks are coming off either from inside or outside (Stallings, W. and Brown, L., 2012). Inside attacks are coming from authorized users who are not accessing for good intentions. Outside attacks are coming through external devices via internet. Security measures designed and explained in this work are for preventing any type of attack. There are three possible ways to recover attacks, accepting, diminishing and transferring. Here are some possible threats that might occur and some recovery options for the network. Threats on hardware devices, equipment that belong to the organization might be stolen or stopped functioning by malicious users. That disables the service functions (Stallings, W. and Brown, L., 2012). Besides that decreases the availability in the system. Another example is the communication between different buildings. Some users need more than one access to different buildings. That means all traffic should be available on the physical infrastructure. Unfortunately there is a risk of an excavator coming and digging out the cabling system in the ground. This risk has low frequency but might have high consequences. So this situation is solved by having wireless connections or links between the buildings. Additionally, natural disasters like fire, flood or a meteor might hit, happen even if the frequency is low or even on a negative side of the chart, the consequences are so high. That might refer to accept that risk and build reserve rooms with backups of databases and servers. The loss of hardware is lowering the confidentiality of information down. Another threat is for software utilities. That threat comes with viruses, Trojan horses, malware programs installed inside the software either via internet or direct installation. That malicious software is able to copy, delete and modify the programs, applications and important information. Additionally they cause loss of confidentiality, availability and integrity, respectively (Stallings, W. and Brown, L., 2012). Modified programs and applications behave differently than normal and might perform additional tasks which are not beneficial for the organization. Security detection programs might come under attack by modification or disablement. Then they are out of detecting viruses, unwanted programs and attacks. Information security is another concern to take into consideration. Deleted files, functionless databases are decreasing the availability of the system. Inside attacks which send information outside the network, unauthorized successful accesses, corrupted data by overcoming the access control would decrease the confidentiality. Malicious data or program which installed on personal devices or on applications is most likely to change the behaviour of current programs and files. This would cause a decrease in the integrity of the system. High security required information might transfer the risk for instance to the insurance companies before

happens if there is no other way to diminish or accept it. Many attacks are taking place by listening or monitoring the communication links. The risks is the destroyed or deleted messages and deactivated or unavailable communication links and protocols (Stallings, W. and Brown, L., 2012). All these decrease the availability. Especially after starting to use wireless LAN in the company, there might be an opportunity for the attacker to listen the traffic. Corrupted email traffic, captured login credentials or personal phones for data transfer through wireless LAN cause a great deal of loss in confidentiality. Modified, delayed or duplicated messages are affecting the integrity of the system. Listening traffic is hard to discover whether it is happening or not. The solution for that is to encrypt the messages before sending. This is diminishing the risk before actually being performed. Attacker may not be able to decrypt the message but might learn the hosts sending/receiving the message. That might cause an identity theft. Stolen ID and password can give damage to system and data integrity. Security is endangered if that stolen credentials are all same for the servers and applications. That is a chance for the attacker to get access into servers which are having the same authentication ID's. Another threat is almost the same for the external users but the difference arises in using different username and password combinations for each server or application (Bashir, K. and Asif, S., 2010). That is something hard to handle it and also not secure. That brings the possibility of phishing, Trojans and malware to give damage to the organization. To solve this problem, organization managers and other partners located in different cities should discuss which applications and servers should have the same credentials to authenticate. To login to a desktop or to a website, internally or externally, requires only a single username and password. There, user sees the commons applications, email and telephony servers. For another domain or server a higher authentication credentials is required to enter. Communication between the partner network located in another city and the main network will enable them to know how they are sharing the information among different domains. According to that, decryption algorithm is created and installed on the system. So it is known that between different domains information is decrypted with that created algorithm. Otherwise, if any information or data transferred is not possible to decrypt then that information is considered as indefinable and be blocked out from the domain (Bashir, K. and Asif, S., 2010). Another network connection loss is if CA servers goes down or break then all systems will be unable to run and not be reachable from the users through the SSO feature. Then nothing on that server would work because the certificates will not be accepted or available for the user purpose.

5.2 Threats and possibilities for the network layout

Layout of network handled in this study has 2 different domains. One domain is restricted and the other is open domain through internet. So the webpage related with the organization is accessible through a separated firewall then the restricted part. User can go through the internet, read and check resources. Unfortunately, using the resources require another access to the restricted domain. In the restricted domain there is different level of securities based on user profiles. Each private sub-system has different regulations to go through. That provides a higher level of security. Each sub-system has one firewall and another firewall for the open cloud which is the internet. If a user wants to take out a resource and publish it on open cloud, a firewall between the restricted domain and open domain should be passed. Information which is tagged as unclassified or restricted becomes an open document after publishing on servers. Logins for the SSO system through a firewall only fail if user has missing authentication requirement, if user is not exist or user is obstructed from the system. And each login attempt is monitored with the details of user ID, total time of logins, total time of failure logins and the user IP that shows performed access (Oracle, 2012d). In the network layout, there is another network which is separated from the restricted and open network. It is a

partner network which is located in the same country. This network belongs to the same organization and is managed on the same level with the main network. Third party for this network is ISP. It allows the traffic open on all common parts to enable to transfer different communications between the firewalls. ISP is assigning IP addresses to each accessed user. Those IP addresses are not unique because that might cause management issues for the devices on the internet. Each user has different certificates installed on the browser and different tokens because there are different services that are sending information throughout the network. Fixed IP structure is used for each user because it is easy to own and control. That IP structure range is only given to ones with the right certificate. Actually this IP structure is used for each of the private network like the IP/Sec for the secure transmission and communication between them. IP communication for the internal network between different domains enables the communication, encryption and data transfer. Even sometimes the given IP addresses are not that much important for the users who are outside the network. Therefore additional authentication mechanisms are used like certificates or tokens for login and browsing. Network has its own CA server, in order to create its own new personal certificates to be used internally for the organization. Level of system management is obtained for user security and system security by giving authentication by certificates to the user. To revoke or disable that given certificate is possible in one day. Even that certificate is valid for a year, after disabling it is not accessible any more. CRL is taking care of these certificate issues. It is not necessary to have CA server more than one in a network. To get a higher security for availability, several copies of CRL is placed in different parts of the network. Updating of certificates or keys is not scheduled on a specific time. Regarding on an important situation update might happen in any time. **Updates are based on user roles, read, write or both.** Because it is role based, the whole system is needed update to make sure that roles are the same, so nothing has been changed. User profiles and the rights in the system are role based but the accesses are individual. Let's imagine the level of the systems as layers. Each layer has different keys or certificates based on the level of security. After a while the use of certificates need to be managed and updated. Every layer has different certificates based on user roles. Some users might own all certificates on that layer or some user owns only one of them. According to separated roles, updates are done for the whole layer of the certificates at the same time, because the certificates are checked on a central place. But in distributed systems, one has to make sure the certificates are synced between different parts of the system. If a user gets a new certificate, the old ones have to be revoked in all other parts as soon as possible. Certificates on one layer have the same security level but have different roles. Another problem occurs when a user is not logged in some specific time to catch the updates for the owned certificates. Then the system might allow, for example a week time, for the user to go online and update. That update can wait in user profile. After that time scale, if the certificate is not updated it will be cancelled. An alternative option for the updating is that, a personal or manual service is put in use for self-update for the certificate when user goes online. This is a solution that might take effect in the system. Therefore the user availability is decreased when the user cannot self-update or reach the work information. The confidentiality is taken care of since the change of the certificates was made possible. So no one actually wanted in the system to be able to look at the updates. Solutions for the SSO offers to carry both the information and information level entering through a firewall and also offers to carry the rights of the certificates to different services. Authentication between the access control and the firewall uses a personal certificate to access for any system. That is either a software or hardware embedded certificate. Different protocols are used for various user accesses. For instance, the HTTP based web applications mentioned using OpenID implementation and SAML SSO standard or Shibboleth. After they authenticate the user, SSO provides a user token to the client-server. This authentication is enabled by RADIUS protocol between the

HTTP requests (Lin, et al., 2012). This is used to provide the security for exchanging information and prevents from the replay attacks. Access control, firewalls, certificates and other communication protocols are parts of the network for the SSO solution. Another part of the SSO solution is the client-server. It is the administration point. Where rules are created and overviewed (Ruuda Consulting AB).

5.3 Evaluation of threats by using ISO Standard 27003:2010

When it comes down to the system part, ISO Standard 27003:2010 has listed many threat areas. These are communicational and operational management, access control and the information itself. Those controls are needed in the network to full fill the SSO requirements. Controls are listed with the definition in Figure 5.1. It shows the required controls which are needed in a SSO system. Possible threats and controls to be considered are listed in rows and columns respectively in Figure 5.2. Those threats are handled by the controls as indicated with the symbol X. Five examples are given to explain the Figure 5.2. First example deals with the control 11.5.2, user identification and authentication, is used to identify users by their given unique identities and given authentication mechanisms. Threats such as unauthorized use, malicious user and collision between network users are applicable by this control. The control 11.6.1 dealing with information access restriction is given as a second example. This is used to control and put restrictions for the access to information and application systems according to the access control policy. Therefore, threats such as information leakage, corrupted servers and applications, altered information, unauthorized use, malicious user, Eavesdropping on confidential information and attacks on sensitive systems are applicable by this control. The third example is control 12.3.1 where policy on the use of cryptographic controls is tackled. This is the given policy on the use of cryptographic controls for protection of information. So threats information leakage, altered information, eavesdropping on confidential information, network traffic spoofing, weak browsers and HTTP request attacks are handled by this control. Fourth example is for 11.4.4, remote diagnostic and configuration port protection. In network systems there are different types of equipment like routers, firewalls and access points. If it is small infrastructure, it is easy to administrate and configure them. But if it is a large infrastructure then it is hard to go around and configure one by one. As a matter of fact, ports are used as virtual connections to communicate and for the administration. During the configuration one has to be aware of the possible threats against that because if an intruder could get in the router or the firewall, they change the configuration to be able to open up the network and trace it for hacking attacks. The solution here is to give a limited access according to the user profile. So that inessential access could be prevented. So threats like unauthorized use, network traffic spoofing, attacks on sensitive systems, operating system modification and stolen or hacked passwords are handled by this control. The fifth and the last example is 12.6.1, control of technical vulnerabilities. Typical example for this is operating systems. Every month or even more often operating systems are getting updates. Those updates are filled with new software to prevent the system from new threats that have been identified. So threats like operating system modification, virus attacks, and software and hardware failure are handled by this control. Additionally, natural disasters listed in Figure 5.2 are not handled with the controls that are selected for this work. For those natural threats, risk treatments are explained in Figure 5.4. Finally, to complete the risk and threat analysis, in Figure 5.5 and Figure 5.6 are showing the threat probabilities and consequences to calculate the risk levels, respectively.

When a threat has extreme consequence, in the matrix it is illustrated by multiplying with five to show its significance when compared with the other threats. Instead of this speciality, other threat calculations are done by multiplying the probability with the consequence. Figure 5.3 shows the matrix to calculate the risk level with the result of the multiplication of the

probability and the consequence. So Figure 5.4 shows the threats, risks according to those threats, probability and consequences, risk levels and the risk treatment based on the given threats. For instance, a threat of nuclear bombs has risk on loss of availability of information. Probability is 1 and the consequence is 5, because it is low probability for that threat to occur, but it has extreme consequence if it happens. The calculation for the risk level is 1 x 5 x 5 = 25. Additional multiplication with 5 comes from Figure 5.6. So according to the matrix in Figure 5.3, it shows that the risk level is high. And the treatment for that risk is to have backups stored in another physical location so then the information is reachable from that physical location. Other risk treatments and the risk levels are written and calculated in Figure 5.4.

Controls			Control Definition
Access Control	**11.1**	**Business Requirement for Access Control**	To control access to information
	11.1.1	Access Control Policy	Established, documented and reviewed policy based on business and security requirements for access
	11.2	**User Access Management**	To ensure authorized user access and to prevent unauthorized access to information systems
	11.2.1	User Registration	Formal user registration and de-registration procedure for granting and revoking access to systems
	11.2.2	Privilege Measurement	Allocation and use of privileges should be restricted and controlled
	11.2.3	User Password Management	Allocation of passwords should be controlled through a formal management process
	11.2.4	Review of User Access Rights	Management should review user access rights at regular intervals using a formal process
	11.3	**User Responsibilities**	To prevent unauthorized user access and compromise or theft of information and information processing facilities
	11.3.1	Password Use	Users should be required to follow good security prectices in the selection and use of passwords
	11.3.2	Unattended User Equipment	Users should make sure that unattended equipment has appropriate protection
	11.3.3	Clear Desk and Clear Screen Policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted
	11.4	**Network Access Control**	To prevent unauthorized access to networked services
	11.4.1	Policy on Use of Network Services	Users should only be provided with access to the services that they have been specifically authorized to use
	11.4.2	User Authentication for External Connections	Appropriate authentication methods should be used to control access by remote users
	11.4.3	Equipment Identification in Networks	Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment
	11.4.4	Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports should be controlled

	11.4.5	Segregation in Networks	Groups of information services, users, and information systems should be segregated on networks
	11.4.6	Network Connection Control	For shared networks capability of users to connect to the network should be restricted with using 11.1 control
	11.4.7	Network Routing Control	Those should be implemented for networks to make sure that computer connections and information flows do not breach the access control policy of the business applications
	11.5	**Operating System Access Control**	To prevent unauthorized access to operating systems
	11.5.1	Secure Log-on Procedures	Access to operating systems should be controlled by a secure log-on procedure
	11.5.2	User Identification and Authentication	All users should have a unique user ID for their personal use and a suitable authentication technique should be choosen to substantiate the claimed identity of a user
	11.5.3	Password Management System	Systems for managing passwords should be interactive and should ensure quality passwords
	11.5.4	Use of System Utilities	The use of utility programs that might be capable of overriding systems and application controls should be restricted and tightly controlled
	11.5.5	Session Time-out	Inactive sessions should be shut down after a defined period of inactivity
	11.5.6	Limitation of Connection Time	Restrictions on conncetion times should be used to provide additional security for high risk applications
	11.6	**Application Access Control**	To prevent unauthorized access to information held in application systems
	11.6.1	Information Access Restriction	Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy
	11.6.2	Sensitive System Isolation	Sensitive systems should have a isolated computing environment
	11.7	**Mobile Computing and Teleworking**	To make sure information security when using mobile computing and teleworking facilities
	11.7.1	Mobile Computing and Communication	Appropriate security measures ahould be adopted to protect against the risks of using mobile computing and communication facilities
	11.7.2	Teleworking	A policy, operational plans and procedures ahould be developed and implemented for teleworking activities

Information Systems Acquisition Development and Maintenance	**12.1**	**Security Requirements of Information Systems**	To ensure that security is an integral part of information systems
	12.1.1	Security Requirement Analysis and Specifications	Statements of business requirements for new information systems, or enhancements to existing information systems should be specify the requirements for security controls
	12.2	**Correct Processing in Applications**	To prevent errors, loss, unauthorized modification or misuse of information in applications
	12.2.2	Input Data Validation	Data input to applications should be validated to make sure that this data is correct and appropriate
	12.2.3	Control of Internal Processing	Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts
	12.2.4	Message Integrity	Requirements for ensuring authenticity and protecting message integrity in applications should be identified and appropriate controls identified and implemented
	12.2.5	Output Data Validation	Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances
	12.3	**Cryptographic Controls**	To protect the confidentiality, authenticity and integrity of information by cryptographic means
	12.3.1	Policy on The Use of Cryptographic Controls	A policy on the use of cryptographic controls for protection of information should be developed and implemented
	12.3.2	Key Management	Key management should be in place to support the organization use of cryptographic techniques
	12.4	**Security of System Files**	To ensure the security of system files
	12.4.1	Control of Operational Software	There should be procedures in place to control the installation of software on operational systems
	12.4.2	Protection of System Test Data	Test data should be selected carefully and protected and controlled
	12.4.3	Access Control To Program Source Library	Access to program source code should be restricted
	12.5	**Security in Development & Support Processes**	To maintain the security of application system software and information

	12.5.1	Change Control Procedures	The implementation of changes should be controlled by the user of formal change control procedures
	12.5.2	Technical Review of Applications After Operating System Changes	When operating systems are changed, business critical applications ahould be reviewed and tested to ensure there is no adverse impact on organizational operations or security
	12.5.3	Restrictions on Changes to Software Packages	Modifications to software packages should be disouraged, limited to necessary changes, and all changes should be strictly controlled
	12.5.4	Information Leakage	Opportunities for information leakage should be perevented
	12.5.5	Outsourced Software Development	Outsourced software development should be supervised and monitored by the organization
	12.6	**Technical Vulnerability Management**	To reduce risks resulting from exploitation of published technical vulnerabilities
	12.6.1	Control of Technical Vulnerabilities	Timely information about technical vulnerabilities of information systems being used should be obtained, the organization exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk

Figure 5.1 ISO/IEC 27003:2010 Standard Controls and Definitions

Threats	Control	11.1.1	11.2.1	11.2.2	11.2.3	11.2.4	11.3.1	11.3.2	11.3.3	11.4.1	11.4.2	11.4.3	11.4.4	11.4.5	11.4.6	11.4.7	11.5.1	11.5.2	11.5.3	11.5.4	11.5.5	11.5.6	11.6.1	11.6.2	11.7.1	11.7.2	12.1.1	12.2.1	12.2.2	12.2.3	12.2.4	12.3.1	12.3.2	12.4.1	12.4.2	12.4.3	12.5.1	12.5.2	12.5.3	12.5.4	12.5.5	12.6.1
Floods		This threat is handled by the other controls																																					
Sandstorms		This threat is handled by the other controls																																					
Earthquake		This threat is handled by the other controls																																					
Landslides		This threat is handled by the other controls																																					
Lightning		This threat is handled by the other controls																																					
Nuclear bombs		This threat is handled by the other controls																																					
Mail bombs																							X							X		X							
Electrical interruption								X											X																				
Fire		This threat is handled by the other controls																																					
Hardware failure								X	X			X				X																								
Software failure (changing without testing Controlling)																			X						X							X	X	X			X			
Telecommunication failure											X	X												X	X															
Liquid leakage																														X									
Information leakage			X							X	X					X				X	X	X															X		
Viruses															X																									
Corrupted servers and applications																			X		X	X				X		X						X					
Unauthorized altered information			X	X	X	X		X	X	X	X		X		X	X	X	X		X	X	X		X	X														
Malicious software																										X					X	X						X	
Malicious user			X	X		X				X	X				X		X	X				X		X	X						X							

Eavesdropping on confidential information								X													X		X	X							X	X									
Network traffic spoofing												X																			X	X									
Weak browsers																															X	X									
HTTP request attacks																															X										
Collision between network users																	X																								
Stolen or hacked passwords					X		X	X	X			X				X		X		X																				
Using information incorrect				X				X		X	X			X		X					X	X						X			X									
Attacks on sensitive systems												X							X		X	X	X																	

Figure 5.2 ISO/IEC 27003:2010 Standard Controls with possible threats

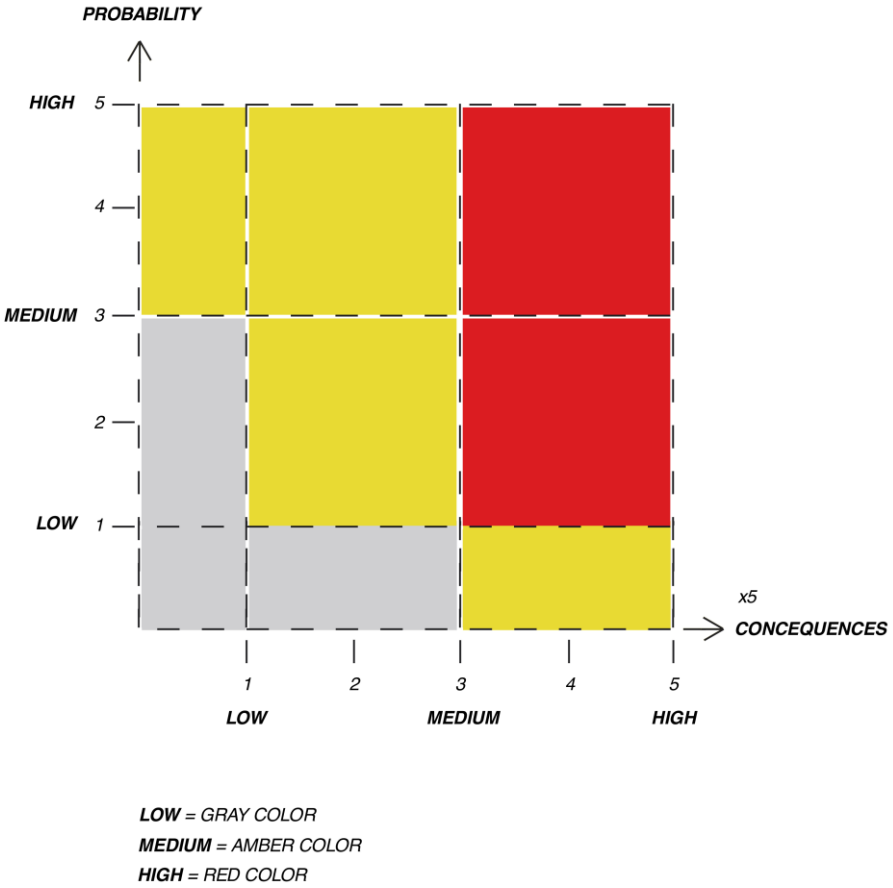

Figure 5.3 Matrix to calculate the risk levels

Threats	Risks	Probability	Consequences	Risk Levels	Risk Treat
Floods	Loss on availability of information	1	4	Medium	Have backups stored in another physical location
Sandstorms	Loss on availability of information	5	2	Medium	Have backups stored in another physical location
Earthquake	Loss on availability of information	1	4	Medium	Have backups stored in another physical location
Landslides	Loss on availability of information	1	4	Medium	Have backups stored in another physical location
Lightning	Loss on availability of information	1	3	Low	Have backups stored in another physical location
Nuclear bombs	Loss on availability of information	1	5	High 5x5	Have backups stored in another physical location
Mail bombs	Interruption on getting access to the email system and disclosure of sensitive information.	3	3	Medium	For private or isolated encrypted sessions is better to use SSL secure protocol and for regular email systems have protocol inspection
Electrical interruption	Loss on availability of information and production depending on the duration of interruption. In electric cuts routers starts communicating before the firewalls that makes the network layout visible to the intruder	3	3	Medium	Use Uninterruptable Power Supply (UPS) and start firewalls before routers
Fire	Loss of equipment, employees, availability and customer information	2	5	High 10x5	Have smoke alarms and inspect the electric code violations, fire extenguisher system

Hardware failure	A system failure cause delays in productivity and loss in availability of information	2	3	Medium	Have backups and raided system or hot stand by system
Software failure (changing without testing Controlling)	Unavailable operating systems or/and applications, output errors and delay in productivity	4	4	High	Test the software before using and trust before installing a new software
Telecommunication failure	Communication and information transaction error, loss on availability of communication and information	2	3	Medium	Allow only the known and identified mobile devices, redundant communication system
Liquid leakage	Damage on hardware equipment and loss of information	1	2	Low	Allow only permitted users or technicians and schedule maintanence times on machines
Information leakage	Disclosure of information, effected organization reputation and economical damage	3	4	High	Information handling standards, follow the given policies
Viruses	Collapsed and unavailable systems, functionless computers and loss of information	4	4	High	Use trusted virus program and update regularly
Corrupted servers and applications	Collapsed and unavailable systems, functionless computers and loss trust in information (traceability)	3	4	High	Use access control and multi-factor authentication is important for servers and applications. Block illegal access using routers of firewalls
Unauthorized altered information	Loss of integrity, reputation and traceability of information.	3	4	High	Monitor user activity logs and the flow of information transaction
Malicious software	Damage on operating systems, servers and information theft	3	4	High	Test the software in secure environment before using and trust before installing a new software

Malicious user	Loss of information, damaged hardware/software systems	3	4	High	Give access only to permitted users according to role based profile and check the terminated user accounts
Eavesdropping on confidential information	Disclosure of sensitive information	3	4	High	Use firewalls and gateways to secure the communication and information exchange
Network traffic spoofing	Non-functional networks due to serious network attacks by mapping the traffic	3	3	Medium	Block unwanted traffic and monitor it through network
Weak browsers	Loss on information confidentiality of protocol exchanges	3	2	Medium	Trust for the third parties and set a minimum level for cryptography enabled browsers
HTTP request attacks	Unauthorized access to information and exposed traffic pattern	3	3	Medium	DNS protocol is not enough only to secure host names. Use for example SSL authentication protocol
Collision between network users	Loss in confidentiality, traceability and reputation of information	1	4	Medium	Give unique credentials for each user in the system and log activities
Stolen or hacked passwords	Loss in confidentiality, traceability and reputation of information	4	4	High	Use complex and safe passwords
Using information incorrect	Loss in confidentiality of information, customer and gives economical harm	3	4	High	Edit checking and follow the given policies
Attacks on sensitive systems	Damaged systems in production, manufacturing and processing of information leads to loss of productivity and possible loss of information	2	4	High	Apply security by using firewalls and encryption devices following the given archtiecture

Figure 5.4 Risks according to the possible threats, risk levels and the risk treatment

Threat Probability				
Low	Low - Medium	Medium	Medium – High	High
1	2	3	4	5

Figure 5.5 Threat probability

Threat Consequences				
Low	Low - Medium	Medium	High	Extreme
1	2	3	4	5 x 5

Figure 5.6 Threat consequences

6. Results

In this chapter, the graphical visualization of all requirements for the information flow and the SSO are presented by using MoDAF architectural framework. Also different SSO solutions are compared based on the use of different technologies. According to this comparison different types of threats are listed for each SSO solution and compared how secure they are in their own rights.

6.1 Application of MoDAF operational viewpoints

After all those definitions about SSO and different solutions offered to SSO, organizational needs are presented by using OV (Operational Viewpoints) from 1 to 7 starting with Figure 6.1. This viewpoint helped to combine different needs expressed by the users and map them together with system requirements. The hierarchy of an organization is built on to show how the information is treated. Therefore, for each viewpoint a data model was shown in models as an example (Ruuda Consulting AB).

First view is the OV-1 High Level Operational Concepts. This concept of view is used to show the graphical view of a whole structure or context of the network system. That graphical view is shown in the introduction chapter as a Figure 1.1. That figure shows private and the public clouds generated for the network with different nodes. Therefore, Figure 1.1 is called as OV-1a high level operational concept. Another view in this concept is OV-1b which is called for operational concept description and shows that users are defined as role based in the system. Important part of the OV-1b is to show the clouds in the system and define roles for each cloud. Therefore, there are defined clouds with the users under a specific role. An example is given from an education sector. One cloud is serving for different purposes and users of different levels. So each cloud has specific roles defined for the system.

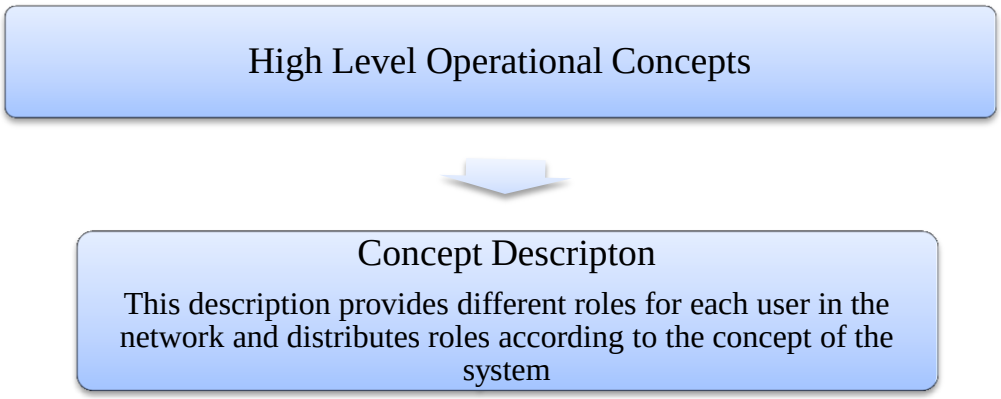

Figure 6.1 OV-1b Operational concept descriptions

Another way of showing OV-1c is where users are tagged with different roles in the system. Those roles are serving for different purposes so that they generate operational performance attributes displayed in Figure 6.2.

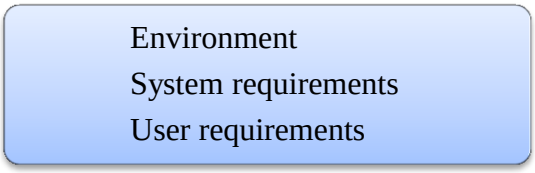

Figure 6.2 OV-1c Operational performance attributes

Second operational view is OV-2, the node relationship description. It shows the relationship between user and different systems. It describes each profile based on user roles which are communicating with these services inside the system. Essentially it shows the information that is build up for the system without including the security measures. For example, Figures 6.3, 6.4 and 6.5 are explaining information and the communication exchange between student, teacher and the administration, OV-2.1, OV-2.2, OV-2.3, respectively. Those figures have the student information, common applications, collaborated with teachers and the administration. Therefore, this is an example of showing how to build OV-2 in figures. Each figure represents centrally students, teachers and administration, respectively. Moreover, roles are defined to communicate with other roles and the information resources based on the user profile.

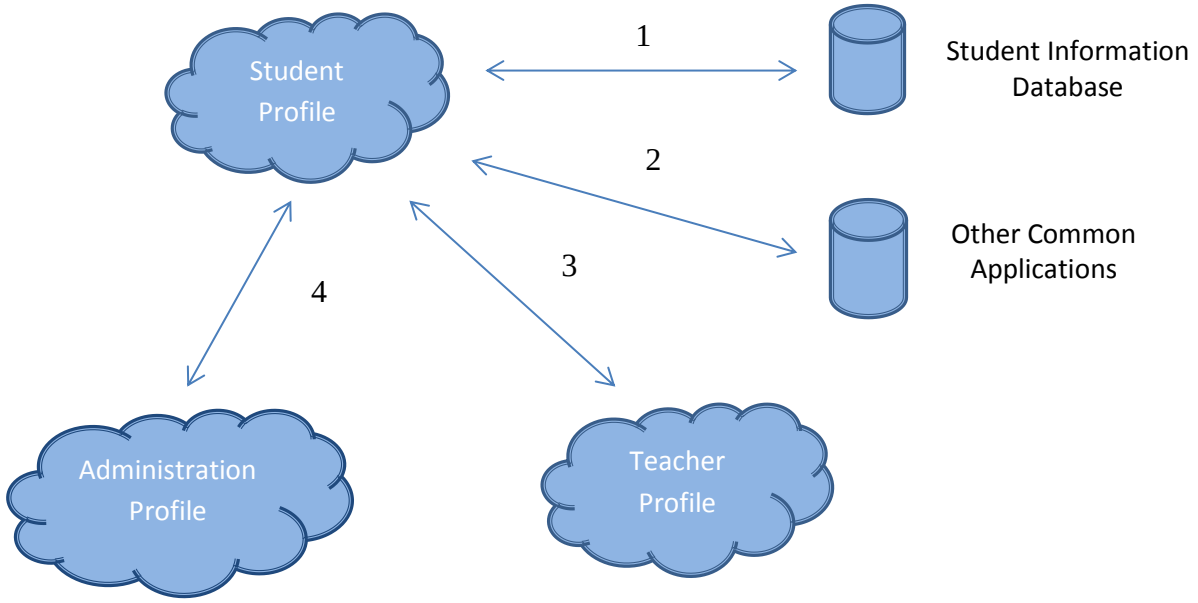

Figure 6.3 OV-2.1 Students centric operational node relationship

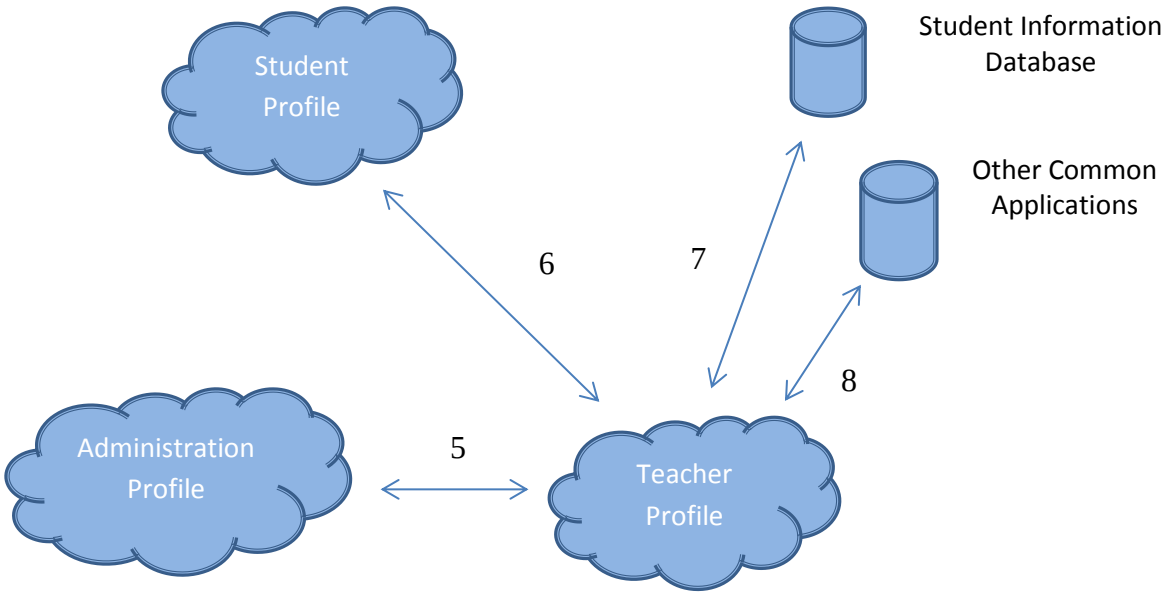

Figure 6.4 OV-2.2 Teachers centric operational node relationship

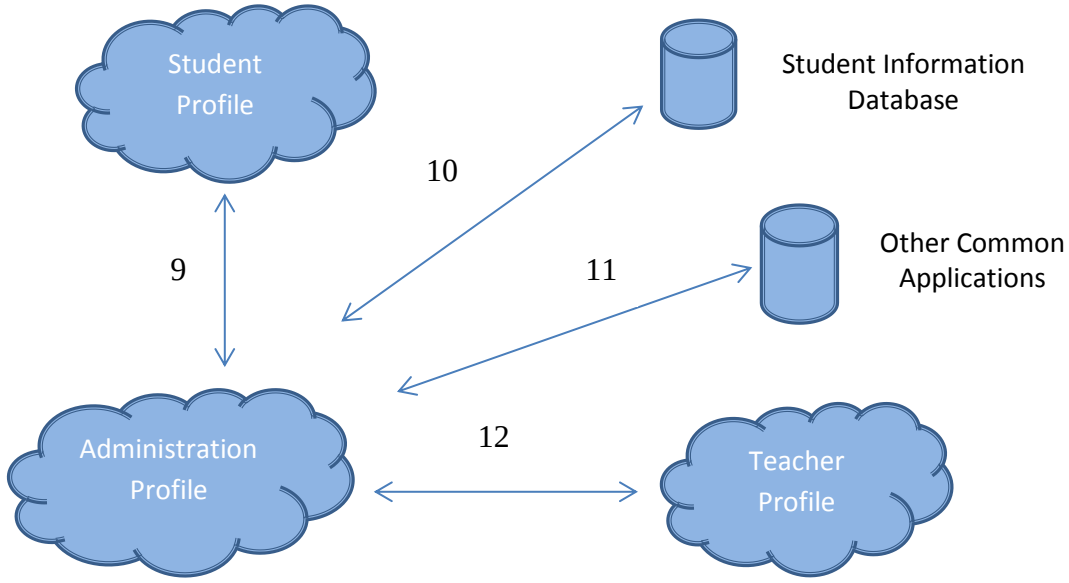

Figure 6.5 OV-2.3 Administrations centric operational node relationship

Administration profile is higher in the hierarchy then teachers and the students. Users in administration role have communication with all services. Therefore they are representing the high level node in the system. Teacher profile is higher than the student profile so they are representing the medium level node in the system. And the last lowest node is the student profile in the system. Because of this sequence, information exchange is depending on the level ranking. Next Figure 6.6 shows consisted information and information exchange. First one shows shared database of student information. For example student blackboards, where all students have share a common system for grading, time tables, course descriptions and other useful tools for the education. Second link shows the communication between other common applications. For instance, a share point named Adobe Connect software is used for conferencing. The third and the forth lines show the communication links between other roles, teachers and administration. Communication between student, teacher and administration

profile is provided by sending and receiving voice, voice videos and emails. Overall, each role in the clouds represents one database in different sub-systems.

1	Shared database of student information system
2	Shared other common applications
3	Student - Teacher communication link
4	Student - Administration communication link
5	Teacher - Administration communication link
6	Teacher - Student communication link
7	Shared database of student information system
8	Shared other common applications
9	Administration - Student communication link
10	Shared database of student information system
11	Shared other common applications
12	Administration - Teacher communication link

Figure 6.6 OV-2 Operational node relationship descriptions

OV-3 Operational information exchange is built up actually to support nodes to achieve a specific operational activity. When it comes down to OV-3, it is building practically on OV-2 to go further and define what kind of information is actually to be sent and received. Essentially, it is describing the arrows in the OV-2 figures. Those arrows are containing the uploading and downloading of information from different sub-systems. In Figure 6.7, the information exchanged between different clouds is listed to exemplify the case.

1	Uploading and downloading documents, lecture notes, discussions, time tables and calenders
2	Downloading administrational agreement papers. Live conference records, voice records
3	Voice, voice video and email exchanges
4	Voice, voice video and email exchanges
5	Voice, voice video and email exchanges
6	Voice, voice video and email exchanges
7	Student profiles, uploding lecture notes, grades, time tables and calenders
8	Meetings, live conference records, voice records, give permission to access webconferences
9	Voice, voice video and email exchanges
10	Student acceptance, administrational agreements about students and downloading student profiles and trascripts
11	Administrational work
12	Voice, voice video and email exchanges

Figure 6.7 OV-3 Operational information exchange

After describing the roles, relations between the clouds and exchanged information, it comes to describe the units. A unit is a group of students, teachers and administration that is

in charge of the organization. And this organization has a communication or an exchange link with the other organization that is the head of the organisation. Additionally, there is headquartering where all services are managed from another organization. This unit of headquarter is built up on top of the previous organization resources. That is the way of showing a hierarchy of the whole organization. As a result, OV-4 organizational relationship chart describes the organization hierarchy. This organization at large has different units in different locations. Therefore, OV-4 explains the need of communication between the organizations. This hierarchy is also built on rules but Figure 6.8 only shows different units connected with different organizations, and roles are all hidden under them.

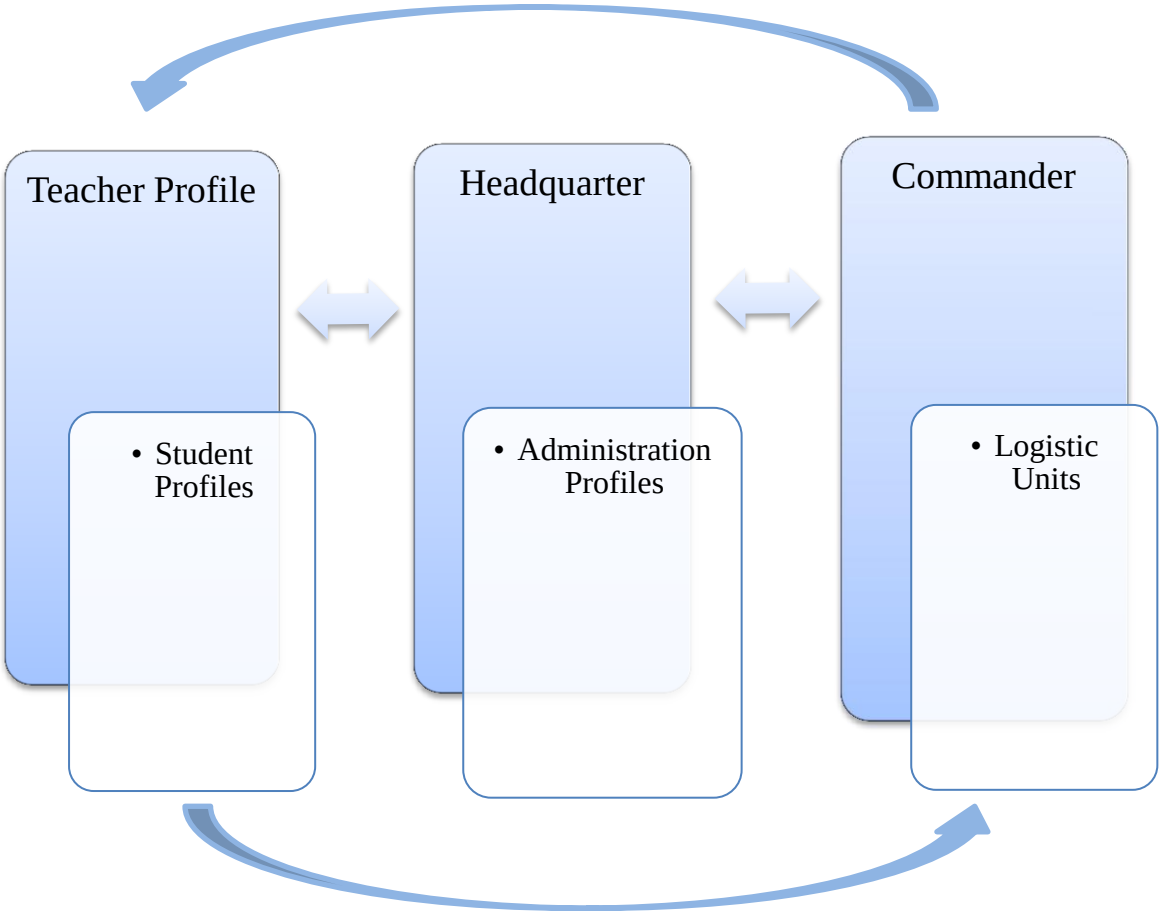

Figure 6.8 OV-4 Organizational relationship chart

Figure 6.8 is an example to show how different organizations are connected to have communication channels and exchange of information. It is just to show the concentration of nodes and where they are standing in the hierarchy. This viewpoint could be constructed differently according to the customer needs. That determines the roles for each user to serve on different purposes in SSO environment with the given permissions. For example, logistics units might perform common applications like for reaching seminars, lecture rooms or booking rooms inside the buildings. And the commander is somebody who is in charge of the buildings or maintenance in the organization. Each node in the organization has different activities to perform. OV-5 Operational Activity Model tries to setup those nodes to be able to perform the activities. Student node is performing reading, writing, compiling and sharing information. It can also perform uploading, downloading of information. Those activities are

already given as an example in OV-3. More or less, OV-5 model is designed to help and show how these activities can apply for the organization like in OV-3 model. Organizations are able to show rules, states and events depending on an activity. And that is done by OV-6 Operational Rules/States/Events. Organizations have some activities and then they add on set of rules to apply. A web seminar example is given in Figure 6.9 to show how compatible it is for an organization.

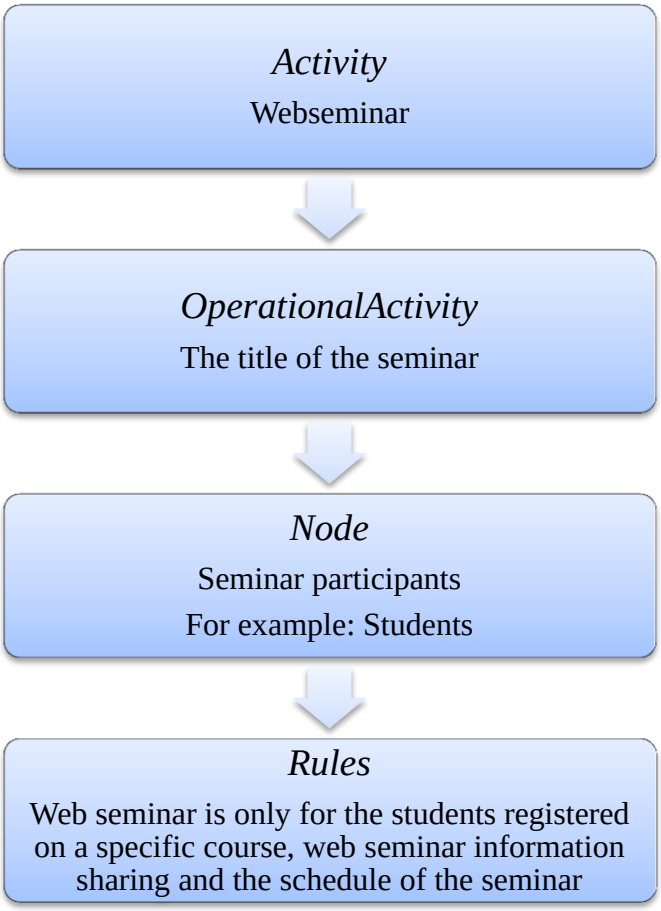

Figure 6.9 OV-6a Operational rules model

In addition to OV-6a, OV-6b is also serving almost for the same purpose. The difference is that OV-6b is using different views combining with the resources from the system view and the service oriented view to show a full model. OV-6b is shown in Figure 6.10 as a continuation of Figure 6.9.

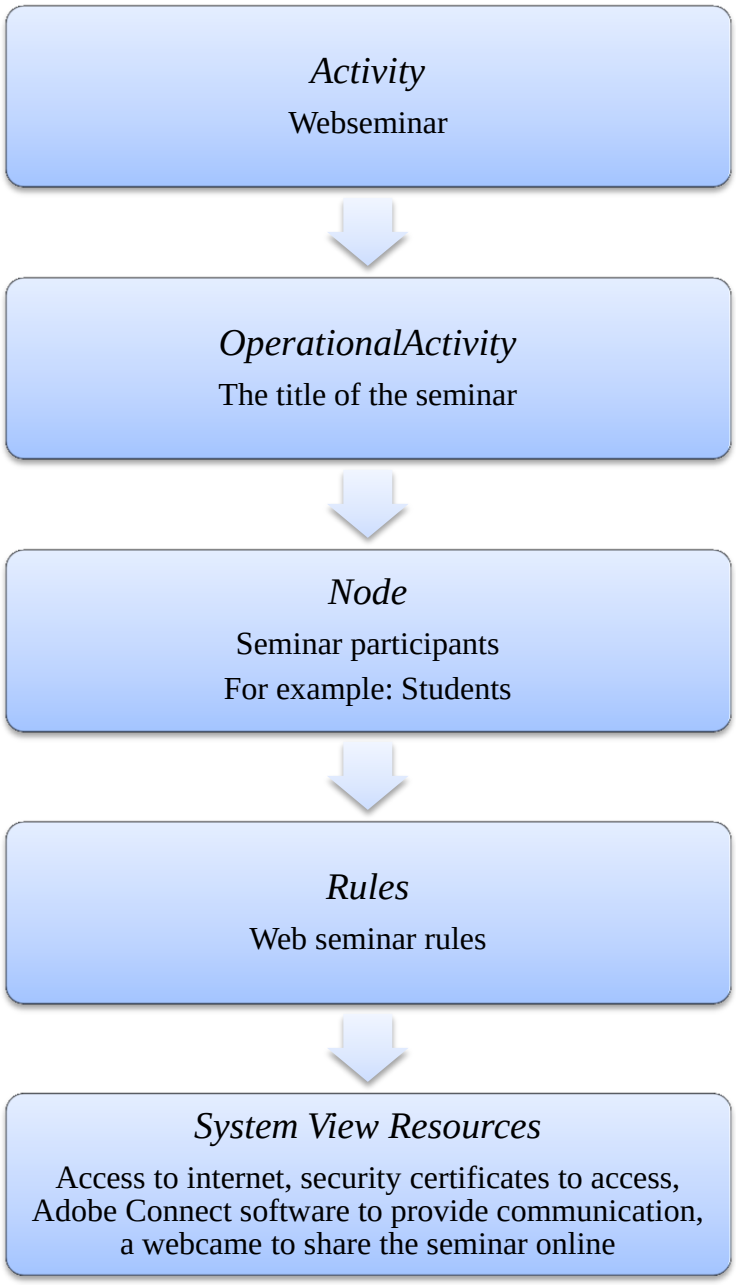

Figure 6.10 OV-6b Operational state transition descriptions

This is the way of defining the resources in a model. First of all here shows all the relationships starting to model it into a system view. The last version of showing OV-6 is OV-6c an event trace description. All required events and the services in the node operation are showed in a timeline. This is the same as the other parts of the level 6. The last view for the operational viewpoints is OV-7 Information model. All the requirements have defined the type of the information. That helps to go down to technical standard view. What is shown in OV-2 is the information exchange. Information detail is given in type OV-3. What were described in OV-5 are the activities. The information is given about how applicable these activities are. That is called a data model. So it is known that some information is needed to apply activities and a work space is needed to build them up. That information is private for the user itself. And there are also other information shared in small groups. For instance,

students need a private domain to communicate with teachers so that no one can see that communication. This shows how the information is treated. Therefore, that requires applying security measures because there are open sources available on the internet. Private information has a higher level of security. However the shared information, between student and the teacher, has at least the same level of security. This hierarchy is same between all the nodes in the system. That shows what information is stored in which sub-system and how it is treated in an information model. In this model information is separated according to their privacy. OV-7 was described as a product taking all different nodes and showing the different sub-systems based on the information. Also it contains different applications, services and shows that the required resources are needed for the SSO. Figure 6.11 shows the OV-7 Information model how to build up and see the system related information. It also includes security measures as an example. Each level has security functionalities that ensure the application security.

		Shared Resources	**Security Measures**
Information Exchange	**Data/Text**	Data Servers	Encryption Device Authentication Mechanisms SSL Protocol RADIUS Protocol for email servers
		Email Servers	
		Voice Over IP	
		Phone Numbers	
		Addresses	
	Voice	Data Servers	Encryption Device Authentication Mechanisms Secure tunnelling for data transport
		Email Servers	
		Voice Over IP	
		Phone Numbers	
		Addresses	
	System Related Information	Certificate Servers	Encryption Device IPSEC to secure the data transport between routers and data communication devices
		SSO	

Figure 6.11 OV-7 Information model

Security measures are given specifically for each type of exchanged information, data/text, voice and system related mechanisms. Encryption methods and authentication mechanisms are for protecting the information. Tunnelling and other protocols are providing secure information exchange. This is the way to describe the technical side of the model. In Figure 6.11 is shown the required resources shared in the network. And to have those shared resources, the system is also need to have a shared SSO system. That is the way to identify the

network. That helps to log the user in the profile, helps to open the VOIP session, email account and the other needed communications relying on the SSO system. It is also important to be able to choose the SSO provider for the applications or for the system to see how they are communicating and what resources are needed to communicate with the SSO service. All these are meant for SSO to support this work with the information systems by showing these MoDAF figures. Those figures show the way of putting all the information exchange into a model and see what kind of resources, applications and the other system related information are needed in the network. Then SSO is applied to send information to all these sub-systems. As a matter of fact, now SSO is helping to reach the data servers, email servers, VOIP, firewalls, authentication servers, certificate authority and LDAP. It is also it is helping to get access to many other applications that are available in the system. Therefore in this context Figure 6.11 shows a structure that is needed for the SSO system to open these shared resources to users. When it comes to the SSO technologies, it is distinguished as classified for the external and internal users. According to different located users, protocols, directories and authentication mechanisms are different than other SSO types. That is briefly shown in Figure 6.12.

Types of SSO	Characteristics of SSO Solution	SSO Technologies
Pseudo SSO	Single authentication mechanisms and multiple authentication server	Self-service password management, password synchronization and out of band authentication
Centralized SSO	Single authentication mechanism and single authentication server	Synchronization of the credentials between the server and the user, multifactor authentication mechanisms, Kerberos and PKI encryption
Web SSO	Using web proxy server Single set of credentials Token based or PKI based	Kerberos, SAML, Cookies, LDAP and OpenID
Federated SSO	Contains more than one organization Multiple set of credentials	SAML, SOAP, LDAP, Multifactor authentication mechanisms and Web Services Security (WSS)

Figure 6.12 SSO Types and Technologies

The SSO types in Figure 6.12 are actually described in chapter 3. Pseudo has its own user information, which means if a user changes a password on one system that means other system passwords should change manually. Pseudo has multiple authentication servers so it needs to have password synchronization in between the servers. Having multiple authentication-servers make the system de-centralized. However, in centralized SSO there is single authentication server which is not dealing with multiple logins. That means it is not using password synchronization. Centralized SSO automatically remembers user credentials and easy to access one application to another by using centrally located SSO server. It is then easier to manage user profiles and auditing than the Pseudo SSO. Web SSO is the key to open

up the environment to the Internet world. It works with web browser enabled applications with using web proxy server to prevent unauthorized accesses. Cookies are used to give permission only for successful accesses. Federated SSO is also used for web applications which are located off the network. That helps to connect applications by identifying user's one application to another. Common scenario to have SSO is to get access to the applications easily, combine external partners to communicate via domains and to give authorization priority for users to get access. From simple SSO to Federated SSO, the system architecture gets more complex and it gives more features about trusting security. But for the complexity of the system is expected to be more complex than the simple SSO. However Federated SSO means that only one type of user credential is used by many different systems. And that makes it easy and user friendly to use. Of course complexity might increase with organizational needs and increase from weak authentication to strong authentication. If it is needed to be more specific about multiple set of credentials, it is shown as a result that server-side credential storing is more secure then the client-side storing. Because of its definition the server-side stores the credentials centrally and not visible all the time to the client-side. It is easy to manage and audit centrally placed servers. Server-side is also using LDAP for storing them. Additionally, there are devices communicating with the network both externally and internally so server-side is reachable from the portable devices. According to a single set of credentials like in centralized SSO it is better to use PKI-based authentication then token-based authentication because PKI-based provides high level of security by using asymmetric cryptography. For such reasons this work is based on asymmetric encryption to encrypt the traffic between the clients and servers. By using asymmetric cryptography, all applications need to be configured to PKI-based authentication. Therefore, there is no need to add extra software to configure each application for token-based. From all these explanations it appears that it is better to use centralized SSO rather than Pseudo SSO. Pseudo SSO is the simplest one and applies to small organizations. By using centralized SSO user is not dealing with multiple logins for different applications so there is no more than one user credential. That means no password synchronization, no self-service password management. The only thing that needs to be used is the primary authentication mechanism to get an access. However from a security perspective regarding Pseudo SSO, it is keeping the user credential similar for password synchronization which could be a problem. And regarding to centralize SSO, single point of failure is a problem.

Each SSO type has specific threats according to their characteristic results. Here threats are shown for each type of SSO system in Figure 6.13. Pseudo SSO is representing a closed network for one organization. In that organization network there are several sub-systems that users are connecting. Each sub-system has different identities but they are synchronized so it appears to be SSO system for the user. That means all information for the SSO is only handling internally in the system. For instance, there is not really a connection with the internet. However there could be a communication access from the external systems to the internal ones done by using remote desktop connection between the external user computer and the client-server. That communication is taken care of as the same way when it comes to authentication. First there is an ID which is used to enter the system. And then it opens the SSO to give access to user for needed sub-system. So that communication is also handled just the same as getting access to the front of the system. That could cause a network traffic spoofing and eavesdropping on confidential information through internal network. The probability of occurring the internal information attack is lower than it happens in the web based SSO. But it depends on the attacker profile which information or the system is wanted. Other possible threats for each SSO types are shown in Figure 6.13.

Pseudo SSO	Centralized SSO	Web SSO	Federated SSO
• Network failure • Eavesdropping on confidential information • Unauthorized altered information • Attack on data exchange between the sub-systems • Stolen or hacked passwords • Internally virus attacks • Communication failure • Corrupted servers and applications (Denial of service) • Operating system modification on the client side	• Network failure • Network traffic spoofing • Virus • Operating system modifications on the server side	• Eavesdropping on confidential information • Man-in-middle attack • Network traffic spoofing • HTTP request attacks • Malicious user • Virus • Identity theft	• Eavesdropping on confidential information • Man-in-middle attack • Network traffic spoofing • HTTP request attacks • Malicious user • Virus • Identity theft • Communication failure

Figure 6.13 Possible threats for each SSO type

Other threats which are not listed in Figure 6.13 are actually not really related with the SSO types. They are just functionality threats that affect the network. For instance, natural threats can affect every type of network. If a company has a wireless connection or satellite communication with mobile access, then it is an advantage that user communication will not get lost because of the earthquake. But if the communication is relying on fixed cable, and if buildings start moving with the earthquake probably cables get stretched and cracked. So the communication will no longer be active for the users. Therefore, to have a wireless communication decreases the risks of a natural disaster. Networks failure threat is possible for all types of SSO. But it is more problematic for centralized SSO because it has a single point of failure as a weakness from a system point of view. But from all other point of views there could be single point of failure. The critical part between the user and the hardware that is used to communicate is always the hardware. That would be the single point of failure in the end. However, unauthorized access is more problematic for Pseudo SSO. It is because each sub-system is secured by different passwords. These passwords for each sub-system are difficult to recall by the users. This could bring the vulnerability for the passwords to be corrupted. Due to the carelessness of users copying the password on a piece of paper and forget it. Man-in-middle is the threat for both web SSO and federated SSO. It means that third party is interrupting the communication between the two other parties. Encrypted messages sent and received between two parties are intercepted by an attacker and replaced with any other messages. So at that point attacker knows the secret keys to communicate (Stallings, W. and Brown, L., 2012). Secret key exchange protocol is vulnerable because it is not

authenticating the communicating users. This attack is prevented by using public-key certificates and digital signatures. Moreover, data exchange through internet has a vulnerability of getting corrupted by HTTP request attacks. This attack might happen with the same probability with web SSO and Federated SSO. From SSO point of view, weak browsers are not a threat but for reading and sending information through a browser might cause a threat for the confidentiality. SSO is using SAML standard to prevent against this threat by protecting passwords, user attributes and redirections to wrong websites. Additionally, identity theft is also prevented by using SAML. It does not allow several identities for one user. It is a trusted standard because it works only inside an organization and only between identified organizations externally. Collision between network users is another threat for the web and federated SSO. Communication is possible for the user profile via internally and externally. For that communication, system is using VPN tunnels which are letting the user to access through a firewall form outside. And on the inside user is back again to their home network. Collision threat between network users might occur when a user is online and working through a profile. At the same time an intruder might try to get an access with that users account causes of a conflict in the network. Then the solution is to allow one session per user in that program. Because then firewalls or something from outside just letting known addresses or known profiles for each network. So the server inside is only reachable from web client or from a client-server. So the communication is done between the clients through the client-server. Preventing network from threats gives appreciative impacts on SSO requirements, security, scalability and deployment. Kerberos standard is used to provide centralized SSO environment for the network. This protocol used first in centralized SSO to avoid threats like stolen or hacked passwords, information leakage and altered information. However, Shibboleth is used on web-based SSO to control the identity authentication based on SAML and Kerberos. As it's known by the definitions, SAML and Shibboleth are aiming first on different service. SAML sends requests to IdP and after directs user to SP. But Shibboleth is sending request to first SP and directing user to IdP service. They are both representing weaknesses and strengths. This is all depending on the SLA and the trusted service inside the network. For instance, networks own resources are protected on the same level with SLA. However there are resources coming externally in to a network. That is an unknown resource on the SLA side and unknown risks could come herewith. High probability is to have first SP trusted service. So requests go first to SP and make sure that the service is up and running through the information. Moreover, first going to SP is like asking permission, checking the availability of the system. After that user redirected to the IdP service to identify and start working. One of the federated standard Microsoft passport is used in web-based environments and having the same logic with Kerberos standard. It helps to encrypt the data structure based on symmetric encryption. User is communicating with web browser through cookies. And the communication is handled with SSL tunnels. Another federated standard Liberty Alliance is using centralized SSO to transfer and store securely the user identity over internet. And it is based on SAML standard for the authentication and authorization. Users have unique identity within each CA domain. This is not like in Microsoft Passport. This is why it is PKI-based and using X.509 certificates together with asymmetric encryption. Requests through HTTP are utilized also with SSL. One weakness about LDAP is that actually provides a lot of information that makes it used often inside the network. It is secured centrally but the information stored inside makes it an important part of the system when it is started using with centralized, web-based and federated SSO. In general, all those standards used in different systems together with different authentication mechanisms are ensuring the information communication securely by identifying users. Furthermore, it is not only users are communicating; applications are also interacting with each other by using license based communication. Certificate based communication letting users to communicate from one

domain to another with valid certificates. That is used to identify users and allow them to reach the information through a web browser or a shared resource. Applications need to communicate with application provider in order to renew or update the software by using the license. That is something the machine needs to stay up to date and running without any problem.

Results set out by modelling first the operational view points, secondly adding the system point of view by showing different types of SSO and third combining with the technical views adding different authentication mechanisms and standards. Figure 6.14 is modelled to show the overall of building a SSO system applying different types of SSO architectures.

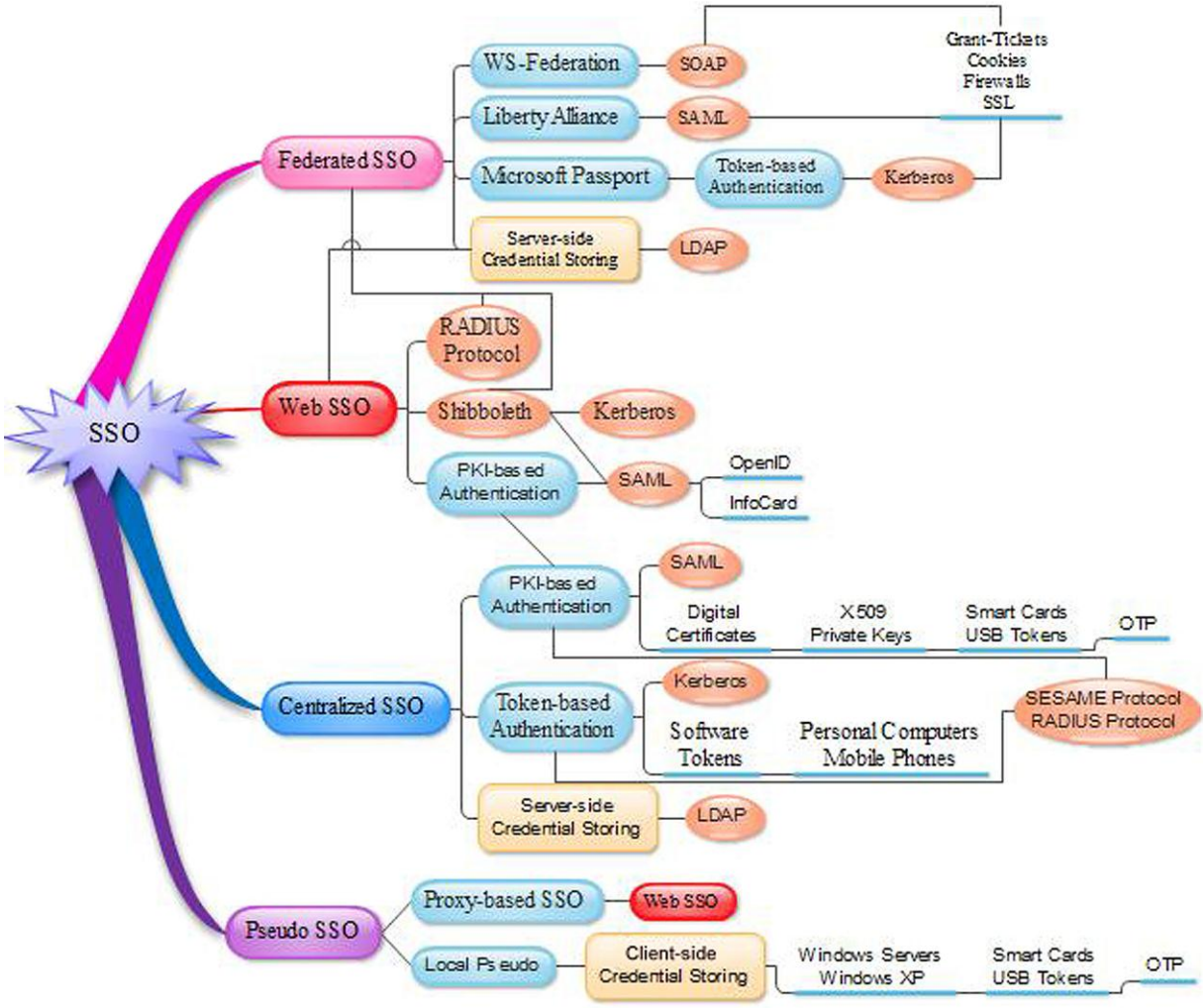

Figure 6.14 Different SSO systems

7 Discussions and analysis

The criteria proposed for the study in chapter 1.2 are discussed on the basis of the results given in chapter 6.

7.1 Information security analysis before implementing SSO

To start with the safety of an enterprise requires an organizational structure of safety to provide a safe working environment. This structure was designed to be built layer by layer configuring all sides concerned for the security of network system. Every layer was planned to contain different security aspects to protect different classified information and to handle most of the security concerns occurring in the system. Then the information was classified according to confidentiality of the information such as unclassified, open classed, restricted, confidential, secret or top-secret based on confidentiality, integrity and availability of information. Distribution of information in network environment was done by creating COI. Interests were defined as resources and in order to reach those resources users are assigned according to their role based profiles. That gave a result; COI together with the information classification was used to break down the information and to point out exactly what each user should be allowed to access. It was thought that minimum access was better to protect and minimize the attacks. The confidentiality of information could be increased in that way. To implement the fundamental security principles, structure was so designed to have systems layer by layer, limited, classified and simplified for users but complex for attackers to stay strong against the attacks.

7.2 Definition of SSO and benefits

Secondly, SSO was applied on different networks to provide security by giving easy access for all multiple sub-systems following the authentication of the user once. This would enable the user to log in different sub-systems safely without remembering any other credentials once his or hers safe authentication was accomplished. Common benefits general for the organizations were expected to have improved communication, security, productivity and availability of users and information. Also this would decrease the management costs. SSO mostly applied on complex systems which require more security on added systems. However troubleshooting got lower together with the growth of the network. Added systems need to be checked for the failures and updates. That makes it difficult to go around and deal with them one by one. For these reasons decision was made to apply centralized SSO both on management side and the security side.

7.3 Functionalities of SSO

Thirdly, some requirements were specified in order to support the implementation of SSO. For the sake of supplementing and improving the terms and conditions for security, a conclusion was made to have a high availability for SSO. So that SSO needs to be updated about the new information or applications which could be added subsequently in the system, because deciding SLA for the system is directly connected to have availability. Different SSO solutions were used in this work and Figure 6.14 shows how they are compatible and deployed with each other in order to have a safe communication and business. They are compatible with the use of different protocols, authentication mechanisms and products. Selecting centralized SSO instead of pseudo SSO indicated that usability of that solution would be high for the users to achieve goals with an effective, satisfied and efficient way. Implementation of this solution might change according to the customer needs in different organizations. Together with the SSO, single sign-off is also important to achieve the

implementation successfully. Single sign-off is a wide subject to discuss and should be studied as part of a future work. Centralized SSO indicated that managing users, login sessions, supported updates, response time from requested information, having backups could be handled easily from a centralized location. This feature of centralized SSO would increase the performance of the network. Network gained privacy by designing the system layer by layer as explained in chapter 2.1. Role based profiles were created to protect the privacy of information. As a matter of fact, only permitted users allowed in each layer according to their profiles. Encryption devices, routed traffic through proxies, VPN tunnels, other authentication mechanisms and trusted third parties could increase the confidentiality and the integrity of the information. The more users are logged, the less privacy would be maintained on the information. This problem could be handled by audit and log management. Log management is used to identify the events, records actions of users, provide long-term storage and configure the log severs to perform log analysis. To keep logs are essential for managing the long-term problems, auditing and identifying security incidents. The use of federated SSO was considerate to increase the scalability of ever expanding network system.

7.4 Architectural guidelines, protocols and directories for SSO users

Fourthly, SSO types indicated to foster different characteristic features from the architectural point of view. It was demonstrated that application of centralized SSO proved to have an easy identity and information management from a user and the system perspective. Having one server centralized like LDAP could be easy to manage but it brings weaknesses together. LDAP is quite appealing by storing valuable information and user credentials in it, which could make it vulnerable against attacks. Therefore a suggestion was made to use honeypot on the network. Honeypot offers a virtual picture of a network to be displayed. The virtual picture is not a real world of a network. Attacker starts to analyse this virtual picture thinking that it is real and draws a conclusion accordingly. When attacker comes through the first line of defence, his or her attention could be divert onto the addresses which are fake, but pretending to be real on machines. Finally, intruder starts to carry out attacks on those virtual machines. This would help to see which pattern the intruder is following. Meanwhile organization itself becomes aware of the traffics that are not generated before on the network. There should not be any illegal traffic other than that generated by the intruder. Intruder is likely to draw patterns asymmetrically to have a new traffic in the network. Then the organization becomes to realise that there is an intruder in the system. Moreover, by adding virtual client-server, firewalls and authentication servers, like in Figure 1.1, it would be possible to see clearly if the intruder will attack the catalogue service. Catalogue service reserves the organization services for the users. There are several ways the intruder might follow during the attack. Firstly if the intruder tends to attack the catalogue service, then it is clear that person is trying to reach for some information. Secondly if the intruder tends to attack the client-server, then it is clear that person is trying to steal a profile or wants to look deeper in to the system. The third possibility is that if the intruder tends to attack on the second line of defence, then this intruder wants to reach and see as much as until mapping the whole system build. In this case a serious damage could be caused to the system. However it could be possible to decrease the damages coming from the intruder by the use of honeypot. It diverts the intruder's attention on some virtual machines to run into. As the future of SSO should be compatible with that kind of development in the system and more additional approaches in the system could be establish. Besides honeypot it is functionally better to have a backup of the LDAP directory. From a system point of view, SSO systems are multi-functional including different security and user mechanisms. A single system failure could affect and cause restarting everything inside the network. System management could save time, cost and productivity by having employed the centralized SSO for the network system

and spare time to make everything up, work and communicate by checking and updating every machine in the network. Using IPSEC, SSL tunnels and other security protocols that have been discussed in the previous chapters, were expected to increase the security of the system.

7.5 Critical functionalities of SSO from users, systems and technical point of views

From a user perspective point of view, working with SSO allows the users not to remember more than one password for each sub-system. That would increase productivity and save time. But at the same time it could simplify attackers' effort on finding out only one password. It was showed that it is not enough to have only one password. This would bring multi-factor authentication in use for the SSO systems. Managing only one set of credential would be sufficient from the management perspective but from the security perspective it is very low. Using biometrics, smartcards and OTP security mechanisms provides a medium, high and low degree of security from the management perspective. However from the security perspective the security provided by smart cards is higher in ranking in the system.

From the system view point, use of asymmetric cryptographic methods was decided on the communication and the information transaction to keep system secure. Before using the encrypted information, it is better to the intrusion detection systems, like virus protection tools or malware detections, to check the harmful data. For federated SSO systems the communication are mostly relied on the SAML protocol. As it allowed only identified, known domains to communicate. After all the SSO requirements and scenarios that have been discussed in this paper were simplified as follows:

1. Register users according to their role based profiles.
2. List the needed applications according to their profiles and decide which type of information is needed.
3. Categorize the information according to their significance and arrange the security measures according to the information priorities.
4. Check all the security standards and protocols which are providing communication inside and outside the network to see if they are all supported with SSO.
5. Trust the third party and the other service providers.
6. Give access to the user.
7. Cancel a user account from one central point by having centralized SSO.

From the technical view point check the following points to have been met:

1. Use safe and strong passwords.
2. See control access as a security check point
3. Use firewalls to control the communication
4. Monitor the traffic and block the unwanted one.
5. Used security communication protocols like SESAME, RADIUS, IPSEC and tunnelling like SSL, VPN.
6. Use the client-server before distributing the users in different sub-systems.

7.6 Descriptions about technical risks with SSO

Finally, both from the system and the user point of view, specific threats and gave possible risk scenarios were given. Risk analyses were motivated by grading the possibilities and the consequences for each given threat. Consequently a matrix was designed to calculate the risk levels and to support each threat by using ISO/IEC 27003:2010 controls. This risk analysis showed that nuclear bomb and any other threats, fire, software failure, information leakage, viruses, corrupted services, unauthorized access, malicious users, eavesdropping on

confidential information, stolen passwords and incorrectly used information could cause high damages to the organization. Specific treatments were given on each threat.

7.7 Further works

Single sign-off is a wide subject to discuss and should be further studied as part of a future work. Also combination of SSO with cloud based system features would be interesting subject to analyse and discuss to provide a good security for cloud systems.

8 List of references

ActivIdentity, 2012. *Software.* [online] Available at: <http://www.activeidentity.net/> [Accessed 26 October 2012].

Alphonso, M. and Lane, M., 2010. The Adoption of Single Sign-On and Multifactor Authentication in Organisations – A Critical Evaluation Using TOE Framework. *Issues in Informing Science and Information Technology.* 7, p.163.

Avencis, 2012.*Single Sign-on.* [online] Available at: <http://avencis.net/wp/en/software/single-sign-on-sso/> [Accessed 26 October 2012].

Barton, et al., 2006. *Identity Federation and Attribute-based Authorization through the Globus Toolkit, Shibboleth, GridShib, and MyProxy.* 5th Annual PKI R&D Workshop.

Bashir, K. and Asif, S., 2010. Important Considerations for Single Sign-On Solution. *International Journal of Multidisciplinary Sciences and Engineering,* 1(1), pp.22-27.

Bellamy-McIntyre, J., Luterroth, C. and Weber, G., 2011. *OpenID and the Enterprise: A Model-based Analysis of Single Sign-On Authentication.* Helsinki: Finland 29 August – 02 September 2011. Auckland, New Zealand.

Bhosale, S.K., 2008. Architecture of a Single Sign on (SSO) for Internet Banking. In: IET International Conference, *Wireless, Mobile and Multimedia Networks.* Mumbai, 11-12 January 2008, Conference Publications.

Bishop, M., 2005. *Introduction to Computer Security.* Boston: Pearson Education

Bui, S., 2005. *Single Sign-on Solution for MYSEA Services. Monterey:Naval Postgraduate School.*

Burroughs, T., 2000. *Oracle Single Sign-On Application Developer's Guide.* [pdf] Reedwood City: Oracle Corporation. Available at: http://docs.oracle.com/cd/A97336_01/portal.102/index.htm [Accessed 29 February 2012].

Byrnes, F.C., and Kutnick, D., 2002. *Securing Business Information, Strategies to Protect the Enterprise and It's Network.* Canada: Intel Press.

CA Technologies, 2012. *Federated Identities.* [online] Available at: <http://www.ca.com/us/access-management.aspx> [Accessed 26 October 2012].

Cantor, S., 2012. *IdP Discovery.* [online] Shibboleth Project Services. Available at: <https://wiki.shibboleth.net/confluence/display/SHIB2/IdPDiscovery> [Accessed 20 August 2012]

Causton, R. P., 2002. *Smart Card Usage for Authentication In Web Single Sign-On Systems.* Master of Science degree thesis. Helsinki University of Technology.

Ciampa, M., 2005. *Security Guide To Network Security Fundamentals.* 2nd edition. Thomson Course Technology.

Ciampa, M., 2007. *Security Awareness: Applying Practical Security In Your World.* 2nd edition. Boston: Thomson Course Technology.

Cobb, M., 2011. Six Decision Factors for Hardware-Based Authentication. [pdf] InformationWeek Reports. Available at: <http://reports.informationweek.com/abstract/13/8257/Outsourcing-Services/strategy-hardware-based-authentication.html> [Accessed at 22 October 2012]

Collan, J., 2009. *Secure Authentication and Authorization Portal Based on Single Sign-on.* MSc thesis. Helsinki University of Technology.

Constine, S., 2010. Facebook Introduces Opt-In Migration for Developers, Single Sign-On for iOS SDK. [online] Available at: < http://www.insidefacebook.com/2010/11/13/opt-in-migration-single-sign-on> [Accessed 26 August 2012]

David, B.M., Nascimento, A.C.A. and Tonicelli, R., 2011. *A Framework for Secure Single Sign-On.* [online] Brazil: Cryptology ePrint Archive. Available at: <http://eprint.iacr.org/2011> [Accessed 28 November 2011].

De Clercq, J. and Grillenmeier, G. 2007. *Microsoft Windows Security Fundamentals.* Oxford: Elsevier Digital Press.

De Clercq, J., 2003. *Introducing Credential Manager.* [online] Windows IT Pro. Available at: <http://www.windowsitpro.com/article/passwords/introducing-credential-manager> [Accessed 16 October 2012].

Duc, B., Bigun, E., Bigun, J., Maire, G. and Fischer, S., 1997. Fusion of Audio and Video Information for Multi-Model Person Authentication. *Pattern Recognition Letters*, 18, 835-843. Available through: Citeseerx scientific literature library [Accessed 21 March 2012]

Dunne, C., 2003. *Build and implement a single sign-on solution.* [online] Available at: <http://www.ibm.com/developerworks/web/library/wa-singlesign/> [Accessed 26 October 2012].

Eduroam, 2012. *Education Roaming.* [online] Available at: <http://libweb.anglia.ac.uk/referencing/harvard.htm> [Accessed 16 October 2012]

Entrust, 2012. *GetAccess for SAML interoperability.* (online) Available at: <http://www.entrust.com/internet-access-control/oasis-saml.htm> [Accessed 16 October 2012].

Epic Software, 2012. *Software.* [online] Available at: <http://www.epic.com/software-index.php> [Accessed 26 October 2012].

Erdem, E. et al., 2010. A Smart Card Based Single Sign-On and Password Management Solution as a Browser Extension. In: ICEMT 2010, *International Conference on Education and Management Technology.* Cairo, Egypt 2-4 November 2010. Chengdu, China: IEEE

Evidian, 2012. *Evidian Enterprise SSO.* [online] Available at: <http://www.evidian.com/iam/enterprise-sso/> [Accessed 26 October 2012].

Gemalto. *What is a smart card?.* [online] Available at: < http://www.gemalto.com/companyinfo/smart_cards_basics/what.html> [Accessed 23 March 2012].

Goode, J., 2012. The importance of identity security. *Computer Fraud & Securtiy,* [e-journal] 2012 (1), pages 5-7. Available through: Science Direct database [Accessed 5 April 2012].

Gross, T., 2003. Security Analysis of the SAML Single Sign-on Browser/Artifact Profile. In: ACSAC 2003, *19th Annual Computer Security Applications Conference.* Las Vegas, USA, 8-12 December 2003, Zurich, IEEE Computer Society.

Grundmann, M., Pointl, E., 2008. Single Sign-On: Reviewing the Field. In: Institut Für ınformationsverarbeitung und Mikroprozessortechnik, *Seminar aus Netzwerke und Sicherheit: Security Considerations in Interconnected Networks.* Johannes Kepler University Linz, 16 January 2009. Austria.

Hallam, P., Kaler, C., Monzillo, R. and Nadalin, A., 2004. *Web Services Security X.509 Certificate Token Profile.* [online] OASIS: Advancing Open Standards for the Information Society. Available at:< http://docs.oasis-open.org/> [Accessed 16 February 2012].

Hijleh, A., 2012. *Facebook Single Sign On.* [online] Soshable Media Block. Available at: < http://soshable.com/facebook-single-sign-on/> [Accessed 16 October 2012]

Hughes, J. et al., 2005. *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0.* [pdf] Security Services Technical Committee. Available at: < http://docs.oasis-open.org/security/saml/v2.0/> [Accessed 6 May 2012].

Huntington, G., 2006a. *101 Things To Know About Single Sing On.* [online] Huntington Ventures Ltd. Available at: http://www.authenticationworld.com/Single-Sign-On-Authentication/101ThingsToKnowAboutSingleSignOn.pdf

Huntington, G., 2006b. Single Sign On Underneath the Hood, *Authentication World,* [online] Available at:<http://www.authenticationworld.com/papers.html> [Accessed 16 February 2012].

Hussein, S. H., 2010. *Double SSO-A Prudent and Lightweight SSO Scheme: Thesis in Programme Secure and Dependable Computer Systems.* MSc. Chalmers University of Technology.

IBM, 2008. *IBM Tivoli Access Manager for Enterprise Single Sign-On.* [online] Available at: <http://on2it.net/downloads/IBM_Tivoli_TAMESSO_Datasheet.pdf> [Accessed 26 October 2012].

Ilex, 2012. *Sign&go.* [online] Available at: <http://www.ilex.fr/Sign-go_en-.html> [Accessed 26 October 2012].

Imprivata, 2012. *Enterprise SSO.* [online] Available at: <http://www.imprivata.com/enterprise_sso> [Accessed 26 October 2012].

Isprint, 2012. *Enterprise SSO.* [online] Available at: <http://www.isprint.com/solutions_enterprise_sso.html> [Accessed 26 October 2012].

Jin, A.T.B., Ling, D.N.C. and Goh, A., 2004. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition* [e-journal] 37 (11) Available through: Science Direct database [Accessed 1 May 2012].

Kaufman, C., Perlman, R. and Speciner, M., 2002. *Network Security Private Communication in a Public World.* 2nd ed. New Jersey: Prentice Hall.

Klingenstein, N., 2009. *Flows and Config.* [online] Shibboleth Project Services. Available at: <https://wiki.shibboleth.net/confluence/display/SHIB2/FlowsAndConfig> [Accessed 20 August 2012]

Klingenstein, N., 2011. *Shibboleth Documentation.* [online] Available at: < https://wiki.shibboleth.net/confluence/display/SHIB2/UnderstandingShibboleth> [Accesseed 7 May 2012].

Kreizman, G., 2010. *MarketScope for Enterprise Single Sign-On.* [online] On2IT. Available at: < on2it.net/downloads/ > [Accessed 30 August 2012]

Kreizman, G., 2011. *MarketScope for Enterprise Single Sign-On.* [online] Gartner, Inc. Available at: < http://www.gartner.com/technology/reprints.do?id=1-17N0ZTD&ct=111011&st=sg> [Accessed 30 August 2012]

Lin, et al., 2012. Single Sign-On for Multiple Unified Communications Applications. In: WorldCIS, *World Congress on Internet Security 2012.* Canada, 10-12 June 2012. IEEE.

Linden, M. and Vilpola, I., 2005. An Emprical Study on the Usability of Logout in a Single Sign-on System In: Deng, R.H. et al. eds. 2005. *Information Security Practice and Experience.* Heidelberg: Springer Berlin. pp.243-254.

Lodha, A. and Sarma, R., 2006. *A Single Sign-On Approach.* Avenue A and Ratorfish are registered trademarks. Available at: <http://slant.avenuea-razorfish.com/0406_slant/SSOApproachPaper.pdf> [Accessed 16 October 2012].

Mahrt, R., 2003. *In Pursuit of Liberty?.* SANS Institute InfoSec Reading Room Database. Available at:<http://www.sans.org/reading_room/whitepapers/authentication/pursuit-liberty_851> [Accessed 5 October 2012].

Microsoft, 2006. *Microsoft Identity and Access Management Series.* [online] Available at: <http://technet.microsoft.com/en-us/library/cc162924.aspx> [Accessed 26 October 2012].

MoD Architecture Framework, 2005. Ministry of Defence. [online] Available at:< http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/InformationManagement/MODAF/> [Accessed 10 November 2011].

MoD Architecture Framework, 2005. MoD Architectural Framework Sustainment Desk book. Issue no: Draft 0.4. Available through: http://www.modaf.com/Archive/

Msdn, 2012. *Understanding Enterprise Single Sign-On.* [online] Available at: <http://msdn.microsoft.com/en-us/library/aa745042(v=bts.10).aspx> [Accessed 30 November 2011]

NetIQ, 2012. *SSO with advanced authentication.* [online] Available at: <https://www.netiq.com/products/securelogin/> [Accessed 26 October 2012].

O'Neill, M., et al., 2003. *Web Services Security.* California: McGraw-Hill

Oracle, 2012a. *Oracle Identity Management.* [online] Available at: <http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index.html> [Accessed 26 October 2012].

Oracle, 2012b. *Oracle OpenSSO.* [online] Available at: <http://www.oracle.com/technetwork/testcontent/opensso-091890.html> [Accessed 26 October 2012].

Oracle, 2012c. *Oracle and Passlogix.* [online] Available at: <http://www.oracle.com/us/corporate/Acquisitions/passlogix/index.html> [Accessed 26 October 2012].

Oracle, 2012d. *Oracle9iAS Single Sign-On Administrator's Guide.* [online] Available at: <http://docs.oracle.com/cd/A97329_03/manage.902/a96115/monitor.htm#1004913> [Accessed 15 November 2012].

Orawiwattanakul, T. et al., 2010. User-controlled Privacy Protection with Attribute-filter Mechanism for a Federated SSO Environment using Shibboleth. In: 3PGCIC, *2010 International Conference on P2P, Parallel, Grid, Cloud and Internet Computing.* Fukuoka, 4-6 November 2010, Tokyo: National Institute of Informatics.

Osterman Research White Paper, 2009. Authentication in the Enterprise: Current and Changing Requirements. Washington: Osterman Research, Inc. Available at: < http://viewer.media.bitpipe.com/1149286151_178/1251217323_698/White-Paper_Authentication-Trends.pdf> [Accessed 29 August 2012]

Park, B. et al., 2006. One touch logon: Replacing multiple passwords with single fingerprint recognition. In: CIT'06, *6th IEEE International Conference on Computer and Information Technology*, Washington, DC, September 2006, Korea University: IEEE

Pashalidis, A. and Mitchell, C.J., 2003. A Taxonomy of Single Sign-On Systems In: Safavi-Naini, R. and Seberry J. eds. 2003. *Information Security and Privacy.* Springer Berlin.

Pehrson, B., 2005. *Web Single Sign-On System for WRL Company.* Master of Science Thesis. Royal Institute of Technology.

Peltier, T. R., 2005. *Information Security Risk Analysis.* 2nd ed. Florida: CRC Press.

Pfitzmann, B. and Waidner, M., 2003. Federated Identity Management Protocols-Where User Authentication Protocols May Go. In: 11th International Workshop on Security Protocols. Cambridge 2003. Springer-Verlag, Berlin 2005.

Pfleeger, C.P and Pfleeger, S.P., 2007. *Security in Computing.* 4th ed. Prentice Hall.

Ping Identity, 2002. *SAML 101 white paper.* [online] Ping Identity Corporation. Available at: <https://www.pingidentity.com/resource-center/SAML-Tutorials-and-Resources.cfm> [Accessed 12 October 2011].

Ponnapalli, R., 2004. *Secure Implementation of Enterprise Single Sign-On Product In an Organization.* [online] Maryland: SANS Institute InfoSec Reading Room Database. Available at:< http://www.sans.org/reading_room/whitepapers/authentication/> [Accessed 12 April 2012].

Rankl, W. and Effing, W., 2003. *Smart Card Handbook.* 3rd ed. Munich: John Wiley & Sons.

Recordon, D. and Fitzpatrick, B., 2007. OpenID authentication 2.0. [online] OpenID Foundation. Available at: <http://openid.net/specs/openid-authentication-2_0.html> [Accessed 25 August 2012]

Sandhu, S.S., 2004. *Single Sign On Concepts & Protocols.* [online] Maryland: SANS Institute InfoSec Reading Room Database. Available at:< http://www.sans.org/reading_room/whitepapers/authentication/> [Accessed 16 February 2012].

Sawyer, J., 2010. Who Are You? Choosing the Right Authentication Strategy. [pdf] InformationWeek Reports. Available at: <http://reports.informationweek.com/abstract/15/3694/Risk-Management/strategy-authentication-.html> [Accessed at 22 October 2012]

Scavo, T., 2005. *Shibboleth Technical Overview*. [online] NCSA, The National Centre for Supercomputing applications. Available at: <http://open-systems.ufl.edu/files/draft-mace-shibboleth-tech-overview-latest.pdf> [Accessed 28 May 2012].

Scavo, T., 2011. *IdP Add Attribute Filter.* [online] Shibboleth Project Services. Available at: <https://wiki.shibboleth.net/confluence/display/SHIB2/IdPAddAttributeFilter> [Accessed 20 August 2012]

Stallings, W. and Brown, L., 2012. *Computer Security, Principles and Practice.* 2nd ed. Harlow: Pearson Education Limited 2012.

Stallings, W., 1998. *Cryptography & Network Security: Principles & Practice*. 2nd edition. Prentice Hall.

Stallings, W., 2011. *Network Security Essentials: Applications and Standards.*4th edition. Prentice Hall.

Sun, S., Boshmaf, Y., Hawkey, K. and Beznosov, K., 2010. A Billion Keys, but Few Locks: The Crisis of Web Single Sign-On. In: LERSSE (Laboratory for Education and Research in Secure Systems Engineering). *New Security Paradigms Workshop.* USA, September 21-23 2010. ACM

Tiwari, P.B. and Joshi, S.R., 2009. Single Sign-on with One Time Password. *First Asian Himalayas International Conference*, pp. 1-4. Available through: IEEE Xplore [Accessed 26 September 2011].

Volonino, L. and Robinson, S.R., 2004. *Principles and Practice Of Information Security, Protecting Computerss From Hackers and Lawyers.* New Jersey: Pearson Prentice Hall.

Wu kaixing and Yu xiaolin, 2008. A Model of Unite-Authentication Single Sign-On Based on SAML underlying Web. In: ICIC2009, *2009 Second International Conference on Information and Computing Science.* The Manchester Conference Centre, UK, 20 February 2009. Handan, China, IEEE Computer Society.

Zvetco Biometrics. *Activiıdentity SSO and Biometrics.* [online] Available at: <http://www.zvetcobiometrics.com/Solutions/Applications/actividentity_sso.php> [Accessed 20 March 2012]

Linnæus University
School of Computer Science, Physics and Mathematics

SE-391 82 Kalmar / SE-351 95 Växjö
Tel +46 (0)772-28 80 00
dfm@lnu.se
Lnu.se/dfm