TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

ERPO ERONEN

STRUCTURAL REDESIGN AND AUTOMATION OF PERMISSION MANAGEMENT IN AN ENTERPRISE

Examiner: prof. Hannu Jaakkola
Examiner and topic approved by the Faculty council of the Faculty of Business and Built Environment
on 3rd of April 2013

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY
Master's Degree Programme in Information Technology
ERONEN, ERPO: Structural redesign and automation of permission management in an enterprise
Master's thesis, 47 pages
May 2015
Major: Software Engineering
Examiner: Professor Hannu Jaakkola
Keywords: Permission management, management structure, performance, information security

The thesis studies the structure of permission management system used in a client organization and the ways to make it better and more simplified. The aim is to study what type of structure would best serve the client company and then create a new permission management structure based on the findings of the research.

This study introduces the needs for permission management, required components for executing a functional permission management system and the implementation of new more functional permission management structure. To find out the best way to introduce the new structure and how it will improve the permission management in the client organization. Firstly the current structure will be examined. Secondly the existing structure will be remodeled to meet the needs of the client organization and to support role based permission structures. Thirdly the new permission management structure will be implemented as a part of the permission management system.

The study results in new permission management structure that can be implemented as a company wide solution for permission management but with little effort can also be used as a basis for enterprise wide solution to permission management. The value of this study comes from the saved time between the permission request and the time of permission delivery, the saved man hours in the permission request process and from increased information security as well as cutting the permissions that are not required for completing user's daily assignments.

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO
Tietotekniikan koulutusohjelma
ERONEN, ERPO: Oikeuksien hallintarakenteen uudelleensuunnittelu ja oikeuksien hallinnan automatisointi yrityksessä
Diplomityö, 47 sivua
Toukokuu 2015
Pääaine: Ohjelmistotekniikka
Tarkastaja: professori Hannu Jaakkola
Avainsanat: oikeuksien hallinta, hallintarakenne, suorituskyky, tietoturva

Työssä tutkitaan asiakasyrityksessä käytössä olevaa käyttöoikeuksien hallintajärjestelmää ja sen parantamista yksinkertaistamalla käyttöoikeuksien hallintarakennetta. Työn tavoitteena on tutkia minkälainen käyttöoikeuksien hallintarakenne sopii parhaiten asiakasyritykselle ja tutkimusten pohjalta toteuttaa halutunlainen rakenne.

Työssä käydään läpi käyttöoikeuksien hallinnan tarpeellisuutta, osia joista käyttöoikeuksien hallinta rakentuu ja uuden rakenteen implementointia, sekä siitä saatuja hyötyjä. Tutustumalla nykyiseen rakenteeseen selvitetään paras tapa luoda uusi käyttöoikeuksien hallintarakenne ja se miten uusi rakenne tulee parantamaan käyttöoikeuksien hallintaa asiakasyrityksessä. Tämän jälkeen luodaan uusi käyttöoikeuksien hallintarakenne saatujen tietojen pohjalta, ottaen huomioon roolipohjaisen käyttöoikeuksien hallinnan tuomat seikat. Toiminnallisuuden parantamiseksi uusi käyttöoikeusrakenne tullaan ottamaan käyttöön osaksi käyttöoikeuksien hallintaa.

Työn tuloksena saadaan käyttöoikeuksien hallintarakenne, joka voidaan ottaa yrityksessä käyttöön sellaisenaan ja pienillä muutoksilla voidaan laajentaa kattamaan myös muiden maiden organisaatiot. Rakenteen uudistaminen tuo säästöjä tietoturvan paranemisen, resurssien valvontaan käytettyjen työtuntejen vähenemisen ja päällekkäisten sovellusten karsimisen kautta.

PREFACE

This thesis has been conducted as a part of Andritz Oy's development project in the field of identity and access management. I would like to thank the Andritz Oy for the chance to conduct my master's thesis as a part of this project.

In addition I would like to thank my master's thesis examiner professor Hannu Jaakkola of all his guidance and wisdom during this project. Also I would like to express humble thanks for my mentor in this project Mika Metsärinne and my boss Markku Hyytiä for their unwavering support and the dream that this thesis would one day see the light of day. Also I would like to thank all the people in Andritz Oy who participated in making this thesis a reality. Last but not least I would also like to thank my parents for pushing me to become a better man and to finish what I had started, thanks guys I love you.

Tampere 5.5.2015

Erpo Eronen
Väinölänkatu 24 as 8
33500 Tampere
Finland

TABLE OF CONTENTS

1. Introduction 1
1.1. Research methods 2
1.2. Goals of the thesis 2
1.3. Structure of the thesis 2
2. Identity and access management 4
2.1. Identity management 5
2.1.1 User management 7
2.1.2. Password management 7
2.1.3. Provisioning 7
2.1.4. Delegated administration 8
2.1.5. Role management 9
2.1.6. Self-service 9
2.2. Central user repository 10
2.2.1 Meta-directory 10
2.2.2. Directory 10
2.2.3. Data Synchronization 11
2.2.4. Virtual Directory 11
2.3. Access management and authorization 12
2.3.1. RoBAC 12
2.3.2. RuBAC 15
2.3.3. ABAC 16
2.4. Authentication 17
2.4.1 Single Sign-on 17
2.4.2. Password service 18
2.4.3. Session management 19
2.4.4. Strong authentication 19
2.4.5. Remote authentication 19
2.5. Information security 20
3. The client company 21
4. Identity and access management in client company 23
5. User study 27
5.1. Challenges with the current structure 27
5.2. Performance issues of the current system 30
5.3. Working features of the current system 31
5.4. Requested improvements 31
6. New permission management structure 33
6.1. Designing the structure 33
6.1.1. Service catalog 34
6.1.2. Organization structure 34
6.1.3. Processes to consider 35
6.2. Creating the new structure 36
6.3. Implementation 39
6.4. Management 40
7. Summary 41
7.1. Further Development 41
7.2. Integrating software to access management system 42
References 44

ABBREVIATION AND TERM LIST

ABAC – Attribute Based Access Control
AD – Active Directory
AG – Aktiengesellschaft (German word for a corporation limited by share ownership and that may be traded on a stock market)
BOYD – Bring Your Own Device
CEO – Chief Executive officer
HR – Human Resource
IAM – Identity and Access Management
ID – Identity
IdM – Identity Management
IP – Internet Protocol
IT – Information Technology
LDAP – Lightweight Directory Access Protocol
LLC – Limited Liability Company
MDF – Medium-density Fibreboard
OY – Osakeyhtiö (Finnish word for a corporation limited by share ownership and that may be traded on a stock market)
RFID – Radio Frequency Identification
RoBAC – Role Based Access Control
RSA – Rivest, Shamir, Adleman Algorithm
RuBAC – Rule Based Access Control
SSO – Single Sign-on
UML – Unified Modelling Language
VPN – Virtual Private Network

1. INTRODUCTION

As functionality of an organization becomes more dependent of the information technology the solutions used for the identity and access management (IAM) are also playing increasing role in a company's daily functions. Despite the fact that identity and access management provides a good business case in terms of a saved labor costs and increased security it is often considered as IT operation. This makes it hard to get the business involved in terms of a costs and workload that goes into build a working identity and access management system. Research published by Gartner shows that the time for new employer to gain all the required accesses and tools to complete his work can take up to three months, while the median time is six weeks. This is six weeks of people not being able to do their daily assignments and according to research this adds the labor costs of the company upwards from 100 000 € each year for a company of around 15 000 employees. Identity and access management is also about protecting the immaterial property of the company, when it is possible to control the tools and resources inside the company effectively the company is less likely to face a data theft or an unauthorized access. These are the main benefit of well-structured identity and access management system. (Gartner, 2013)

In order to implement a working identity and access management system there are some prerequisites. Company has to have ways of identifying users logging in the company computers, there must be a system that allows files being made available for only the people who really need the information, and in addition the supervisors have to be aware of the needs of their employees. There are several systems that make managing these prerequisites easier such as Single Sign-On (SSO), Role Based Access Control (RoBAC) and Meta directories such as Microsoft Active Directory, rest will be introduced throughout the thesis. Meta directories make it possible for administrators of the network to grant and deny access to specific files and folders and even the network itself. RoBAC systems are used to identify the needs of certain roles within the company, for example salesmen can be offered a remote working solutions and software and file shares that make it easier to present why the client should choose a this particular supplier. SSO solutions are there just to make end users life easier when the need of remembering all passwords is omitted and users only need to remember one password to get the access to all the systems they have an access to.

1.1. Research methods

This Master's thesis uses two main research methods. Interviews with some key figures working on different fields of the company and literature research. Most of the theory comes from literature research. Information used to complete this research comes from articles, books and documentation from IAM system vendors/consults. In addition, there are several researches that were commissioned by Andritz Oy in order to complete this research. Information regarding the client is gathered from the internal websites of the company and can be found more inaccurately from the Internet.

The theory gathered for this thesis will be compared to the surveys which were conducted in order to gain further knowledge of the IAM and to determine the new IAM structure and the means to implement it in the company's information technology (IT) operations. The first survey was made by Propentus Oy the survey's focus was to gain further knowledge of the current IAM and to develop it. The second survey was made within the company and it was targeted to the key users of the IAM system. It contained questions about the usability of the product, suggestions for a new IAM structure, overall pros and cons, and open word where users could give feedback and suggestions regarding the whole system. For the second survey 24 key users of the IAM system were interviewed in order to get a deeper understanding on how the end users see the system. (Propentus Oy, 2013)

1.2. Goals of the thesis

This thesis aims to create a new, better suited and more optimized identity and access management structure for Andritz Oy. The new structure will be tested by Andritz Oy Finland in order to cut costs and time consumption that occurs when new employee is hired to the company. After successful tests the new structure could be implemented as a company-wide system for identity and access management. However the main goal is to make the hiring and access granting processes within the company more flexible and less time consuming.

1.3. Structure of the thesis

Chapter 2: Identity and access management is the theory part of this thesis that gives an overall insight to identity management: what can be accomplished by having and identity management system in place and the risks of not having a functioning identity management solution. This chapter also explains what is needed for working access management system and the benefits of such system. The problems presented in this chapter are the ones every organization involved with implementing an identity and access management system have

to deal with. The information presented here is gathered from literature and surveys made by companies providing identity and access management services. The concept of identity and access management is being used as the baseline for the whole thesis with other chapters giving some additional information about support systems used with identity and access management and how an IAM works in a large enterprise organization.

Chapter 3: answers the questions about company's business area, geographical- and employee structure, in order for reader to get a better picture of the challenges that the enterprise organization sets in terms of identity and access management.

Chapter 4: Identity and access management in client company chapter illuminates how the IAM is done in Andritz Oy and what features are used for the best user experience possible without compromising the safety of company data.

Chapter 5: User study analyses the information gathered for this thesis from client's organization. The Chapter consists of four parts: challenges with the current structure, performance issues with current system, working features in current system and requested changes in the system. The goal is to determine how to improve the existing IAM solution used in the client company.

Chapter 6: New permission management structure gives a deeper insight to the future of identity and access management in the client company by going through some key features that build up to working identity and access management system. These findings and changes play an important role in client's identity and access management solutions.

Chapter 7: Summary features the conclusions this project brought up, the actual outcome of the project, some ideas the client has for the future of this project and how the system could be implemented as an enterprise wide solution for IAM.

2. IDENTITY AND ACCESS MANAGEMENT

Identity and access management is one of the major factors in terms of information security. IAM describes processes and technologies that allow an organization to identify accurately their users and the resources they are able to access. In small companies the need for managing users can be almost non-existent, although this is linked directly to the amount of resources the company has. In large companies and businesses where the use of subcontractors and other temporary workers is more common, managing users can be a daily nightmare. (Rich, 2014)

Describing identity and access management is simple, and anyone can say how it should work. Implementing an IAM to a company in a practical, time- and cost-efficient way is a whole lot harder. Company that has hundreds of resources and thousands of workers, will find out that keeping track of those can be impossible or at least extremely challenging task, when company opens its resources to subcontractors and business partners the problems grow even bigger. (Rich, 2014)

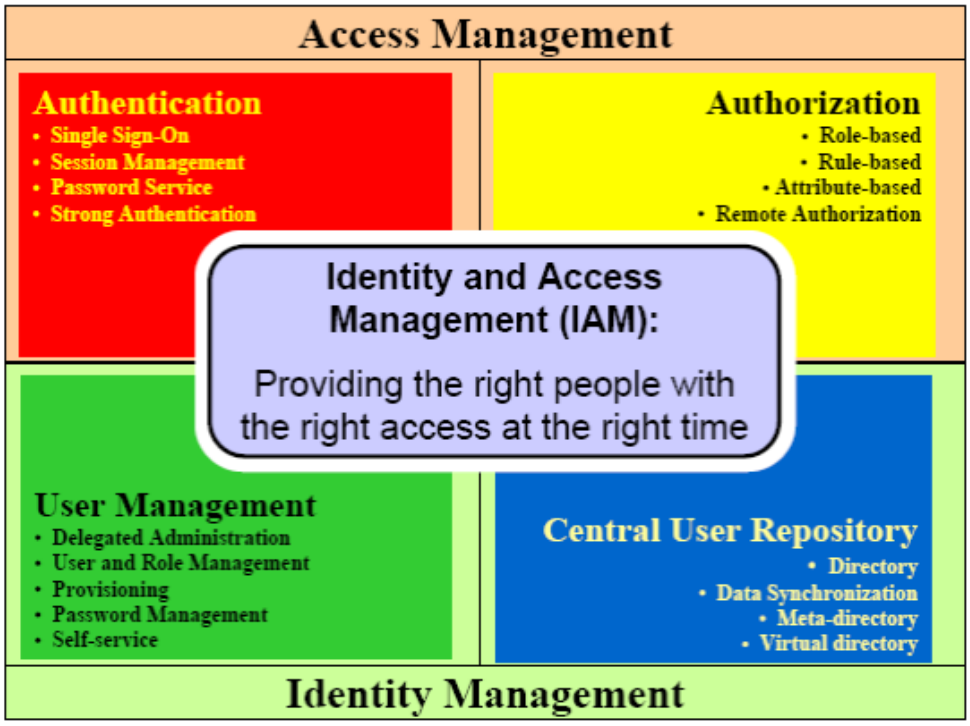

Figure 2-1. What is identity and access management (ITS of HKPolyU, 2009)

Previous figure (figure 2-1) illustrates the core components of both identity and access management and sums the goal of most IAM projects into one sentence. Because of the simplicity of the figure and overall coverage of what is normally considered to be IAM this figure will also act as a rough structure for this chapter. (ITS of HKPolyU, 2009)

2.1. Identity management

Identity management (IdM) is administrative area that deals with the management of individual identifiers in the system (such as an enterprise, a network or a country). There are five main components to IdM which are user management, password management, provisioning, delegated administration and role management. In some instances it is also seen to cover authentication, but in this thesis the authentication is treated as an individual entity. The identity management targets for increasing security and productivity while decreasing cost, downtime, and repetitive tasks. (Identity management task force, 2008)

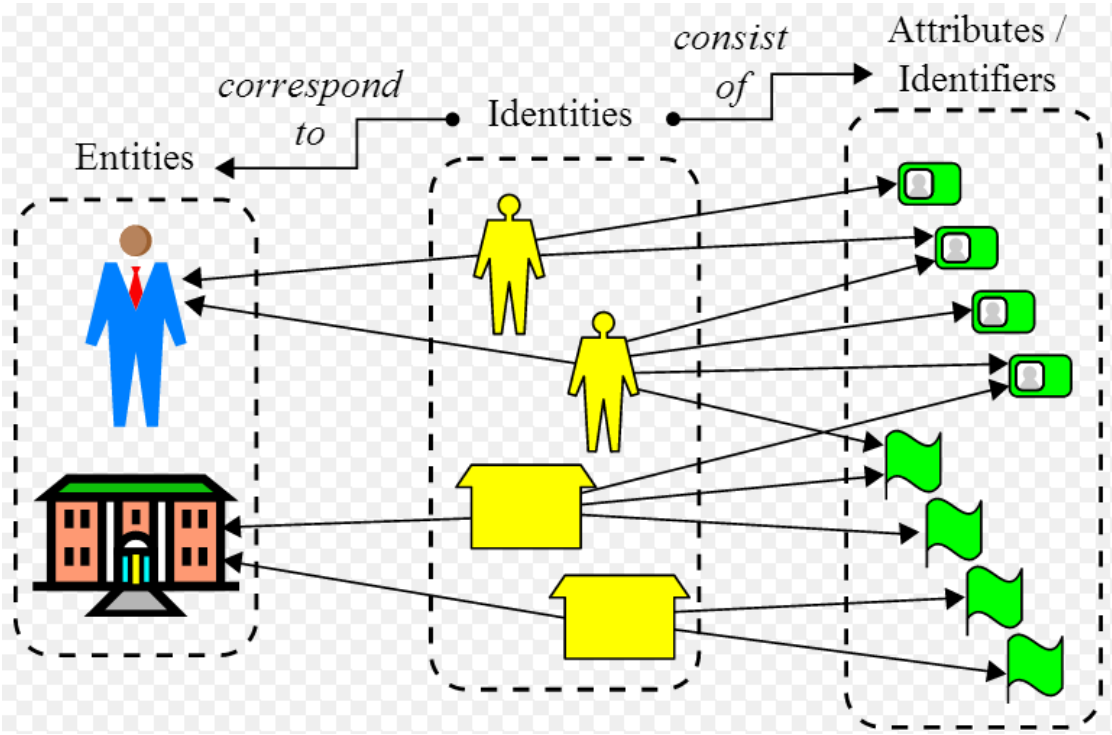

Figure 2-2. Concept of Identity (Wikipedia, 2015)

Reason for IdM is the organizations need for a single integrated, authenticated, and universally accessible identity management system which can be used as a database against which the users are authenticated or against which the salaries are paid. Many organizations are striving to achieve a centralized and decentralized IdM implementation that eliminates the inefficiencies and vulnerabilities of independent decentralized approaches. A unified infrastructure will provide centralized, highly automated capabilities for creating and managing trusted user identities. It allows administrators to define user access rights with a high degree of flexibility and granularity, in keeping with business goals and security policies. It also validates identities and enforces rights and policies consistently across the enterprise, thereby further enhancing security and supporting compliance requirements. RSA defines IAM as "an integrated system of business processes, policies, and technologies that enable organizations to facilitate and control user's access to critical online applications and resources — while protecting confidential personal and business information from unauthorized users." (Krause, 2006)

For security reasons, tools for managing identity management should run as an application on a dedicated network appliance or server, either on-premises or in the cloud. At the core of an identity management system are policies defining which devices and users are allowed on the network and what a user can accomplish, depending on his device type, location and other factors. All of this also depends on appropriate management console functionality, including policy definition, reporting, alerts, alarms and other common management and operations requirements. An alarm might be triggered, for example, when a specific user tries to access a resource for which they do not have permission. Reporting produces an audit log documenting what specific activities were initiated. (Krause, 2006)

Many IdM systems offer directory integration, support for both wired and wireless users and the flexibility to meet almost any security and operational policy requirement. Because bring your own device (BYOD) is getting more common in today's business world, time-saving features such as automated device onboarding and provisioning, support for a variety of mobile operating systems and automated device status verification are becoming common. (Gartner, 2013)

Previously mentioned five processes that IAM consists of can be companied by self-service feature for user and role management, this will allow users to perform simple tasks such as password recovery, applying for roles and changing their personal information among other things. With all the parts of IdM in place it is possible for a company to execute a successful user account policy that is robust, adaptable to change and easy to keep up to

date all at the same time. Following chapters will explain aforementioned processes and the role they play in the whole IAM system. (Gartner, 2013)

2.1.1 User management

User management is the feature that allows an employee to be granted with a user account that is used for the IAM process and to keep a track of users working for the company. When a new employee starts in the organization they are normally given an ID number and if they are using company computers the unique username and corresponding password are also created. The identifiers mentioned above allow user to gain an access to company computers and some files alike. ID number is also considered as a prerequisite for the company to start paying salary to an employee. In order to institute a working user management solution an integrated workflow capability is also required, this is used for approving some user actions such as provisioning and de-provisioning. (Blue Coat Systems inc., 2007)

2.1.2. Password management

Password management feature is important factor in making sure users use passwords that are safe enough for the internet use and that the passwords are changed frequently to avoid the data thefts that can go on for years. Password management sets the rules for password lengths, the type of characters passwords need to include for them to be accepted to be used in company network and the rules of not allowing the use of same exact password too often. (Tipton & Krause, 2007)

Rules for passwords are monitored when passwords are created or changed and they can include the mandatory use of capital letters, numbers and special characters, they can also define the amount of previous passwords that your new password must differ from before it is possible to use the same password again. Managing passwords is highly automated function conducted by authentication server according to the rules determined by the system administrator. (Tipton & Krause, 2007)

2.1.3. Provisioning

In IdM provisioning means the creation, maintenance and deactivation of user objects and -attributes, as they exist in one or more systems, directories or applications, in response to automated or interactive business processes. Software used for user provisioning usually includes one or more of the following processes: consolidated user administration,

delegated user administration, federated change, self-service workflow, and control change propagation. Employees, partners, vendors, contractors, customers or other recipients of a service are presented as user objects. Services may consist of inclusion in a published user directory, e-mail or access to a database, network or mainframe. Provisioning is particularly useful within organizations, where users may be represented by multiple objects on multiple systems. (Wikipedia, 2015)

2.1.4. Delegated administration

For organizations employing thousands of people one of the biggest challenges is dealing with data access, systems, applications, and networks when employees are hired, moved within the organization, or terminated. This challenge is compounded for external users, such as contractors, vendors, partners, and customers. Complexity of delegated administration presents linear correlation between size/scatteredness of the company and increasing complexity of delegated administration. Successfully applying delegated administration as part of end to end IAM process, will allow users obtain system and application access more quickly, thereby becoming more effective and productive as quickly as possible. Good management represents a cost savings to the organization and can provide a demonstrated return on investment. The challenge is even greater for organizations that are highly distributed with independent functions doing the granting and the management of account. It is even more complex when parts of the administration function are centrally managed and other parts are de-centrally managed. Another complexity is presented when employees move between sites or have access to multiple individual business units within one larger entity, these problems are mainly experienced by members of a larger corporations. (Tipton & Krause, 2007)

One of the most important changes to an account or a user profile occurs upon termination. It is imperative that terminated employees be immediately removed from the system or, at least that their access be immediately terminated. In cases of suspension, after completion of file cleanup and fulfillment of delegated responsibilities and other administrative processes, actual deletion of the account should quickly follow. In highly decentralized and distributed organizations, supporting many applications and systems, it is important to coordinate the termination and account revocation process centrally and to automate this process to the extent feasible. It is also imperative to have a human resource (HR) system interface to the IdM system to compare the IdM database to the HR database to highlight and react to changes. This functionality may be provided by another meta-directory such as Microsoft’s Active Directory (AD) as long as it is the designated and established authoritative source. (Gartner, 2013)

2.1.5. Role management

As soon as the user starts working for a company he is added to the company database with distinctive information from name to bank account number. User is also granted with a job title based on his standing in the company and the kind of work he does. In most cases the job title can also be considered as user's role in a company. Managing the user and role information is not done on daily basis because these are the type of information which is not that likely to change as rapidly and often as for example the network resources the person needs to get the job done. (Lehnert, 2010)

The reason for role management is to ensure that the information regarding user roles is up to date because these roles are used to determine the level of access the user is granted with, while using role based access control. Removing the role from a user is also the easiest way to cut down their access in case of a termination of the contract or other similar situation when user no longer should have the access to sensitive company data. Also the biggest security threat for companies is usually the one that comes from inside and with proper role management this can be reduced greatly since users do not have an access to data they should not have seen in the first place. (Oracle, 2013)

2.1.6. Self-service

User management self-service model relies on end users IT-awareness because if this type of service is implemented as a part of the IT infrastructure users are given some moderation privileges to the systems that are traditionally been under the IT or HR departments supervision. However when using information from the HR or IT departments the information could have changed over the course of time without these entities knowing it which would cause the data to be outdated and therefore useless. Allowing users to update their personal information such as phone numbers, division information, work and home addresses, job titles and so on, the information can be kept up to date more effortlessly because people are normally more aware of their own information than the company servers where not all the information is logged. Also providing users with a service where they can open locked user accounts for example in case of a forgotten password and too many attempts, can significantly reduce the workload of the IT-department, however implementing this type of service would need strong authentication to allow unlocking the account and changing the password, but since personal ID cards have become more common it should not be hard thing to set up at least for the companies using the aforementioned technology. (Gamby, 2010)

Self-service user management is not however the perfect solution, it is true that the boxes of up to date and more accurate information can be checked by allowing users to participate in collecting this data but there are also some problems that may arise from implementation of self-service user management. The human nature however brings out some flaws in this functionality. It is known that some people are competitive by nature and for them being able to change their job title in the system may come as a tool to highlight their standing in the organization or even modify their actual job title to correspond the one they think they are entitled to. For example in a situation where the company is using automated RoBAC that compares user's job title from the user information database with list of roles and automatically grants user the access based on their changed role. Activity like this could cause the user to have access to files they were not supposed to have rights to, here by compromising the security of the data. (Gamby, 2010)

2.2. Central user repository

Central user repositories are used to store and deliver identity information to other services, while also providing a service for verifying user credentials sent by the client. Central user repository provides an aggregate or logical view of identities of an enterprise. The central user repository is most commonly built on LDAP directory server where it gets all the information it needs. The following subchapters introduce the central components and features of central user repository. (ITS of HKPolyU, 2009)

2.2.1 Meta-directory

Meta-directories are systems that provide the flow of data between one or more directory services and/or databases. Meta-directories are enterprise solutions for unification and central management of disparate directories. The idea of searching several databases for single piece of information is ineffective and time consuming, meta-directory addresses this issue by combining all the information from different directories and databases into one meta-directory which holds the information regarding the data location. When user searches for the information, meta-directory works as a middle man providing the user with wanted information using less of the resources than the traditional multi server search. (Wikipedia, 2013)

2.2.2. Directory

In its most simplified form directory is a table that consists of names and values. It can be used to lookup the values corresponding the names in the directory. Since one name can be

associated with more than one piece of information the size of directory is directly related to use of value fields. For example a phone book that only has name of a person and phone number is much smaller in size as the company directory that can hold over 20 different attributes for one person. Directory is a database that is used to store data in organized manner. The data in directory can be accessed using directory service software. (ITS of HKPolyU, 2009)

2.2.3. Data Synchronization

"Data synchronization is the process of establishing consistency among data from a source to a target data storage and vice versa and the continuous harmonization of the data over time." The process of data synchronization is used to make sure that all the systems have the latest data at their disposal. In the terms of user management the valid user information such as job title and division user is working for are business critical. Having outdated information regarding the user's work place can lead them to be given access to files they do not need or they should not be allowed to access, it can also cause the user not to have sufficient access to files and resources they would need the access to get the job done. (Roebuck, 2011)

In addition to user management the data synchronization between end user devices and company servers plays major role in case of an hardware failure, if data between end user device and server has been done all the important data can be saved from the server and this can save days or even weeks of work for the company. Data synchronization is commonly described as the most useful information security function in case of a major disaster or hardware failure, because it allows company to rebuild its databases from the last restore point rather than from the ground up. (Gartner, 2013)

2.2.4. Virtual Directory

"A virtual directory or virtual directory server is a software layer which delivers a single access point for identity management applications and service platforms." A virtual directory operates as lightweight abstraction layer that offers high-performance and resides between client applications and different types of identity-data repositories, such as proprietary and standard directories, databases, web services, and applications. (Wikipedia, 2014)

Virtual directory works as a middle man receiving queries and directing them to the appropriate data sources by virtualizing and abstracting data. The virtual directory gathers

the identity data from multiple data stores and re-presents it as though it were coming from only one source. Ability to reach into different kinds of repositories makes virtual directory technology ideal for consolidating data stored on multiple servers and in a distributed environment. (OptimalIdM, 2014)

2.3. Access management and authorization

Access management is concept for making sure that the resources are only accessible for those who have been granted with the sufficient level of access. In order to apply access management into the system the users accessing the resources must be identified. Without identification there is no information about the user trying to access the data which makes it impossible to determine if the user actually needs an access to resources he is requesting. (Tipton & Krause, 2007)

There are many ways to determine which files and resources the user gets the access to, these include role based access control, rule based access control and attribute-based access control. Before the users are granted an access to company network they must be authenticated which can be done using the username and password combination, ID-card and password combination or some other form of authentication available. Following subchapters will cover the previously mentioned authorization methods in more in depth manner, with an emphasis on Role-based access control. (Tolone, Ahn, Pai & Hong, 2005)

2.3.1. RoBAC

Role-based access controls define who or what process may have access to a specific system resource, and it can also determine which type of access is permitted and the ones that are rejected. These controls can be implemented in destination system itself or in external devices which will oversee the access control. In role-based access control, access is granted based on the roles that individual users have within the organization. Users are assigned roles (such as salesman, HR-manager, designer, secretary). The process of defining roles should include input from all departments of an organization and should be based on a thorough analysis of how an organization operates. UML model of RoBAC is pictured below (figure 2-3) and explained in more in-depth manner in following chapters. (Shuriya & Sumathi, 3/2013)

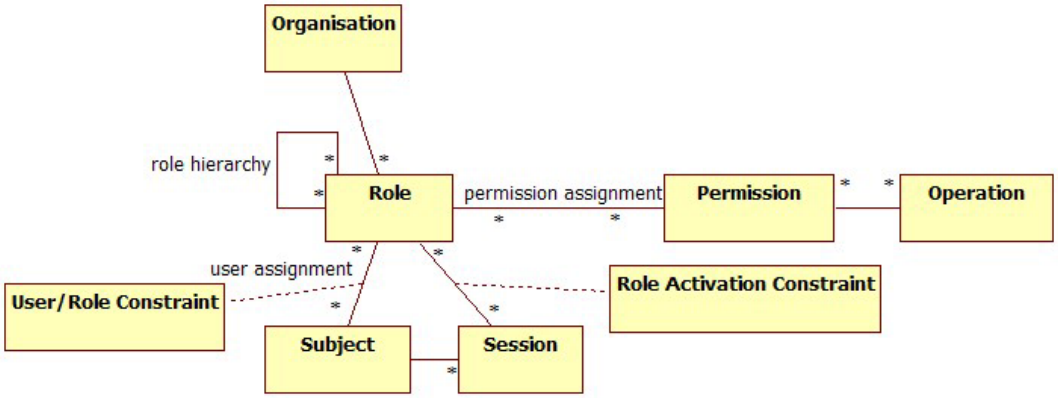

Figure 2-3. UML model of RoBAC (CSDN.NET, 2012)

Access rights are grouped by role name, and the use of resources is restricted to individuals who has the role associated with given resource. For example, HR-manager can have access to salary records, personal information of employees and a tools for hiring new employees; whereas salesman does not have any access to HR tools, but can have variety of project documents and tools for calculating structural strengths and prices for the product and maintenance deals. Roles can be used to control access in effective manner but also for developing and enforcing enterprise-specific security policies. Having well defined roles for access control can also streamline the security management process. (Kizza, 2008)

General RoBAC framework defines that users are granted membership into roles based on their competencies and responsibilities in the organization. Permissions the users are given are based on role they were assigned to. User roles can easily be revoked and new roles assigned as the position within organization changes. Role associations can be established when new operations are instituted, and old operations can be deleted as organizational functions change and evolve. This helps to simplify the administration and management of privileges, because this eliminates the need for updating individual privileges and allows updating of right centrally through existing role. (Kizza, 2008)

RoBAC aims for concept of least privilege which means that user roles associated with users give no more privileges than what is necessary to perform their jobs. There are some prerequisites for using the concept of least privilege such as identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more. In systems that are not effectively controlled, this is often difficult or costly to achieve. It is difficult to tailor access based on various attributes or constraints and this can result in employee being

granted more privileges than needed for their job category. Overlapping responsibilities between job categories, could cause maximum privileges being granted for each job category which in turn could cause unlawful access. (Kizza, 2008)

RoBAC allows users to have roles which can have overlapping responsibilities and privileges. This is made possible because, users belonging to different roles may have common operations they need to perform. Normally there are some general operations which be performed by all employees (such as working hour reporting and travel expense reporting). Regarding general operations, it would be inefficient and administratively cumbersome to apply these general operations for each role new that gets created. Role hierarchies can be sculpted to adapt the natural structure of an organization. A role hierarchy is used to define roles that have unique attributes and which could contain other roles; that is, one role may implicitly include the operations associated with another role. (Ferraiolo, Kuhn & Chandramouli, 2003)

Role hierarchies are a natural way of organizing roles to reflect authority, responsibility, and competency: a user can be assigned to multiple roles at the same time depending on accesses needed for the job position and responsibilities the user has. Previously mentioned operations and roles can be made a subject to organizational policies or constraints. Hierarchies of roles are usually established, when operations overlap. Role hierarchies allow organizations can put constraints on access through RoBAC, instead of instituting costly auditing to monitor access. For example, it may seem sufficient to allow secretaries to have access to all project data records if their access is monitored carefully. With RoBAC, constraints can be placed based on secretary's access so that only those records that are associated with a particular secretary's location can be accessed. (Ferraiolo, Kuhn & Chandramouli, 2003)

An operation represents a unit of control that can be referenced by an individual role, subject to regulatory constraints within the RoBAC framework. An operation can be used to capture complex security-relevant details or constraints that cannot be determined by a simple mode of access. For example, there are differences between the access needs of a teller and an accounting supervisor in a bank. A company defines a teller role as being able to perform a savings deposit operation. This requires read and write access to specific fields within a savings file. A company may also define an accounting supervisor role that has teller's privileges of seeing account information, however the accounting supervisor may not be allowed to initiate deposits or withdrawals but only perform corrections after the fact. Likewise, the teller is only allowed to initiate deposits and withdrawals, but not to perform any corrections once the transaction has been completed. The difference between

these two roles is the values that are written to the transaction log file and also the operations that can be executed by the roles. (Ferraiolo, Kuhn & Chandramouli, 2003)

The RoBAC framework provides administrators with the capability to regulate who can perform what actions, when, from where, in what order, and in some cases under what relational circumstances: only those operations that need to be performed by members of a role are granted to the role. Granting of user membership to roles can be limited. Some roles can only be occupied by a certain number of employees at any given period of time. The role of manager, for example, can be granted to only one employee at a time. Although an employee other than the manager may act in that role, only one person may assume the responsibilities of a manager at any given time. A user can become a new member of a role as long as the number of members allowed for the role is not exceeded.

RoBAC system that is administered properly enables users to carry out a broad range of authorized operations, while providing great flexibility and breadth of application. This allows system administrators to control access at a level of abstraction, natural to the way that enterprises conduct business. This is achieved by establishing and defining the roles, role hierarchies, relationships, and constraints that statically and dynamically regulate users' actions. After the RoBAC framework is established for an organization, the main objectives are keeping role descriptions up to date and the granting and revoking of users into and out of roles. Compared to more conventional user access management where access is controlled object-by-object basis this requires more work to get started, but in exchange offers centralized and companywide access control. (Roberts, 1999)

Further, it is possible to associate the concept of a RoBAC operation with the concept of "method" in Object Technology. This association leads to approaches where Object Technology can be used in applications and operating systems to implement a RoBAC operation. For distributed systems, RoBAC administrator responsibilities can be divided among central and local protection domains; that is, central protection policies can be defined at an enterprise level while leaving protection issues that are of local concern at the organizational unit level. For example, within a distributed healthcare system, operations that are associated with healthcare providers may be centrally specified and pertain to all hospitals and clinics, but the granting and revoking of memberships into specific roles may be specified by administrators at local sites. (Kizza, 2008)

2.3.2. RuBAC

The basic idea of Rule based access control (RuBAC) is very much alike the idea behind the role based one, but with the one major difference, the rule based access control relies on

list of access rules that define the users that are allowed to access a certain file or folder. Keeping rule list of every single folder is massive task and it requires a very well established server administration. RuBAC is often disregarded as an option to deliver a functioning and secure access control, because implementation and administration of it in large company can prove to be an impossible task. (Brachman, 2006)

RuBAC is best fit for smaller companies where not as many rules have to be applied to gain the desired results. Also for large companies with active and hand on approach to administrating their IT systems could see RuBAC as a valid option, however it would require least one person working fulltime updating the rulesets. (Gentry, 2012)

2.3.3. ABAC

Attribute-based access control (ABAC) is a so called next generation access model which provides, context-aware and risk-intelligent access control. ABAC helps to achieve efficient regulatory compliance, effective cloud services, reduced time-to-market for new applications, and top-down approach to governance through transparency in policy enforcement. (Axiomatics, 2014)

“ABAC uses attributes as building blocks in a structured language that defines access control rules and describes access requests. Attributes are sets of labels or properties that can be used to describe all the entities that must be considered for authorization purposes. Each attribute consists of key-value pair such as “Role=Service Engineer”.” (Axiomatics, 2014)

The following figure shows how ABAC combines the best of both RoBAC and RuBAC with adding some unique features to the process. Use of several attributes in implementation of access control will make the setting ABAC even more demanding and resource consuming task than setting up its predecessors but one can be sure to get most out of their access control when it the ABAC has been successfully set up. (Radhakrishnan, 2012)

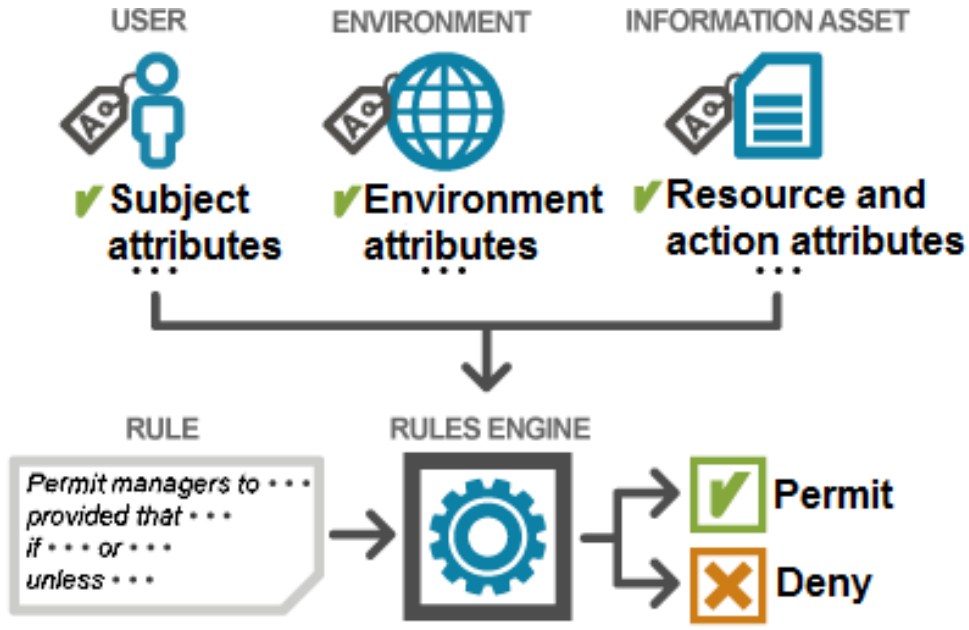

Figure 2-4. How attribute-based access control works (Axiomatics, 2014)

2.4. Authentication

Authentication is a process of identifying an entity or validating the truthfulness of an attribute. In IT the authentication is most commonly used in validating the identity of a user or truthfulness of data. In access management when authentication is discussed it always means validating the user to be who he claims to be, this is commonly done by requesting username and password from the user. These days however it is common for a company to apply more than one form of authentication before the user is granted access to data and this can be done for example by requesting user to present a physical keycard that allows user to access their workplace or some digital authentication method that defines which files or resources user is allowed to access. (European commission study, 2013)

2.4.1 Single Sign-on

Single sign-on is a technical functionality that allows a user to move from system to system or application to application without having to re-enter authentication credentials every time. There are several ways to implement this functionality. Two common ways are to rely heavily on the directory and constantly refer to it for authentication information or by implementing an authentication system such as Kerberos. Implementation of single sign-on should be conducted in secure manner or it may have audit and security implications. A

password or credential that is compromised will equate to a breach of all systems or applications the user is authorized to access. When adequate security controls are implemented with the single sign-on solution, there will be no audit impact. (Authentication world, 2006)

Implementing an SSO feature to company systems is not going to bring any direct cost benefit for the organization, but there will be an enormous perception of benefit from the users and it could help with administrative workload that comes from users forgetting individual passwords. Users will be thrilled not to type in their password all the time or remember multiple passwords, and they will view this as a significant time savings. The client company is currently using Evidian SSO for single sign-on operations for these purposes. (Gartner, 2013)

2.4.2. Password service

The password management features of IdM are the most attractive to organizations, and many enterprises have third-party self-service password reset tools that enable users to change their own passwords upon expiration or to reset passwords when they have forgotten them and have locked themselves out of the system. Self-service password management makes it possible for users who have forgot their passwords to authenticate themselves via an alternative method and if successful then given an access to the password reset function. In the case of a forgotten password, the tool requires the user to enter the answers to a predetermined set of questions or predetermined e-mail address or phone number where the restored password can be sent. Controls should specify the number of times a user can enter an incorrect answer before locking the user account or alerting the system administrator for manual intervention. The answers must be kept secure and treated like sensitive information, with limited access and audit and monitoring enabled. (Scarfone & Souppaya, 2009)

Third-party self-service password reset tools are most commonly adapted to enterprises in which a large percentage of help-desk calls are for password resets. The tools not only reduce the cost of end-user support but also provide a more secure method for resetting a password, because user or requestor identity is authenticated through the prompting for private information, provided earlier by the user. Manual password changes to the help-desk are frequently not authenticated without an automated password management process. This practice is not compliant and is heavily subjected to security compromise and error. (Scarfone & Souppaya, 2009)

2.4.3. Session management

Session management tools are used to track unexpected disconnections, session time, logon attempts and it can be activated to track all the moves user is performing while session is active. The general use of session management covers the amount of failed access attempts, session time normally set for security purposes so that no one is capable to work on company servers and steal data endlessly if they only have one strong authentication password combination at their disposal. (Gartner, 2013)

Session management function brings increased security and traceability of company data to the identity and access management systems with almost no effort and man hours required in exchange. It has been debated that since the easiest way for users to steal company data is via VPN connection that is not monitored, the efficiently executed session management could be the best way to stop data from leaking to the unwanted third parties. (Gartner, 2013)

2.4.4. Strong authentication

Strong authentication also called as two-factor authentication is a way of double checking users credentials using a some form of additional identification that only the specific user has an access to, this can be RSA-key, passcode sent to a mobile device, an additional password list or today pretty much anything from ID chip card to implanted RFID tags. The idea of strong authentication is to make unauthorized access to sensitive company data harder for the intruders without making the authentication process much harder for end users. (Rosenblatt, 2013)

The traditional authentication relies on single password, which in worst case can allow an intruder to have a company wide network access. The problem with single password solutions is the fact that a single password can easily be obtained by hacking or phishing, but if the authentication requires a secondary key that is connected to user with some physical element like phone, RSA-key, ID-card, password list or other such solution it is much harder for intruder to get their hands on and in most cases it would require them to physically steal something from the user. (Rosenblatt, 2013)

2.4.5. Remote authentication

Remote authorization is way of making resources available for users that cannot connect to the company network. Remote authorization can be done in many ways, but it is normally reserved for the users who are known to travel off-site, for example there are not many

companies that automatically grant their office assistants with remote access to the company network. Certificates are one of the easiest ways of delivering remote authorization for devices on top of which user should always be authenticated using strong authentication methods. (Oracle, 2010)

2.5. Information security

According to a recent research conducted by Lawless Research LLC the most common reason for company to have an IAM solution is improved security of their credentials with 60% of companies stating this to be the main reason an IAM solution was implemented. When the newly implemented IAM solutions and ongoing IAM projects are considered the number of companies that stated the data security to be the number one reason for the implementation was 57%. This effectively proves how important a well-constructed IAM solution can be for company in a sense of improving information security. (Platt, 2013)

Information security itself consists from a set of measures and controls that are implemented to protect the information against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of data. Information security consists of all physical access and software functions, characteristics and features such as operational procedures, accountability procedures, and also access controls at the central computer facility, remote computer, and terminal facilities. Also managing constraints like physical structures and devices; and personnel and communication controls are needed to provide a required level of protection to minimize the risk for the system and for the data and information contained in the system. Information security should include the totality of security safeguards needed to provide a required protection level for the data handled by the company. (Slade, 2006)

3. THE CLIENT COMPANY

ANDRITZ Oy is a leading global supplier of systems, equipment and services for the pulp and paper industry including wood processing, fiber processing, chemical recovery, and stock preparation. In addition, ANDRITZ Oy offers biomass boilers and gasification plants for energy production. Total sales of the company is around EUR 600 million. Andritz Oy has around 1000 employees and somewhere around 300 subcontractors working around the globe. The Headquarters are located in Helsinki, Finland with side offices in Kotka, Tampere, Lahti, Savonlinna, Varkaus and Lappeenranta. Chairman of the Board of Directors is Dr. Wolfgang Leitner (ANDRITZ AG) and President and CEO Harry Rickman. The company is owned by ANDRITZ AG of Austria. The Andritz Group is a global market leader for customized plant, systems and services for the pulp and paper, hydropower, metalforming, steel and solid/liquid separation industries. In addition, ANDRITZ offers technologies for certain other sectors including automation, the production of animal feed and biomass pellets, pumps, machinery for nonwovens and plastic films, steam boiler plants, biomass boilers and gasification plants for energy generation, flue gas cleaning plants, plants for the production of panelboards (MDF), thermal sludge utilization, and biomass torrefaction plants. The Group is headquartered in Graz, Austria and has a staff of approximately 23,800 employees worldwide. It develops and makes its high-tech systems at production, service and sales sites all around the world. (Andritz Oy Intranet & Andritz AG, 2013)

Andritz Oy consists of 10 divisions and its business is divided to five regions, which are North America, South America, North Europe, Central Europe and Asia. Following chapters will introduce two of the biggest divisions in Andritz Oy. (Andritz Oy Intranet, 2013)

The Wood Processing Division is the world's leading supplier of systems, equipment and processes for all steps required in a wood yard - from the arrival of the logs to their subsequent preparation into wood chips – all the way to the production of chemical and mechanical pulps. The headquarters of the Wood Processing Divisions is located in Lahti, Finland. In addition, it has several sites abroad for example in USA, Canada and Brazil. (Andritz, 2013)

The Pulp Mill Services Division covers the service activities for the Wood Processing and Kraft Mill Systems Divisions. Primary emphasis is on production efficiency and availability, services (engineered wear parts, replacement parts, equipment rebuilds, shutdown services, service contracts and upgrades) to kraft pulp mills and woodyards supplied either by Andritz or other manufacturers. Apart from the traditional service business, the division works with its customers to maximize reliability and overall production efficiency, by providing added value services and innovative solutions. The Pulp Mill Services Division serves the large installed base of Andritz equipment all over the world. The main sites are located in North America and Europe, but there are local service centers in more than 30 countries worldwide. The headquarters for the Pulp Mill Services is located in Savonlinna, Finland. The Division has approximately 285 employees, from whom roughly 50 % in the USA, 40 % in Europe and 10 % in the rest of the world. The production facilities for rebuilds and parts are located in Finland and in the USA. In addition, the division has local rebuilt partner shops in New Zealand, Indonesia, South Africa, Brazil, and Portugal. (Andritz, 2013)

4. IDENTITY AND ACCESS MANAGEMENT IN CLIENT COMPANY

As many other systems the working IAM is a collaboration of several software solutions and implemented processes. Because of the aforementioned fact it is very hard to design a solution that would not get swamped over the changes in used software or when something new is added. The client company has over 1000 employees in Finland alone working with wide range of hardware from different vendors and with more than 100 different software excluding the different versions of these. This kind of environment adds its own challenges to the equation, because not all of the programs and solutions used are compatible with all the systems used for everyday tasks. The main idea of successful IAM is to be able to handle everyday tasks and the most common requests efficiently and even in great volatilities, but when the environment is not fully standardized the work needed to make such system work is greater. If IAM is successfully made part of the large company's IT systems it will also yield greater benefits because the amount of man hours that it saves are also greater than in smaller companies.

In order to achieve a functional IAM process several prerequisites must be met. There must be a way to track the identities, this can be done using LDAP servers which serve as meta-directories storing all the user information on the server and when authenticating checking that the information given on an end point device corresponds the information on the server. The matter of user having at least one user account they can be identified with makes it possible to move forward to the access management part of the process.

Access management starts when a new user is created into the human resource department's database. The creation of user now allows him to come to the work and go to his workplace. To make this physical access easier user normally also gets an electric key with which the user can go through the locked doors of the office. Even commonly mistaken as first level of access management the physical key to the office is already higher level of access management allowing the person to come and go as they please, mostly bound to some sort of a timeframe but without an escort. After the physical access to the workplace is granted for the person it is time to look things from the IT perspective of things. The physical paper documents are not regarded in this study because their existence

is gradually decreasing and because all the information that once was on paper is now stored on company servers, computer hard drives.

Accessing company's intranet or network resources would require a physical device which is allowed to connect to the company network and to gain this access person needs to have a user account which is normally created when person is stored into HR database. After user account is created and activated the person is able to access all the desktop and laptop computers in the company however giving them only a limited access to the company data since most of the projects are located on secure servers which can be only accessed by authorized employees. This level off access also allows a person to access company intranet with some documents for the internal use of the company. The data on the intranet is not business critical and therefore it is also available for people with lower level clearance to the company's data. This type of leveled approach is most commonly seen way of doing access management. Employees are only given a very restricted access to the company systems to begin with, but when they start working for different projects the required access rights are added for them to use.

After having a user account the person has possibility to make permission requests for the software, hardware, physical access to other offices, network resources and even the remote networking/virtual private network which allows them to work from home or anywhere like they were at the office. This is normally the phase when user starts making requests for the software they think they will need in their current job. Even not business critical by any means the access to software is one of the highest sources of costs in IT sector and therefore monitoring the access rights to the software is important and it allows the company to keep track of the amount of software licenses needed here by saving money when no unnecessary licenses need to be paid for.

After an access to required software is granted a user needs an access to files located on company servers. To get this a user is required to make a request for permission to access the files and/or folders located on the company servers. In this part of access management the key is to know what type of work the person is going to do for the project and adjusting their access rights accordingly. If a person is given too little access for the data needed in their job it might be impossible for them to complete the tasks assigned for them. But too much access can also lead to problems if a person is incompetent or they are trying to harm the company by destroying or modifying files based on false data. This is one of the main reasons why all the data on servers are backed up, because both intentionally and unintentionally caused harm can set a project back for couple minutes or in the worst case a whole day. This is the reason why only the people with absolute need to modify data on

project files are granted a full access to the files, rest of the project team is normally working with a read-only rights. Another issue is removing the access rights to the project files after the person is no longer working for the project. This is simply because if person is no longer working for the project he should not have any need to access the project files, this kind of situations are most likely to happen if person is changing companies and going to work for the competitor. In previously mentioned situation an employee might be tempted to grab some files regarding previous employers project in order to secure themselves a better pay or some additional benefits in the future company.

One of the most commonly used access types in today's world of endless remote working possibilities is VPN connection which allows user to access data on the company's network from pretty much anywhere in the world. Even the VPN technologies have changed over the years and these days can be used simply to provide a single program for remote user they are still commonly used to create a full VPN tunnel between the client computer and the company network. Some companies allow this type of connection to the company network from any computer with VPN client. General VPN connectivity overview is pictured on the next page (figure 4-1).

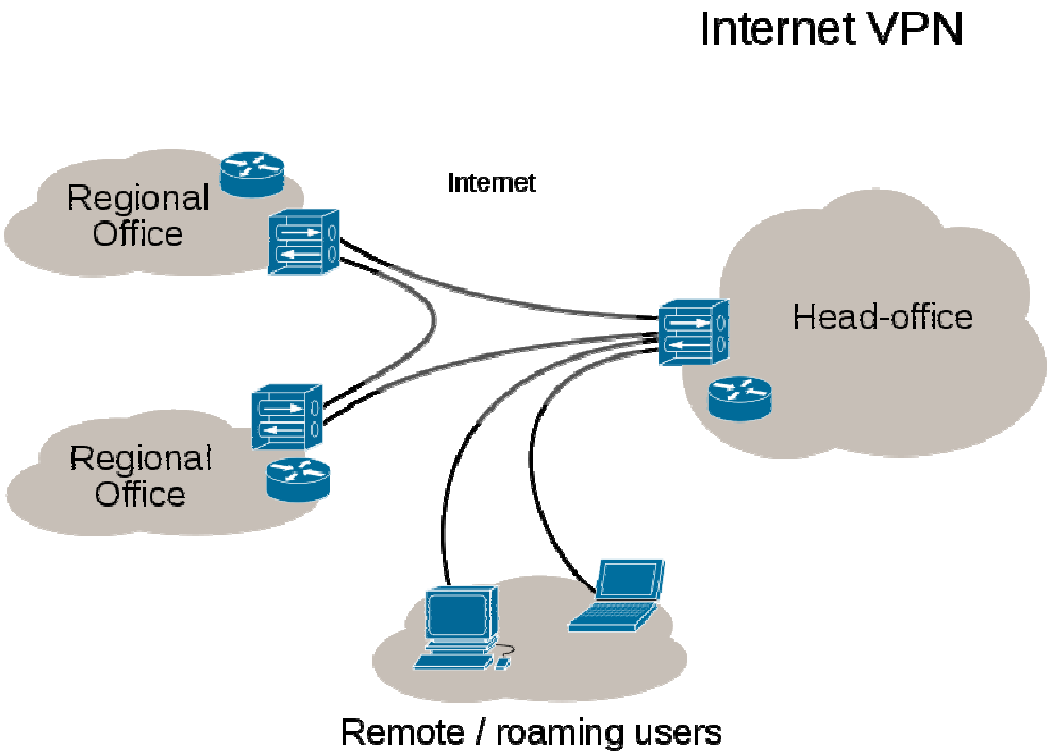

Figure 4-1. Overview of VPN network (Wikipedia, 2015)

If the company does not have an IAM solution that terminates user's access to VPN solution as soon as their contract end there is a chance that some users might look to gain access to confidential company data over VPN from their own devices even after they are no longer working for the company and this is just one of the many ways IAM solution is protecting the company that uses it. (Wikipedia, 2015)

5. USER STUDY

In order to gain further knowledge regarding the problems and the features that users found useful within the current permission management system, company decided to launch survey to heavy users of the system. The survey had a wide scope targeting all the business areas and the support functions. During the survey it came clear that the roll out of the current system had not gone the way it was supposed to and that was the main reason why people were put off by the whole system. However after the first version of the system it had improved drastically and currently it was almost tolerable to work with even though there were still some performance issues in the process especially when new employee was required to start work within a short time frame. The following chapters will explain the findings of the user study and provide a more detailed view to the pros and cons of the current structure.

5.1. Challenges with the current structure

During analysis of the data collected from the employees it was clear that the biggest problems the former structure had was that it had too many levels. Creating a new structure with fewer levels makes the whole structure clearer and easier to use for the employees after all they are ones who are going to be asking permissions through the system. Erasing levels from the old structure was not the hard job, but getting all the elements to match the new structure would not be easy because the systems are integrated and with fewer levels pinpointing the person who can grant user the requested permissions. Studies showed the reason why previous version of the system had so many levels was because the company was using both matrix management structure and tree management structure in its everyday tasks. Use of two different management styles is causing employees to have more than one immediate supervisor that led to the case where people were not sure which division or process they should apply the permissions under because in some cases even the supervisors would not know they had this person working for them.

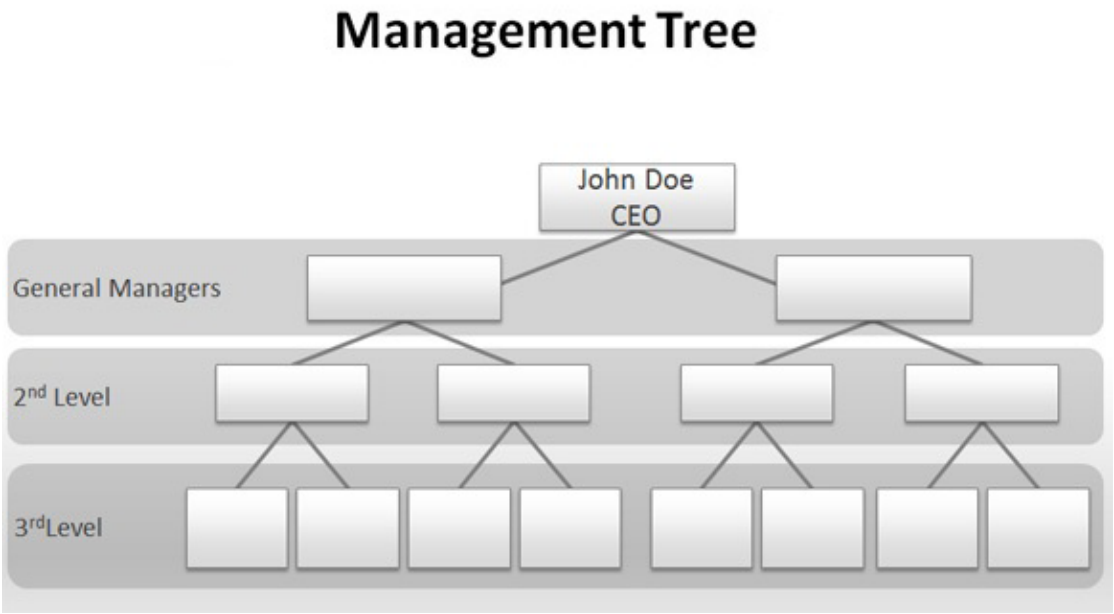

Figure 5-1. Management structure: Tree (fppt.com, 2015)

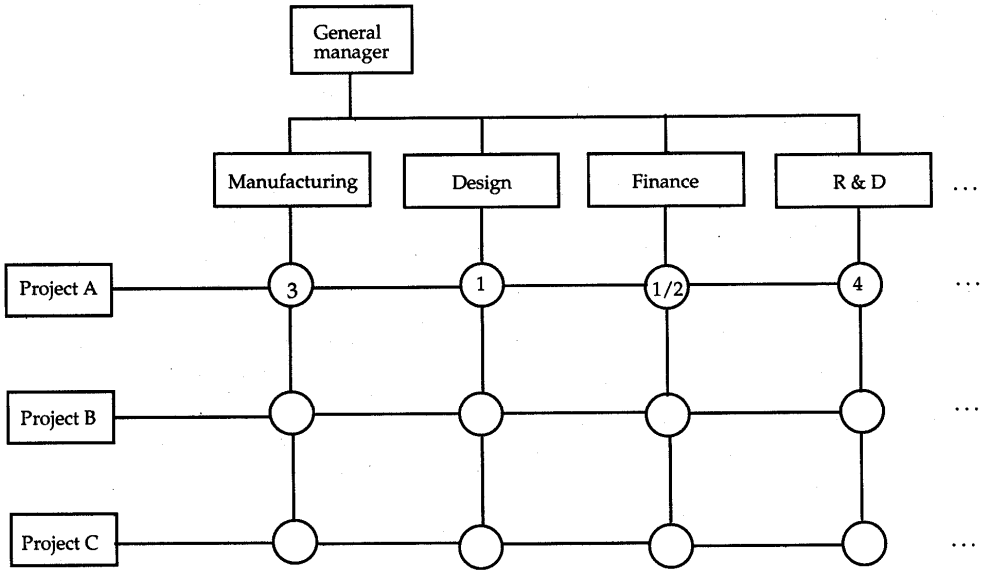

Figure 5-2. Matrix management structure (Seavus, 2015)

Figure 5-2, shows the problem in the matrix management that is the same problem the client company has, but in addition the client company is also using a tree management structure that is used together with matrix management style that leads to a situation where an employee might be working for three different divisions and in worst case three different managers at the same time. The easiest way to see the problems that occurred in combined tree & matrix management system is to place tree management system into one of the circles in matrix management structure and see how many levels of supervisors it creates. This can however be solved by assigning permission management tasks for one person who is high enough in the chain of command in this situation it would be project manager who if needed asks further permission from dedicated department head.

Studies also showed there was a problem in identifying the owners of the data. In some cases the ownership of the data was given to the project manager and in others to the manager of operations, however the system how the owner was decided was not consistent and in some cases the owner of the data would not sign off for some employees to get access to files because they did not know the employees needed the access and more than that several users were given access to more files they should have been given access to. This problem would not be as hard to solve if the company was very small, but in an enterprise with hundreds of projects and over a thousand workers the work of finding proper owner for every project would be extremely time consuming and hard.

One of the major challenges is when people from other countries come to Finland to work and need permissions to access the network drives or need specific programs installed on their computers. This is a problem because the current IAM system is only being used in Andritz Finland and not in the other countries, in this case it is possible to make a request for these access rights because the permission management system is connected to the company wide meta directory, but the request approval goes to this persons supervisor who has never even heard of the system and have no user information to access these requests. These cases can of course be handled as the people were subcontractors, but since the people are actually Andritz employees it would not make much sense to do so. In some cases the services provided by Andritz Finland are more widely used in other countries as well and since the system is also used to track the use levels of the systems it does not give accurate information since not all the people using the system are listed in the permission management system since it is not used in their country.

Another challenge that comes from the enterprise nature of the company is that there are legal units that are inside single country and can easily be addressed with the currently used permission management system, however the business units are global and the manager of

such unit can be located in a totally different country which makes it harder to create a working management chain inside the system so that people are not being left without the tools to request permissions and hardware needed, but also so that there is always someone who can grant these items to a person who has requested them. Because the system is so comprehensive and the company structure is global rather than local it has been pointed out that the system would be most beneficial when implemented to a global use within the company.

5.2. Performance issues of the current system

Studies showed that there were several issues with the current structure and system. This chapter will provide more detailed information about the issues within the system. One of the main issues within the permission management system as it is was renewing the user rights for some of the permissions such as VPN connection and AD- account. Current system requires a lot of work to be done by the manager, whose employees are in question. This was a feature which most managers found intolerable because of the fact that it cuts the productivity of everyone who is part of the approval chain. This issue was partly caused by the system itself for not having a proper AD integration and therefore not being able to automatically renew permits making it easier for managers. Part of the problem was however the big number of subcontractors working for the company because subcontractor's contract length is not stated in AD and therefore subcontractor permissions can only be applied for time period that is significantly shorter than company's own employees.

Second largest issue that was raised involved with lengthy wait of needed equipment and the problem was split in two separate issues. Firstly the problem of gaining access to personal computer for employer or subcontractor who is supposed to start working on really tight schedule, within a day or two from the announcement. This problem is most clearly visible during peak seasons when lots of subcontractors are employed in bursts. Even it is possible to install and get computer ready in one day it is practically impossible because the people installing the computers also have other tasks assigned to them and those tasks might be in more vital role for company than an installation of a single computer. Secondly the problem of getting new cell phone, in this situation you always need to make a request to permission management system, but in some offices people also needed to send one or two e-mails to get the process started. This is because IT only installs the company standard software on the new cell phones but HR is in charge of the acquisition of the phones.

Thirdly the lack of role component was something people were also pointing out saying it would help their work immensely if there was a possibility to create personalized roles for some key job titles so managers would not need to remember all the permissions their subordinates need in order to perform in effective and productive manner. There were also notes that the IT department is taking too long to process the requests for new permissions and some saying that it might be because of the cut backs. The message however was a clearly stated fact that in order for system to work properly it should work smoother and more effectively.

Some managers noted that it would be easier if they themselves could add new subcontractors to the system so they would not have to burden the IT department every time new subcontractor is hired, however this would require administrator privileges to be given for all the managers through-out the company and it would cause a large scale IT security threat that would not be worth the benefits gained by doing so.

5.3. Working features of the current system

Users seem to think that a system which makes it easier to track what access rights everyone in the company has is a good thing and therefore even with some major issues remain to be worked out there was also a lot of positive feedback. IAM- structure was something that shared opinions, some thought it worked just fine, but for some there was a clear issue there. Many people implied that the structure ran a bit too deep and there were issues with not knowing what some things you could order were. You could also order yourself items more than you needed for example you can order yourself an engineering software license for all the divisions of the company even you only needed one license to be able to use the software.

Study also showed that the users thought the feature of the system which allowed them to view their own permissions was good tool for tracking your access rights. The same tool also allowed a person to request for new permissions before they were needed in cases when the person was starting to work on a new project, which contributed to man hours saved.

5.4. Requested improvements

There was one request that rose over the rest and it was ability to make your own set of access right for the request tool. This is because for many people there seemed to be issue of forgetting, the resources they were supposed to order for their employees this would mainly help in the case of new employment but also similar set of access rights could be

used for subcontractors. Creating a set of access rights is pretty much similar to the role component that can be implemented to the current system, however because there are no role based software and permission lists in use the creating them is also going to be an improvement compared to the current system. At the same time the new roles that will be created can be used to make company's access granting process more straight forward and simplified when users are no longer offered the permissions to the systems they are not going to need.

Managers also demanded an ability to add a subcontractor to the system without IT department's involvement this way making it easier and faster process. Even this option was considered during the process it was made clear that the security policy company has implemented would not allow regular users or even managers to add new users to the system because of the integration to the meta directory that holds all the user accounts of the company and if everyone would have rights to create new users to the company it would end up corrupting the security of the user accounts within the company.

6. NEW PERMISSION MANAGEMENT STRUCTURE

Permission management structure developed in this thesis is based on needs of the company, but also on needs of the users. The company had learned that the previous permission management structure was too unclear and some employees found it so hard to use they simply went and worked around it by asking the permissions required straight from the IT-helpdesk. These actions put a strain on IT department and because of this extra work people in the IT department were not able to fully focus the jobs they were hired for. In order to solve this problem, the employees were asked how the new permission management structure could be better and what would need to be done to make the system more user-friendly. Also literary studies and the study conducted by Propentus Oy were part of the material used in creation of new permission management structure.

6.1. Designing the structure

While designing the new permission management structure it is very important to make it adaptable to change. This is among the most important features, mainly because the software used is bound to change every now and again, and if the structure cannot withstand the change the structure will become swamped and thereafter become useless. Adaptability is also a great asset when pitching the product for enterprise wide use, because not all the software and hardware used within the enterprise are the same. The new structure should also be as simple as possible without sacrificing any of the must have information required in order to provide the employees the permissions suited for their specific needs. The simplicity is of a great importance because if the structure has too many levels or it is otherwise too complex there will be a problem with users making the requests for new permissions. Since the whole system is used to provide a service that would make users life easier and that would save time while making requests for new permissions it is very important that the users feel this is what the software is doing for them.

Also one of the key features for the new permission management structure is that it combines all the permissions available for the employee, this is an upgrade from the previous structure that was a bit light with the software listing available in the company and bit too generous with other permissions person could request. In the new structure this problem is being taken care of with the role attribute that is an optional extra for the basic

system, but since there is a clear need for such possibility it will be added to the system and tested as part of the new permission management structure. The role functionality allows the creation of roles with certain permissions pinned to them so that when new user is created it will automatically get the permissions required by the person with their job title.

The new structure has been designed to use the existing information about the user's location and division allowing the reduction of structure levels that were used in the previous version. The user's division and location information was imported from HR database that allowed some drastic simplifications compared to the previous identity management structure.

6.1.1. Service catalog

The study used the existing service catalog of the company to ensure that all the required permissions would be included in the new permission management structure. However some of the services were not included in the previous structure and the extra value of adding those into the new structure could be questioned, it was clear that the new structure should be connected to the service catalog to make the management of the new structure easier. Also it is easier to keep a track on the people responsible for the specific software since the service catalog has information that certain person is responsible for the certain service. When person responsible gets an approval request for permission regarding this service; If person is actually responsible he will approve the request as intended but if they are not then they will contact the IT department and ask what is going on and then the IT department tracks down the person who really is responsible for the service and update their files.

6.1.2. Organization structure

Organization structure is one of the major factors in permission management and the requirements it sets for the system are challenging. Automating an organization structure into the system requires integrating the permission management with a HR database, which will lead to challenges regarding the information security. Also the validity of the data if imported from other databases than the HR database could be questioned. So the question with the organization structure is not as simple as one could assume.

Importing the organization structure information from the external database is one of the biggest advances the new system will provide and it allows the reduction of unwanted extra levels from the permission management structure. It will also ensure that the employees

requesting for permissions are asking them from a right source and not selecting the organization unit they think is correct. Current system has allowed some people to ask permission for a single software from several divisions or locations which leads to situation that the system has a person running three license even he is actually using just one and because the system says the person has three licenses all the organizations the person requested the licenses for are being billed for the single license. Another advantage of the imported information is the fact that the permission management structure will stay anonymous for the users and this way they do not feel the people in different locations are unequal compared to each other.

6.1.3. Processes to consider

The fact that there are three processes that are not even remotely alike makes designing the new permission management structure a nightmare. However designing one structure with all the required components and making three substructures from that one is a whole lot simpler. The following paragraphs will provide a glance to these processes and an idea how they can be united as one without sacrifices.

The sales process is high mobility profile with practically no need for adjusting the previously created documents. The most important feature of the sales process is to make sure that the salesperson has all the required file shares in their disposal and that the connection between their laptop and the company servers is available. Because the sales process is the most important one for the company's survival because that is the one which defines the revenue of the company it is mandatory that all the parts of this function are working perfectly. To assist this all the computers are installed with required viewing and documentation software so that it is possible to use any workstation within the company to make a sales call. On top of this salesperson is required to have a VPN connection so they can access the files on company servers, but this is in no way connected to the single workstation so as long as the user is granted a VPN access he/she can use any workstation from the company to download the VPN client over the internet. On top of that the VPN connection can be made via several different sites so it is highly unlikely for all these options to be unavailable at the same time.

Second process is the execution which is the actual designing and producing the designs. This process also requires some level of mobility but has more advanced software needs than the sales process. People working on execution process often have their designs and documents stored on their own personal hard drive as well as the company server so the access to data is not the biggest concern here. However execution process uses several

programs that require user licenses to be borrowed from the company's license pool. So before the user takes off to the client meeting or to the production site they are required to export a license to their laptop so they will be able to use the applications required for the process. Of course it is possible for people working on execution process to connect to company network via VPN and be able to use all the software as they were at the home office, but the problem is normally more directly related to the lack of a basic internet access at the production sites.

Last but not least are the support functions. The employees working on support processes are less mobile or even when not at their normal workplace they are still generally using company's own facilities somewhere and therefore have an access to the internal network of the company. Support processes often use many applications not installed on any computers of the sales or execution processes, people working for support processes also often have a high amount of network file shares they are allowed to access because of data restore and maintenance functions that are part of everyday work in this process.

The differences between these three processes might not seem like much, but in a fact they are so different that if one structure was produced to accommodate all three processes it would defy the whole purpose of this project of making the permission management structure simpler. Therefore the idea of making a one structure to accommodate all the permissions available for users from which the administrator can pick the required permissions and make a substructure for a specific process sounds like a valid way of creating a new permission management structures.

6.2. Creating the new structure

During the design phase of the project it had become clear that there was no need to start from the scratch with the new structure. The idea which the previous structure held in terms of the dividing permissions into four distinct areas of network connections/ resources, hardware upgrades, office equipment and software was still valid. There was one major change however that was executed when new structure was created, the permission for file share was brought on to same level with the previously mentioned four categories instead of it being buried under the network connections / resources. This change was powered by the understanding that the most commonly requested permission of all was in fact the access to different file shares. The understanding described here is a combination of statements gathered from the IT workers in the company and the fact that most of the requests regarding new permissions were file share related. The reason why file share related permission requests were most common ones can easily be explained with project

nature of the business. Each project has a core group who are handling the everyday stuff regarding the project, but even with the wide area of expertise these people possess an outside expert is often needed and this can be a person from different project, someone familiar with the culture of a specific region or someone with the knowledge of something closely related to the project. In terms of efficiency most of the employees within the company are working with several projects at the time and new projects are being launched if not daily but weekly basis and therefore the smooth flow of permission management regarding the file shares is a matter of outmost importance. During the tough economic times it is normally a buyers-market and the schedule for a project can be significantly shorter than normally for this reason the permission management process for the file shares can easily make a difference between a successful project and losing the deal to a competitor. Pictured below is the first level of the new structure with file share tab alongside with others.

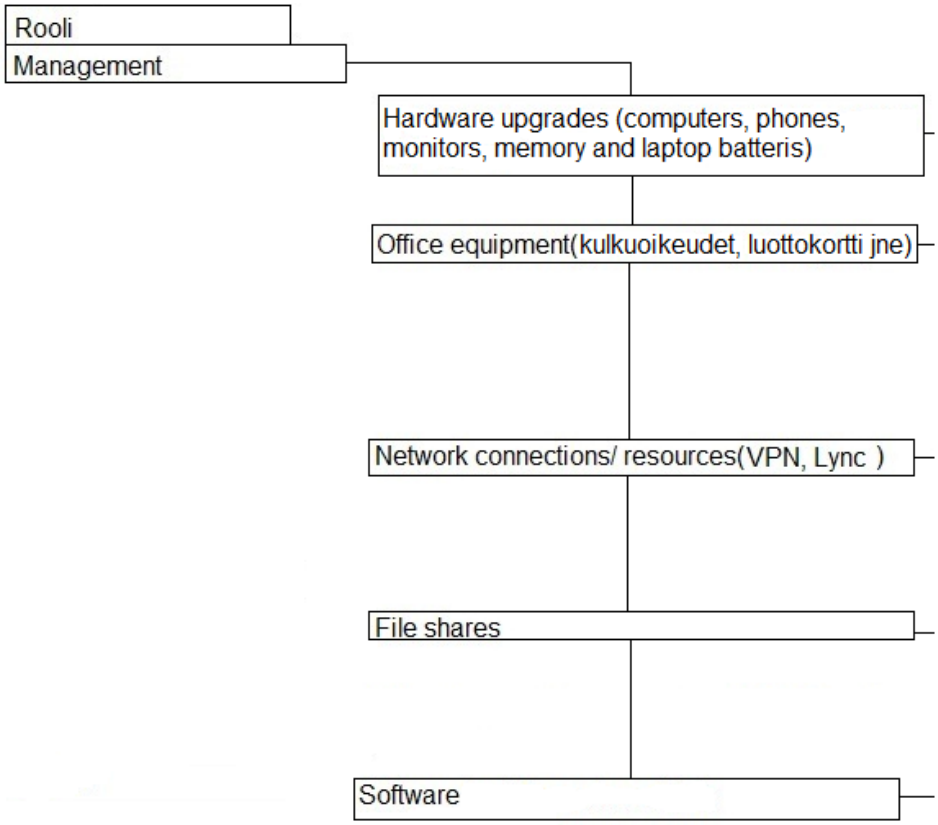

Figure 6-1. First level of new permission management structure

While designing the new structure the removal of unnecessary levels from the permission management structure was one of the key solutions that were raised, the need to cut out the excess levels was based on the fact that the previous structure was too unclear to use

because of the excess depth in its structure. Because the evolution in software used for managing permissions it has become possible to automatically fetch some of the information that was previously inserted manually. These information objects include division the person is working for and the location of the person. The following picture will show the permission management structure before and after the aforementioned changes.

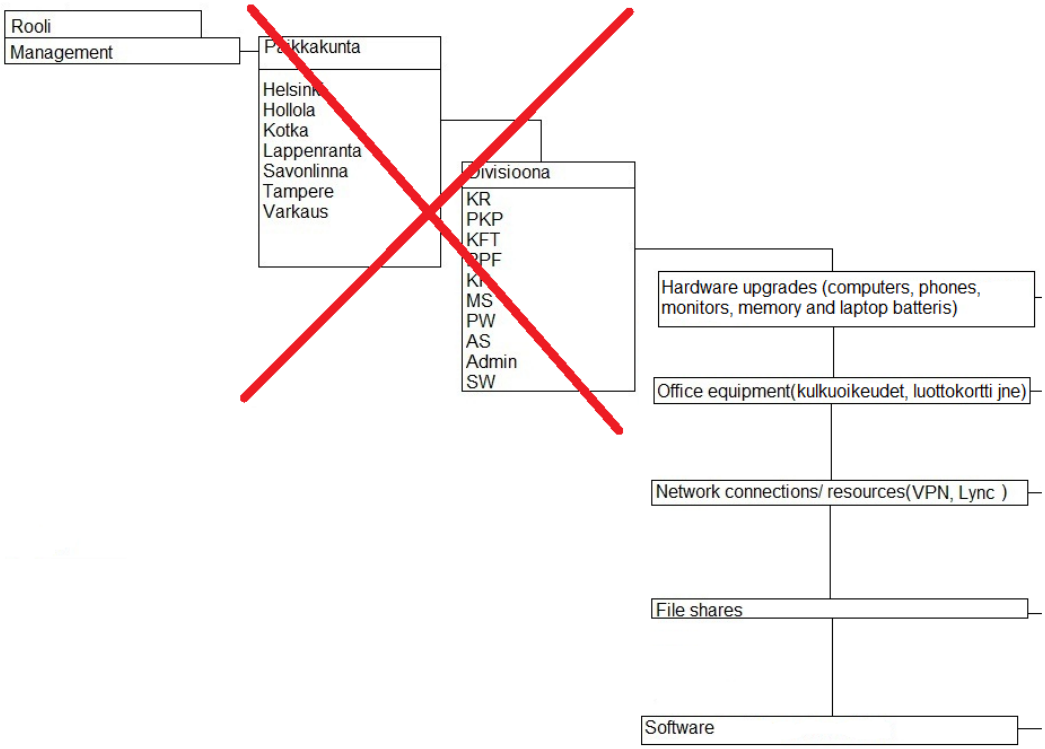

Figure 6-2. The structure before and after the excess levels

Another requirement set for the new structure during the design phase was the fact that it should provide the user a comprehensive list of the software available for all the users because needs of a different divisions can change as soon as they realize there is some useful new software that the guys on some other division are using. Because of the fact that programs used can be useful for more than one functions it was decided that the software listing should include all the software that is used within the company. Also having a complete list of software under the software tab of the structure eliminates the unclear situations where people did not really know what the name of the software they wanted was, but instead they wrote description what this program they want should do to the info field of the permission request.

The bigger changes described above among with some smaller changes made on the permission level have made the permission management structure what it is today clearer,

simpler and more efficient. Also to be considered is the fact that it was possible to reuse the old permission management structure and this way the great deal of extra work was avoided, which is always ideal when working on projects that in general do not require a whole new base to build the system on.

6.3. Implementation

Implementing the new permission management structure for the client company has been designed to be a four step project. In first phase the new structure was evaluated by the user study group on paper to see how they felt about the new structure compared to previously used structure. After this evaluation cycle was completed the new structure was implemented on test server and rolled out for the use of the test groups. After the roll out there was a test phase of two months culminating to survey regarding the new permission management structure. These phases will be opened up a bit more in following chapters.

The first round of evaluation was done without an actual user interface that would allow the test group to see how the final product would function in production use. However it was clear that the new structure had lost many unnecessary levels of depth making it much lighter and easier to use. The test group's findings in this evaluation phase show that the reduction of depth in permission management structure would make the structure easier to use and more simple to the everyday user of the system, were consistent with the information received from data analyzed in the literary study phase of this thesis. However there were some concerns regarding the structures functionality in case the person is working for several divisions, and the person has a need for different division specified software which are not available for his role. However this issue was already taken into consideration with a selection that makes the whole permission list available for whomever it may need.

The second round of evaluation was more thorough than the first, but the fact that most users in the test group had used the program and the previous structure it was pretty straight forward and there was not that many questions regarding the structure and the new features that were added to the system, because these were already addressed in first phase of evaluation. The majority of the comments received during second round of evaluation was positive and made it clear that the study had succeeded in its goals. Especially the new role based permission requests gathered great deal of positive feedback.

At last the new permission management structure was released for company wide use, but to avoid the issues the previous launch had the company had decided to make a document explaining how the permission management system should be used. The documentation

also explains the main features that have been added to the system since the initial launch of the product. Releasing the how to document with the release of new structure makes the full use of the program as easy as possible even for the users who have not worked with the system before. In addition the company held demonstrations regarding the new permission management system to ensure that the transition between old and new was as painless as possible but also to provide a possibility for employees to make questions for development team regarding the system.

As every major roll out should be followed with gathering of feedback to ensure that the future roll outs will go as smoothly as the previous one or even better if possible. Therefore the fourth phase of the implementation was the internet feedback form that was be sent to everyone in the company. This way everyone was able give anonymous feedback regarding the problems with the new system and/or the implementation process. It is well known fact that the people are not too keen on filling out questionnaires so an incentive price was introduced here to get the maximum number of answers regarding the new structure. The feedback received was mostly positive and there were not many requests for change regarding the new structure.

6.4. Management

As it often is the work does not end even if the new system would be up and running, however the type of work needed to maintain the system functional is totally different when compared to the previous steps of the project. Managing the new structure is also a matter of great importance so the structure won’t get swamped and thereafter become useless. The managing that the structure stays up to date is very low effort maintenance work, but same as with the machines if they are not tuned every so often they will break. The key elements in the management phase of the project are making sure that the connections between different servers and the permission management systems are updated if there are changes in the server names, IP addresses or in location of data stores. Another important task in the management phase of the project is the modification of the permission list so it is up to date with the latest permissions employees can request an access to, but also so that the permissions that are no longer used in the company are deleted from the structure and this way keeping the structure from swamping.

7. SUMMARY

Wasted time bringing the biggest costs to the companies these days, has made it a constant battle to automate processes and making things simpler. If a process that employs directly and indirectly around 20 people could be automated the savings over a year are easily counted in hundreds of thousands and in some situations even in millions. Because of the current economy everyone is working to cut costs and normally the support functions that affect the whole chain of production but bring no revenue are first ones to be audited in order to find more effective and less time consuming procedures.

Creating a new permission management structure for the client company was a challenging task which still has some issues that remain to be solved. This being said the study has provided a deeper insight to the issues of the system and raised valid measures to overcome these issues and to make the system functional. In addition the study yielded a base for the new permission management structure that was implemented as functioning replacement for the previous structure without significant effort or work. The study has also produced some ideas to be passed on to the human resource department regarding the titles people are given in the organization. The value of this study also presents itself with profiles that were made for every title used in the client company with complete works of what software and hardware people are using. This allowed creation of title based roles that consist of a software, hardware and permissions tailored for a specific title, which in its own right makes it possible for new employees to gain access to everything they need simply by requesting a single role for them instead of several individual permissions.

7.1. Further Development

The client company should seriously consider the further development of its permission management because the possibilities to save company resources with this type of systems are significant and can easily be quantified by saved man hours and/or license costs. By the end of this study the company now has a functional permission management structure that can easily be used to make requests for needed permissions. The new structure is also more intelligent compared to its predecessor and offer the employee those permissions specified for his title and/or division/location. However the company should invest into role module

available for the system because this would allow the HR to create user with a certain profile and while the person is created to HR database the user would immediately be granted with permissions required for his/hers job description within the company.

When the previously introduced development ideas have been executed it would most likely benefit the company a great deal to make this system an enterprise wide standard for permission management. The benefits of having enterprise wide permission management system are largely the same as having a companywide permission management system, but in much larger scale. Also there would be some additional benefits that would include ease of sharing the resources across the company borders. Nowadays the company uses separate software for sending large files over the internet, but because all the company networks are entwined and have an access to one and other this would also be more secure option, if controlled properly. This would also bring savings in form of reduction of overlapping software as the previously introduced example shows.

Having an enterprise wide permission management system would also enhance the mobility of the labor and hopefully help with standardization of other enterprise wide systems as well. Even there are some enterprise wide standards not all the systems are the same which can cause issues with people traveling to other countries even in internal business matters.

7.2. Integrating software to access management system

The permission management software used by the company offers an application interface which allows software from different vendors to be integrated as a part of the system. This interface is mainly focused in providing the connection between two separate programs and allowing them to communicate with each other. However the permission management software only offers a limited number of plug and play type of connectivity other integrations has to be bought from the software vendor or programmed by the company itself.

At the time of the project the client company’s only integration to identity management system is the HR master database and e-mail system. There are some serious plans for running a separate integration project that would result in all the main systems within the company to be integrated into the identity management system, however the project of redesigning the identity management structure is a separated from the integration project so it remains to be seen what will happen and if the other project is actually going to go forward. As this project has concluded IAM will be part of the information security in the client organization and pretty much all companies worldwide right now and well off to the distant future. The impact that an function IAM solution has in terms of security and cost

saving determines that it is something every large enterprise will have to address, if not now then in a very near future.

REFERENCES

AuthenticationWorld.com, 2006, Single Sign On, Huntington Ventures Ltd. (http://www.authenticationworld.com/Single-Sign-On-Authentication/) (Haettu 16.10.2013)

Axiomatics, 2014, Attribute Based Access Control (ABAC) (http://www.axiomatics.com/attribute-based-access-control.html) (Haettu 30.1.2014)

Blue Coat Systems inc., 2007, technology primer: user management (https://www.bluecoat.com/sites/default/files/documents/files/User_Management.8.pdf) (Haettu 3.4.2014)

Brachman B., 2006, Rule-based access control, IBM developer Works (http://www.ibm.com/developerworks/library/ws-soa-access/) (Haettu 28.12.2013)

CSDN.NET, 2012, Role-Based Access Control (http://m.blog.csdn.net/blog/ajian005/1501329) (Haettu 6.5.2015)

European commission study, 2013, Feasibility study on an electronic identification, authentication and signature policy (IAS) 79-83 p.

Ferraiolo D., Kuhn R.D., Chandramouli R., 2003, Role-based Access Control, Artech house, 55-59 p.

fppt.com, 2015, Management tree template (http://www.free-power-point-templates.com/articles/how-to-make-a-management-tree-template-in-powerpoint-from-a-genealogy-diagram/) (Haettu 6.5.2015)

Gamby R., 2010, Self-service user identity management: Pitfalls and processes (http://searchsecurity.techtarget.com/tip/Self-service-user-identity-management-Pitfalls-and-processes) (Haettu 2.5.2015)

Gartner Inc. Technology Research, 2013, Identity and Access Management study for Andritz Oy, 23-26 p. (Independent report ordered for the company use)

Gentry S., 2012, Access Control: Models and Methods (http://resources.infosecinstitute.com/access-control-models-and-methods/) (Haettu 27.12.2013)

Identity management task force, 2008, Identity management task force report 2008, 25 p. (https://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-identitymgmt-2008.pdf) (Haettu 10.11.2013)

Information Technology Services Office of The Hong Kong Polytechnic University, 2009, Identity and Access Management (http://www.polyu.edu.hk/ags/Newsletter/news0911/IAM_details.html) (Haettu 23.8.2013)

Kizza J., 2008, Securing the information infrastructure, Cyber Tech Publishing, 187 p. (https://books.google.fi/books?id=UTkZStCQpNsC&pg=PT202&lpg#v=onepage&q&f=false) (Haettu 14.5.2014)

OptimalIdM, 2014, An Introduction to Virtual Directories (http://optimalidm.com/introduction-to-virtual-directories/) (Haettu 27.3.2014)

Oracle, 2010, Authentication and authorization for remote access, Oracle corporation (http://docs.oracle.com/cd/E19683-01/817-0365/concept-31/index.html) (Haettu 2.9.2014)

Oracle, 2013, User and Role management (http://docs.oracle.com/cd/E27363_01/doc.121/e25143/user_and_role_management.htm#OPCAG204) (Haettu 23.4.2014)

Platt D., 2013, Could, cost and complexity: Challenging traditional identity management model (http://www.wired.com/insights/2013/12/cloud-cost-complexity-challenging-traditional-identity-management-model/) (Haettu 2.5.2015)

Radhakrishnan R., 2012, The Fifth and Final Frontier of Access Control Model, 5 p. (http://www.isaca-washdc.org/presentations/2012/201211-session3_article.pdf) (Haettu 7.8.2013)

Rich J., Satut M., Woo K., Yehl K., Baker S., Christian S., McLean K., Reeme J., Board T., Keown D., Tracy P., 2014, Identity and Access Management at Northwestern University, 6-9 p. (http://www.it.northwestern.edu/bin/docs/cio/identity-access-management-working-group-report-082914.pdf) (Haettu 3.5.2015)

Roebuck K., 2011, Failover: High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors: High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors; Emereo Pty Ltd., 133-134 p.

Rosenblatt S., 2013, Two factor authentication: what you need to know (FAQ) (http://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/) (Haettu 25.2.2014)

Scarfone K., Souppaya M., 2009, Guide to enterprise password management (draft), 24-25 p. (http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf) (Haettu 12.10.2013)

Seavus, 2015, Organizing the Organization for Project Management (http://pmtips.net/Blog/organizing-organization-project-management) (Haettu 6.5.2015)

Shuriya B., Sumathi S., 3/2013, Study of an RBAC System, Indian Journal of Applied research, 104-106 p.

Slade R., 2006, Dictionary of Information Security, Syngress Publishing, 133-134 p.

Tipton H.F., Krause M., 2007, Information Security Management Handbook, Taylor & Francis Group, 829-831, 836 p.

Tolone W., Ahn G-J., Pai T., Hong S-P., 2005, Access control in collaborative systems, ACM Computing Surveys (CSUR), 29-41 p.

Wikipedia, 2013, Metadirectory (http://en.wikipedia.org/wiki/Metadirectory) (Haettu 27.3.2014)

Wikipedia, 2014, Virtual directory (http://en.wikipedia.org/wiki/Virtual_directory) (Haettu 27.3.2014)

Wikipedia, 2015, Provisioning (http://en.wikipedia.org/wiki/Provisioning) (Haettu 2.5.2015)

Wikipedia, 2015, Identity management (http://en.wikipedia.org/wiki/Identity_management#/media/File:Identity-concept.svg) (Haettu 6.5.2015)

Wikipedia, 2015, Virtual Private Network (http://en.wikipedia.org/wiki/Virtual_private_network) (Haettu 6.5.2015)