TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY
Julkaisu 779 • Publication 779

Mikael Linden

Organisational and Cross-Organisational Identity Management

Tampere 2009

Tampereen teknillinen yliopisto. Julkaisu 779
Tampere University of Technology. Publication 779

Mikael Linden

Organisational and Cross-Organisational Identity Management

Thesis for the degree of Doctor of Technology to be presented with due permission for public examination and criticism in Tietotalo Building, Auditorium TB109, at Tampere University of Technology, on the 28th of January 2009, at 12 noon.

Tampereen teknillinen yliopisto - Tampere University of Technology
Tampere 2009

ISBN 978-952-15-2077-8 (printed)
ISBN 978-952-15-2113-3 (PDF)
ISSN 1459-2045

Tampereen Yliopistopaino Oy, 2009

ABSTRACT

We are all familiar with the overwhelming number of usernames and passwords needed in our daily life in the networked world. Services need to identify their end users and keep record on them. Traditionally, this has been done by providing the end user with an extra username and password for each new service. Managing all these isolated user identities is painful for the end user and work-intensive for the service owner. Having out-of-date user accounts and privileges is also a security threat for an organisation.

Identity management refers to the process of representing and recognising entities as digital identities in computer networks. In an organisation, an end user's identity has a lifecycle. An identity is created when the user enters the organisation; for example, a new employee is hired, a student is admitted in a school or a company gets a new customer. Changes in the end user's affiliation to the organisation are reflected to his identity, and when the end user departs, his identity needs to be revoked. Organisational identity management develops and maintains an architecture that supports maintenance of user identities during their life cycle. In cross-organisational identity management, these identities are used also when accessing services that are outside the organisation.

This thesis studies identity management in organisational and cross-organisational services. An organisation's motivations for improving identity management are presented. Attention is paid to how the person registries in an organisation should be interconnected to introduce an aggregated view on an end user's identity. Connection between identity management and introduction of more reliable authentication methods is shown. The author suggests what needs to be taken into account in a usable deployment of single sign-on and PKI for authentication.

Federated identity management is a new way to implement end user identity management in services that cross organisational boundaries. This thesis studies how to establish a federation, an association of organisations that wants to exchange information about their users and services to enable cross-organisational collaborations and transactions. The author presents guidelines for organising a federation and preserving an end user's privacy in it. Finally, common use scenarios for federated identity management are presented.

PREFACE

Research for this thesis was carried out in 2000-2008 while working at CSC, the Finnish IT Center for Science and the Information Management of Tampere University of Technology. Preparation of publications for the thesis can be described as a side activity from my main occupation as an engineer developing services for Finnish higher education. My dual role at the university campus provided me an opportunity to observe the academic community both from the scientific and research perspective and from the perspective of providing IT service to the highly demanding user community. Indeed, the academic environment with skilled end users, sophisticated services and good networking connections has been an excellent laboratory for research and development of identity management and related services.

I would like to thank my supervisor professor Jarmo Harju and lecturer Jukka Koskinen for supporting me in my long way towards this thesis. I would also thank the examiners of this thesis, doctor Arto Karila and professor David Chadwick, for the new perspectives and fruitful suggestions regarding contents of the manuscript.

I want to express my gratitude to my employers for providing a supportive atmosphere for my research. Klaus Lindberg, Janne Kanner and Manne Miettinen of CSC had confidence in my vision of developing an identity federation for the Finnish higher education, although there were no federation models available at the beginning. Arto Tuomi, Mika Suvanto, Pekka Järveläinen and Jussi Tella put the operations of Haka federation into practice, not to forget the numerous colleagues in the IT service units of Finnish universities and in other national research and education networks abroad. I would also thank Jussi-Pekka Pispa and Martti Jokipii of Tampere University of Technology for the discussions on how things actually work in an organisation like a university and how that should be taken into account in designing identity management.

In the final stage, the funding provided by TeliaSonera Oyj:n tutkimus ja koulutussäätiö made it possible for me to dedicate myself fully to preparing the thesis. Finally, the proof-reading done by Outi Kaikkonen has once again ensured the correct spelling of the manuscript.

Tampere, November 2008

Mikael Linden
mikael.linden@iki.fi

CONTENTS

LIST OF PUBLICATIONS

Publication 1

Mikael Linden. Study on Organisational Identity Management in Finnish Higher Education. Proceedings of the 12th International Conference of European University Information Systems EUNIS, 2006. 69–76

Publication 2

Mikael Linden, Pekka Linna, Mika Kivilompolo, Janne Kanner. Lessons Learned in PKI Implementation in Higher Education. Proceedings of the 8th International Conference of European University Information Systems EUNIS, 2002. 246–251

Publication 3

Mikael Linden, Inka Vilpola. An Empirical Study on the Usability of Logout in a Single Sign-On System. Proceedings of the 1st International Conference in Information Security Practice and Experience. Lecture Notes in Computer Science 3439. Springer-Verlag, 2005. 243–254

Publication 4

Mikael Linden. Towards Cross-organisational User Administration. Informatica, Volume 27, Issue 3, 2003. 353–359

Publication 5

Mikael Linden. Organising Federated Identity in Finnish Higher Education. Computational Methods in Science and Technology, Volume 11, Issue 2, 2005. 109–118

Publication 6

Mikael Linden, Viljo Viitanen. Roaming Network Access Using Shibboleth. Selected papers of Terena Networking Conference 2004. http://www.terena.org/publications/tnc2004-proceedings/

1. INTRODUCTION

This section first provides a short description of identity management and its position and motivation in an organisation. Background, motivation, goals and research methods of this thesis are introduced next. Finally, an overview of the subsequent sections is presented.

1.1. Positioning Identity Management

When a new person needs to be represented in an information system, a new identity is created for him. This may require adding a new record to a user database, issuing him a username and a password for authentication and granting him access to resources he needs to use. Identity management and related concepts of identity, authentication, authorisation and auditing are going to be introduced in detail in Section 2.

Identity management is not a new subject of interest. Since the early years of information technology, computers have stored and processed person records. User accounts have been used for separating end users' processes and files already years before networks and the Internet. When a user has needed to access his user accounts, he has proved the ownership of the account by typing in a password.

The proliferation of the Internet, especially the World Wide Web, has lead to a situation where each end user has a multitude of user accounts in systems managed by different organisations and placed around the Internet. It has been relatively easy for the system owners to set up a new isolated user database for each service. However, for common end users, the number of separate usernames and passwords has become unmanageable.

To manage the increasing complexity, there have been attempts to detach the identity management from services and establish a separate middleware layer between the network and the services to take care of tasks related to end users' identities and authentication (Figure 1). The middleware layer can span one organisation (organisational identity management, c.f. local area network, LAN) or several organisations (cross-organisational identity management, c.f. wide area network, WAN). However, so far, the attempts to establish a single Internet-wide identity management system (such as a global X.500 directory [ITUT05] or Microsoft Passport [MICR04, OPPL04]) have not succeeded.

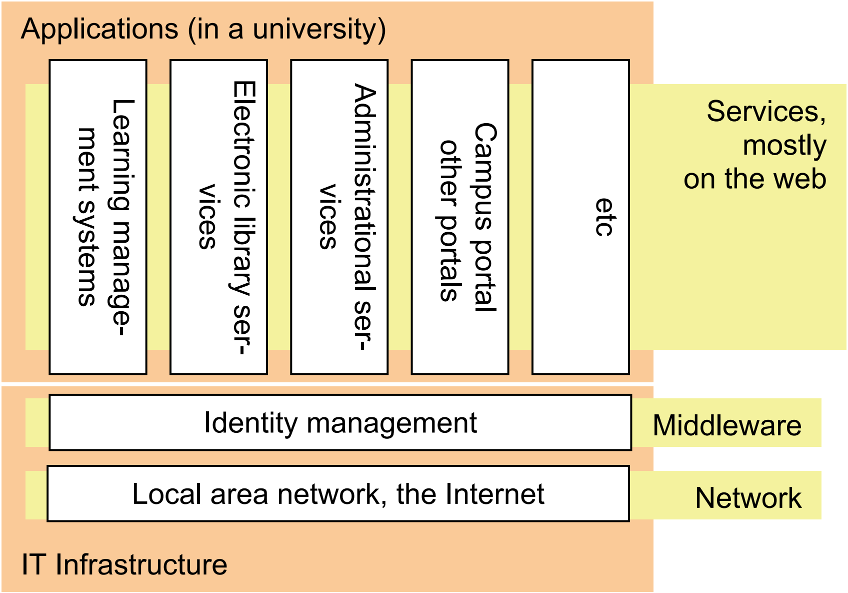
Applications (in a university)
Learning management systems
Electronic library services
Administrational services
Campus portal other portals
etc
Services, mostly on the web
Identity management
Middleware
Local area network, the Internet
Network
IT Infrastructure

Figure 1. Identity management as a middleware layer between the network and services

During recent years, identity management has grown into an area of interest of its own, with its roots in other topics, such as computer security. Identity management is also motivated by efficiency and the potential new business opportunities it may provide. Table 1 depicts organisations' motivations for identity management; i.e. what kind of results an organisation is expecting from an investment in identity management.

Table 1. Motivations for an organisation to invest in identity management

Motivation	**Focus**
Information security	Adequate protection with minimal costs. Balancing costs and risks
Efficiency	Investing in identity management to get cost reductions by increased efficiency
New business opportunities	Investing in identity management to get new revenue or to enable new ways of operation that have not been possible otherwise

An obvious motivation for identity management is information security. Their close relationship is apparent in the definition of computer security as the prevention and detection of unauthorised actions by users of a computer system [GOLL99:9]. From an information security perspective, identity management is a necessity for an organisation's business. It does not bring competitive advantage regarding competitors, but its poor implementation may risk the organisation and its reputation. Identity management is considered mostly an expense that risk management tries to balance with the potential loss of realised risks. The goal is to implement adequate protection with minimal costs.

Maintaining an individual’s identities in several isolated systems causes inefficiencies for the organisation and for the end user who needs to remember multiple usernames and passwords. The second motivation for identity management in an organisation is efficiency. Investments in identity management are expected to lead to reduced costs by eliminating overlapping work. In addition, the quality of information increases as the amount of overlapping (and, sooner or later, conflicting) information is reduced.

The third and maybe the most challenging motivation is the potential for businesses that would not have been otherwise possible or would have been too cumbersome for end users. This covers both potential new revenues for companies and new, more flexible ways to organise the internal services of an organisation. Potential for new businesses is especially in cross-organisational (a.k.a. federated) identity management, which is still a new and evolving area with undiscovered business opportunities.

It is worth noticing, that the three motivations presented above are not conflicting with each other. Instead, they can be considered as alternative perspectives of the same issue, each of them emphasising different objectives. If planned well, actions taken to improve an organisation’s identity management are able to gain results that serve all the three dimensions. For instance, reducing the number of independent usernames and passwords increases efficiency (the users need not remember and IT support needs not maintain so many of them) and information security (if there are fewer passwords the users are able to remember them and do not need to write them down).

The three motivations also demonstrate the interdisciplinary nature of identity management and this thesis. Besides information security, identity management can be studied also in a larger context of computer science and engineering (for instance, communications, software and systems engineering) or information systems science (which introduces the management and financial perspectives to the topic). Nevertheless, it can be argued that information security provides a good starting point for a study on identity management, because even a highly efficient and advanced identity management architecture is useless if it is insecure.

The focus of this thesis is identity management from the point of view of an organisation which provides end users with services, and, thus, needs to take care of identity management in those services. An end user is a person having a relationship to the organisation, such as being an employee, a student or a customer. The relationship also characterises the life cycle of the identity, including its creation, maintenance and removal.

It can be questioned how restrictive this limitation of focus actually is. A fundamental characteristic of organisational identity management is that the organisation has an interest to ensure the quality of the end users' identities, and this holds true for most scenarios including those of an employee, a student and a customer above. Services where the end users represent themselves, not an organisation such as their employer, are maybe the opposite scenario. User-centric identity management technologies [BHAR06] (such as OpenID [RECO06, RECO06b]) try to cover this scenario.

1.2. Background and Motivation

In Finland, there are 20 universities and 29 polytechnics with 41 200 employees, 307 300 degree students and 174 200 other students in the Ministry of Education sector [MINE06, MINE06b]. Having more than half a million potential end users with considerable turnover, identity management is a notable challenge for Finnish higher education. Students and employees are skilled Internet users and in the institutions they have a modern IT environment in place. This makes higher education institutions a prominent laboratory for identity management related research and engineering.

Since 2000, I have been working in identity management related activities in Finnish higher education. My first assignment was the FEIDHE project, a common project for the IT service units in Finnish universities and polytechnics, which looked for ways to make use of PKI and smart cards for authentication of university staff and students. The project was concluded in 2002 and I and my colleagues published the results (Publication 2) in the annual conference of EUNIS, the association of European universities' IT service units.

After the authentication-focused FEIDHE project, improving organisational identity management in general was considered important. In other words, whereas the FEIDHE project aimed at replacing the password with a smart-card-based authentication, the follow-up activities focused to end users having just one username in their organisation. Current and best practices of the institutes were collected and disseminated in a series of workshops called School in User Administration, which, over a three year period, covered the staff responsible for identity management in 69 percent of the institutions. The School in User Administration is described in Publication 1.

During the projects, cross-organisational (a.k.a. federated) use of resources was identified as an item of interest. Universities and polytechnics co-operated by sharing IT services, and cross-organisational identity management was expected to ease their use. Federated identity management had also become a subject of research [e.g. BUEL03, SHIM05].

The Haka project, another project initiated by the IT service units in Finnish universities and polytechnics, studied federated identity, based on open source implementations developed by the US universities. In February 2004, the project was concluded and the results proposed the establishment of the Haka federation, the identity federation of Finnish higher education, which was launched in May 2005. I have been strongly involved in the development, coordination and operation of the federation. Publication 3, Publication 4, Publication 5 and Publication 6 have been made in connection with this work.

1.3. Research Goals

Research in IT must address the design tasks faced by practitioners [MARC95]. The goal of this thesis is to build and validate models and a methodology for organisational and cross-organisational identity management. As a part of the thesis, instantiations of organisational and cross-organisational identity management are built, evaluated and theorised.

A lot of enabling technology is already available for organisational [PERK07] and cross-organisational [RAGO06, LIBE07] identity management, but there are not so many research results on how to organise the use of this technology in a way that also takes into account issues like privacy laws and usability. This thesis is mostly focused on cross-organisational identity management, but because the cross-organisational dimension builds on organisational identity management, they are both covered in this thesis.

1.4. Research Methods

The taxonomy of research methods by Järvinen [JÄRV01] is presented in Figure 2. On the top level, research approaches are divided into the approaches studying reality and the approaches studying mathematics, i.e. symbolic systems such as formal languages and algebraic units. Approaches studying reality are split into the approaches stressing utility of innovations and the approaches stressing what reality is. Approaches for innovation (a.k.a. constructivism) are further divided to building and evaluating innovations. Research stressing what reality is is divided into conceptual-analytical approaches and empirical studies, which is further split to theory-testing approaches and theory-creating approaches.

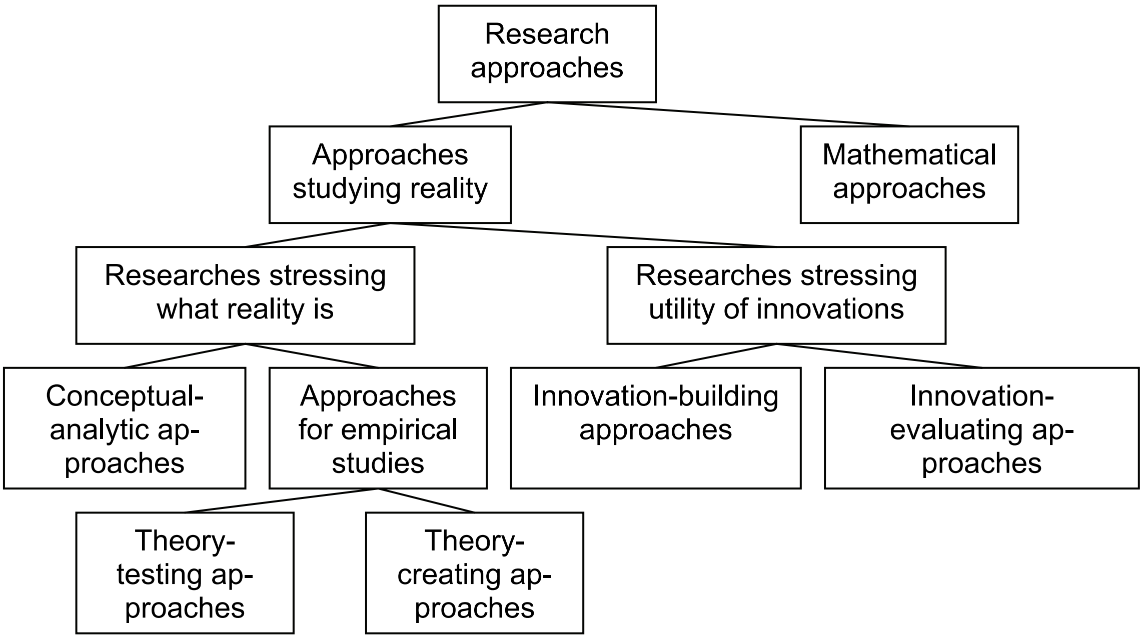
Research approaches
Approaches studying reality
Mathematical approaches
Researches stressing what reality is
Researches stressing utility of innovations
Conceptual-analytic approaches
Approaches for empirical studies
Innovation-building approaches
Innovation-evaluating approaches
Theory-testing approaches
Theory-creating approaches

Figure 2. Taxonomy of research methods [JÄRV01]

Physics is considered a prototype of empirical approaches testing theory. The goal is to model reality to an extent that makes it predictable. Sciences like sociology and psychology are empirical sciences that try to understand the world and create theories explaining it. Design sciences are considered research stressing utility of innovations. Whereas natural sciences try to understand reality, design science attempts to build technical, organisational and other innovations that serve human purpose. Its products are assessed against criteria of value or utility – does it work? [JÄRV01, MARC95]

The main research method of this thesis is constructivism. However, Publication 3 on usability is based on empirical approach. For Publication 3 we used focus group discussions and quantitative test sessions to create and test a theory on “what the world is”, in this case, how do users expect an easy-to-use system to work. The research outputs of the publications are further elaborated in Section 8.

1.5. Structure of the Thesis and the Author’s Contribution

Section 2 introduces basic concepts for this thesis, including identity, authentication, authorisation and auditing. Section 3 places the concepts in the context of an organisation, making end users employees of an employer, students of a school, customers of a company and so on, depending on the context. The section and related publications contain the author’s findings in organisational identity management, including typical shortcomings. Based on a significant practical experiment, recommendations and guidelines for deployment of a PKI based authentication system are presented. Additionally, the first empirical study available in the literature regarding usability of logout in a single-sign on system is presented, supplemented by guidelines for designers of future systems.

The rest of the thesis is devoted to cross-organisational a.k.a. federated identity management, where end users use services provided by other organisations than their home organisation. Section 4 introduces the concept of federated identity management. The author has presented its requirements and one of the first interpretations of what implications the EU privacy laws impose on a compliant deployment. Section 5 presents organisational aspects of federated identity management, including the concept of a federation. The author has presented an analysis on the possible alternative ways to organise a federation and the reasoning why one of the alternatives was selected for deployment in Finnish higher education. Some other examples of existing federations are also presented.

Finally, Section 6 suggests ways to make use of federated identity, and presents some application areas for it. As an example application of federated identity, the author has presented one of the first adoptions of federated identity for authorisation of network access. Section 7 concludes the thesis. Additionally, Section 8 presents research outputs and activities and the author's contribution in the publications.

2. CONCEPTS OF IDENTITY MANAGEMENT

In this section, the basic concepts of identity management are introduced. The perspective of identity management in an organisation is emphasised. The section is concluded as an analysis of the concepts in a timeline.

2.1. Identity and Identifiers

A digital identity is an abstraction of an individual[1] in information systems. In computer sciences, it is important to distinguish the concept of digital identity from the concept of identity in the psychological and sociological sciences. In psychology, identity means the distinguishing character or personality of an individual [MERR07]. In order to determine their identity, people try to discover who they are, what their strengths are and what kinds of roles they are best suited to play in their life [FELD99:446]. However, in computer sciences, the digital identity is not anything more than bits and bytes. From this on, for brevity, we call digital identity just an identity.

An identity consists of attributes, which are any kind of characteristics associated to the individual [CAMP04]. Some attributes describe the demographic properties (such as age and sex) or preferences (such as preferred language) of the individual. Some attributes (such as a customer number or employee's job title) describe his relationship to a particular organisation. Liu et al [LIU04] call these attributes the organisational (or position) identity, as opposite to the personal (or agent) identity.

Attributes that uniquely identify the individual within a context of a specific namespace are particularly interesting; they are called identifiers [CAMP04]. Each namespace has an authority that controls the namespace and is responsible for maintaining the uniqueness of the identifiers. For instance, IT services unit of Tampere University of Technology (TUT) ensures that the email address *mikael.linden* belongs at most to one individual at a time[2]. However, in a namespace other than TUT, the identifier *mikael.linden* may be assigned to another person.

Identifiers, such as email addresses, usernames and employee numbers, have organisation-oriented namespaces. Typically, it is necessary for an organisation to

[1] Other principals, such as legal persons and computers, also have digital identities with attributes such as street addresses, domain names, IP addresses etc. However, in this thesis, only human users are considered.

[2] Actually, it may be desirable to preserve some uniqueness over time, as well. When a user departs TUT reserves his email address for two years before it can be reassigned to another person [TUT07]. This is considered as an adequate protection to prevent the emails of the new and previous email address owner from being mixed. Other identifiers, such as social security numbers, are never expected to be reassigned.

assign several identifiers to an individual. Information systems need to uniquely identify all user accounts, and if an existing identifier cannot cover the user base of the system, a new locally administered identifier needs to be introduced. External identifiers, such as the national identification numbers that governments assign to citizens, cause difficulties for the same reason; a foreign user does not have one, not necessarily even in his home country, because some countries do not use them [OTJA06]. In Europe, the national identification numbers are also considered sensitive [OTJA06].

Hierarchies can be used for making the local identifiers globally unique. Parts of a hierarchical namespace can be delegated to subordinate naming authorities. For instance, the Domain Name System (DNS) [RFC1035] of the Internet ensures that the identifier *mikael.linden@tut.fi* is globally unique in the SMTP based Internet email system. Respectively, the X.500 directory specification [ITUT05] uses country codes [ISO 3166] for constructing the globally unique identifier (called the Distinguished Name) of an object.

Use of global naming schemes has also faced criticism. Initiatives such as SPKI [RFC2693] and SDSI [RIVE96] have proposed to abandon the strivings for a global hierarchy and make use of local identifiers, instead. A local name is meaningful only for the one that assigns the name (for instance, “next door’s Bob”), and the local names can be chained to make them reach more people (“Alice is a friend of next door’s Bob”). If necessary, the public key of an object can be used as its globally unique identifier.

The identity of an individual is often considered the universal set of his attributes spread over a large number of information systems. In rare circumstances, one information system holds *all* the attributes of one individual – from the privacy perspective such an information system would present a huge privacy risk. Instead, the attributes are stored in several information systems; each set of attributes constituting *a partial identity* of the same individual.

The concept of partial identity is depicted in Figure 3, which presents an identity, consisting of four partial identities; one in a telecom company, one in an airline, one in a car rental company and one in the employer of the individual. Attributes like name and address are present and required for each of the four partial identities. To differentiate the individual from the others, the maintainers of the partial identities have assigned identifiers to the individual (such as, the employee number by the employer, the frequent flyer number by the airline, the customer number by the car rental company and the phone number by the telecom company). The credit card number is known only to the airline and the car rental company, which use it for crediting their services. Attributes like birthday and birthplace are not known to any of the four parties.

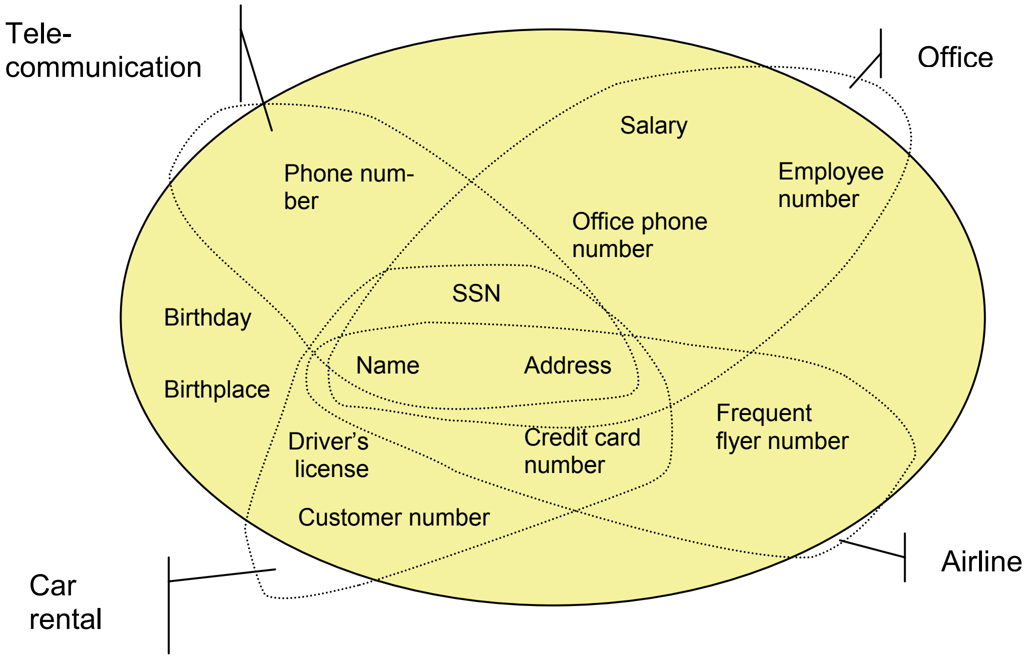

Figure 3. Partial identities of an individual [DAMI03].

None of the four parties possesses all the attributes of the individual. This is a desirable property from the privacy perspective, which is defined as the right of individuals to determine for themselves when, how, and to what extent information about them is communicated to others [WEST67]. Surveys show that people are concerned about their privacy [e.g. IBM99] and how and in which conditions their personal data is collected for profiling [CULN99].

According to Section 10 of the constitution of Finland, everyone's private life is guaranteed [CONS99]. Personal data act [PF99], implementing the European Union's data protection directive [EP95], provides more detailed provisions on the protection of personal data. The objectives of the act are to implement, in the processing of personal data, the protection of private life and the other basic rights which safeguard the right to privacy, as well as to promote the development of and compliance with good processing practice.

It is often not even possible to make a connection between the partial identities of an individual. For example, in Internet chatrooms, people use pseudonyms[3] to hide their identity, i.e. to complicate linking their partial identity in the chatroom to their other partial identities. However, there are also situations where linking the

[3] Greek: pseudo-onum (false name) means a name other than the real name.

partial identities is desirable for an organisation or for the individual, which is an essential theme in this thesis. Some of the reasons are as follows.

User convenience. People may consider their convenience more important than keeping their partial identities apart. This happens, for example, in a single sign-on scenario.

Organisation's business goals. An organisation's business goals make it necessary to be able to link a person's partial identities. For example, to avoid the abuse of social subsidies, it may be necessary for public bodies to get an aggregated view on all the subsidies and incomes an individual has.

Efficiency. In an organisation, maintaining several overlapping partial identities for an individual is inefficient, and lowers the quality of data. It is often more efficient to construct and maintain an aggregated view on the identity of an individual.

Information security. In order to protect information systems and, more widely speaking, the society where people live, it is often necessary to be able to trace people's transactions. Since this is also conflicting with the individuals' privacy, drawing the line between the individual's privacy and the society's rights to infringe it is a continuous discussion.

Mueller [MUEL04] points out that the interests of an individual and an organisation are often in conflict which each other. For an end user, issues like convenience of use, ability to have multiple identities (for instance, to separate work emails from private ones) and switching costs (cf. portability of telephone numbers in telecommunication services) are considered important. For the organisation maintaining the identities, issues like economics of scale, value of the data obtained (for example, regarding a user's behaviour as a consumer) and value of the resources protected (for example, company secrets) are of importance. Both of these interests need to be taken into account.

2.2. Authentication

As mentioned above, an identity is an abstraction of an individual in an information system. Authentication of identity, in turn, is making a binding between the partial identity and the corresponding individual in real life. By some means, the authenticator wanting to make the binding is assured that the individual in flesh-and-blood is the same person that has the partial identity in the information system. During authentication, some cryptographic material, such as a session key, is typically generated to secure the communication, and the binding exists as long as the cryptographic keys do.

Authentication always makes a connection between two events in time. It answers a question such as; is this person the same person who received his username and password two months ago in the helpdesk of the organisation? Is this person the same one who opened his bank account and deposited 1000 euros two years ago? Is this person the same individual who was issued a passport 8 years ago, when he was a kid of 10 years, accompanied with his parents? We often end up with a chain of authentications; the passport is used for opening the bank account and user account, and when a person wants to renew his passport, he again needs to present his previous passport or other proof of identity.

In the face-to-face world, the authentication can be done, for example, by means of a passport or other photo ID document issued by a party trusted by the authenticator, or the authenticator may recognise the face of the person being authenticated. In the on-line world, there are several means available with varying reliability. Literature often uses the following categories for authentication of people [RENA05:104]

- **Something people know** (such as PIN codes and passwords) or are able to recognise (such as faces or photos they have seen before)
- **Something people hold** (such as keys, smart cards or devices generating one-time passwords)
- biometrics, i.e. **something people are** (such as fingerprint or iris pattern) or how they behave (such as voice recognition or typing patterns).

All these authentication mechanisms have their well-known pros and cons. For instance, passwords and PINs are cheap and easy to deploy and nearly everyone is familiar with them, but people use them carelessly and they can be eavesdropped and replayed easily. Keys and cards need additional hardware, and biometrics is still considered a new and evolving technology. As analysis of different authentication mechanisms and their reliability is not in the core of this thesis, they are not further elaborated here. A framework for assessing the reliability of authentication is provided, for instance, in [BURR06].

It is important to distinguish between authenticating the identity of a person and a machine. The three categories above are available for weak authentication, when a machine needs to authenticate a human user. In a machine-to-machine authentication, there is an additional method called strong authentication, which utilises means provided by the cryptographic sciences. As humans cannot make the necessary cryptographic calculations manually, strong authentication cannot be used to authenticate a human user. However, strong authentication may play a role also in authenticating human users. For example, the user may hold a smart card with an on-board cryptographic processor, which uses a PIN code or fingerprint to authenticate the user. A server in the network, in turn, uses strong authentication to authenticate the smart card. As a result, the overall reliability of authentication increases. This setup (Figure 4) is typical in smart-card-based PKI and was the theme of Publication 2.

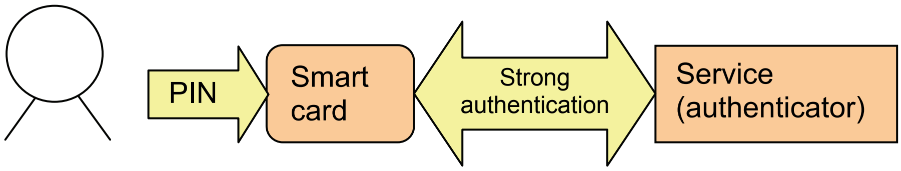

Figure 4. Weak and strong authentication in a chain

As will be seen, in the landscape of identity management, authentication is mostly a technical thing and there are a plenitude of technical ways and products to handle it. On the other hand, for common people familiar with a computer prompting for username and password, authentication is the thing that makes identity management concrete. Thus, in the media, it is a common misconception to think identity management is all about authentication.

As mentioned above, authentication makes a binding between an individual in-real-life and his partial identity. As a final remark, it should be pointed out that often it is not necessary for a service to know the identity of the end user. *Anonymity* is defined as the state of being not identifiable within a set of all the possible subjects [PFIT05]. Following the Personal data act, the Finnish Government Information Security Management Board VAHTI has adopted the view that, by default, an individual should be served anonymously. An individual needs to reveal his identity only if identifying the customer is necessary for the service [VAHT06b]. This principle can be applied to private services, as well.

2.3. Authorisation and Access Control

Authorisation is a decision to allow a particular action based on an identifier or attribute [CAMP04]. Introduced for the first time in the 1960s [LAMP69], an access control matrix has been the traditional way to express authorisation. In an access control matrix, each subject (end user) is represented by a row and each object (resource) by a column. A subject's authorisations to the objects are presented in the cells, using actions that are relevant in the context of the system. Each column of the matrix is called an access control list of the object, and each row the capabilities of the subject. [ANDE01:53]

Table 2 presents an access control matrix of a file system, using actions read (R) and write (W). Alternatively, in an access control matrix of an application for managing travel expense reports, the objects would be the travel expense reports and the actions, for instance, create a new report, approve a report and initiate payment.

Table 2. Access control matrix

Subject \ Object	/users/bob/	/tmp/foo	/etc/passwd
Alice	-	WR	-
Bob	RW	R	-

In a complex system with a multitude of subjects and objects, the access control matrix becomes very large and difficult to manage. End users leaving the organisation or changing their position make maintaining the access control matrix even more challenging. This has lead to the introduction of roles as a level of abstraction between subjects and the actions they are able to carry out for objects. In the 1990s, role-based access control (RBAC) has become a subject of research [e.g. FERR92, FERR95, SAND96, BARK97, FERR00]. For an organisation that experiences a large turnover of personnel, a role-based security policy is the only logical choice [FERR92].

In RBAC, each user is assigned one or more roles, and each role is assigned one or more privileges to carry out operations. Roles may have hierarchies and the separation of duties can be done using constraints. Since this thesis focuses on identity management in organisations, RBAC is an attractive tool for authorisation in subsequent sections.

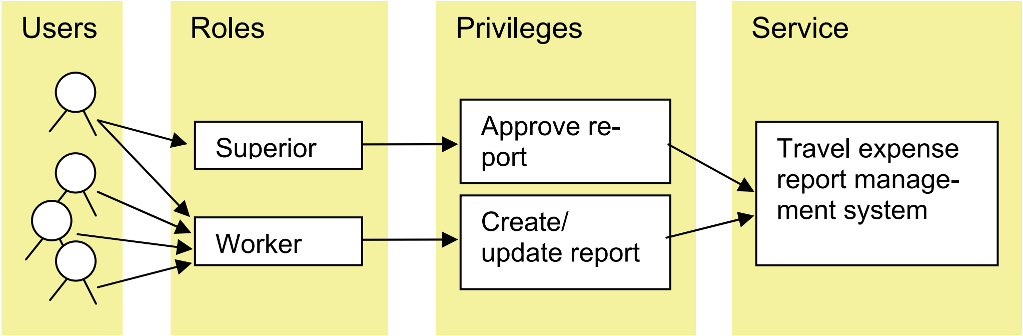

Figure 5. An example of role-based access control implementation in management of travel expense reports

Figure 5 illustrates an example of a travel expense report management system. In the organisation, all the employees have the role “worker” and the superiors have an additional role “superior”. The role-based access control policy of the travel expense report management system is that all the workers are allowed to make business trips (and claim travel expenses) and the superiors approve their workers' travel expenses. Now, an end user makes use of his role as a worker, when he signs in to the system, to use his create/update privileges. For approving the travel expenses, the superior signs in using his role, to use his privilege of approve report. Role hierarchies can be introduced to allow superiors to create/update their own travel reports, through the process of privilege inheritance.

RBAC has also limitations. Suppose that a service is permitted for any adult resident of Tampere, and each end user has two attributes; the place of domicile and the date of birth. For RBAC, a new role "an adult resident of Tampere" should be maintained for every end user (in practice, by deriving if from the two attributes). An end user may be permitted to use several different services whose access control may be based on distinct roles. As a result, potentially a large number of roles need to be maintained for each end user.

Attribute-based access control (ABAC) extends RBAC to make it more flexible. According to ABAC, permissions can depend on any attribute of the user, service or the environment [YUAN05]. The fundamentals of ABAC are presented in the access control framework by ISO/ITU-T [ISO96, ITUT95]. The framework bases an access control decision on any relevant information on the initiator and the target of the request, on the request itself and on its context.

If roles are considered to be attributes of the end user, ABAC is able to cover all the RBAC use scenarios. The access control can also be based on an attribute of the resource (for instance, the owner of the file) and on the environment (for instance, the date and the strength of user authentication). Using ABAC, access to an adult resident of Tampere could be grant, if the following equation is true:

(CurrentDate-DateOfBirth)≥18 years AND PlaceOfDomicile="Tampere"

Whether it is implemented using access control matrix, RBAC or ABAC, an essential principle in authorisation is the principle of least privilege. End users should not be given more privileges to resources than they need to accomplish necessary tasks. Separation of duties, a concept known in financial administration for centuries [ANDE01:187], augments the principle of least privilege by presuming that at least two persons are needed to carry out the most sensitive tasks. For instance, considering the example in Figure 5, it is necessary to introduce a constraint that prevents a supervisor from approving his own travel expenses.

Windley recognises the principle of least privilege as a good guideline, but in practice often difficult to implement to a full extent, because it implies very fine-grained modelling of permissions in the system. Essentially, every action that might ever be taken by any user on any resources needs a permission defined. Any change in the system or the way it is used affects the permissions in the system, which makes maintenance too cumbersome. Windley proposes that instead of implementing highly fine-grained permissions based on least privilege, a more coarse-grained model for permissions is enough if supplemented by accountability-based access control, which is going to be introduced in Section 2.4. [WIND05:65]

The ability to delegate is a fundamental issue in authorisation. Delegation means a subjects ability to transfer his privileges to another subject. This is a typical situation in an organisation, where many kinds of things contend for people's time. For example, a company policy may set the circumstances where heads of the units may delegate their privileges to approve travel expenses.

Access control relates closely to authorisation. Whereas authorisation is a rather abstract concept, covering an organisation's policies, practices and decision-making, access control is the concrete function in an information system that answers yes or no to the question "is this subject authorised to perform this action to the object". Access control is often divided into two functions; Policy Decision Point (PDP) which uses the available information on authorisations to produce the "yes or no answer", and Policy Enforcement Point (PEP) which enforces the decision made by the PDP. Extensible Access Control Markup Language (XACML) [MOSE05] defines a standard for expressing authorisation requests and responses and access control policies in XML format.

This section introduced authorisation as a process that follows authentication of the end user's identity. As a final remark, it is now pointed out that, for authorisation, it is not always necessary to uniquely identify an individual. Merely, it may be enough to ascertain a certain attribute of the individual. For example, a policeman asking for a driving license of a driver is usually interested in the person's permission to drive the vehicle, not in his name or other attributes. The same applies in the electronic world, and there have been proposals like SDSI [RIVE96] and SPKI [RFC2693] which make use of authorisation certificates without revealing the end user's identity to the service. Federated identity management opens new possibilities to provide authorisation without identification. They will be covered in Section 6.1.3.

2.4. Auditing

As different information systems have become more integral and important to businesses, risks of failures in peoples access rights and the way people use them have grown. Complementing authorisation and access control, the importance of having proper mechanisms for auditing and accountability has grown, partly as a consequence of the Sarbanes-Oxley Act of 2002 [USAC02] in the United States. Providing reporting tools for audit purposes has become an ordinary feature of available commercial products.

According to the Government Information Security Management Board VAHTI [VAHT06], reporting tools should provide reports on

- what roles are given to a user
- what privileges are assigned to a role
- what privileges are assigned to a user (combination of the two above)
- which users have a given role
- which users have a given privilege

Using the tools, identity management audits should be conducted in a regular basis to find out

- if there are end users who are no more employed by the organisation
- if there are roles which are no more in use
- if there are objects or privileges which are no more in use
- if there are orphaned authorisations (i.e., to an object that does not exist any more)
- that separation of duties is implemented properly and the end user's privileges do not cause dangerous combinations
- that roles, objects and processes have owners with well-defined responsibilities
- that identity management processes are defined and followed

As mentioned in the Section 2.3, Windley points out that the permission-based access control model is difficult and expensive, if applied to the full extent. Windley proposes that it is more practical to augment the permission-based model with what he calls accountability-based access control; user actions are logged, and when the logs show an unauthorised access by a user, appropriate action is taken afterwards. According to Windley, accountability-based access control scales better than permission-based access control, because it is a log processing problem that can be done offline by a separate system. In a real-world scenario, organisations should consider what is the risk they can tolerate, and balance the use of permission-based and accountability-based access control. Accountability-based systems are considerably cheaper to implement and operate. [WIND05:66]

Windley does not make it explicit, how the logs should be processed to disclose unauthorised use. If there was a fully automatic system that reads log files and flags unauthorised access, why not to use it as a Policy Decision Point that generates a negative response to an unauthorised access request on-the-fly, not afterwards? Apparently, Windley means that there is some human intervention involved; log files are examined when there are doubts that unauthorised access has taken place. For instance, in Finland, every now and then it turns out that individual civil servants have misused the population registry to query personal data on public figures for curiosity. The government states that, besides educating civil servants, there are afterwards controls in place to detect improper use of the population data [WIDE03]. While this can work as a deterrent for misuse, it can hardly discover all the misuse that happens.

Regarding accountability-based access control, it should be noticed that processing log files identifying an individual is processing personal data. In Finland, the Personal Data Act [PF99] and the Act on the Protection of Privacy in Working Life [PF04] set limitations on how log files may be processed. As an example, Windley proposes audits of the email server logs to ensure that the company secrets are not sent to the competitors by email [WIND05:66]. However, for an employer, this is currently forbidden in the Finnish law [PF04].

A properly implemented inerasable audit trail should take into consideration the fact that end users' identities and authorisations change over time. It is possible, that the user had the authorisation when carrying out the action but has later departed or changed his position. At the time when the audit records are examined, he would not have the authorisation. Whether permission-based or accountability-based access control is used, the audit trail should be able to answer, why an end user was permitted to do the action at the time when it was carried out.

2.5. Putting the Concepts in a Timeline

To conclude the introduction of identity management concepts, the concepts are now placed on a timeline in order to find out in which order the concepts typically take place in an organisation. In real life, the order of some of the events may vary, but certain common characteristics can be identified.

Depending on the history of the organisation and its information systems, role-based authorisation is a prime candidate for the first thing to happen. For example, in a well-established organisation, the company policy for approving travel expenses has probably been done years ago, for example, by the board of directors (noted as the man with the tall hat in Figure 6). The policy can be, for example, that "the heads of the units are permitted to approve travel expenses". Hence, the authorisation is done, effectively, when this policy has been agreed on, and everything that follows (for example, assigning privileges to the heads of the units) is just implementing the policy.

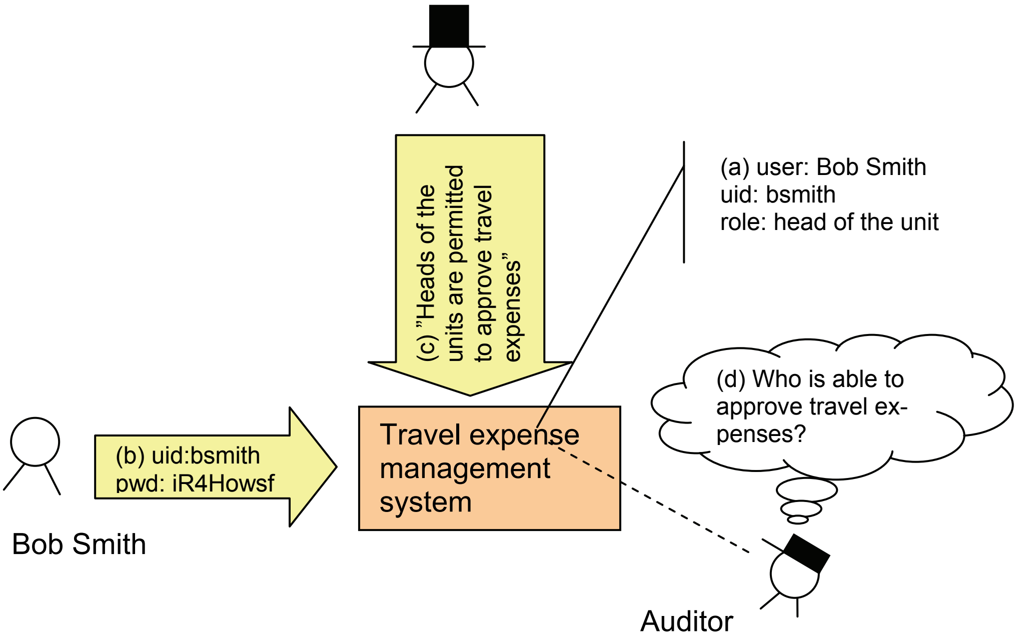
(c) "Heads of the units are permitted to approve travel expenses"
(a) user: Bob Smith
uid: bsmith
role: head of the unit
(d) Who is able to approve travel expenses?
(b) uid:bsmith
pwd: iR4Howsf
Travel expense management system
Bob Smith
Auditor

Figure 6. Example of identity (a), authentication (b), authorisation (c) and auditing (d) in a travel expense management system

A candidate for the second concept to be addressed is identity. To be more specific, this covers creating a partial identity for an end user (Bob Smith in the figure) and assigning one or more identifiers (bsmith in the figure) to him to ensure his unique identification. The partial identity is supplemented with appropriate attributes, such as the role and privilege attributes for the travel expense management process. Once created, the partial identity has to be maintained as well, as the user's attributes and roles change during his job career. From the information security point of view, the most important change takes place when a user finally leaves the organisation; related changes to his identity and attributes need to be made in order to stop him from using the organisation's information systems that he is no more authorised to use.

Considering the timeline, authentication and access control are the two things that take place when a resource is being used. During authentication, the information system ensures that the end user, located somewhere in the Internet, is the person who has a partial identity in the user database of the information system. In Figure 7, Bob presents his identifier (bsmith) as a claim of his partial identity, and the claim is verified with a password.

Once the identity has been verified, the subsequent access control procedure makes the decision whether the end user is permitted to access the resource or not. In the figure, role-based access control is implemented; Bob Smith has a role "head of the unit", and the company policy is "heads of the units are permitted to approve travel expenses", thus, Bob is permitted to approve travel expenses. Once Bob completes his task, he closes his session, and the authentication and access cease.

Audits can be done before or after the end user uses the information system. If done beforehand, the question is often "which users are authorised to use this system in this role" or "what actions is this user authorised to carry out". If auditing is done afterwards, the question is "which users have used this system during a certain period of time" or "what tasks has this user carried out in the system during certain periods of time".

This concludes the introduction of the four concepts of identity management. From a technical perspective, the goal of identity management is to ensure that the end user is able to make only the actions he is authorised to do. From a juridical perspective, identity management ensures that an authenticated person can be kept accountable for the actions made using that identity. Together with the identity management practices and the audit trail, those actions can be traced back to a person in-real-life. This shows how these four concepts are intertwined and cannot be considered separately from each other.

3. IDENTITY MANAGEMENT IN AN ORGANISATION

Organisations, whether they are private companies or public bodies, store identity information of people affiliated to the organisation, such as employees, customers, patients and students. In an organisation, identities have lifecycles. When a new person (say, employee) enters the organisation, his identity is created to related information systems (provisioning). When attributes of the identity are changed (e.g. employee changes his position), the changes need to be reflected to the information systems, and, finally, when the person's affiliation to the organisation ceases, his authorisations in the information systems needs to be revoked (de-provisioning).

Traditionally, identity management in an organisation has meant integrating information systems for user provisioning, password management and access control [DJOR05]. For this thesis, the definition of identity management has been adopted as the process of representing and recognising entities as digital identities in computer networks [JØSA05].

Usually, identity management also covers authentication, authorisation and auditing.[4] On the other hand, in identity management, there are also scenarios in which an identified user does not actually "log in". For example, tax authorities gather data from an individual, his banks and his employer, and identity management (in practice, the national identification number) ensures that incomes and taxes are registered for the correct taxpayer. However, currently in Finland, electronic tax declaration is not in use and the taxpayer (the identified user) cannot actually log in (although tax inspectors do log in). In that sense, identity management is a wider concept than user administration, which is considered to mean keeping track of the information system users and their privileges.

Managing identities in an organisation's information systems has been a familiar topic for practitioners for years. However, as noted by Fuchs and Pernul [FUCH07], it has not gained significant attention in the research community. There are some case studies available [e.g., BLEZ02, ANCH03, LARS05, RIEG07]. Many practical issues are covered in Phil Windley's book Digital Identity [WIND05].

3.1. Benefits of Centralised Identity Management

In isolated identity management, each information system manages its own identity data independently. In centralised identity management, the organisation has

[4] Sometimes, the concept of Identity and Access Management (IAM) is used instead to underline authentication, authorisation and auditing as part of identity management.

built interconnections between the identity data in its information systems. Instead of having partial identities in each of the organisation's information systems, individuals have one unified partial identity that covers all (or, in practice, most of) the information systems. An end user has a unique identifier which identifies him in the information systems, or there is at least[5] a mechanism (such as a directory) which is able to map the identifiers a person has.

For the owner of an information system, centralised identity management often reduces routine work related to identity management. The system owner does not have to care about creating identities to new persons and making sure they are up-to-date and deactivated appropriately, when the person departs. Furthermore, if the end user has a password for logging in, credentials provided by the centralised identity management can be utilised, and the system owner does not have to care about, e.g., resetting forgotten passwords. In short, the system owner can concentrate on doing his business and leave administrational routines, like identity management, to the organisational unit responsible for them, such as to the IT service unit.

For an end user, centralised identity management enables the principle of one login credential; for example, a single username and password. Because a user has to remember only one frequently used password, it is easier to learn and remember, and there is less need to write passwords down on a piece of paper. Furthermore, it is realistic to put more requirements for the single password, regarding its quality and renewal times. As a result, security of password-based authentication is enhanced.

From the information security perspective, centralised identity management also makes it easier to ascertain that end users' accounts and permissions to use information systems expire as they depart from the organisation. Forgetting to close people's accounts when they leave is considered a major security risk for an organisation. Furthermore, new and more reliable authentication mechanisms can be introduced to several information systems at once, because the new authentication credential can be coupled with the end user's identity in one centralised place. Finally, having an aggregated view on a person's identity makes it easier to implement tools for auditing purposes.

All in all, centralised identity management increases an organisation's efficiency by reducing the overlapping work in identity management. End users are happier

[5] For instance, in the HR system, the identifier is typically the employee number and in Unix, it is the uid of the user. However, it may be impossible to use the employee number as the unique identifier in other systems, because users other than employees do not necessarily have them. The HR system, on the other hand, may be a legacy system not supporting the use of external

with fewer passwords to remember, and information security is increased. Furthermore, introducing new information systems becomes easier as there is an identity management infrastructure in place, on which the new systems can rely.

To conclude the chapter of the benefits, it is worth noticing that despite its benefits, the applicability of centralised identity management has also limitations. If not designed for compatibility, software products may not necessarily have interfaces that could be used for integration to the organisation's centralised identity management, or the integration cost of the product (especially, if the number of users is small) could just be too big. Traditionally, software products used to be monolithic systems with no modular interfaces for external authentication and access control. Instead, authentication and access control was coded directly to the programme code. Furthermore, depending on the policy of the organisation, the most sensitive systems may not want to rely on an identity management external to the system, either.

3.2. Identity Flows in an Organisation

Software vendors have recognised that real organisations do not have coherent information system environments acquired from a single vendor. Instead, organisations do and will have several systems carrying identity records of the same individuals. For example, the human resources (HR) system carries the personal details of employees and their employment, telephone exchange their phone numbers, Windows Active Directory their user accounts in the Microsoft environment and so on. The way forward is to interconnect these information systems so that identity changes in one system are reflected to other systems in a predefined way.

In order to rationalise identity management in an organisation, some person registries are elevated to **base registries**, which are the registries where new identities enter the organisation. Once a new identity has been created in a base registry, it is available to other connected registries as well. New persons cannot be entered to connected registries without entering them to a base registry. On the other hand, if an identity is removed from a base registry, it is de-provisioned or deactivated in the connected registries as well. One can say that a base registry owns an identity object in the identity management system of the organisation.

Authoritative sources complete the picture; they are person registries which own a certain attribute of an identity object. Changes to the attribute are propagated from authoritative sources to other connected systems. Prominent authoritative sources are, for example, email server for email address, telephone exchange for

identifiers, such as uids. It is sufficient that the centralised identity management is able to map the two identifiers.

phone number and for employee number the employee registry, which can also be a base registry for an entire identity object.

Agreeing on the authoritative source for each attribute in the organisation aims at removing overlapping maintenance of the same piece of information. If there are two organisational units maintaining independent instances of the same information (for example, in a university, both the student administration and the library maintains students' home addresses in their systems), it is likely that changes to the information are not done consistently, causing loss of integrity of the data.

Agreement on authoritative sources can be compared to a normalised database, a concept that database designers are familiar with. Both of them increase the quality of data by removing potentially conflicting instances of the same data. Actually, one could see organisational identity management as one big logical database with update rights granted to different parts of the organisation.

An enterprise directory is a core middleware architecture that may provide common authentication, authorisation and attribute services to electronic services offered by an institution [BELL02]. The processes used for feeding the enterprise directory with data from the base registries and other authoritative registries are called **a metadirectory** [BELL02]. A metadirectory can be implemented as a home-grown set of scripting, database views etc. However, during recent years, several commercial metadirectory products have entered the market [PERK07].

An alternative way to implement an enterprise directory is **a virtual directory**, which, unlike a metadirectory, does not make copies of identity data from authoritative sources to an enterprise directory. Instead, a virtual directory provides a view of a single directory, but when a connected system makes use of the directory, personal data is actually fetched from base registries and authoritative sources on-the-fly. [WIND05:87]

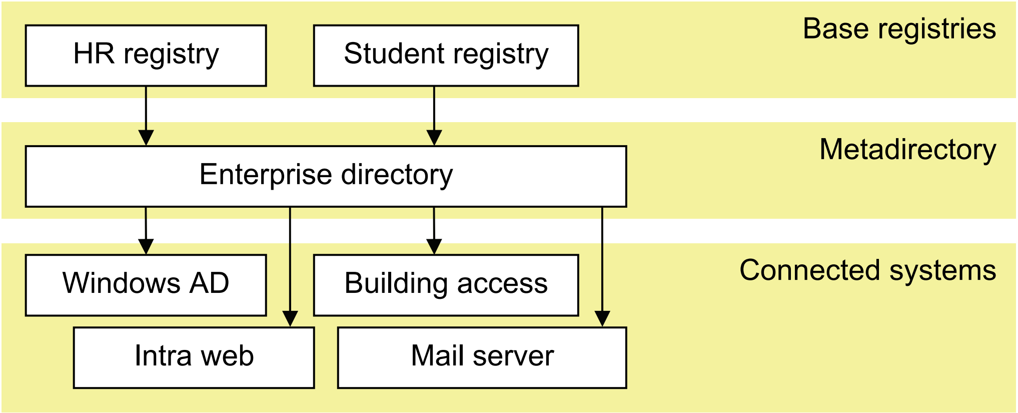

Figure 7. Identity flows in a university

Figure 7 illustrates an example of a university. The two main groups of people affiliated to a university are students and employees. The student registry stores data on the students' target degrees, enrolments and credit units, and is by nature the place where the students' role information is most up-to-date in a university. In the same way, the Human Resources (HR) registry is the registry used for paying salaries to employees, and the data can be expected to be of high quality. These two registries are most likely base registries in a university. Depending on the institution, there may be additional base registries for the alumni, library patrons etc. It is worth noticing that the same individual may exist in several base registries at the same time and the identity flow has to take that into account.

In the figure, the metadirectory connects the registries. When a new identity is entered to a base registry, the metadirectory uses predefined rules to provision the identity to the other registries. Consequently, the email server may take the responsibility of creating the user's email address, which then flows back to other registries, possibly including the base registry. Thus, the email server is the authoritative source for the user's email address.

The end user himself can also be the authoritative source for some attributes. The password is a typical example; when the password needs to be changed, the end user types in the new password, which is then propagated to the registry/registries making use of it. Depending on the organisation, office room number or office hours of a professor are other potential attributes for self-administration. However, an attribute used for authorisation should typically not be administered by the user himself.

Publication 1 describes a study on the present identity management systems in Finnish universities. The study was conducted as part of a several-year project to improve identity management in Finnish universities and polytechnics. In the project, staff of the institutions' IT service units were interviewed to investigate current identity management practices. The study, which covered 61 percent of the higher education institutions in Finland, showed that most of the institutions make use of the student registry as the base registry for students' identities. However, for employees' identities the use of the HR registry is considerably lower. In connected systems, email servers, operating system accounts and intranet accounts make use of the enterprise directory, mostly because they are all maintained by the information management unit. Other organisational units, such as the library and the learning technology centre, do not make use of the enterprise directory. Instead, they provide end users with an extra username and password and maintain the identities separately.

The study showed that Finnish higher education institutions have a lot of potential in making their identity management more efficient. In the project, an attempt was made to disseminate best practices from the forerunners to the other institutions. Details on the dissemination activities are presented in the publication.

3.3. Object model for Identity Management in an Organisation

Based on the introduction of the concepts in Section 2 and the identity flows introduced in Section 3.2, this section presents an object model for identity management in an organisation. The model is visualised in Figure 8 using a class diagram of UML [OMG07], which is the most important and widely used specification language for object modelling in the software industry [HAIK04:117]. The attributes and methods of the classes are context-specific and omitted from the figure.

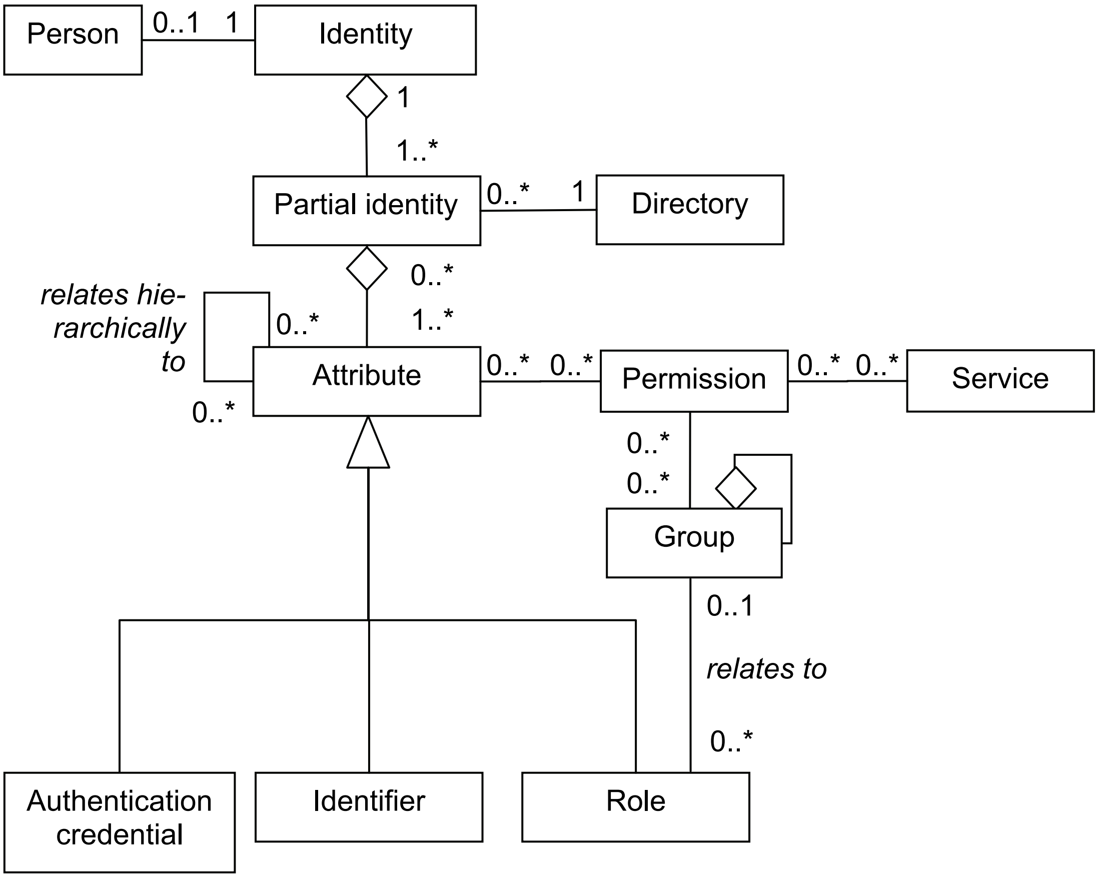

Figure 8. A UML class diagram of identity in an organisation

Following the convention adopted in Section 2.1, each living **person** has exactly one **identity**, which is a universal aggregation of the **partial identities** representing him in different information systems. For accountability purposes, the identity remains after the person dies or (in the context of organisational identity management) departs, implying that the identity can be associated to zero or one living person. On the other hand, in this model, each partial identity belongs to exactly one identity. Otherwise, the identity would represent not a single person but a group of persons.

In the context of organisational identity management, a partial identity is stored in a **directory**. If all the information systems in the organisation were connected to the centralised identity management, an end user would have just one partial identity, which is stored in the enterprise directory (see Section 3.2) of the organisation[6]. However, if the organisation has information systems which do not make use of the centralised identity management, identities in those are considered as separate partial identities and stored in other directories (e.g. in a local user database of the system). For instance, if the organisation has centralised identity management with an exception of three information systems having an isolated identity management, an end user may have four partial identity instances in the organisation, one in the enterprise directory and three in the local directories.

As mentioned in Section 2.1, a partial identity consists of **attributes** describing the individual. **Identifiers** are attributes which deserve special attention; they identify uniquely a partial identity (and, hence, a person) in their context. For usernames, the context is, typically, an information system or the organisation as a whole. E-mail addresses are globally unique, whereas national identification numbers have one country as their scope. One partial identity may have one or several identifiers associated to it, some of them (such as an employee number or a username) assigned locally by the organisation and some (such as a national identification number) by an external organisation. To ensure unique identification in all circumstances, at least one locally assigned identifier is necessary. Otherwise, the organisation faces problems with end users who do not have external identifiers (such as a national identification number) or whose external identifier is not known to the organisation.

Introduced in Section 2.3, **roles** are attributes describing the user's relationship to the organisation in order to facilitate access control. Some roles describe the person's relationship to a **group**. The person may, for instance, be a member or a chairman of a group, or the group may be the project team of a project manager. Groups may have hierarchies as well, that is, they may have subgroups. Any number of individuals may be related to (e.g. be a member of) a group. On the other hand, in this model, a role (e.g. a membership) can be related at most to one group. If a person is a member in two groups (for instance, a group and one of its subgroups), he has two separate role attributes.

[6] In practice, the metadirectory synchronises local identity copies in the connected systems as proposed in Figure 7. In the UML diagram, the directory represents the identities in the connected systems, as well.

Authentication credentials are attributes which assist in making the binding between an end user and his partial identity. By possessing an authentication credential, an end user proves that he is the person the partial identity represents. An authentication credential is personal i.e. belongs to one or zero persons (zero, if the person has died or permanently lost the authentication credential).

In this model, only individuals can be authenticated. A group cannot be authenticated per se, because, as mentioned in Section 2.5, the audit trail must ensure that the actions taken in an information system can be traced back to a person in-real-life. If groups were authenticated principals, it would not be possible to trace an action back to the individual. Instead, in this model, an individual needs to be authenticated first and then his role attribute examined to find out his group membership.

An authentication credential can be, as mentioned in Section 2.2, e.g. a password, an asymmetric key pair or some biometric data. Some authentication credentials, such as asymmetric key pairs, are also unique identifiers, because nobody should possess the same asymmetric key pair (if it were not, then the key generation process would be seriously flawed and the public key system implementation should be abandoned [RFC2693]). Some credentials need not to be unique; for instance, two different persons may accidentally use the same password. Usually, an end user enters his password together with his unique identifier (e.g. a username).

Attributes, or some of them, may be arranged in a hierarchy, which is defined as a graded or ranked series of values [MERR08]. For numeric attributes, such as the date of birth, weight or seniority, the hierarchy is obvious. Job titles, military ranks and security clearances can be hierarchical, as well. Also roles may have hierarchies and having a higher role in the hierarchy implies the lower role [FERR00]. For instance, if a project manager is defined to be higher in the hierarchy than an employee, a project manager has automatically the role employee, as well. Furthermore, a hierarchy may apply to authentication credentials. A framework (such as, NIST SP 800-63 [BURR06]) may be in place for assessing the strength of authentication mechanisms and deducing that some authentication credential may provide stronger authentication than the other.

On the right side, **services** are the information systems that the end user is using. An end user may have a **permission** to make operations (such as, read or write a file or approve a travel expense report) in the service. Each permission may allow the end user to do various actions in the service (for instance, the end user may both create and update a travel expense report) and, on the other hand, several different permissions can be defined for a service (a worker can create a travel expense report and his supervisor approve it). How the permission depends on the service is context-specific and not answered by the object model. In an implementation, a permission may, for instance, depend on the ownership of a file. During log-in, other conditions (such as the date and the strength of authentication[7]) may also affect the decision to grant or deny access.

The object model makes use of the attribute-based access control model (ABAC) that was presented in Section 2.3. In ABAC, a permission is based on any security relevant attribute of an end user (such as, the name, age, organisational unit, home postal code or a role). Alternatively, a permission may be given to a group and the users belonging to the group may use the permission.. If the permission is based on a hierarchical attribute, superior attributes inherit the permissions of the lower attributes in the hierarchy [FERR00]. For example, if a student of a course is permitted to access a learning management system, and a teacher is superior to a student, then the teacher is permitted to access it as well. If teachers are not actually permitted to access the learning management system then they should not be made superior to students in the role hierarchy

Groups, people and attributes have some similar properties, but they also have differences. The differences between a group, a person and an attribute are as follows:

- groups are entities in their own right and may have attributes that describe them such as address, term, officers, etc. Attributes do not have similar properties
- people are members of groups and this is signalled by the person having a group membership attribute. Groups may also signal this by having a membership attribute that list the people who are its members.
- people are entities with authentication credentials but groups are entities that do not have authentication credentials

As mentioned in Section 2.3, an access control matrix and role-based access control are special cases of ABAC. If the attribute to which the permission is assigned is an identifier of a partial identity, the traditional access control matrix is used. If the permission is assigned to a role, role-based access control in use. According to the UML diagram, a permission could be assigned to an authentication credential, as well. This is useful if the authentication credential is a certificate, but assigning permissions directly to passwords may not be reasonable.

[7] Several authentication assurance frameworks, such as NIST SP 800-63 [BURR06] and EC IDABC Interoperability [IDAB07], pay attention not only to the authentication mechanism used in the beginning of the session, but also on the assurance of who possesses the authentication credential (including, e.g. the initial proofing of identity and the delivery of the credential to the end user). In this object model, the static aspect can be expressed as an attribute of the authentication

A class diagram for user identities is probably part of the design documentation in many software projects in the industry. In the literature, there is some previous work available, as well. Emig et al [EMIG07] have presented an access control model for web service-oriented architecture (WSOA). The model aims at supporting a problem typical for web services; has a permission been granted for an authenticated subject to invoke a WSOA service.

Focused on WSOA, Emig et al model the service-related side of the object model more carefully, including the web service operations and their parameters. Still their model has a lot in common with the object model presented in Figure 8. The most notable difference is that Emig et al have an indirection between roles and permissions that they admit is not consistent with RBAC; roles are not attributes of an identity, but a user's attributes can be derived from her roles and permissions can then be associated to the attributes. Furthermore, Emig et al do not introduce partial identities in their model because they consider them irrelevant for their WSOA focused model. However, they are relevant for this thesis with a focus on identity management in an organisation.

There are also object models focusing on smaller parts of the model presented in this thesis. Shin et al [SHIN00] have presented an object model on role-based access control. The model is more specific and covers also role constraints and sessions. Basin et al [BASI06] have supplemented RBAC with a hierarchy of actions as an additional layer of abstraction between permissions and services. Furthermore, Basin et al assign roles to the subject class, and users and groups are subclasses of the subject class. In other words, according to Basin et al, the authenticated principals can be either groups or individual users. In this thesis, the subjects are always individual users, because Section 2.5 has emphasised the ability to trace the transactions back to the individual for accountability purposes. If the authenticated subjects were groups, the identity of the individual group member could not be revealed.

This section introduced an object model for identity management in the context of an organisation. In Section 4, the thesis is extended to cover identity management in contexts which consist of several organisations. We will see that in federated identity management the partial identity of an end user needs not to be managed by the same organisation that manages the service. Later, in Section 6.1.3, it will be also discussed which of the parties will manage the roles and permissions of the end users.

credential object class. It is a responsibility of the authentication service to make sure that the actual perceived strength of authentication in the beginning of a session does not exceed it.

3.4. PKI in Authentication

Whereas identity flows and authorisation often happen in the back-end systems, authentication and access control ("the machine prompting a username and password") is where identity management becomes visible to an end user. This tends to emphasise the importance of authentication as part of identity management in an organisation. People not familiar with the big picture of identity management try to find ways to enhance identity management by enhancing authentication, which are two separate, although interconnected, issues.

In a public key infrastructure (PKI), an attribute of an end user's identity is his public key. The private key corresponding to the public key should be in the sole control of the end user, for example, in a smart card in the end user's pocket. In order to authenticate in an information system, an end user uses his private key to respond to a cryptographic challenge presented by the authenticator. A more complete description of PKI, smart cards and their utilisation in an organisation can be found in the author's licentiate thesis [LIND02].

PKI, as defined in the X.509 standard [ITUT00], is the infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services. According to PKIX (the Internet Engineering Task Force working group for X.509 based PKI), it is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography [RFC4949]. PKI is another method of managing end users' identities. A public key certificate, signed by a trusted certificate authority, and a signed message from the keyholder can be used for authenticating the keyholder, and other unique identifiers, attributes or even permissions of the end user can be extracted from his certificate.

PKIs and directories are complementary ways to implement identity management in an organisation. In a directory based implementation, the relying party (e.g. the service the end user is using) needs an on-line access to the directory for authentication and retrieval of attributes. In a PKI based implementation the attributes are available in the certificate(s) signed by one or more certificate authorities. Using the public key in the certificate, the end user can be authenticated in a distributed manner and the certificate authority's signature guarantees the integrity of the data in the certificate. It is also possible to deploy a conversion for certificate and directory based identity management. For instance, certificates can be issued on-the-fly based on the attributes provided by the directory.

Several studies have shown that PKI is too difficult for common end users to understand [WHIT99, BALF05, WIND05:56]. Users do not have intuitive understanding of public key cryptography and how PKI is used to achieve a goal, for example, to send an encrypted message. Requesting and using a certificate may be easier, when a user has a concrete medium – a smart card – to be inserted for authentication, but the drawback is the need for additional hardware and software (smart card reader with related drivers). [8]

Publication 2 presented results of a project that looked for ways to introduce PKI relying on smart cards in Finnish higher education. The two-year FEIDHE project, featured by eight pilots, took place in 2000-2002 and was a common project for all the Finnish universities and polytechnics. The publication presents seven conclusions regarding security, interoperability and branding of a PKI smart card and to whom and how the smart cards should be introduced.

An essential finding in the publication was that whereas certificate-based authentication increases the reliability of authentication, the first step is to introduce a centralised identity management in the organisation. In centralised identity management, an end user has one identity in the organisation, and the public key can be introduced as an attribute for that identity. As a result of the publication, focus in identity management in Finnish higher education was moved from PKI-based authentication to organisational identity management.

A usability study [TAUC02] made as part of the project showed that if a PKI with smart cards is introduced as an authentication mechanism for end users, they expect that all or at least a majority of services are available with the smart card authentication. The end users become frustrated in a mixed world, where some of the services are available with smart card authentication and some with traditional passwords. So, from the usability perspective, PKI and smart-card-based authentication make sense only, if they can be introduced to a large number of services simultaneously. The only reasonable way is to first introduce the centralised identity management, and then introduce the public key as one attribute of an end user in the centralised identity management. Finally, the PKI-based authentication can be introduced to services, provided that applications and end user devices support it and that support and helpdesk have been organised for end users.

Studies have also concluded that equipping an end user with the necessary hardware and software and organising training and support makes PKI/smart card deployment expensive [DAMI03, WIND05:56]. Fulfilling the end users' expectations of a smart card-based authentication to all the services may turn out to be too costly. Publication 2 suggests that PKI-based authentication is introduced based on the need; first, to the most sensitive applications and to end users, such as adminis-

[8] It is still to be seen if integrated architectures, such as a private key placed in the SIM card of a mobile phone, manage to alleviate the problem.

trators, whose reliable authentication is important. Windley shares this view [WIND05:57].

3.5. Single Sign-on and Logout

Information security and usability[9] (”the ease of use”) are often considered as competing design goals. Concepts like single sign-on (SSO) can alleviate the confrontation by making security systems more usable. Nevertheless, security designers too often neglect the whole issue, resulting in introduction of systems with usability flaws. Users are known to be the weakest links for security and a security system with a usability flaw is a trap that is set for an unsuspecting end user. In Publication 3, one trap was located in the logout functionality of common single sign-on systems.

Single sign-on is one step beyond authentication; it means that an end user only has to authenticate once and, then, all the services permitted to him are available without further authentications. The authentication mechanism can be anything, nowadays often username and password.

Pashadilis et al [PASH03] and De Clercq [CLER02] have presented architectures and systems for single sign-on not only in the web but in information systems in general. In his taxonomy, Pashadilis presents four categories for single sign-on systems. These categories are summarised in Table 3. The closest corresponding categories by De Clercq are presented in parentheses.

Table 3. The four categories for single sign-on (SSO) systems by Pashadilis et al [PASH03]. De Clercq’s corresponding categories are in parentheses [CLER02].

	Local SSO systems	Proxy-based SSO systems
Pseudo-SSO systems	Local pseudo-SSO systems (secure client-side credential caching)	Proxy-based pseudo-SSO systems (secure server-side credential caching)
True SSO systems	Local true SSO systems (public key infrastructure - based SSO systems)	Proxy-based true SSO systems (token-based SSO systems)

In pseudo-SSO systems, no modifications are necessary for the actual service. Instead, there is an intermediate pseudo-SSO component between the user and the

[9] ISO 9241-11 standard defines usability as the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. [ISO98]

service. The component authenticates the user and provides his cached credentials to the service. In a true SSO system, there is no cache for user credentials. Instead, the services are modified to trust assertions made by a specific Authentication Service Provider that takes care of the actual authentication of the user.

In a local SSO system, single sign-on is implemented by a component installed in the user's workstation or other client device, whereas in the proxy-based mode, there is a separate server dedicated for authentication between the user and the service.

A usable implementation of single sign-on has its challenges. Logout in a single sign-on setup is often a neglected functionality. For Publication 3, the authors carried out an empirical study on end users' expectations of logout in a web single-sign on system. The study focused mostly on the intranet of an organisation and was the first that drew attention to this often-neglected side effect of single sign-on. The results have implications on how usable services should be implemented in a single sign-on environment.

The following scenario clarifies the logout problem in a single sign-on environment.

1. An end user signs in to service A with his web browser and is prompted to enter his username and password.
2. Having used service A, the end user follows a link to service B. Because of the single sign-on, he is able to start using the service without further authentication.
3. Finally, the end user presses a logout button in service B.
4. If the end user now browses back to service A, does he expect he has to enter his username and password again?

The study showed that when single sign-on is in place, end users also expect single logout. It means that when an end user clicks logout in one of the applications he is logged in to, he expects that he will be logged out of *all* of the applications in the single sign-on environment. This is doable in a pseudo single sign-on system (see Table 3), where all the traffic goes through the proxy; the session between the end user and the pseudo-SSO component is simply torn down, and the end user cannot use any of the services any more. The functionality could be implemented also in a local pseudo-SSO system. However, common web browsers, for instance, do not usually provide logout functionality for session making use of the HTTP Basic Authentication, and the only way to logout is to close the browser.

However, in true single sign-on systems, logout is cumbersome. Somehow, the protocol used for single sign-on should implement a transaction that tears down the existing sessions with all the applications the single sign-on covers. In the context of web applications, this typically includes removing a cookie from the cookie store of the end user's browser. This covers also any federated services that will be introduced in Sections 4 and 6.2.

Furthermore, the study also concluded that the users should be fully aware whether they are unauthenticated or authenticated end users in the service. This can be accomplished, for example, by showing the name of the authenticated user in the user interface.

3.6. Identity Management Architecture

Section 3.2 presented a conceptual infrastructure for identity management. However, a lot of managerial work has to be carried out before an organisation is in a position where it is able to set up an enterprise directory, connect it to existing registries and let the users enjoy the single sign-on experience. Identities are closely coupled to the organisation's business, and introducing an enterprise directory means unifying the organisation's policies and procedures.

Windley defines identity management architecture as a coherent set of standards, policies, certifications and management activities which are aimed at providing a context for implementing a digital identity infrastructure that meets the current goals and objectives of the business, and is capable of evolving to meet the future goals and objectives [WIND05:134]. According to Fuchs and Pernul, identity management is based on three pillars; technologies, processes and policies [FUCH07]. Identity management architecture is a result of an actively managed evolutionary process, also covering issues which have little to do with the actual identity management at the first sight.

For example, suppose that the HR registry is elevated as a base registry as proposed in Section 3.2. Entering a new person to the HR registry triggers provisioning his identity to the other connected registries and removing it when the contract ends. Earlier, the HR department has considered that their primary task is that monthly salaries are paid in time, and the clerks in the department have phased their work to serve that goal. As a result, the practice may be that the clerks gather new contracts of employment and enter them to the HR registry once a month, and it turns out that the only day the HR registry is up to date is the day the salaries are paid. However, if the HR registry is used for provisioning and de-provisioning employees' identities, the registry should be updated on a daily basis. As Mueller [MUEL04] points out, use of the HR department as the entry point for user data may cause unanticipated problems, because HR people are not focused on how other departments use the data.

As another example, during projects in the Finnish universities, the author has often faced a practice that employees have several periodical contracts of employment in a sequence. When a new period starts, there may be a gap of a few days or weeks before the busy head of the institute is at the office for signing the new contract. Meanwhile, the employee contacts the IT service desk and asks some grace period for his user accounts to be able to continue his work. However, this is curing the consequence, not the cause of the problem. Missing contracts of employment[10] may cause also other problems, for instance, with insurances and, after all, it is modest that the employee is able to be confident that he is really employed and will be paid salary. Instead of designing and maintaining processes for the problems caused by delayed renewals of contracts, the organisation should pay attention to the efficiency of the process for hiring and renewing the contracts of employment. Timely renewal of contracts is desirable both for the employee and the employer.

Centralised identity management means processes and data flows across organisational units. One of the practical challenges of identity management architecture is unifying syntax and semantics of the data flows. What are the codes and vocabularies used in different organisational units? What do they mean and how are they used? Codes and vocabularies cover, for instance, structure of the organisation, project codes and job titles, different types of user identities etc. Unifying attribute syntaxes and semantics is a requirement, if attributes are used for authorisation. Role- or attributes-based authorisation does not make sense, if the parties do not have a common view on what a particular value means.

For instance, university libraries intend to license scientific journals to their students, faculty and supporting staff, irrespective of where they are located, and to their other regular and registered users on-site [LIGU07]. Earlier, the access control of electronic journals was based on the campus IP address space and there was no technical means to make a fine-grained enforcement. Anyone using a machine on campus was able to access the material. There was no need for distinguishing between degree students, open university students and further education students, or researchers that were actually employed by the university (i.e., had a contract of employment) and researchers working on a grant. Nowadays, identity management systems make this distinction possible, bringing libraries to face a new question; how do they define a student and a faculty member?

[10] The law recognises also an oral contract of employment, but in the Finnish public sector, including higher education institutions, all the decisions should have written form, including decision to employ someone.

A fundamental requirement for centralised identity management is that organisational units are not reluctant to co-operate with each other. As shown by a study in the UK universities, there may be a significant amount of mistrust between the organisation's IT service unit and other organisational units on the same hierarchical level. A reason for that is lack of communication, understanding and coordination within the administration and between the functions of the institutions. According to the study, many departments considered the services provided by the IT service unit inadequate and developed their own IT services and IT support staff. Centralised identity management means centralised control of data and it is hard to achieve in an organisation with lack of trust and confidence. [ALLE02]

3.7. A Method for Improving Organisational Identity Management

Previous sections have presented issues that should be taken into account when designing organisation's identity management. To conclude this section, a method to improve organisational identity management architecture is presented. The method consists of six steps.

Step 1. Identify the owner of identity management infrastructure

At first, ownership for the identity management related issues in the organisation needs to be decided. Usually, the owner is located in the senior management of the organisation's IT services unit. The owner needs to have a broad perspective of the business of the organisation, which makes it easier to focus the refinements on the issues that are most essential for the success of the organisation. The owner has also potential to become the project's key proponent in the organisation. In project management literature [SCHW07:75], this role is often known as the champion of the project.

Step 2. Get top management support

Identity management related projects have influence and need commitment and resources in several parts of the organisation. In order to drive changes affecting several organisational units, the commitment of the top management is a success factor of the project. This is a well-known advice both in project management literature [SCHW07:58] and in business process re-engineering literature [VOND96:151].

Top management support is needed, because identity management projects cause not only technical changes, but also the changes in the processes in the organisation. Otherwise, the ideas would be rejected by the middle management. As described in Section 3.6, organisational units do not necessarily see how their processes relate to the identity management architecture of the organisation, and tend to optimise the processes to reflect their own needs.

Step 3. Analysis phase

The analysis phase reflects the three motivations of identity management presented in Table 1 (page 2). The risk analysis examines the probability and severity of realisation of risks related to identity management. What are the assets that require most protection? Are there risks related to unauthorised access, reliability of authentication or inerasability and non-repudiation of the audit trail? How to balance the risks and the costs of protection?

Analysis of the potential to improve efficiency focuses on reducing costs. Is there potential to cut overlapping maintenance of identity information in the organisation? Could improved authentication and single sign-on reduce the time people spend on logging in to information systems? Could role-based authorisation policies or a general-purpose workflow engine for applying and granting permissions ease management and auditability of authorisation?

Analysis of potential for new businesses or new ways to organise internal information management tries to identify ways how improved identity management could enable issues that have not been possible or have been too difficult earlier. For instance, standard interfaces could ease outsourcing of information systems. New information systems which make use of the rich set of attributes available for end users could be introduced.

Step 4. Requirements specification phase

Based on the three dimensions of the analysis phase, requirements for the organisational identity management architecture are specified. Are there external regulations that the organisation needs to comply with? What are the needs for identity flows in the organisation? How soon should an end user's account be closed when he departs? What kind of attributes does the organisation want to utilise in its identity management and which of them have potential in authorisation? What are the needs for authentication; who needs to be authenticated strongly and where? What are the requirements for audit trail?

Step 5. Design phase

In the design phase, the identity management architecture fulfilling the requirements is designed. Owners for different pieces of identity information are agreed on; for instance, the HR unit becomes the owner of employees' names and employee numbers and IT services unit owns their email addresses. Once the owners of attributes are known, they are able to decide the authoritative sources for the attributes; for example, the authoritative source for employees' name and employee number might be the HR registry. The owners of the attributes become also responsible for defining the attribute semantics, including vocabularies, if any.

Having agreed on authoritative sources, some of them are elevated to base registries, which are the places where new identities enter the organisation. A map of the organisation's IT systems can now be drawn, where some systems are base registers for identities, some are authoritative sources for attributes and the rest of the systems rely on the identity data provided to them. This results in a design of identity flows in the organisation.

Because the identity management architecture is strongly coupled with the processes in the organisation, necessary changes to the processes need to be identified and designed. For instance, if HR registry is used as the base registry for employee's identities, process changes may be needed to ensure that the data in HR registry is always up-to-date. If identity data is designed to flow from HR registry to the building access system, the management process of the building access system need to be changed so that the porters will not any more enter employees' identity data to the system when providing them with access cards. If permissions to use information systems have been based on circulating signed paper forms, replacing them by a workflow engine causes process changes. Designing the process changes requires considerable amount of understanding of the organisation's functions.

Step 6. Incremental implementation phase

In the implementation phase, the design is put into practice. The organisation acquires necessary products, such as a metadirectory, and integrates them to the base registries, authoritative sources and other connected systems. Necessary changes to the organisation's identity data semantics and vocabularies are implemented and new processes introduced. Necessary changes to the processes of the organisation are implemented.

The first five steps followed the well-known waterfall model for systems development lifecycle. For the implementation phase, an incremental model is proposed, consisting of a series of partial products (increments) throughout the project timescale [GRAH92]. New systems and features are delivered gradually, trying to minimise the disturbance it causes to the daily life of the organisation. Early results of the project can be shown, inspiring further development of the identity management architecture. Benefits of the identity management architecture can be first introduced where the analysis has shown biggest benefits, whereas the less important features can be delivered later.

This section presented a method to improve the implementation of organisational identity management architecture. However, improving identity management is a continuous process. Changes in the organisation's business, new needs and the new possibilities provided by technology lead to changed requirements and the re-design of the identity management architecture. Some of them may be influenced by federated identity management, which is going to be introduced next.

4. FEDERATED IDENTITY MANAGEMENT

So far, this thesis has discussed identity management in the context of one organisation. However, the Internet is an inherently cross-organisational construct and all the more (typically, web-based) services provided by different organisations expect users to log in. Of course, each organisation can set up an identity management infrastructure of their own, as presented in the Section 3. However, during the last years, cross-organisational (a.k.a. federated) identity management has become a subject of research. Well-known standards have also emerged, and software vendors have introduced compliant products, paving the street for use in production environments.

In cross-organisational identity management, organisations establish loose partnerships to share the identity data of their end users. *Federating* end users' identities has become the best-established concept for this, the term expressing that people's partial identities in several organisations and their services are coupled together. The main motivation of federated identity management is to enhance user convenience and privacy as well as to decentralise user management tasks through the federation of identities among business partners [SHIN04]. This section studies the concept of federated identity management in more detail.

Traditionally, authentication and authorisation of end users have been closely coupled to the application itself. From the software engineering perspective, the principal idea behind federated identity management is to make use of Web service technology to separate authentication and authorisation mechanisms from the applications themselves [GAED05].

4.1. A Model for Federated Identity

Publication 4 used a model presented by early Shibboleth documents [ERDO02] for federated identity management. A similar model has become predominant among standardisation bodies and software vendors. The Liberty Alliance's terms Identity Provider (IdP) and Service Provider (SP) have superseded the terms Origin and Target site. The model is depicted in Figure 9. Depending on the context, the term Identity and Service Provider may refer either to a server running related service or to the organisation responsible for the service.

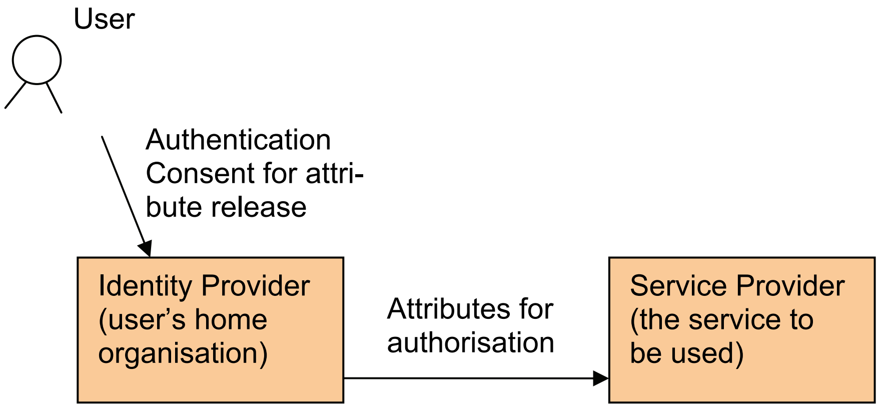

Figure 9. A model for federated identity management

An Identity Provider is the party responsible for issuing and maintaining an end user's identity, including related attributes and authentication credentials. The actual set of attributes depends on the context. In public sector services, attributes like National Identification Number[11] or being guardian of an underage child are important, in commercial service attributes like credit card number, and in universities the ones describing the end user's relationship to the university, such as being a degree student, professor, lecturer of a particular course etc. The model does not stop Service Providers from keeping attributes of their own, and several Service Providers probably want to maintain user preferences and other attributes related to customising their service for the particular end user.

The Identity Provider is also the party responsible for the authentication of the end user. There may be several authentication methods available, and depending on the service and the user's role and permission in the service, a Service Provider may expect some degree of reliability of the authentication carried out by the Identity Provider. The Identity and Service Provider need to have common standards for expressing the reliability of authentication. For instance, the US National Institute of Standards and Technology (NIST) has presented a four-level categorisation for assurance of authentication, covering both identity proofing of new end users and the authentication mechanisms used when an end user signs on to a service [BURR06]. The European Commission has suggested a similar model for government services in EU [IDAB07].

Based on the attributes (and a sufficiently high authentication level), the Service Provider may decide what kind of service to provide to the end user. The attributes

[11] According to a study by Otjacques et al [OTJA06], all the EU countries, except Germany and Hungary, have or are planning to have at least national identification numbers. Some countries also have sector-specific identification numbers.

provided by an Identity Provider help the Service Provider in this decision. They also provide means for role-based access control, giving the end user permission to certain functionalities based on his role as expressed by the Identity Provider. If more fine-grained access control mechanisms are needed the Service Provider may be coupled to an authorisation infrastructure, such as PERMIS [CHAD06, XU05]. A user's right to opt-in for attribute release will be covered in Section 4.3.4.

The unique identifier of an end user is a particularly interesting detail, not in the least from the privacy and anonymity perspective. A Service Providers' ability to track[12] an end user's behaviour and aggregate his personal data depends strongly on it. Pfitzmann et al [PFIT05] define five kinds of pseudonyms, which are listed below in the order of increasing strength of anonymity.

- Person pseudonyms (such as a national identification number and a phone number) are regarded as a representation of the holder's civil identity and are not designed to preserve his anonymity.
- Role pseudonyms (such as a customer pseudonym or an Internet account; attributes like eduPersonPrincipalName [INTE06]), which are limited to specific roles. Roles may be assigned by the end user himself or by an organisation, such as a company or an employer.
- Relationship pseudonyms (for example, eduPersonTargetedID [INTE06]). A different pseudonym is used for each communication partner. The Identity Provider uses the same pseudonym every time a given end user accesses a given Service Provider, but for different Service Providers the end user has a different pseudonym. This pseudonym corresponds to the persistent identifier of SAML [RAGO06].
- Role-relationship pseudonyms. For each role and for each communication partner a different role-relationship pseudonym is used.
- Transaction pseudonym. For each transaction, a transaction pseudonym non-linkable to any other pseudonym is used. This corresponds to the transient identifiers of SAML [RAGO06] and to the concept of a handle in early Shibboleth documentation [ERDO02]. Transient identifiers are used only during one session. A given end user has a different pseudonym every time he enters the same Service Provider. This is the scenario with the strongest anonymity, where there is actually no unique identifier for an end user at all. The Identity Provider merely releases a set of attributes to the Service Provider, and if the attributes do not

[12] As noticed by Pfitzmann, an Identity Provider may have an extensive log of services the user has been using, which may become another privacy threat [PFIT03b]. Bhargav-Spantzel et al recognises this as a disadvantage of a relationship-focused system such as SAML [BHAR06].

uniquely identify the individual, the Service Provider has little means to deduce, who the user is.

In addition to Identity and Service Providers, there can be a third kind of party, called an Attribute Provider. An Attribute Provider has no means to authenticate an end user, but is authoritative to some attribute of him. An attribute provider can be, for example, in conjunction with an Identity Provider; the Identity Provider authenticates an end user and is responsible for a basic set of his attributes, and the Attribute Provider provides additional attributes on him.

Others have also proposed models for federated identity management. Djordjevic's model [DJOR05] identifies more primitive functionalities than the author's model, such as secure token service (STS) for issuing and validating assertions carrying attributes and Policy Decision Point (PDP) for making access control decisions, and analyses their roles in existing federated identity architectures. Gaedge et al [GAED05] have also considered single sign-on and self-service identity management interface as part of their federated identity model. In the author's work, these issues are covered by organisational identity management.

4.2. Requirements for Federated Identity

The model of federated identity in the previous section provided basic roles for the parties involved. This section introduces a set of issues that the Identity and Service Providers need to agree on. The community that decides on the issues is called an identity federation, which will be introduced in Section 5.

This section is based on Publication 5. These requirements were used and found beneficial by the author in the early years of federated identity, when few people were familiar with the concept. In the requirements, the familiar technical and non-technical pieces (protocol, schema, PKI and trust) are used to construct the larger picture of federated identity, making the concept easier to understand and adopt. Finally, the requirements are compared to those presented by others.

4.2.1. Federating Protocol

Holzmann defines a protocol as a set of rules that govern the interaction of concurrent processes in distributed systems [HOLZ91]. In federated identity, the federating protocol provides the basic means for the Identity and Service Provider to exchange identity related messages with each other. Over the years, several protocols have been proposed, such as the proprietary .NET Passport protocol of Microsoft [MICR04]. This section mostly concentrates on SAML, which has got a wider support in the industry. WS-Federation is also briefly introduced. An extensive study on federating protocols is available, e.g., in [IDAB07b].

The Security Assertion Markup Language (SAML) standard of Oasis Open defines an XML-based framework for describing and exchanging security information between on-line business partners [RAGO06]. Being an open standard, it is supported by several software vendors, making it a prominent candidate as a widely-used technical protocol for federated identity.

SAML makes use of features such as HTTP redirects and HTTP POSTs, which make SAML currently mostly intended for the web environment. SAML is a zero-footprint protocol, meaning that an end user only needs a standard web browser [PFIZ02]. This is an important feature, since it is evident that end users are reluctant to install any protocol-specific software in their clients [GROS03].

SAML version 1.1, released in September 2003, was adopted by Liberty Alliance, a global organisation of players in IT, finance, telecommunications, media, manufacturing, government and education [LIBE07]. Liberty Alliance introduced the Liberty ID-FF 1.2 in November 2003. In higher education and research, Internet2, a networking consortium comprising more than 200 U.S. universities [INTE07], introduced Shibboleth, which specifies and implements a profile of SAML1.1, in summer 2003.

The security of SAML-based protocols has been a subject for research. Gross [GROS03] identified vulnerabilities and proposed attacks on Browser/Artefact profile of SAML version 1.0. Pfitzmann et al [PFIT03] discovered a vulnerability to a man-in-the-middle attack by a malicious Service Provider on one of the profiles in the Liberty version 1.0 specification. The vulnerability was fixed in the next specification release.

Version 2.0 of SAML, released in March 2005, was influenced by both Liberty and Shibboleth. SAML 2.0 works in the environment of standard web browsers. This short introduction is based on SAML 2.0 technical overview [RAGO06].

SAML has four main components; assertions, protocols, bindings and profiles. Assertion is a statement about a subject, such as an end user, expressed in XML. In SAML 2.0, one assertion may carry any number of statements of three kind; authentication statements (the subject was authenticated with a password), attribute statements (the subject's name is Bob Smith) and authorisation statements (the subject is entitled to a certain transaction in the service).

SAML protocols define seven request/response pairs making use of the assertions. Authentication request protocol is used when a Service Provider asks an Identity

Provider to authenticate a subject. Single logout protocol carries out the logout in single sign-on scenario (see Section 3.5). Assertion query and request protocol defines a set of protocols for obtaining SAML assertions. Artefact resolution protocol is used, when assertions are obtained by a reference (called an artefact). Name identifier management protocol is used for managing the identifier linking partial identities in the Identity and Service Provider or to cut an existing link. Name identifier mapping protocol makes it possible to link partial identities of an individual between several Identity and Service Providers.

SAML Bindings define how the protocols above are mounted on underlying transport protocols. HTTP redirect, HTTP POST and HTTP Artefact bindings utilise a web browser's HTTP redirect or HTTP POST functionalities to pass on an assertion or artefact. SAML SOAP binding makes use of SOAP protocol directly between the Identity and Service Provider, whereas reverse SOAP (PAOS) makes the browser pass the SOAP messages. Finally, SAML URI binding defines means for retrieving existing SAML assertions by resolving a URI.

In previous paragraphs, assertions with three kinds of statements, seven protocol definitions for carrying the assertions, and six bindings for carrying the protocols were shortly described. SAML profiles define how the other components shall be combined to make products interoperable. Eight profiles are defined, including profiles for single sign-on and single logout, Identity Provider discovery for picking up the correct Identity Provider and so on.

WS-Federation [LOCK06] is another well-known industry standard for federated identity. WS-Federation covers mainly web services based scenarios where two servers communicate using SOAP protocol. WS-Federation defines also a Web Passive Requestors profile to support browser-based scenarios, providing functionality that is comparable to SAML.

WS-Federation is based on Oasis Open's standards WS-Security [NADA06] and WS-Trust [NADA07] and extends them to cover federated identity scenarios. WS-Trust defines a service model called Security Token Service, implementing a protocol for requesting and issuing security tokens. A security token is a collection of attributes, dubbed claims in the WS-Trust specification. The token format of WS-Trust is flexible and, for instance, SAML assertions can be used as security tokens. Using Security Token Service, it is possible to construct the model of an Identity Provider and a Service Provider (called Resource Provider in the specification) as presented in Section 4.1. [GOOD07]

4.2.2. Schema for Attributes

In addition to the federating protocol, the Identity and Service Providers have to agree on the attributes that are exchanged. The specification for attributes is often called a schema, and it covers both the syntax (for instance, the attribute's value consists of characters a-z, A-Z) and the semantics (for example, the attribute describes its holder's home postal address).

The concept of schema has its origins in LDAP directories (Light-weight Directory Access Protocol), and their way to construct their schema as object classes. Indeed, the SAML-based protocols re-utilise the object classes well known in the LDAP world, such as Person [RFC4519], OrgPerson [RFC4519] and InetOrgPerson [RFC2798]. Whereas Internet standards-based schemas provide a good basis for interoperability, they often have to be supplemented by context-specific attributes. For instance, in higher education, Educause has specified an additional object class called eduPerson [INTE06], specifying concepts peculiar to higher education, such as a person's role as a student, staff member or an alumnus. Furthermore, Trans-European Research and Education Networking Association Terena has supplemented eduPerson with European specialties, such as those related to the Bologna process [TERE07].

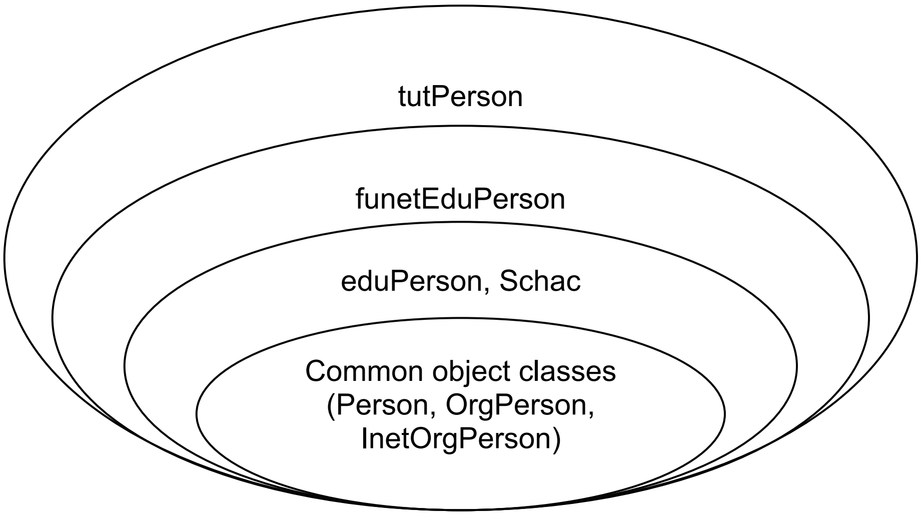

Figure 10. The schema onion

Putting the object classes together results in a schema onion (Figure 10). The widely supported common schemas are in the core of the onion, surrounded by object classes specific to a certain business or geographic location. In the outmost sphere, there are attributes that are perhaps used only by one or some Identity and Service Providers, limiting their use in federated transactions. In the figure, funetEduPerson [CSC06] refers to the schema containing Finnish specialities, and tut-

Person are attributes that are defined and used locally in the Tampere University of Technology.

In a federated scenario, an Identity Provider decides which attributes to adopt and populate for its end users. The identity federation may agree that some attributes are mandatory and the rest are optional. However, individual Service Providers may set additional requirements for attributes; for example, an employer may sign in to the extranet services of a occupational health service only if his Identity Provider is able to release his national identification number, which is used as his unique identifier in the Service Provider. In the end, this results in a demand-and-supply markets of attributes; Service Providers try to find out what are the attributes available in an Identity Provider, and Identity Providers try to decide, what attributes they should populate in order to serve the Service Providers needs.

4.2.3. Security Infrastructure

The Internet provides an insecure transport for messages, and intermediate parties are able to capture, tamper and replay messages on it. Extra protection for messages exchanged by Identity and Service Providers has to be implemented, in order to provide confidentiality for the assertions exchanged and to ensure their integrity (that they are genuine messages sent by the other party) and authenticity (that they are not replays of earlier messages [ANDE01:11]).

There are many cryptographic mechanisms to provide confidentiality, integrity and authenticity services for assertions. Timestamps and nonces can be used for countering replay attacks. Symmetric cryptography can provide protection against confidentiality threats. A common denominator for a large-scale use of federated identity seems to be making use of public key cryptography and PKI to ensure the identity of the communicating parties and exchanging the symmetric key that is used to ensure confidentiality of the assertions.

The usability of PKI has hampered its use for authenticating individuals. However, in federated identity, an end user does not have to have a public key of his own; it is sufficient that the Identity and Service Providers are able to exchange messages secured by a public key cryptosystem and the certificates issued to the servers. The only step where an end user faces a certificate is when he uses his web browser to enter the Identity and Service Providers, which are expected to use SSL connections with the web browser.

4.2.4. Trust

As McKnight and Chervany have shown, there are various definitions of trust in different disciplines. In this thesis, McKnight's and Chervany's definition of trusting intention has been adopted: trust is the extent to which one party is willing to depend on the other party in a given situation with a feeling of relative security, even though negative consequences are possible. This definition includes that (a) there is a prospect of negative consequences (i.e., a risk); (b) the truster is dependent on the trustee and (c) willing to be that with feelings of security; (d) the truster cannot control the trustee, and (e) the trust is situation-specific (e.g., covers managing identities, not flying an airplane). [KNIG96]

Federated identity cannot establish trust – it can only communicate it [WIND05:130]. Among isolated, centralised and federated identity management models, federated identity is the one that requires the most trust assumptions [JØSA05]. Because of its non-technical nature, establishing trust is maybe the most difficult engineering problem in federated identity. There are incomplete or no technical means to ensure that the trusted party is actually trustworthy. Having faced the limits of engineering, it is necessary to find non-technical means to establish trust between the parties, this being when the lawyers are called in.

The organisational and contractual aspects of an identity federation will be covered in Section 5. In brief, a Service Provider must trust that the authentication carried out by the Identity Provider has been done as reliably as the Service Provider expects and the attributes provided are up-to-date. The Identity Provider must trust that the Service Provider does not use the attributes in a way that infringes the end user's privacy. And the end user must trust that neither the Identity Provider nor Service Provider is endangering his privacy.

Federated identity management is a triangle where the Identity Provider releases the end user's possibly sensitive personal data to the Service Provider. Typically, the end user has a relationship with the Identity Provider; for instance, he might be an employee, a customer or a student of the organisation. The end user trusts the Identity Provider at least to the extent that lets it process his personal data, but the Service Provider may be new for him. The Identity Provider, on the other hand, has a business relationship with the Service Provider, either directly or via an identity federation as will be explained in Section 5.

For example, the employer has outsourced the occupational health care and buys it from a company providing health care services. The parties have agreed that self-service in the web and federated identity management is used when employees reserve their appointments to the reception. During the first login, the employer (the Identity Provider) provides the health care company (the Service Provider) with necessary personal data, including the employee's national identification number, which is considered sensitive in several European countries [OTJA06]. The employee, however, may not have previous knowledge of the company but uses the service of necessity.

This leads us to the question of transitivity of trust, which will be introduced in detail in Section 5.2. In short, if the end user trusts the Identity Provider, and the Identity Provider trusts the Service Provider, does the end user trust the Service Provider? If the answer is an exclusive yes, how long chains are we able to construct (for instance, see the discussion of interfederations in Section 5.4). If the answer is a definite no, difficult occasions may be encountered. For instance, if an employee does not trust a Service Provider but his employer expects him to log in to it (and, thus, to release his personal data to it), does the employee refuse to do his job and can be fired? Or, in the case of an outsourced occupational health care service, how can he use the service his employer is obliged to offer to him? Luckily, in European Union, the law protects the end user strongly. The data protection directive's implications to federated identity management will be covered later in Section 4.3.

It is worth noticing that the division of responsibilities described in Section 4.1 makes it easier for the parties to trust each other. There are mechanisms in place to control which attributes are released to a Service Provider. Sensitive attributes, especially passwords, do not have to be exposed to a Service Provider at all. Other privacy-enhancing properties are introduced in the Section 4.3.

4.2.5. Previous Research

Others have also presented requirements for federated identity management. Damiani et al [DAMI03] have proposed a broader model for identity management, covering issues such as identity lifecycle management and support for mobile devices. Damiani's proposal is more complete and is not limited to the requirements for federated identity management. He and Zhang present a framework with three requirements; user convenience, controlled information disclosure and preserving the privacy of the user [HE05].

Subenthiran et al [SUBE04] have proposed some more specific requirements, such as self-service for an end user and identity life-cycle management for the organisation maintaining the identities. In this thesis, all these requirements are considered part of organisational identity management. Mobility and roaming, a requirement proposed by Subenthira, is in this thesis considered an application of federated identity management and will be covered in Section 6.2.3. Scalability is a natural requirement for a system. Finally, Subenthiran identifies the billing of services as one of the requirements – an aspect that is indeed necessary for commercial services.

Jøsang et al [JØSA05] have studied trust requirements in federated identity. They have also identified the scenario, where two or several Service Providers band together to share user identities. Jøsang et al require that Service Providers do that only on user consent and adhere to the accepted policy. Furthermore, care should be taken to make sure the mapping of identities between Service Providers is correct.

During recent years, trust negotiation has been a topic for research. Trust negotiation deals with concepts such as formulating security policies and credentials, determining whether particular sets of credentials satisfy the relevant policies, and deferring trust to third parties. A trust negotiation consists of iteratively disclosing certified credentials as depicted in Figure 11. During negotiation, parties incrementally establish trust by disclosing credentials to verify properties of the negotiating parties. [BERT04]

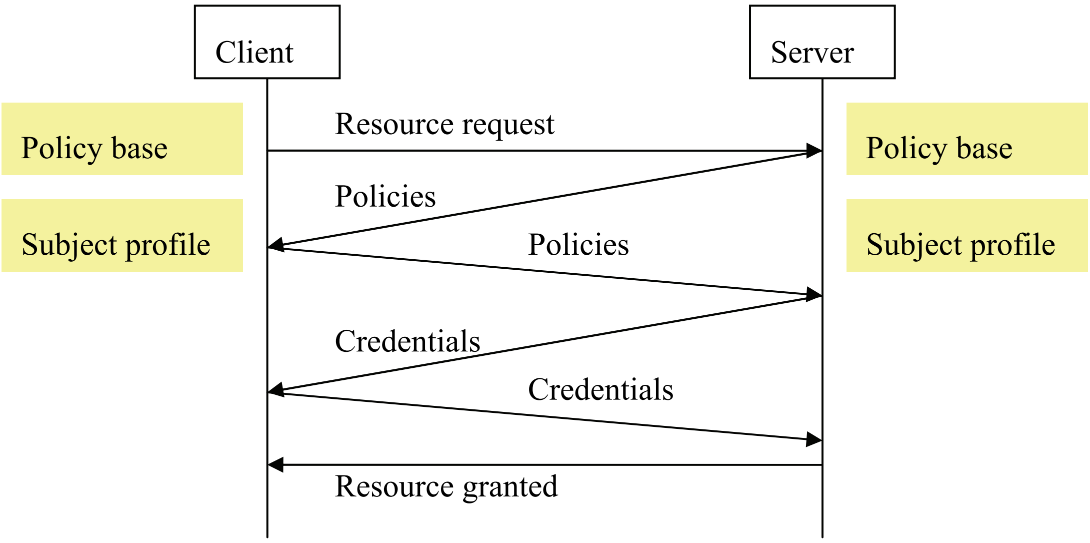

Figure 11. Trust negotiation process [BERT04].

Trust negotiation is intended for parties which do not have pre-existing direct trust relationships, although they must both trust the same trusted third parties. [BERT04]. However, they need to have an agreement on language and system requirements as presented by Bertino et al, including semantics for the policies and credentials, certification authorities and other trusted third parties, privacy protection mechanisms etc. These are also requirements for federated identity. A topic for future research is how federated identity and trust negotiation could leverage each other.

This section has discussed the requirements of federated identity and concluded that trust between the Identity and Service Providers and an end user is a necessity – a property to which Sampath et al [SAMP06] refer as the system trust. In addition to that, for transactions between people in the networked world, there is a requirement of trust between end users of the system, dubbed by Sampath et al as interpersonal trust. In their paper [SAMP06], Sampath et al present a reputation-based architecture, where the trust of an end user can be measured as a function of observations by peer users, recommendations of Service Providers and history of evidence of the user. End users get their good or bad reputation little by little, depending on how they behave in the Services, and their measured trust becomes part of their identity.

4.3. Privacy Considerations in Federated Identity Management

Whereas schemas define syntax and semantics for attributes and federation protocols, like SAML, how to exchange them, neither of the two explains how to comply with the privacy laws in an attribute exchange. This is the point where the scope of this thesis must be widen from technical perspective to cover also the legal sides of federated identity management.

In Section 4.3.5, a survey will be made on previous research available on privacy in federated identity management. Research articles provide important impulses to further research and development work in federated identity. However, the concrete problems practitioners need to solve are how to make their implementation compliant with current legislation.

In the European law, the data protection directive [EP95] regulates the processing of personal data and sets the legal basis for federating identities as well. In Finland, the personal data act [PF99] implements the data protection directive in the national Finnish legislation.

Publication 5 provides an interpretation of the data protection directive in the context of federated identity. It arose from the practical need to understand how federated identity can be deployed into production without infringing the privacy laws. This Section 4.3 is based on the publication, which has also been the basis for the federation deployments the author has been involved in.

4.3.1. Definitions in the Directive

Article 2 of the data protection directive defines personal data as any information that relates to an identified or identifiable natural person. Any attribute, that can be considered uniquely identifying, such as a username, email address and social security number, are personal data. An individual may be identified by a set of attributes, such as “female”, “lecturer” and “Software systems laboratory of the Tampere University of Technology”, provided that there is only one or a very small set (called an anonymity set [PFIT05]) of them. Article 29 Data Protection Working Party of European Commission points out that the possibility of identifying an individual no longer necessarily means the ability to find out his or her name [ARTI07]. The definition of personal data is very wide, covering pseudonyms, cookies, IP addresses, log entries identifying an individual etc. According to the UK Information commissioner, in the context of the on-line world, the information that identifies an individual is that which uniquely locates him in that world, by distinguishing him from others [UKIC07:12].

In the directive, processing of personal data is defined as any operation or set of operations which is performed upon personal data, such as collecting, storing, disseminating and so on. It is clear that user accounts in an Identity Provider are personal data, and, therefore, the Identity Provider processes personal data. The Service Provider processes personal data, if the attributes provided by the Identity Provider together with other records collected by the Service Provider relate to an identified or identifiable individual.

4.3.2. Purpose of Processing Personal Data

The dependency on the purpose of processing personal data is fundamental to privacy laws in Europe. According to the data protection directive, (Article 6) *Member states shall provide that personal data must be (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.*

The purpose of processing personal data in the Identity Provider typically follows the organisation’s charter. For example, in higher education institutions, personal data are processed to support research and education in the institution, in banks to provide banking services to a customer and take care of his customership.

Releasing personal data from an Identity Provider to a Service Provider is processing personal data. Following the article cited above, the Service Provider must specify beforehand, for what purposes it is going to collect personal data. Releasing personal data from an Identity Provider to the Service Provider is possible only, if the purpose specified by the Service Provider is compatible with the purpose of processing personal data in the Identity Provider.

4.3.3. Relevance of Attributes

According to the data protection directive (Article 6) *Member states shall provide that personal data must be (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.*

When releasing personal data from an Identity Provider to a Service Provider, both parties are responsible for taking care that only relevant personal data are released by an Identity Provider to a Service Provider. An Identity Provider is responsible for finding out which attributes the Service Provider needs and making sure that no more than adequate attributes are released. The Service Provider may gather only relevant attributes. The relevance of attributes depends on the context: For government and health care services, social security number is probably often a relevant attribute as it is used for identifying individuals. Then again, for schools and universities, social security number is often excessive, because schools use student numbers instead.

4.3.4. Informed Consent

According to the directive, an individual's consent is the basis for processing personal data. *(Article 7) Member States shall provide that personal data may be processed only if:*

(a) the data subject has unambiguously given his consent;

(b) processing is necessary for performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the data subject which require protection under Article 1(1).

Regarding article 7, several scenarios in federated identity probably fall to some other category than a). However, another fundamental of the data protection directive is informing the data subject on processing his personal data. *(Article 11) When the data have not been obtained from the data subject; Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except when he already has it:*

a) the identity of the controller and of his representative, if any;

b) the purposes of the processing;

c) any further information, such as the categories of data concerned, the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning him

in so far such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

Thus, when personal data is released for the first time, the Identity and Service Provider are responsible for providing the end user with the information above. A convenient way to do it is to combine it with the step when an Identity Provider asks user consent for attribute release. Services in the Internet typically take care of the responsibility by publishing their privacy policy, answering the questions. A way to organise the responsibility in practice is presented in Publication 5.

There are already mechanisms available for publishing the privacy policy of a service. The Platform for Privacy Preferences Specification (P3P) is a W3C specification [WENN06], enabling sites to express their privacy policies in a standard machine-readable format retrievable by user agents. In the HTTP headers, a web browser gets a reference to a web site's privacy policy, expressed in XML. Based on the policy, a user agent may take automated actions, such as show or reject the web page or prompt the user.

4.3.5. Research on Privacy in Federated Identity Management

Liberty Alliance has also published guidelines on privacy and EU data protection [LIBE05]. The work was independent and done at the same time, and confirms both the author's results and the importance of the topic for real-world deployment.

Privacy in federated identity management has been a subject for research. Pfitzmann and Waidner [PFIZ02, PFIT03b] have listed the following privacy requirements, some of which are overlapping with the author's; user consent for attribute release, ability for an end user to pick up one of his/her several roles or identities in a service, protection against traffic analysis (for instance, the service URL the end user is accessing) and ability to support multiple attribute providers (called wallets), which may be also local to the end user's machine. Unlike the author's study, Pfitzmann's and Waidner's paper does not use the EU data protection directive as the starting point.

Ahn and Lam noticed that federated identity management lacks a well-defined standardised structure for privacy policies and a mechanism to match the policy and a user's consent. They propose PREP, a language that an Identity Provider uses to maintain the end user's consent and preferences for attribute release. When releasing attributes, the Identity Provider compares the attributes requested by the Service Provider to the preferences set by the end user. [AHN05]

Mont et al [MONT03] have expressed their concern that once an attribute has been released to a Service Provider, there are few technical means to control that the attribute is not leaked to a third party or used in a way that conflicts with the privacy policy. They propose a "sticky" privacy policy that is strongly associated to the attribute by means of encryption; a Service Provider cannot access the attribute value before it gets a decryption key from a trusted third party called Tracing and Auditing Authority (TAA). For accountability, TAA keeps log of to whom it has provided the decryption key. The architecture makes use of identifier-based encryption, Trusted Computing Group technology and tagged operating system technology.

Clauss et al [CLAU05] have presented attack goals and models for privacy breaches and propose related protection methods. According to Clauss et al, in an attack against privacy, the attacker tries to find out information on a user that this user does not want to disclose. As a means for an attack, the attacker can use a database he may have access to, or by observing the communication and interactivity the victim is a part of. For instance, if the attacker is able to observe a victim's encrypted web traffic and simultaneous changes in a database he has access to, he may have committed a successful attack.

Finally, concerns on privacy have initiated a new concept of user-centric identity management, which Bhargav-Spantzel et al define as giving an end user control on his attributes, in particular on the aspect of releasing attribute information [BHAR06]. In their publication, Bhargav-Spantzel et al have presented the requirements of user-centric identity management. Examples of user-centric identity management implementations are the OpenID platform [RECO06, RECO06b] and Windows CardSpace [CHAP06].

4.4. Federated Identity and Reliability of Authentication

It is often questioned, how federated identity management relates to the reliability of authentication. Some people have the opinion that because of the risk of an identity theft, it is safer to have separate identity islands. Identity and authentication (i.e., verification of identity) are two distinct, although connected, issues, as presented in Figure 12. Federated identity can be implemented with weak or strong level of authentication. Using the SAML protocol and SAML authentication contexts (see Section 4.2.1), the Service Provider can ask the Identity Provider to conduct the authentication on a level that fulfils the Service Provider's needs.

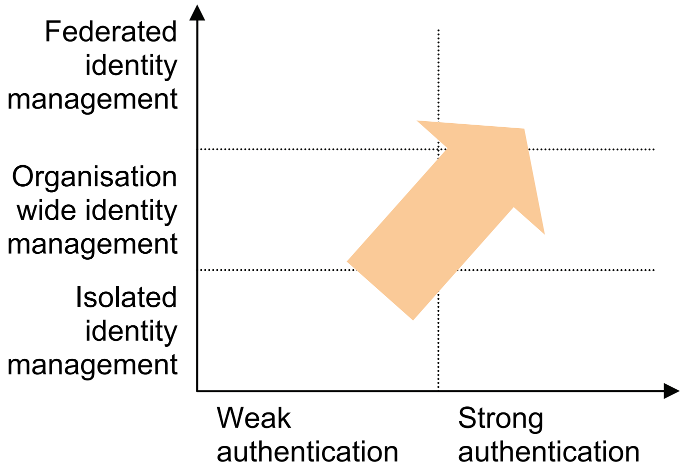
Federated identity management
Organisation wide identity management
Isolated identity management
Weak authentication
Strong authentication

Figure 12. Scope of user identity and reliability of user authentication [GNOM07]

In Publication 4, it was proposed that introducing federated identity management also increases the need for strong authentication (the arrow in Figure 12); as more services are available with single authentication credentials, the damages caused by an identity theft become larger. Madsen et al confirm the results in their paper [MADS05], where they present ways how federated identity helps to address certain aspects of the identity theft problem. Madsen et al also point out that federated identity may even increase the reliability of password-based authentication, because the frequency of authentication decreases and users can be educated to give their passwords only to the Identity Provider. The quality of passwords can also be expected to be higher, if end users have fewer passwords to remember.

As concluded by Madsen, federated identity can even accelerate the introduction of authentication mechanisms that are stronger than passwords. Because authentication is carried out by Identity Providers, the Service Providers do not have to set up the necessary technology and provide end users with, for example, the hardware tokens necessary for strong authentication. Instead, the task can be carried out by dedicated Identity Providers, who serve several Service Providers and are specialists in authentication and identity management.

5. IDENTITY FEDERATION

Section 4 discussed federated identity management mostly from the technical point of view. This section introduces the organisational aspects of federated identity and the concept of an identity federation.

5.1. Definition

In this thesis, the identity federation definition by inCommon, the federation of the US higher education, has been adopted. A federation is an association of organisations that come together to exchange information, as appropriate, about their users and resources in order to enable collaborations and transactions [INCO07]. This definition points out that an identity federation is an organisational entity, "an association of organisations", not a technical entity. This is essential, because the goal of a federation is to establish trust (see Section 4.2.4) and trust is between organisations, not between technical artefacts. The association has a purpose; *to enable collaborations and transaction*, and a plan how to reach the purpose; *to exchange information about their end users and resources*. Whether a federation is actually an association as defined in civil law is another story. The legal form of a federation will be discussed in Section 5.2.

In literature, there are other definitions for a federation as well. Madsen et al define a federation as an establishment of business agreements, cryptographic trust and user identifiers or attributes across security and policy domains to enable more seamless cross-domain business interactions [MADS05]. Jøsang et al define a federation as the set of agreements, standards and technologies that enable a group of service providers to recognise user identifiers and entitlements from other service providers within a group [JØSA05].

An identity federation, or a federation in short, is the concept used in research papers [e.g., MADS05, BERT06]. Liberty Alliance, however, uses the term Circle of Trust (CoT) instead of federation [LIBE07b]. The term federation, as understood by Liberty Alliance, is the transaction that links together two partial identities of an individual. From a technical perspective, according to Liberty Alliance, a federation happens when an Identity Provider provides a pseudonym of an end user to a Service Provider, causing the end user's partial identities in the Identity and Service Providers to be linked. The reverse action, where linking of the partial identity is undone, is called defederation.

5.2. Federation Patterns

This section presents four patterns for the contractual framework of a federation. This section is based on Publication 5, which was written based on the concrete need to give a legal shape for the use of federated identity. When deploying federated identity in Finnish higher education in 2004-2005, decisions had to be made on what kind of contractual shape was needed, what kinds of contracts the joining institutions had to sign, how the federation was governed and so on. Later, Liberty Alliance has also provided guidance in the contractual framework of a federation [LIBE07c].

Section 4.2.4 defined trust as the extent to which one party is willing to depend on the other party in a given situation with a feeling of relative security, even though there is a risk of negative consequences. This holds true for organisations joining a federation, as well. A key element in assessing and managing the risk is having a contractual relationship with the other federation participants. The contract makes it explicit what are the rights and obligations for the organisations, what are the consequences in case of a breach of the contract and how the federation is governed.

Phillip Windley has presented three federation patterns [WIND05:125] and believes that organisations will explore all the three patterns in a sequence. Windley's results confirm the results presented in Publication 5. In this section, Windley's terminology is used.

This section analyses also the trust properties of the federation patterns presented. Some of the patterns require transitivity of trust, which makes trust establishment more difficult. Transitivity of trust means that if organisation *a* trusts organisation *b* and organisation *b* trusts organisation c, organisation *a* trust organisation c as well. If predicate $\tau(a,b)$ is used for denoting "a trusts b" and a, b and c belong to a set X, transitive of trust can be defined using predicate logic:

$$\forall\, a,b,c \in X,\ \tau(a,b) \wedge \tau(b,c) \Rightarrow \tau(a,c)$$

Ad hoc federation (Figure 13) is characterised by bilateral relationships of organisations wishing to enter a federated identity arrangement. Based on our definition, this is strictly speaking not an identity federation ("an association of organisations"), but use of federated identity technology on a bilateral basis. The ad hoc federation is easy to set up, but does not scale, if there is a large number of organisations with several Identity and Service Providers involved.

The trust relationships (the dashed lines in the figure) of the organisations follow the contractual relationships and are strictly bilateral. There is no need for transitivity of trust. The organisations need not to be aware of any other organisations with whom their contract partner may have a trust relationship.

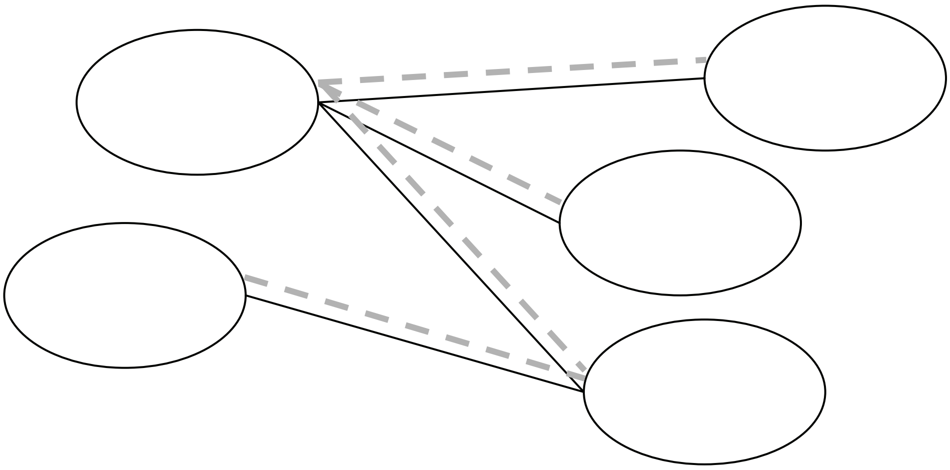

Figure 13. Ad hoc federation is based on bilateral trust between organisations. Solid lines represent agreements and dashed lines trust relationships, which in this pattern are the same

This pattern can be sufficient in simple setups, for example, when an organisation outsources some of its IT systems from a subcontractor. In that case, there is perhaps just one Identity and Service Provider, and the necessary agreements for bilateral trust can be part of the outsourcing contract.

A hub-and-spoke federation is dominated by a large company in the centre, setting the rules of the federation for their own advantage. Small players have few chances to affect the dominating central organisation, but they will participate out of necessity.

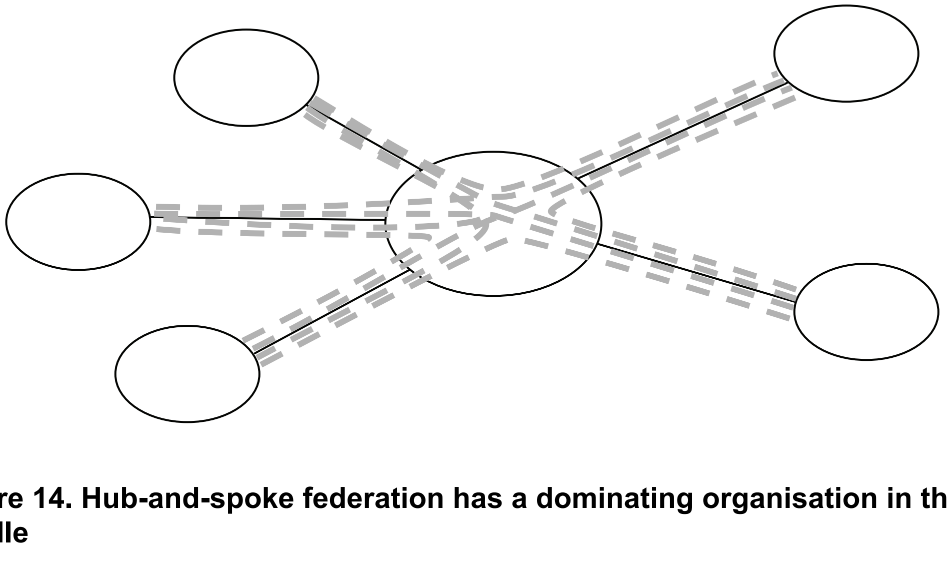

Figure 14. Hub-and-spoke federation has a dominating organisation in the middle

As mentioned in Publication 5, a hub-and-spoke federation (Figure 14) is typically organised as a service provided by a central organisation. Each federation participant signs a service agreement with the organisation in the middle, which is able to set the federation rules. Federation participants are highly dependent on the organisation in the middle; if they want to change the organisation, they, effectively, have to set up a new federation.

A hub-and-spoke federation is based on transitive trust. Each federation participant trusts the organisation in the middle and, transitively, any other participant with whom the central organisation has a trust relationship. The organisation in the middle decides who is accepted to join the federation and who is not.

Identity network is an independent entity founded and focused only on the technical and administrative aspects of the identity federation. It gains support when a sufficient number of individual participants become frustrated with the challenges of the ad hoc federation or the hub-and-spoke federation.

In an identity network, there are no organisations dominating the administration of the federation; the federation participants are able to affect the policy-making in the network. In an identity network (Figure 15), trust relationships (the dashed lines) are directly between the participants. The participants trust each other directly and there is no need for transitive trust.

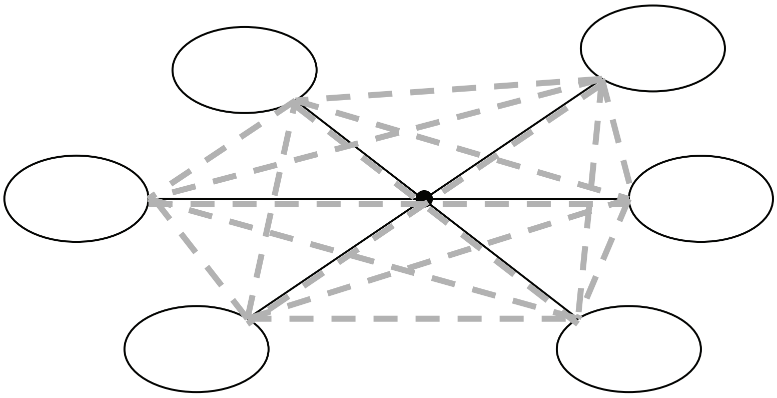

Figure 15. Identity network is a consortium of organisations which have signed a multilateral agreement

As mentioned in Publication 5, an identity network can be organised as a consortium, which is, by definition, an agreement, combination or group (as of companies) formed to undertake an enterprise beyond the resources of any one member [MERR07]. In a consortium, federation participants sign a multi-lateral agreement, defining the governance of the federation. In the figure, the crossing of the solid lines in the center reflects the multi-lateral agreement. In a consortium, participants have direct contractual relationships with each other.

Liberty Alliance has also published a contractual framework for Circles of Trust [LIBE07c]. In the document, Liberty Alliance has further split the identity network into two alternative patterns; a consortium and a collaborative model. The consortium model was as presented above. In the collaborative model, federation participants create a separate legal entity (such as an association or a company), which is dedicated to the administration of the federation, and each participant has a vote. Additionally, federation participants may have a separate service agreement with the legal entity. The figure of the collaborative model is similar to that of the hub-and-spoke federation (Figure 14).

Theoretically, also other kind of federation patterns can be constructed. In **a mesh federation,** organisations establish arbitrary transitive trust relationships. An organisation joins the federation by entering into a contract with any federation participant. In a mesh of organisations, any two organisations are connected via intermediate federation participants.

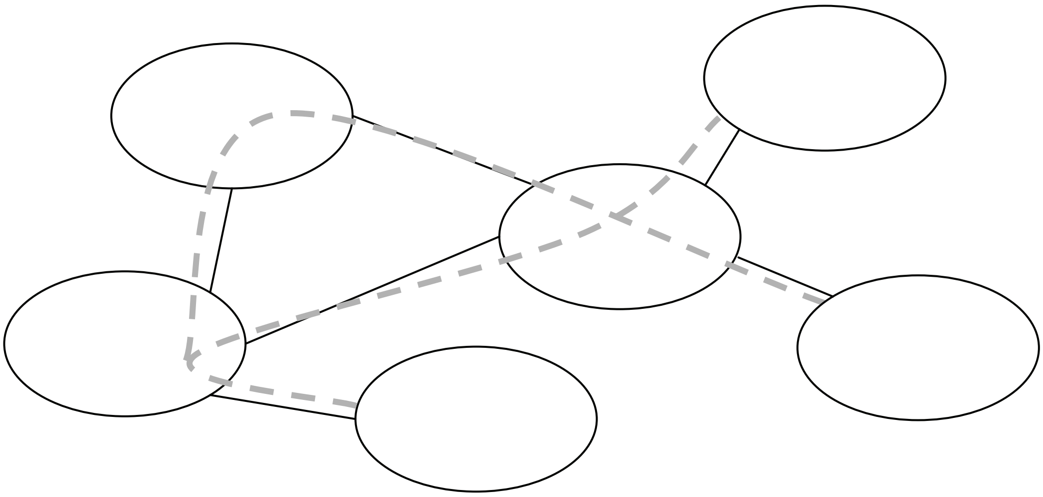

Figure 16. In a mesh federation, organisations have arbitrary transitive trust relationships

In a federation mesh (Figure 16), there is at least one pair of federation participants with the shortest trust path traversing two organisations, making trust establishment more difficult than in a hub-and-spoke federation (Figure 14). Administering a federation mesh is also challenging as there is no single point in the mesh where all the contractual relationships face.

Table 4. Summary of federation patterns and the maximum number of trust transits

Federation pattern	Maximum number of transits
Ad hoc federation	0
Hub-and-spoke federation	1
Identity network	0
Mesh federation	n

The four federation patterns and their needs for transitivity of trust are presented in Table 4. The second column presents the maximum number of trust transits in a federation representing the pattern. Ad hoc federation and identity network are the two federation patterns where all the federation partners have direct trust relationship with each other and transitive trust is not necessary. In a hub-and-spoke federation, every federation participant needs to trust the organisation in the middle who mediates trust between the participants. In a mesh federation, there is at least one pair of participants who have at least two intermediaries in their trust fabric.

5.3. Administrations of a Federation

Federation participants are responsible for operating their Identity and Service Providers and having a proper organisational identity management in place. As presented in the previous Section 5.2, in the hub-and-spoke federation and identity network, there is an organisation on top taking responsibility on administering the federation itself.

This section presents some of the responsibilities in the administration of a federation, splitting them into the categories of coordination and operations. This model, which was shortly introduced in Publication 5, is based on practical experience of identity federations. Lately, in a project that the author has been involved in, the state government of Finland has proposed the adoption of a similar model [MINF07].

5.3.1. Coordination of a Federation

The coordinator of a federation is the organisation in the middle in the hub-and-spoke federation and the consortium or the legal entity in the identity network. There is no coordinator in the other models. The federation coordinator is responsible for the policies of the federation. The policy is made binding by incorporating it to the agreement the participating organisations commit to when joining the federation.

The membership policy defines **who is eligible** to join the federation and what kind of procedure is in place for organisations joining and leaving the federation. For example, in a federation for higher education, only higher education institutions may be eligible to join as full members. Other organisations, like commercial content providers, may join as partners who are able to register only as Service Providers, not Identity Providers, to the federation.

The federation participants need to have a sufficient level of trust of each other regarding, for instance, organisational identity management as described in Section 4.2.4. The policy of the federation needs to cover the levels of **assurance for the quality of identity management** in the eligible participants and best practice for implementing privacy mechanisms, as introduced in Section 4.3. If there is peering with other federations (see Section 5.4), the coordinator is the party that makes the decision on behalf of the federation.

The federation coordinator is also responsible for **organising the daily operations** of the federation, as introduced in the next Section 5.3.2. As in any other service, the coordinator may decide to do the operations by itself or outsource them. The federation coordinator must also **cover the costs** of running the federation, including the outsourcing contract of the federation's operations, if any. The costs of a federation can be covered by fees to the federation participants, depending on the context.

5.3.2. Operations of a Federation

The operator of a federation is responsible for the daily technical operations of a federation, following the policies set by the federation coordinator. The obligations and responsibilities, such as the expected service level, are specified in an agreement between the coordinator and the operator.

From a technical perspective, an identity federation can be decentralised or centralised (Figure 17). In a centralised setup, there is an Identity Provider to which all the Service Providers redirect their end users for authentication. The Identity Provider acts as a proxy (IdP proxy), redirecting end users to their own Identity Providers, maintained by the federation participants, and relaying related assertions back and forth. In such a centralised setup, it is the responsibility of the federation operator to maintain and operate the IdP proxy, whose availability and security are crucial for the federation. In a decentralised setup, there is no IdP proxy but the Identity and Service Providers communicate with each other directly. There may be, however, a need for a separate service that discovers the Identity Provider to which the end user should be redirected for authentication.

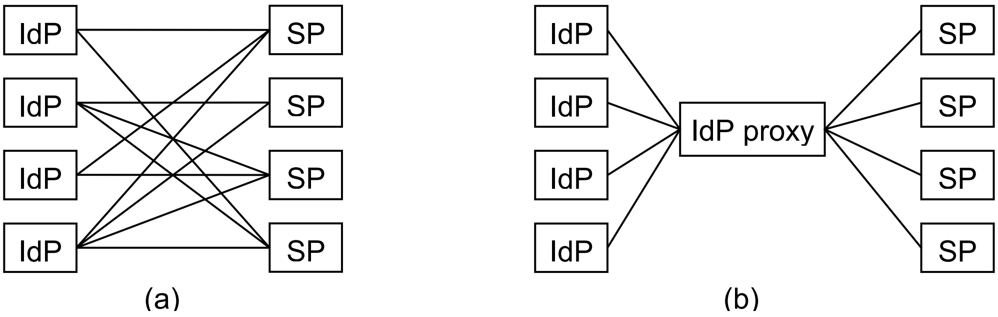

Figure 17. The technical setup of a federation can be decentralised (a) or centralised (b)

Maintaining a record of the Identity and Service Providers in the federation is the fundamental duty of the operator. The record may contain, for instance, the Providers' technical addresses, supported protocols and profiles, certificates and contact persons. In a decentralised setup, the record is a file, for example, a signed XML document as defined in SAML metadata specification [CANT05]. The operator distributes the federation metadata file to all the Identity and Service Providers in the federation. In a centralised setup, the record is a configuration file in the centralised IdP proxy.

When a federation participant registers a new Identity or Service Provider to the federation, the Provider must fulfil the requirements set by the federation policy. For example, the Identity Providers have to qualify certain minimal requirements for the identities of its end users regarding the freshness of the end users' attributes as described in Section 3. Furthermore, the Identity Provider has to provide a certain level of authentication for its end users. The operator of the federation takes necessary steps to make sure the requirements are met, such as external audit or a self-audit conducted by the federation participant.

As described in Section 4.3.3, a consequence of the data protection directive is making sure that only attributes relevant for the service are released from an Identity Provider to a Service Provider. **Maintenance of a list of attributes considered relevant for a service** is one task for the federation operator. The list of required attributes can be included to the SAML 2.0 metadata file.

Providing test servers for federation participants is a task that may be beneficial to be done centrally by the operator. When a federation participant is going to register a Service Provider to the federation, the participant is able to test the Service Provider with the operator's test Identity Provider, which is configured as production level Identity Providers in the federation, and vice versa. Furthermore, the expertise regarding problem solving is likely to accumulate to the federation operator, and, by **providing a helpdesk**, this expertise can benefit the federation participants in resolving problems, both when registering a new Identity or Service Provider and during operations of the federation.

An additional service that can be centralised in a federation is **monitoring** the Identity and Service Providers in a federation. While each federation participant is expected to maintain its own Identity and Service Providers, it may be more efficient to set up a centralised service that regularly polls the Identity and Service Providers in a federation and uses a pre-defined procedure to raise an alarm, when some of them are not working properly.

5.4. Interfederations

So far, this thesis has studied a setup where organisations willing to enter federated transactions form a federation, and identities are shared between participants of the federation. Now it is time to shortly introduce another layer of abstraction, a federation of federations.

It is obvious that a single federation cannot cover all the parties willing to enter federated transactions. Federations will rise, covering certain geographical areas or/and business, and the federations are willing to establish greater fabrics. The terminology in the area is not yet well-established; concepts like interfederation, confederation, cross-federation and federation peering are used.

Four Nordic countries (Finland, Sweden, Norway and Denmark) each have a national identity federation or a federation project for higher education. In order to support collaboration of Nordic researchers and university teachers, the four countries are committed to forming a confederation, where the end users in one country are able to access Service Providers in other countries. The Kalmar Union, which is the proposed name of the confederation, will be established by the coordinators of the four federations by signing a consortium agreement. The work is described in more detail in [TVET07].

Other interfederation proposals have been presented to interconnect the inCommon federation of the US higher education with the E-Authentication federation of the US federal government [ROTM06]. The eduroam confederation and the project Fidelity are two more interfederation projects, which will be introduced in Sections 5.5.3 and 5.5.4.

5.5. Federation examples

This section presents some examples of federation projects and operational identity federations. The examples spread over higher education, banking and telecommunications industry.

5.5.1. The Haka Federation of Finnish Higher Education

The Haka federation [CSC07] is the identity federation for Finnish universities, polytechnics and research institutions. End users in the federation are students and employees of the organisations. The proposal for establishing the federation was done in February 2004 and the federation was formed in May 2005, when the first universities signed the federation service agreement. The federation became operational in August 2005, when the first Identity and Service Providers were registered. The author has been strongly involved in establishing the federation. According to available information, the Haka federation was the first SAML-based identity federation in Finland, and the second[13] after SWITCHaai [SWIT07] in higher education in Europe [REFE07].

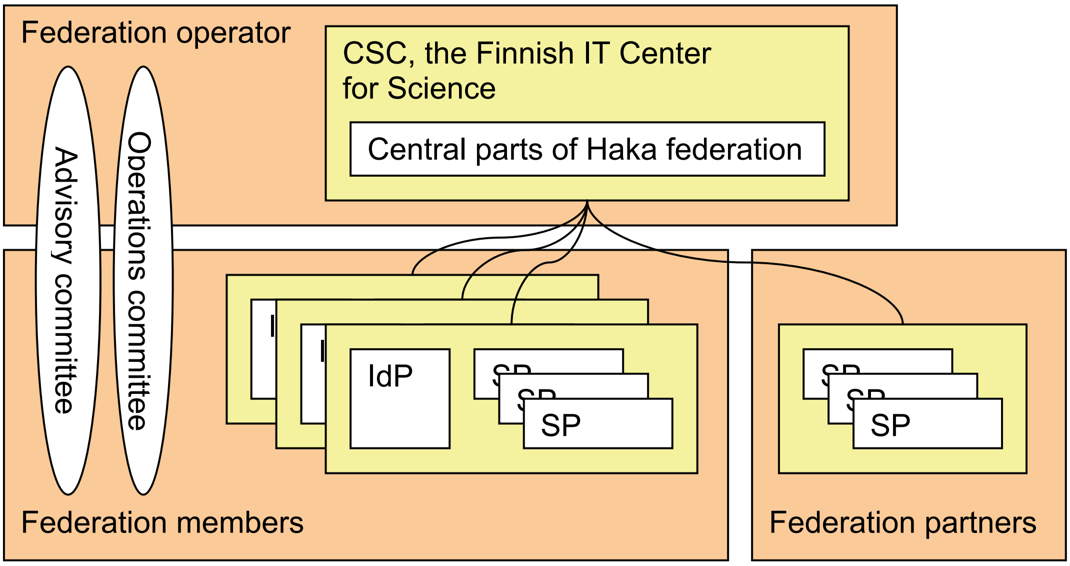

Figure 18. Organisation of the Haka federation

The Haka federation is a hub-and-spoke federation with CSC, the Finnish IT Center for Science in the middle (Figure 18). CSC is both the operator and the coordinator of the federation, and any joining participant signs a federation service agreement with CSC. In order to balance CSC's strong position, the federation has an advisory committee and an operations committee to whom CSC has to listen in

[13] Before SAML, some countries, such as Norway, Spain and the UK, have had federations based on proprietary protocols.

predefined circumstances, such as in changing the requirements for joining participants.

The federation has two participant categories, members and partners. Universities, polytechnics and research institutions are eligible to join the federation as members, and they are able to register both an Identity Provider and Service Providers to the federation. Federation partners, such as library content providers, may register only Service Providers.

From technical perspective, the Haka federation is decentralised (See Figure 17 a) and currently makes use of Shibboleth, a SAML-based federating protocol designed and implemented by Internet2 [INTE07] and the funetEduPerson schema [CSC06]. Currently, there are 29 Identity Providers and 53 Service Providers registered to the federation, and the number of logins is around 300 000 per month. The Haka federation is presented in detail in Publication 5.

5.5.2. TUPAS of the Finnish Banks

For banks, the Internet has become a standard way of providing banking services, and customers are used to logging in to the bank's Internet service. Becoming a customer of an Internet bank in Finland requires signing a contract with the bank and receiving credentials for authentication. Currently, the banks use one-time passwords for authentication.

Banks have also started to provide authentication of their customers as a service to third parties. TUPAS [FBA05] is a proprietary specification developed and published by the Finnish Bankers' Association. TUPAS specifies an interface between the Finnish Internet banks and third party services (such as public sector services), making use of the HTTP POST method for passing their customers identity to third party web services. The integrity of the message exchange is ensured by a symmetric key and authenticity by timestamps and nonces. Each bank has an independent implementation of the TUPAS interface. Currently, seven Finnish banks provide the TUPAS service.

The TUPAS service is an ad hoc federation where the bank is one of the two parties. The bank sets the rules of the service, including prices for the third parties. Bank customers are not charged for utilising the TUPAS interface to authenticate to third party services. The attributes passed in the federation are minimal, consisting only of the Finnish national identification number (formerly known as social security number, carrying the birth date and sex of the customer) and the name of the user for convenience. The only role data that can be extracted from the transaction is that the user is a customer of the bank.

A problem of TUPAS for a third party is that in order to cover all the Internet bank customers he has to sign a contract and implement and configure the interface to all the seven Internet banks one by one. A public sector service called VETUMA has solved the latter problem by adding another layer to the architecture, hiding all the seven banks behind one technical interface. Still, the third party has to sign contracts with all the seven banks. Thus, VETUMA, as it is currently organised, does not make a change to the ad hoc pattern of the federation .

5.5.3. The Project Fidelity

In the previous Section 5.5.2, an identity federation based on Internet banks was introduced. Other potential private sector players in federated identity management are telecommunication operators, who also have tight relationships with their customers. This includes face-to-face authentication of the new customers, up-to-date customer records for billing and credentials for strong authentication such as SIM cards. Thus, teleoperators are potential actors in federating their customers' identities to third party services.

An example of a teleoperator-initiated identity federation was project Fidelity, which started in 2005 and concluded in 2006. Project Fidelity belonged to the Eureka cluster programme Celtic, which initiates and stimulates R&D programmes in telecommunication systems and services [CELT07].

The Project Fidelity introduced an ad hoc federation with the teleoperator as the Identity Provider and services such as 'Find the nearest restaurant', 'Book a hotel room', 'Purchase a game' and 'Student interchange' as Service Providers. In the project, four identity federations, one in Norway, Finland, France and Spain each, were set up. In order to let customers from the Norwegian, Finnish, French and Spanish federations use services in other countries, the four federations were interfederated. The federations used Liberty Alliance specifications as the federating protocol. [QUIN06]

5.5.4. The Eduroam Confederation

All the examples above are intended for web-based application access. Eduroam, being part of the European Commission-funded GEANT2 project, is an example of a federation for network access. The eduroam confederation was established in January 2007 as an international interfederation of national eduroam federations.

Eduroam aims at serving nomadic end users in European higher education. Students and employees are able to use their home institutions' (Identity Provider) credentials to attach to a wireless or wired network in an institution they are visiting (Service Provider). On a national level, the institutions form a hub-and-spoke federation by signing a federation agreement with the national research and education network (NREN). The NRENs, in turn, form the international identity network by signing the multilateral confederation policy. As the result, students in, say, Tampere University of Technology (TUT), are able to use their TUT-provided usernames and passwords to log in to the wireless LAN in the University of Porto. The federation currently makes use of RADIUS as the federating protocol. [WIER05]

6. MAKING USE OF FEDERATED IDENTITY MANAGEMENT

Sections 4 and 5 have introduced the technical foundations of federated identity management and the concept of an identity federation as the association of organisations utilising federated identity. This section makes a walk-through to making use of federated identity management in applications. Finally, some subjects for further research are proposed.

First, a look is taken into the kinds of functionalities federated identity management provides to a service, and, then, some service categories for federated identity management are examined.

6.1. Benefits of Federated Identity Management

This section introduces three basic functionalities federated identity can provide and how they benefit services and their developers and administrators. The three services; authentication, identity provisioning and authorisation, are in the order that is likely when making use of federated identity. The benefits are related to those introduced in Section 3.1, but now in a cross-organisational context.

6.1.1. Authentication and Single Sign-on

When federated identity is used for authentication, an end user is not given separate credentials (e.g., username and password) for each new service introduced. Instead, the end user is able to utilise the credentials used by the Identity Provider for authentication. Whether this also leads to single sign-on (the need to authenticate only once) is a separate issue and depends on the system configuration.

For an end user, being able to use a single set of credentials for all the services is a major benefit of federated identity. If username and password are used for authentication, it is easier to remember only one username and password, when it is used in a large variety of services on a regular basis. This increases both information security and usability.

A Service Provider does not have to care about forgotten passwords because it is a responsibility of the Identity Provider. If an end user has a problem with his user account and password, the first-level support is provided by his home organisation’s helpdesk. The Identity Provider, in turn, may introduce additional quality requirements to the single password the user has. This can include, for example, minimum password length, resistance to dictionary attacks and periodic renewals, depending on the policy of the organisation and the federation. Since the end user has only one username and password, it is fair to expect that he obeys the security best practice and does not write his password down in a small piece of paper next to his workstation. Introduction of stronger authentication is also easier, because it can be done in one place, i.e., in the Identity Provider.

6.1.2. Identity Provisioning

Using federated identity for identity provisioning means that when a new user enters the organisation and his identity is created in the Identity Provider, the attributes provided by the Identity Provider are used for creating an identity for him also in a Service Provider. When the attributes are changed in the Identity Provider, the changes are reflected to the Service Providers. This can take place, for example, when the end user signs in to the service the next time, utilising the attribute assertions provided by the Identity Provider during the browser-based attribute exchange. Alternatively, some backend channel, such as the SOAP binding of SAML or SPML (Service Provisioning Markup Language) [COLE06] can be used for regular user data updates, for example, every night.

From an information security perspective, de-provisioning is even more critical than provisioning. For instance, if an employee is fired, the Identity Provider takes care of closing his account as described in Section 3.2, and the end user is no more able to log in to the service. However, unless de-provisioned, his identity in the service remains unchanged. This may be problematic, if he is part of a workflow in the service. For example, in an invoice management service, invoices may be still circulated to the fired employee for approval. In such services, a backend channel for de-provisioning is necessary.

As mentioned in Section 3.1, provisioning and de-provisioning reduce overlapping work in an organisation. New end users do not need to be created manually to a service, which generates a significant amount of work in an organisation. Once federated identity is introduced for authentication, it is lucrative to extend its use to provisioning and de-provisioning as well.

6.1.3. Authorisation

As introduced in Section 2.3, authorisation means an end user's permission to carry out an action in an information system. Federated identity management may have a role in taking care of authorisation in a service. In cross-organisational environments, utilising federated identity for authorisation makes it easier to base end user's privileges on up-to-date identity data as provided by the Identity Provider. As mentioned, role-based access control (RBAC) is powerful in complex environments such as in an identity federation. Different ways of implementing RBAC in the context of federated identity are presented and discussed next.

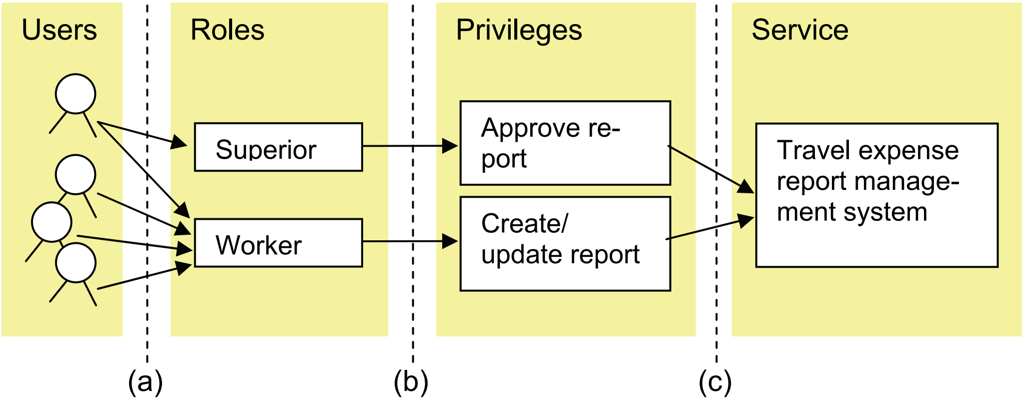

Figure 19. Role-based access control in federated identity

Figure 19 is a refined version of Figure 5 in page 15. The figure proposes three different ways (the dashed lines) to split the responsibilities related to authorisation between the Identity and Service Provider. The alternatives are further clarified in Figure 20.

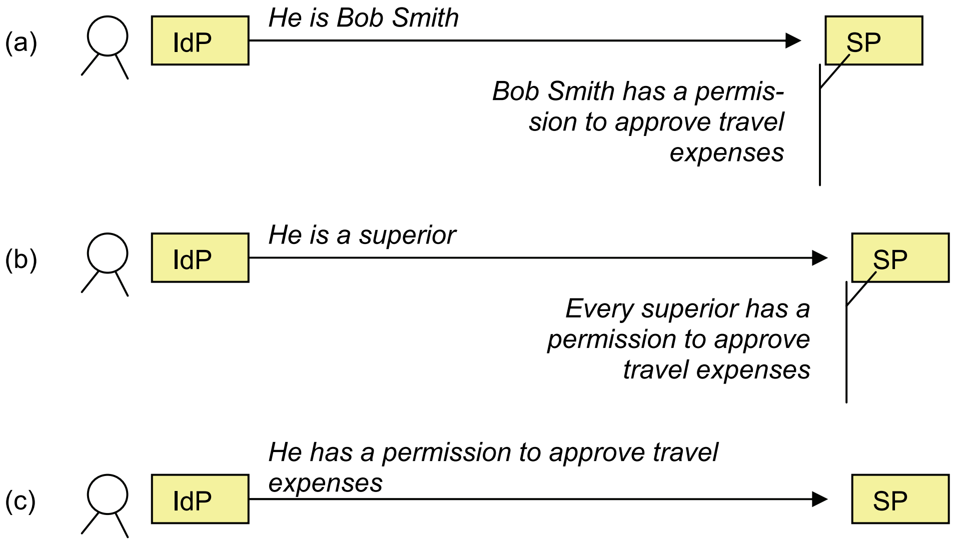
(a)
IdP
He is Bob Smith
SP
Bob Smith has a permission to approve travel expenses
(b)
IdP
He is a superior
SP
Every superior has a permission to approve travel expenses
(c)
IdP
He has a permission to approve travel expenses
SP

Figure 20. Splitting the responsibility of authorisation in federated identity.

The first alternative (a) makes the service fully responsible for authorisation. Federated identity is used just for authenticating the user and providing his identifier to the service, and the rest is up to the service. An end user needs to use some out-of-band mechanism (for instance, a written or electronic application form) to acquire proper authorisations to use the service. As the outcome of the authorisation process, the service administrator may, for example, add required privileges manually to the user's account.

The second alternative (b) uses a role attribute to split the responsibility of authorisation between the Identity Provider and the service. The Identity Provider, which knows the end user and his position in the home organisation best, assigns him a role attribute. Based on the role attribute, the service decides what kind of permissions (if any) the end user has in the service.

The third alternative (c) makes the Identity Provider fully responsible for authorisation. All the service needs to do is to trust the Identity Provider in its judgement. In other words, the Policy Decision Point (PDP) is placed in the Identity Provider and the Policy Enforcement Point (PEP) in the Service Provider, whereas in alternatives (a) and (b) they are both placed in the Service Provider.

The alternative (a) represents the traditional scenario, where end users use out-of-band means to get a permission to use the system. When federated identity management is introduced to a service, it is likely that it is used for authentication at first, making the alternative (a) a starting point. Later, the service may move towards the alternatives (b) and (c).

The alternative (b) contains an elegant division of responsibility. By definition, the Identity Provider is the party that knows best its end users and their position and role in the home organisation. The Service Provider is the party that is the specialist of the service and is also given the control regarding who may use it. Compared to the alternative (a), this alternative increases the functionality and complexity that needs to be implemented in the Identity Provider. On the other hand, in the home organisation, maintenance of the role information can be integrated to the organisational identity management architecture as was described in Section 3.6.

As a downside, the alternative (b) expects a common vocabulary for roles that both the Identity and Service Provider (or, in a federation of several organisations, all the involved Identity and Service Providers) use. This may be possible for simple roles, but defining and maintaining a complete vocabulary for roles in a multi-organisational context may turn out to be simply too difficult. However, if a vocabulary exists and is sufficient for assigning permissions in the service, this is a very light-weight way of implementing access control in federated services. Consider, for instance, an extranet service that is available for any end user employed by the Human Resources unit of any home organisation.[14]

The alternative (c) removes the need for a common vocabulary for roles. Instead, in a simple setup, each service defines an entitlement value that is considered as a permission to use the service and it is a responsibility of the Identity Provider to

[14] In this case, any end user with the role ”organizational unit (ou) = HR management” would have read privileges. In practice, there is no vocabulary for the ou attribute, but maintaining a couple of alternative ou values is still easier than using the alternatives (a) or (c), instead.

populate the value for those end users who are permitted to use the service. In more complex setups, an authorisation assertion can be passed from an Identity Provider (PDP) to a Service Provider (PEP) using, for instance, a SAML authorisation statement or XACML (Extensible Access Control Markup Language) response context [MOSE05].

From an Identity Provider's perspective, the difference between the alternative (b) and (c) is that in (c), introducing a new service to a federation requires that each Identity Provider needs to assign a new privilege to each end user of the service. In alternative (b), the service makes use of the existing set of role values, and if the values are already populated in an Identity Provider, no new attribute values need to be assigned to the end users in the Identity Provider. Additionally, in both alternatives (b) and (c), each Identity Provider needs to be configured to release proper attributes to the new service, but it is a relatively easy task and can be delegated to the operator of the federation, as proposed in Section 5.3.2.

The need to assign new entitlement values for the users of each new service makes the scalability of the architecture (c) weaker than the alternative (b). However, integration to the organisational identity management and internal use of RBAC may ease this work in the Identity Provider. For instance, if the end user has a role of a supervisor inside the organisational identity management and, according to the company policy, supervisors are permitted to approve travel expenses, the organisational identity management can automatically populate him the entitlement for approving travel expenses.

In a cross-organisational context, Identity and Service Providers are in separate organisations. A potential obstacle in adoption of alternatives (b) and (c) is the traditional way of thinking that the service owner needs to have the final word regarding who is permitted to use the service. In the alternative (a) this is the case, when the service administrator, for instance, authorises each end user one by one. The authorisation may be very nominal, for example, receiving an application, signed by the applicant and his supervisor in the Identity Provider, filing the application and assigning necessary privileges to the end user manually. Considering this scenario, a leap to the alternatives (b) and (c) may feel long, because the manual authorisation is replaced by automated grant of necessary privileges based on an assertion from the Identity Provider. However, effectively, the only thing that is changed is that routine work is automated, increasing the efficiency as a whole. Of course, the Service Provider needs to trust the assertions that carry the end users' permissions, but this belongs to the nature of federated identity management, as explained in Section 4.2.4.

As a final remark, the alternatives (b) and (c) open new possibilities in preserving the end user's privacy. For authorisation purposes, the Identity Provider needs not reveal the end user's identity to the service. It is enough to provide an assertion that contains the role or privileges of the end user, not his identity. In a way, this is close to the idea of using authorisation certificates instead of binding an end user's privileges to his name, as presented in SPKI [RFC2693] and SDSI [RIVE96]. Contrary to the traditional approach where end users have their identities in each service, this could reduce unnecessary processing of personal data in services in the Internet.

What is said above applies to processing personal data for authorisation purposes only. Of course, there are services which still need to know the identity of the user, for example, to maintain his profile in the service or to send him notifications by email. Also the accountability requirements may imply that the identity of a user should be easily traced.

6.2. Services Relying on Federated Identity

Publication 5 presents some typical service categories benefiting from federated identity in higher education. For completeness, this section provides a more generic view on what kind of service categories can benefit from federated identity management.

6.2.1. Application Service Provisioning

Earlier, organisations used commercial software by acquiring a license to use it in their own server. Nowadays, organisations often increase their efficiency by focusing on their core business, and activities, such as maintenance of information systems, are outsourced. Application Service Provisioning (ASP, a.k.a Software as a Service, SaaS) means that an organisation purchases an application as a service from another organisation that is focused on its maintenance. The software runs in the machines of the ASP provider. The end users in an organisation typically use a web browser to use the service.

Software running as ASP is becoming richer in functionality, and all the more end users in the organisation need to use it. This incorporates workflow applications, such as circulation of invoices, and self-service interfaces to applications, such as an employee self-service access to the HR system. It is typical that all these services expect a large number of end users to log in. Without federated identity management, the end users would be expected to learn another username and password for each service. If an end user needs to log in, for instance, to the HR system just a couple of times a year to propose the date for his summer vacation, it is obvious that remembering the username and password is a problem.

In federated access to ASP services, an end user uses his existing username and password and the organisation's Identity Provider to sign in to the ASP service. In addition to authentication, federated identity can be utilised to provision a new end user to the service. Furthermore, depending on the service, an end user's authorisation to use the service can be done on the Identity Provider side as was introduced in Section 6.1.3, and there is no need to manage the end users' privileges manually in the service.

6.2.2. Extranet Services

In the networked world, organisations collaborate with each other, forming partnerships and supply chains where individuals from different organisations work closely together in order to conduct business. This often incorporates providing customers or suppliers with access to the organisation's business systems via web-based extranet services. End users representing other organisations need to be authenticated and authorised to use the organisation's information systems.

The organisation employing a person is the one that knows best the issues related to his employment. If an employee resigns, the employer removes his entry from the base registry as described in Section 3.2. In the business environment of the organisation, the end user's authorisation to use the business partner's extranet services ceases as well. Utilising federated identity to enforce access control provides extranet services more protection against orphaned accounts that are potentially misused.

6.2.3. Mobility and Roaming Network Access

In addition to web-based applications, federated identity can be utilised in network access itself. Subenthiran et al define terminal mobility as a user being able to change location or access technique (WLAN, UMTS, Bluetooth etc.) while keeping the same terminal. With roaming, the users are able to obtain access from a visited network different from the home network they have subscribed to [SUBE04]. The eduroam confederation mentioned in Section 5.5.4 is an example of a federation providing roaming service.

The eduroam federation, as it is nowadays, utilises RADIUS as the federating protocol [GEAN06]. An end user's credentials are passed to the Identity Provider on a RADIUS request/response pair carrying some of the various EAP authentication protocols available, such as EAP-TTLS and EAP-TLS. The Identity Provider sends an acknowledgement as a response to the request, if the credentials are successfully verified. The requests and responses are passed between the Identity and Service Provider via a hierarchy of RADIUS proxy servers.

A downside of the current eduroam setup is that it does not cover authorisation. Instead, authorisation is implicit; if authentication succeeds (typically, if the end user has an account in the Identity Provider and knows the password), the end user is authorised to access the network provided by the Service Provider.

Publication 6 introduced a refinement to this architecture, introducing the HTTP-based SAML as a replacement for RADIUS as the federating protocol. The architecture was implemented and is currently used in the University of Helsinki [HUPN07]. A SAML-based architecture made it possible to use SAML attribute assertions for authorisation of network access. For example, on its premises, the University of Helsinki could allow roaming WLAN access only to staff members of other Finnish universities, but not to students. A downside of the architecture is that it lacks layer 2 encryption, which is nowadays commonly ensured by IEEE 802.11i protocol [IEEE04], also known as WPA2.

The idea of using SAML in network access control, which was introduced in Publication 6, is being further elaborated in the European Commission-funded GEANT2 project, whose activity DAMe (Devolved Authorisation Methods for eduroam) considers using SAML and XACML assertions and the DIAMETER protocol [RFC3588] for authorisation in network access. As a result, a new NAS-SAML architecture is being specified, making it possible for an eduroam Service Provider to utilise attributes provided by an Identity Provider in the access control decision. [CANO07]

6.3. Future research

Finally, some topics for further research are suggested in this section. Federated identity management is still a young subject of interest, and various problems need to be addressed.

Auditing and reporting was introduced as one basic concept of identity management in Section 2.4. For audit purposes, it is necessary to have tools for investigating who has certain privileges to a system and what actions an end user has done in a system. In commercial services, accounting may be necessary for billing purposes, too.

A cross-organisational use of federated identity introduces additional complexity for reporting tools. If an end user's identity and privileges are maintained by separate entities (see alternatives (a) and (b) on Section 6.1.3), providing an aggregated view of an end user's privileges means fetching and combining identity information from several Service Providers. If the Service Providers are placed in separate organisations, this may incorporate release of personal data between several person registries. Further research is necessary to understand the related technical and legal challenges.

Section 4.1 introduced a bipolar architecture for federated identity management, having an Identity Provider responsible for end user identity and authentication and a Service Provider that consumes identity assertions issued by the Identity Provider. Extending this model to a **multipolar architecture** would provide new research and engineering challenges.

In a multipolar architecture, issuance of authentication, attribute and authorisation assertions could be done by different entities or even organisations. In the world of networking and collaboration, it is usual that the organisation responsible for an end user's identity does not control all his roles and privileges. For instance, in universities, there are formal and informal collaboration groups, often termed Virtual Organisations, which span multiple organisations.

The SAML standard supports a multipolar architecture and the first proposals for multipolar architectures have already been presented [e.g. ROBI06, CHAD07]. Still, there is work to do in studying the different approaches and engineering them to production level services. A multipolar architecture could also open new opportunities for commercial services related to federated identity management. For example, a commercial company could develop a workflow engine for applying and granting privileges to end users in an organisation. The engine would have a web-based self-service interface for end users applying for privileges. The customer representatives responsible for granting the privileges could have a separate web interface for handling the applications and printing out reports on current privileges. The engine could then be provided as a service that provides authorisation assertions to Service Providers.

Ability to delegate privileges was mentioned as one dimension of identity management in Section 2.3. There are use scenarios for delegation in federated identity management, too. For instance, using the well-worn example of travel expenses, the person with privileges to approve travel expense reports might need to delegate his role or privileges when he is off for a holiday. Additional research and engineering is suggested for finding out how to technically implement delegation and what kind of functional entities (such as a Delegation Authority [GOMI05]) should be introduced to an identity federation.

The current SMTP (Simple Mail Transfer Protocol) based email system of Internet is suffering from unsolicited bulk email a.k.a. **spam**, which consumes resources and is annoying for end users. Currently, spam messages are usually sent by hacked computers which have been turned into open relays for the SMTP traffic that the spammers generate.

In an identity federation, Service Providers have a mechanism to authenticate the Identity Providers (possibly, via interfederations) and Identity Providers are responsible for identifying and authenticating the end users. A possible topic for further research is how this could be utilised for preventing spam. For instance, in order to drop a letter to the receiver's mailbox, the sender would be redirected to his Identity Provider for authentication. A Service Provider built in the receiver's mail server would rely on the user authentication carried out by the Identity Provider. The end user would be allowed to drop the email directly to the receiver's mail server. Dropping letters directly to the receiver's mailbox would also increase confidentiality of the current Internet mail.

7. CONCLUSIONS

As more and more information systems keep records on their end users and expect them to log in, identity management has become a subject of interest for researchers and practitioners. This thesis focused on identity management in an organisation maintaining end users' identities in several information systems. In organisational identity management, functions in the organisations are rationalised so that end users (e.g., employees, students, customers, patients) have a single identity that spans all or at least the most prominent information systems in the organisation. In cross-organisational identity management, the identities are used also in information systems provided by other organisations.

Developing organisational and cross-organisational identity management improves the organisation's information security, as changes in an end user's identity (such as the departure of an employee) are reflected to other information systems in a timely manner. An end user has a single set of credentials, and if stronger authentication means are needed, they can be introduced to several information systems in one go. Having a single view of an end user's identity lays also ground for auditing.

Identity management can be used for developing an organisation's efficiency. The amount of maintenance of overlapping (and soon also conflicting) data on the same individuals in different information systems is reduced. A change in an end user's identity flows from his home organisation's authoritative data sources to other systems in the organisation and in other organisations. Finally, investing in organisational and cross-organisational identity management opens new business opportunities or new ways of organising functions that would not have been possible otherwise.

In an organisation, the first action to take is improving organisational identity management. Metadirectories, virtual directories and other technical constructs are used to establish a single view of an end user's identity in the organisation. In the next step, it is then easier to introduce new, more reliable authentication mechanisms (such as PKI and smart cards) because, being part of the single identity, they can be introduced to several information systems at once. High-quality organisational identity management is also a requirement for cross-organisational identity management, which enables information systems in other organisations to rely on an end user's identity in his home organisation.

Improving identity management is not just installing metadirectories or Identity and Service Providers for federated identity. Introducing an identity management architecture is an actively managed project, where parties agree on responsibilities, policies, processes, technical specifications and standards and syntax, semantics and vocabularies for personal information exchanged. This applies both to organisational and cross-organisational identity management.

Identity management is based on trust. In organisational identity management, trust is between the organisation's IT services unit, maintaining the centralised identity management system, and other units that rely on and make use of the identity management system. In cross-organisational identity management, the trust is between organisations who establish a federation, "a circle of trust", to exchange information about their users and resources.

Additionally, an end user needs to trust the way his identities are managed in the organisations. After all, an end user is the principal whose needs and daily routines identity management serves. If implemented properly, identity management can greatly ease an end user's interactions with different information systems. On the other hand, having a single view on an end user's identity also raises new concerns on his privacy. Attention should be paid to this at both a technical and a policy level.

8. AUTHOR'S CONTRIBUTION

In their article regarding research on IT, March et al present four classes of research outputs; constructs, models, methods and instantiations. **Constructs** form the vocabulary of a domain. They constitute a conceptualisation used to describe problems within the domain and to specify their solutions. A **model** is a set of propositions or statements expressing relationships among constructs. In design activities, models represent situations as problem and solution statements. A **method** is a set of steps (an algorithm or a guideline) used to perform a task. They are based on a set of underlying constructs and models. **Instantiation** is a realisation of an artefact in its environment, operationalising constructs, models and methods. Instantiations demonstrate the feasibility and effectiveness of the models and methods they contain. [MARC95]

On the other hand, March et al present four kinds of research activities; build, evaluate, theorise and justify. **Build** refers to the construction of the artefact, demonstrating that such an artefact can be constructed. The basic question is: does it work? **Evaluate** refers to the development of criteria and the assessment of artefact performance against those criteria. The basic question is: how well does it work? Build and evaluate are the two basic activities in design sciences (cf., innovation implementation and assessment in Section 1.4).

Given an artefact whose performance has been evaluated, it is important to determine why and how the artefact worked or did not work within its environment. **Theorising** explicates the characteristics of the artefact and its interaction with the environment that result in the observed performance. Given a theory, we must **justify** that explanation, that is, we must gather evidence to test the theory. Theorise and justify refer to the two basic activities of natural sciences (cf., methods creating theory and methods testing theory in Section 1.4). [MARC95]

Given the categories for research output and research activities by March et al, the research results of Publications 1-6 can now be presented in Table 5. Numbers in the table refer to the corresponding publication. The publications are then examined one by one in the order of publishing, evaluating their research results and the author's contribution.

Table 5. Results of Publications 1-6 using the research framework by March et al

Activities/ Outputs	Design sciences		Natural sciences	
	Build	Evaluate	Theorise	Justify
Constructs				
Model	5	5	5	
Method	4, 5, 6	1, 3, 4, 5, 6	3, 4, 5, 6	3
Instantia-tion	2, 4, 5, 6	1, 2, 5, 6	2, 5, 6	

Publication 2, "Lessons Learned in PKI Implementation in Higher Education" (published in 2002) was the first of the six publications. For the publication, an experimental PKI deployment was built and evaluated in Finnish higher education. As a result of theorising, the seven conclusions presented in the publication were drawn by the project team, Mr Pekka Linna being the secretary. The author was responsible for the publication and the reasoning presented.

Publication 4, "Towards Cross-organisational User Administration" (published in 2003) was an early result of the HAKA project. Based on an early Shibboleth document [ERDO02] of Internet2, the publication presented a method for cross-organisational identity management. At the time, there was little prior work available.

Publication 6, "Roaming Network Access Using Shibboleth" (published in 2004) was based on Mr Viljo Viitanen's idea and implementation. As March has noted, an instantiation may actually precede the complete articulation of its underlying constructs, models and methods [MARC95]. The author was responsible for evaluating the idea and theorising it and drawing the connections to other roaming-related work done.

Publication 5, "Organising Federated Identity in Finnish Higher Education" was published in 2005, when the Haka federation was rolled out. The publication theorised several non-technical issues, such as how to organise a federation, how to formulate the organisations' responsibilities and how to comply with privacy laws. According to Järvinen, an innovation may cover not only technical artefacts, but also organisational innovations [JÄRV00]. The model and methods were implemented in the Haka federation.

Publication 3, “An Empirical Study on the Usability of Logout in a Single Sign-On System” (published 2005) was a spin-off in the work that the author had done with organisational and cross-organisational single sign-on systems. Having realised that few single sign-on systems covered logout at all, the author got an idea of studying the subject from an end user perspective. This publication was the author’s voyage to empirical sciences; together with a usability researcher, the author studied end user’s expectations on logout in a single sign-on scenario, created theories and justified them in usability tests. Mrs Inka Vilpola was responsible for the empirical methodology used in usability research and the author was responsible for the substance of the study.

Publication 1, “Study on Organisational Identity Management in Finnish Higher Education” (published in 2006) completed the big picture of the thesis. Current identity management implementations in Finnish higher education institutions were evaluated against defined criteria. The work was based on data that was gathered over years in the workshops the author had organised to IT service centre staff.

As shown in the table, research in this thesis falls mostly to the category of design sciences, whereas generic theories can be considered as belonging to natural sciences, “explaining how and why things are” [MARC95]. In most cases, justification of the theories has been done, effectively, by external parties who have ended up with similar theories [e.g. LIBE05, LIBE07c]. Research outputs are focused on models, methods and instantiations, whereas the constructs of the domain were already available.

9. REFERENCES

AHN05 Ahn, G., Lam, J. Managing Privacy Preferences for Federated Identity Management. Proceedings of Digital Identity Management '05. ACM, 2005. 28–36

ALLE02 Allen, D. Information infrastructures, information behaviour and trust. Proceedings of EUNIS2002, the 8th International Conference of European University Information systems, 2002. 167–178

ANCH03. Anchan, A., Pegah, M. Regaining Single Sign-On Taming the Beast. Proceedings of SIGUCCS'03 Conference. ACM, 2003. 166–171

ANDE01 R, Anderson. Security Engineering. John Wiley & Sons Inc, 2001. 612 pages

ARTI07 Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data. WP 139. June, 2007

BALF05 Balfanz, D., Durfee, G., Smetters, D. Making the Impossible Easy: Usable PKI. In Cranor L., Garfinkel, S. (eds): Security and Usability. Designing Secure Systems That People Can Use. O'Reilly Media Inc, 2005. 319–333

BARK97 Barkley, J., Cincotta, A., Ferraiolo, D., Gavrila, S., Kuhn, D. Role Based Access Control for the World Wide Web. 20th National Computer Security Conference, 1997

BASI06 Basin, D., Doser, J., Lodderstedt, T. Model driven security: From UML models to access control infrastructures. ACM Transactions on Software Engineering and Methodology (TOSEM). Volume 15, Issue 1, January 2006. 39–91

BELL02 Bellina, B. (ed): Metadirectory Practices for Enterprise Directories in Higher Education. NFS Middleware initiative, 2002

BERT04 Bertino, E., Ferrari, E., Squicciarini, A. Trust Negotiations: Concepts, Systems, and Languages. IEEE Computer, July-August 2004. 27–34

BERT06 Bertono, E., Bhargav-Spantzel, A., Squicciarini, A. Policy Languages for Digital Identity Management in Federation Systems. Proceedings of the seventh IEEE International workshop on Policies for Distributed Systems and Networks (POLICY'06), 2006

BHAR06 Bhargav-Spantzel, A., Camenisch, J., Gross, T., Sommer, D. User Centricity: A Taxonomy and Open Issues. Proceedings of Digital Identity Management '06. ACM, 2006. 1–10

BLEZ02 Blezard, D., Marceau, J. One User, One Password: Integrating Unix Accounts and Active Directory. Proceedings of SIGUCCS'02 Conference. ACM, 2002. 5–8

BUEL03 Buell, D., Sandhu, R. Identity Management. IEEE Internet Computing, Volume 7, Issue 6, November-December 2003. 26–28

BURR06 Burr, W., Donson D., Polk, W. Electronic Authentication Guideline. NIST Special Publication 800-63, version 1.0.2. National Institute of Standards and Technology, 2006. 54 pages

CAMP04 Camp, J. Digital Identity. IEEE Technology and Society Magazine, Fall 2004. 34–41

CANO07 Canóvas, Ó., Gómez-Skarmeta, A., López, G., Sánchez, M. Deploying Authorization Mechanisms for Federated Services in eduroam (DAMe). Internet Research, Volume 17, Issue 5, 2007. 479–494

CANT05 Cantor, S., Moreh, J., Philpot, B., Maler, E. (eds): Metadata for the OASIS Security Assertion Markup Language (SAML) v2.0. Oasis Open, March 2005. 43 pages

CELT07 Celtic - Telecommunication solutions. http://www.celtic-initiative.org/ Referenced 30.6.2007

CHAD06 Chadwick, D., Zhao, G., Otenko, S., Laborde, R., Su, L., Nguyen T. Building a Modular Authorization Infrastructure. In All Hands Meeting, Nottingham. September, 2006

CHAD07 Chadwick, D., Inman, G., Klingenstein, N. A Conceptual Model for Attribute Aggregation.

CHAP06 Chappell, D. Introducing Windows CardSpace. Windows Vista Technical Articles. April, 2006

CLAU05 Clauss, S. Kesdogan, D., Kölsch, T. Privacy Enhancing Identity Management: Protection Against Re-identification and Profiling. Proceedings of Digital Identity Management '05. ACM, 2005. 84–93

CLER02 De Clercq, J.: Single sign-on architectures. In: Davida, G., Frankel Y., Rees, O. (eds): Proceedings of Infrastructure security, International Conference, InfraSec 2002. Lecture Notes in Computer Science 2437. Springer-Verlag, 2002. 40–58

COLE06 Cole, G. (ed) OASIS Service Provisioning Markup Language (SPML) version 2. Oasis Open, April 2006. 190 pages

CONS99 Parlament of Finland: The Constitution of Finland. 731/1999. 11 June 1999. Unofficial translation

CSC06 CSC, the Finnish IT Center for Science. funetEduPerson Schema. Version 2.0. June, 2006

CSC07 CSC, the Finnish IT Center for Science. Haka federation. http://www.csc.fi/english/institutions/haka/ Referenced 19.7.2007

CULN99 Culnan, M., Armstrongm P. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science, Volume 10, Number 1, January-February 1999. 104–115

DAMI03 Damiani, E., De Capitani di Vimercati, S., Samarati, P.: Managing Multiple and dependable identities. IEEE Internet Computing, November-December 2003. 29–37

DJOR05 Djordjevic, I., Dimitrakos, T. A note on the anatomy of federation. BT Technology Journal, Volume 23, Number 4, October 2005. 89–106

EMIG07 Emig, C., Brandt, F., Abeck, S., Biermann, J., Klarl, H. An Access Control Metamodel for Web Service-Oriented Architecture. Proceedings of International Conference on Software Engineering Advances (ICSEA 2007). IEEE, 2007. 57–64

EP95 Directive 95/46/EC of the European Parlament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Official Journal L 281, 23/11/1995, 0031–0050

ERDO02 Erdos, M., Cantor, S. Shibboleth-Architecture Draft v05. May, 2002

FBA05 The Finnish Bankers' Association. Banks' Tupas Certification Service for Service Providers. Service description and guidelines. Version 2.1. October, 2005. 22 pages

FELD99 Feldman, R. Understanding Psychology. The fifth edition. McGraw-Hill, 1999. 774 pages

FERR92 Ferraiole, D., Kuhn, R. Role-Based Access Control. Proceedings of the 19th National Computer Security Conference, 1992

FERR95 Ferraiole, D., Cugini, J., Kuhn, R. Role-Based Access Control: features and Motivations. Proceedings of the 11th Conference in Computer Security Applications, 1995

FERR00 Ferraiole, D., Sandhu, R., Gavrila, S., Kuhn, D., Chandramouli, R. A Proposed Standard for Role-Based Access Control. National Institute of Standards and Technology. December, 2000

FUCH07 Fuchs, L., Pernul, G. Supporting Compliant and Secure User Handling – A Structured Approach for In-House Identity Management. Second International Conference on Availability, Reliability and Security (ARES'07). IEEE, 2007. 374–384

GAED05 Gaedge, M., Meinecka, J., Nussbaumer, M. A Modelling Approach to Federated Identity and Access Management. Proceedings of the WWW 2005 conference. ACM, 2005. 1156–1157

GEAN06 GÉANT2. European Eduroam Confederation Policy. Version 1.1. 13 pages. Available in http://www.eduroam.org/

GNOM07 Greater NOrdic MIddleware Symposium (GNOMIS). http://www.gnomis.org/ Referenced 12.7.2007

GOLL99 D. Gollman. Computer Security. John Wiley & Sons Inc, 1999. 320 pages

GOMI05 Gomi, H., Hatakeyama, M., Hosono, S., Fujita, S. A Delegation Framework for Federated Identity Management. Proceedings of Digital Identity Management '05. ACM, 2005. 94–103

GOOD07 Goodner, M., Hondo, M., Nadalin, A., McIntosh, M., Schmidt, D. Understanding WS-Federation. Version 1.0. May, 2007. 49 pages

GRAH92 Graham, D. Incremental Development and Delivery for Large Software Systems. IEE Colloquium on Software Prototyping and Evolutionary Development. IEE, 1992. 2/1–2/9

GROS03 Gross, T. Security Analysis of the SAML Single Sign-on Browser/Artifact Profile. Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC 2003). IEEE, 2003. 298–307

HAIK04 Haikala, I., Märijärvi, J. Ohjelmistotuotanto. 10th edition. Talentum, 2004. 440 pages.

HE05 He, J., Zhang, R. Towards a Formal Framework for Distributed Identity Management. Proceedings of the 7th Asia Pacific Web Conference 2005. Lecture Notes in Computer Science 3399. Springer-Verlag, 2005. 913–924

HOLZ91 Holzmann, G. Design and Validation of Computer Protocols. Prentice-Hall, 1991. 543 pages

HUPN07 University of Helsinki. HUPnet – Helsinki University Public Network. http://www.helsinki.fi/atk/yhteydet/hupnet/index_en.html Referenced 1.7.2007

IBM99 IBM Multi-National Consumer Privacy Survey. IBM Global Services. October, 1999

IDAB07 IDABC Programme, eID Interoperability for PEGS. Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms. European Communities. December, 2007. 73 pages

IDAB07b IDABC Programme, eID Interoperability for PEGS. Report on interoperable eID Management technical solutions. European Communities. December, 2007. 46 pages.

IEEE04 IEEE Standard for Information Technology – Telecommunications and Information Exchange between System – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 6: Medium Access Control (MAC) Security Enhancements. IEEE Standard 802.11i-2004, 2004

INCO07 InCommon Federation. InCommon glossary. http://www.incommonfederation.org/glossary.cfm

INTE06 Internet2. EduPerson Object Class Specification (200604a). April 14, 2006; amended May 15, 2007. http://www.educause.edu/eduperson

INTE07 Internet2. http://www.internet2.edu/ Referenced 28.6.2007

ISO06 International Organization for Standardization. 3166-1 Codes for the Representation of Names of Countries and Their Subdivisions – Part 1: Country Codes. ISO/IEC 3166-1, 2006

ISO96 International Organization for Standardization. 10181-3 Information technology – Open systems interconnection – Security frameworks for open systems: Access control framework. ISO/IEC 10181-3, 1996

ISO98 International Organization for Standardization. 9241-11 Ergonomic Requirements for Office Work with Visual Display Terminals (VDT)s – Part 11 Guidance on Usability. ISO/IEC 9241-11, 1998

ITUT95 International Telecommunication Union. Information technology – Open systems interconnection – Security frameworks for open systems: Access control framework. Recommendation X.812 (11/95)

ITUT00 International Telecommunication Union. Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks. Recommendation X.509 (03/00)

ITUT05 International Telecommunication Union. Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services. Recommendation X.500 (08/05)

JØSA05 Jøsang, A., Fabre, J., Hay, B., Dalziel, J., Pope, S. Trust Requirements in Identity Management. Australasian Information Security Workshop 2005. 99–108

JÄRV01 Järvinen, P. On Research Methods. Opinpajan kirja, July 2001. 190 pages

KNIG96 McKnight, H., Chervany, N. The Meanings of Trust. MISRC Working Paper Series 96-04, Management Information Systems Research Center, University of Minnesota, 1996

LAMP69 Lampson, B. Dynamic Protection Structures. AFIPS Conference Proceedings, Fall Joint Computer Conference, 1969. 27–38

LARS05 Larsson, A. A Case Study: Implementing Novell Identity Management at Drew University. Proceedings of SIGUCCS'05 Conference. ACM, 2005. 165–170

LIBE05 Liberty Alliance Project. Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation. February, 2005

LIBE07 The Liberty Alliance Project. http://www.projectliberty.org/ Referenced 28.6.2007

LIBE07b The Liberty Alliance Project. Liberty Technical Glossary. Version 2.0

LIBE07c. The Liberty Alliance Project. Liberty Alliance Contractual Framework Outline for Circles of Trust. March, 2007. 11 pages

LIGU07 Ligue des Bibliothèques Européennes de Recherche. LIBER Licensing Principles for Electronic Information. http://www2.kb.dk/liber/news/981116.htm Referenced 19.7.2007

LIND02 Linden, M. Public Key Infrastructure, Smart Cards and Their Utilization in an Organization. Licentiate Thesis, 2002

LIU04 Liu, L., Yu, E. Intentional Modeling to Support Identity Management. In: Atzeni, P. et al (eds): Proceedings of the 23th International Conference on Conceptual Modeling (ER) 2004. Lecture Notes in Computer Science 3288. Springer-Verlag, 2004. 555–566

LOCK06 Lockhart, H., Andersen, S., Bohren, J., Sverdlov, Y., Hondo, M., Maruyama, H., Nadalin, A., Nagaratnam, N., Boubez, T., Morrison, S., Kaler, C., Nanda, A., Schmidt, D., Walters, D., Wilson, H., Burch, L., Earl, D., Baja, S., Prafullchandra, H. Web Services Federation Language (WS-Federation). Version 1.1. December, 2006. 124 pages

MADS05 Madsen, P., Koga, Y., Takahashi, K. Federated Identity Management for Protecting Users from ID Theft. Proceedings of Digital Identity Management ‘05. ACM, 2005. 77–83

MARC95 March, S., Smith, G. Design and Natural Science Research on Information Technology. Decision Support System, Volume 15, Issue 4, 1995. 251–266

MERR07 Merriam-Webster's Online Dictionary. Encyclopaedia Britannica, Inc. Referenced 29.6.2007

MERR08 Merriam-Webster's Online Dictionary. Encyclopaedia Britannica, Inc. Referenced 6.10.2008

MICR04 Microsoft Corporation. Microsoft .NET Passport Revied Guide. January, 2004. 37 pages

MINE06 Ministry of Education. Statistics from KOTA database 2005. Publications of the Ministry of Education 2006:37. 58 pages

MINE06b Ministry of Education. Statistics from AMKOTA database 2005. Publications of the Ministry of Education 2006:42. 147 pages

MINF07 Ministry of Finance. A Project for Authenticaton and Authorization of Civil Servants. Preparatory Study report. June, 2007. (In Finnish)

MONT03 Mont, M., Pearson, S., Bramhall, P. Towards Accountable Management of Privacy and Identity Information. Proceedings of the ESORICS 2003 conference. Lecture Notes in Computer Sciences 2808. Springer-Verlag, 2003. 146–161

MOSE05 Moses, T. (ed) Extensible Access Control Markup Language (XACML) Version 2.0. Oasis Open, February 2005. 141 pages

MUEL04 Mueller, M. Identity Economics and Policy for Distributed Systems. 1st International workshop on Grid Economics and Business Models. IEEE, 2004. 83–94

NADA06 Nadalin, A., Kaler, C., Monzillo, R., Hallam-Naker, P. (eds): Web Services Security: SOAP Message Security 1.1 (WS-Security 2004) Oasis Open, February 2006. 76 pages

NADA07 Nadalin, A., Goodner, M., Gudgin, M., Barbir, A., Granqvist, H. (eds): OASIS WS-Trust 1.3. Oasis Open, March 2007. 75 pages

OMG07 OMG Unified Modelling Language (OMG UML), Infrastructure, V2.1.2. November, 2007

OPPL04 Oppliger, R. Microsoft .NET Passport and identity management. Information Security Technical Report, Volume 9, Number 1. Elsevier, 2004. 26–34

OTJA06 Otjacques, B., Hitzelberger, P., Feltz, F. Identity Management and Data Sharing in the European Union. Proceedings of the 39th Hawaii International Conference on System Sciences. IEEE, 2006

PASH03 Pashalidis, A., Mitchell, C.: A Taxonomy of Single Sign-On Systems. In: Safavi-Naini, R., Sebarry, J. (eds): Proceedings of the 8th Australasian Conference on Information Security and Privacy. Lecture Notes in Computer Science 2727. Springer-Verlag, 2003. 249–264

PERK07 Perkins, E., Witty, R. Magic Quadrant for User Provisioning, 2H07. Gartner RAS Core Research Note G00150475, 2007

PF99 Parlament of Finland: Personal Data Act. 523/1999. Unofficial translation

PF04 Parlament of Finland: Act on the Protection of Privacy in Working Life. 759/2004. Unofficial translation

PFIT02 Pfitzmann, B., Waidner, M. Privacy in Browser-Based Attribute Exchange. Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society. ACM, 2002. 52–62

PFIT03 Pfitzmann, B., Waidner, M. Analysis of Liberty Single Sign-on with Enabled Clients. IEEE Internet Computing, November-December 2003. 38–44

PFIT03b Pfitzmann, B. Privacy in Enterprise Identity Federation – Policies for Liberty Single Signon. Proceedings of the Third International Workshop on Privacy Enhancing Technologies PET 2003. Lecture Notes in Computer Sciences 2760. Springer-Verlag, 2003. 189–204

PFIT05 Pfitzmann, A., Köhntopp, M. Anonymity, Unlinkability, Unobservability, Pseudonymity and Identity Managememt - Consolidated Proposal for Terminology. V0.22. July, 2005

QUIN06 F, de Quinto, M. Medina. Best Practices in Federated identity scenarios. In eChallenges 2006

RAGO06 Ragouzis, N., Hughes, J., Philpott, R., Maler, E. (eds): Security Assertion Markup Language (SAML) v2.0 Technical Overview. Working Draft 10. Oasis Open, October 2006. 61 pages

RECO06 Recordon, D., Fitzpatrick, B. OpenID Authentication 1.1. May, 2006

RECO06b Recordon, D., Reed, D. OpenID 2.0: A platform for User-Centric Identity Management. Proceedings of the Digital Identity Management ’06. ACM, 2006. 11–15

REFE07 Terena TF-EMC2. Federation Survey. http://www.rediris.es/wiki/tf-emc2/index.php/Federations Referenced 12.7.2007

RENA05 Renaud, K. Evaluating Authentication Mechanisms. In Cranor L., Garfinkel, S. (eds): Security and Usability. Designing Secure Systems That People Can Use. O’Reilly Media Inc, 2005. 103–128

RFC1035 Mockapetris, P. Domain Names – Implementation and Specification. Internet Engineering Task Force. RFC 1035. November, 1987

RFC2693 Ellison, C., Frantz, B., Lampson, B., Rivest, R., Thomas, B., Ylönen, T. SPKI Certificate Theory. Internet Engineering Task Force. RFC 2693. September, 1999

RFC2798 Smith, M. Definition of the inetOrgPerson LDAP Object Class. Internet Engineering Task Force. RFC 2798. April, 2000

RFC3588 Calhoun, P., Loughney, J., Guttman, E., Zorn, G., Arkko, J. Diameter Base Protocol. Internet Engineering Task Force. RFC 3588. September, 2003

RFC4519 Sciberras, A. Lightweight Directory Access Protocol (LDAP): Schema for User Applications. Internet Engineering Task Force. RFC 4519. June, 2006

RFC4949 Shirley, R. Internet Security Glossary, Version 2. Internet Engineering Task Force. RFC 4949. August, 2007

RIEG07 Rieger, S., Neumair, B. Towards usable and reasonable Identity Management in heterogenous IT infrastructures. 10th ISIP/IEEE International Symposium on Integrated Network Management. IEEE, 2007. 560–574

RIVE96 Rivest, R., Lampson, B. SDSI – a Simple Distributed Security Infrastructure. 1996

ROBI06 Robinson, J., Gemmill, J., Scavo, T., Welch, V. Building Systems with Shibboleth. Proceedings of Terena Networking Conference 2006.

ROTM06 Rotman, L. Internet2 Community Demonstrates Shibboleth Middleware Interoperability with National Science Foundation’s FastLane. Press release, December 2006, https://mail.internet2.edu/wws/arc/i2-news/2006-12/msg00004.html

SAMP06 Sampath, R., Goel, D. RATING: Rigorous Assessment of Trust in Identity Management. Proceedings of the First International Conference on Availability, Reliability and Security, ARES’06. IEEE, 2006

SAND96 Sandhu, R., Coyne, E., Feinstein, H., Youman, C. Role-Based Access Control Models. IEEE Computer, Volume 29, Issue 2, February 1996. 38–47

SCHW07 Schwalbe, K. Information Technology Project Management. Fifth Edition. Thomson Course Technology, 2007. 521 pages

SHIM05 Shim, S., Bhalla, G., Pendyala, V. Federated Identity Management. IEEE Computer, Volume 38, Issue 12, December 2005. 120–122

SHIN00 Shin, M., Ahn, G. UML-Based Representation of Role-Based Access Control. Proceedings of the 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2000 (WET ICE 2000). IEEE, 2000. 195–200

SHIN04 Shin, D., Ahn, G., Shenoy, P. Ensuring Information Assurance in Federated Identity Management. IEEE International Conference on Performance, Computing, and Communications, 2004. IEEE, 2004. 821–826

SUBE04 Subenthiran, S., Sandrasegaran, K., Shalak, R. Requirements for Identity Management in Next Generation Networks. The 6th International Conference on Advanced Communication Technology, 2004. 138–142

SWIT07 SWITCH, the Swiss Educatoin and Research Network. Authentication and authorisation infrastructure. http://www.switch.ch/aai/ referenced 19.7.2007

TAUC02 Tampere Unit for Computer-Human Interaction. Usability evaluation in FEIDHE project. Final Report. Department of Computer Sciences, University of Tampere. February, 2002. 101 pages. (In Finnish)

TERE07 Trans-European Research and Education Networking Association. Schema for Academia. Attribute Definitions for Individual Data. Version 1.3.0. December, 2006

TUT07 Tampere University of Technology. IT Services. User Accounts. Closing the Account. TUT Intranet, referenced 27.12.2007.

TVET07 Tveter, W., Melve, I., Linden, M. Towards interconnecting the Nordic identity federations. Campus-Wide Information Systems, Volume 24, Number 2, 2007. 252–259

UKIC07 The UK Information Commissioner. Data Protection Act 1998. Legal Guidance. 105 pages

USAC02 The Senate and House of Representatives of the United States of America in Congress assembled: An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. 2002

VAHT06 The Government Information Security Management Board. Principles and practices for identity management. VAHTI 9/2006. Ministry of Finance. 50 pages

VAHT06b The Government Information Security Management Board. Electronic Authentication in Public Services. VAHTI 12/2006. Ministry of Finance. 37 pages

VOND96 Vonderembse, M., White G. Operations Management. Concepts, Methods and Strategies. Third Edition. West Publishing Company, 1996. 845 pages

WENN06 Wenning, R. Schunter, M. (eds): The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. World Wide Web Consortium, 2006

WEST67 A. Westin. Privacy and Freedom. Atheneum, 1967

WHIT99 Whitten, A., Tygar, J. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. The 8th USENIX Security Symposium, 1999. 169–184

WIDE03 Wideroos, U-M. The Minister's Answer to Representative Jyrki Kasvi's Question on the Misuse of Government Databases. Written Question 252/2003, Parlament of Finland, 2003

WIER05 Wierenga, K. Florio, L. Eduroam: past, present and future. Selected papers of Terena Networking Conference 2005

WIND05 P. Windley. Digital Identity. Unmasking Identity Management Architecture (IMA). O'Reilly Media Inc, 2005. 234 pages

YUAN05 Yuan, E., Tong, J. Attribute Based Access Control (ABAC) for Web Services. Proceedings of the IEEE International Conference on Web Services (ICWS'05). IEEE, 2005. 569–577

XU05 Xu, W., Chadwick, D., Otenko, S. Developing a Flexible PERMIS Authorisation Module for Shibboleth and Apache Server. Proceedings of 2nd EuroPKI Workshop, University of Kent. July, 2005

PUBLICATIONS

Publication 1

Mikael Linden. Study on Organisational Identity Management in Finnish Higher Education. Proceedings of the 12th International Conference of European University Information Systems EUNIS, 2006. 69–76

Study on Organisational Identity Management in Finnish Higher Education

Mikael Linden

CSC, the Finnish IT Center for Science, Finland

Mikael.Linden@csc.fi

Abstract

In an organisation, various information systems store users' personal attributes, such as usernames, roles and profiles. Over time, the users' affiliation to the organisation may change and her attributes and authorisations in the systems should follow the changes. To enhance information security and efficiency, organisations have deployed metadirectories, which utilise predefined rules to synchronise personal data between systems.

Higher education institutions are organisations with thousands of users, such as students and employees. This paper presents the results of a study on organisational identity management in Finnish universities and polytechnics. The study focuses on the integration level of the institutions' base registries and the enterprise directory and on the scale in which other information systems rely on the enterprise directory in their user administration. Based on the results, generic conclusions on organisational identity management are drawn.

Keywords: identity management, user administration, metadirectory

1. Introduction

Computer security deals with the prevention and detection of unauthorised actions by users of a computer system [7]. User accounts are widely used for distinguishing between the users and for deducing their privileges in a system. After having authenticated a user, the system uses some additional information, for example, access control lists, to find out if the user is authorised to carry out the operation.

A user account is an example of an individual's network identity: a real-life person abstracted in a computer system. In a computer system, identity is a collection of attributes describing a user as well as her properties and roles in an organisation. Some attributes, such as usernames, uniquely identify her; some attributes, such as her role as a student in the university, are useful in role-based customisation and access control.

The proliferation of electronic services has caused a rapid growth in the number of parallel, independent identities an individual has in an organisation. For example, in a university, a user may have a user account for her email, another in the Windows domain, a third one in a learning management system of a laboratory, a fourth one in the services provided by the university administration, such as travel expense reporting or student registry, etc. Furthermore, people also have identities without necessarily accounts for login, for example, in the building access system, telephone exchange and payroll system.

All these partial identities represent the same real-life person, and, in an organisation, their changes are interrelated. For instance, when an organisation hires a new employee, she is entered into the payroll system, the building access system and the telephone exchange, and necessary user accounts with related passwords are created for her. If her role in the organisation changes (for example, a student becomes a staff member in a university) or she leaves the organisation, related updates in her identity should take place. Managing all the identities independently causes overlapping work in the organisation, and, usually, lowers data quality, as the updates are not necessarily propagated everywhere.

Higher education institutions are organisations with thousands or tens of thousands of users. This has made identity management an issue too extensive to be neglected. According to a recent survey among European higher education institutions, heads of the IT services rank identity management as the most time-consuming issue they deal with [16]. In the US higher education, CIOs consider identity management as one of the most important IT issues for their institutions to resolve for strategic success [12].

This paper studies organisational identity management in Finnish universities and polytechnics. The aim of the paper is to first present the current state of identity management and, based on that, find out typical phenomena, which can be generalised. The study is based on a comprehensive survey made among IT services of Finnish universities and polytechnics during 2003-2005.

The second chapter of this paper provides some background information on identity management in an organisation. Chapter three describes the research context and methods, and chapter four presents the research results and discussion. In chapter five, activities aiming at improving organisational identity management in Finnish universities and polytechnics are presented. Chapter six concludes the paper.

2. Identity Management in an Organisation

User identity and account management has been a subject of work for IT practitioners for a long time. First, this chapter discusses the interconnection of organisational identity management and information security. Then, some basic principles and techniques of organisational identity management are introduced. Finally, the connection between organisational identity management and federated identity management is argued for.

2.1. Identity Management and Information Security

In an organisation, a change in a person's position also changes her access rights in systems and creates needs to start using new systems or cease to use the ones she has been using before. The most evident change takes place as the person leaves the organisation.

If a role change creates a need to start using a new information system, it is typically in the interest of the user to make sure she has all the tools, including the user accounts, necessary for her new position. For instance, when a new employee is hired, she or her supervisor will probably harass the IT services until necessary user accounts are created.

The more critical issue affecting security is the closing of accounts, when the user is no more authorised to access them, for example, as an employee leaves the organisation or a student graduates. In opposite to account creation, the closing of accounts is typically not of interest to the account holder. It is either simply unimportant or the user would perhaps even like to continue using the familiar tools and email addresses – not to forget that fired employees may want to cause harm to the organisation. Thus, it is in the interest of the organisation to make sure that only authorised users have accessible accounts. This makes the importance of smooth organisational identity management not only an issue of efficiency, but also an issue of information security.

2.2. Fundamentals of Identity Management in an Organisation

In an organisation, different organisational units typically control information systems carrying personal data. For example, in a university, the HR department is often responsible for the payroll system, the student administration for the student registry, the IT services for Windows and Unix accounts and so on. In the maintenance of personal data, each organisational unit has typically deployed their processes to reflect their own needs.

Polishing organisational processes is necessary for the implementation of organisational identity management. The focus has to be elevated from the organisational unit level to the organisational level, as the processes related to identity management cross the boundaries of organisational units. Techniques play quite a small role here; instead, experts from different parts of the organisation need to be gathered together in order to collect the understanding of how identity information should optimally flow in the organisation, when, for instance, a person is hired or fired. To initiate a change process that potentially affects several organisational units, the commitment has to be made in a sufficiently high level in the organisation. Thus, identity management is not an issue driven only by IT professionals. The support must come from the management of the organisation.

Base registry is the database to which new people are added when they first enter the organisational identity management system. The identities for new persons are created in the base registry and then propagated to the other connected registries. There may be several base registries in an organisation; for example, the payroll system for employees in the organisation, the student registry for students in a school, the customer database for customers etc. Fundamental to the selection of a base registry is that it should by nature be the registry that is kept up to date. For example, the payroll system is probably up to date for employees' data as the payment of salaries depends on it.

In an organisational identity management system, new persons cannot be added to registries other than the base registry. However, other registries may be authoritative for some individual attributes. For example, the telephone exchange is a prominent candidate as the authoritative register for a person's phone number, as the telephone exchange is responsible for the assignment of phone numbers in an organisation. In the same manner, the mail server is probably a tempting choice as the authoritative register for mail addresses. The phone numbers and mail addresses can then be propagated from the telephone exchange and the mail server to the other connected registries, such as the payroll system. However, an entirely new person cannot be entered to the identity management system by adding her directly to the telephone exchange or the mail server, unless the organisation has decided to promote either of these as a base registry in the organisation.

Optimally, adding a new person to a base registry triggers a chain of events that causes her personal data being provisioned to all the other relevant registries. For example, adding a new employee to the payroll system causes also the creation of a new record in the building access system and the telephone exchange, the creation of a user account to the Unix or Windows system and so on.

Different registries in an organisation are typically placed in different organisational units, depending on the units' areas of responsibility. On the other hand, the units do not necessarily have the general picture on how the identity management system reflects changes between their registry and other registries in the organisation and how other organisational units use the data. Müller [15] has identified this as one potential problem of identity management systems.

2.3. Implementations of Identity Management in an Organisation

Organisations may use homegrown techniques to implement an organisational identity management system to synchronise the person registries. A common way is to set up an enterprise directory, which is “a core middleware architecture that may provide common authentication, authorization, and attribute services to electronic services offered by an institution” [3]. The processes used for feeding the enterprise directory with data from the base registries and other authoritative registries are called a metadirectory [3]. The technical implementation of the enterprise directory can be, for instance, a relational database or an LDAP directory that is accessed with standard LDAP protocol. To implement the metadirectory, the organisation may use, for example, scripting, such as Perl.

Homegrown scripting has got commercial competitors. Companies have developed specific metadirectory products that have existing connectors and other tools to ease their integration to well known legacy systems, such as payroll systems, Windows and Unix systems, relational databases and LDAP directories. For instance, Microsoft has the Identity Integration Server 2003 product and Novell the Identity Manager product.

There are several case studies available on the implementation of organisational user account management. Blezard et al [4] has presented, how they use available commercial tools to synchronise Unix and Windows accounts to the student registry in the University of New Hampshire. Anchan et al [2] has carried out the task by using an LDAP directory and SUN RPC in the Ringling School of Art and Design. Bellina [3] has collected generic practices for deploying enterprise directories and metadirectories in the US higher education.

Independent of whether the organisation decides to use commercial metadirectories or homegrown scripting, the importance of well-defined identity management processes is equal. Neither commercial nor homegrown metadirectories can be deployed without clear organisational responsibilities and defined workflows for identity information.

2.4. Crossing the Organisational Boundaries

The networking of organisations has caused organisations to set up services (sometimes called extranet services) dedicated to their customers or partners. To decrease the maintenance burden of the extranet user accounts and to increase user convenience, the concept of federated identity management has become a topic of research [5, 6].

In an identity federation, the organisations maintaining the user identity and authenticating them are called Identity Providers. When an end user logs in to a Service Provider in an identity federation, she is authenticated by her Identity Provider, which then federates her identity to the service in question.

From the organisational identity management point of view, becoming a Service Provider in an identity federation means that the organisation can provide services to end users that it does not have in its own base registries. On the other hand, if the organisation joins the identity federation as an Identity Provider, the persons that have an identity in the organisation can also enjoy services provided by other organisations.

Becoming an Identity Provider in an identity federation means that the quality of organisational identity management is not only an internal issue for the organisation any more. Instead, other organisations also become dependent on the freshness of user data in the organisational identity management system. Thus, having a properly implemented organisational identity management system is a requirement for joining an identity federation, and it is suggested that identity federations cover this issue in their policy documents [11].

3. Research Context and Methods

In Finnish higher education, there are 20 universities and 29 polytechnics in the administrative sector of the Ministry of Education. In universities, there are 157 200 degree students and 26 600 employees. The largest one is the University of Helsinki with 36 800 degree students, and there are also five other universities with more than ten thousand students. On the other hand, the smallest universities have just a few hundred students. The polytechnics have altogether 130 900 degree students and 10 900 employees. Regarding the size of polytechnics, the scale is not so wide as in the universities. The largest polytechnics have less than ten thousand degree students, while the smallest one has more than one thousand. [13, 14]

The study was conducted as a part of the “School in User Administration” workshops that will be introduced in detail in Chapter 5. The representatives of the Finnish higher education institutions’ IT service units were provided with a document template and asked to fill in the template with details on the present identity management system in place in their institution. To avoid misunderstandings, the basic concepts of identity management were first explained to the IT service staff.

1. Organisational environment
1.1. Description of the institution
1.2. Description of user categories
1.3. Administration of servers and workstations
1.4. Applications
2. Current identity management practices
2.1. Scope of the description
2.2. The big picture of identity management
2.3. Degree of centralisation of identity management
2.4. Opening of user accounts (students, staff,

other users)
2.5. Closure of user accounts (students, staff, other users)
2.6. Contents of the enterprise directory
2.7. Applications relying on the enterprise directory
3. Implementation details
3.1. Usernames
3.2. Authentication means
3.3. Email addresses
3.4. Other

Table 1. Contents of the study template.

The document template is outlined in Table 1. First, some background information on the institution, its users and the administration of servers and services were asked. The second chapter consisted of the description of the current identity management system, including the services that were in the scope of the document, how the identity management was implemented in general, what kind of processes were defined for opening and closing the user accounts, what attributes about users were stored in the enterprise directory and which applications relied on the enterprise directory in their user administration. Finally, some implementation details were asked, such as namespaces, formats for usernames and email addresses and what kind of authentication means were available in the institution.

Altogether, 30 institutions of the 49 participated in the study. Thus, 61 percent of Finnish higher education was covered by the study. How well the 30 institutions represent the entire population can be argued on; the institutions that have paid little attention to identity management perhaps did not participate the “School in User Administration” either. However, there were also institutions that did not participate the “School” as they considered they already have proper identity management in place.

The survey does not form a snapshot of the situation in any particular point of time. Instead, the survey was conducted in the institutions one by one during the years 2003-2005. It is evident that the first organisations have already made progress in improving their identity management since 2003. However, eventually, the results are expected to provide an overview on the current issues in identity management in Finnish higher education as a whole.

4. Research Results

This chapter presents the results of the study. First, some qualitative results regarding relevant organisational issues are presented. The quantitative results on the connected information systems and the level of integration to the base registries describe how deeply integrated identity management systems are in place in the institutions covered. Finally, some discussion based on the results is presented.

4.1. Qualitative Results of the Study

In Finland, universities and polytechnics differ slightly from each other as organisational entities. All the universities are state universities and, thus, government agencies. The organisational status of polytechnics in turn varies a lot; some are municipal institutions, while others are maintained by a federation of municipalities etc. For identity management, this has the consequence that all the universities have a payroll system of their own, whereas many of the polytechnics do not, as their salaries are paid by the municipality etc. Using the payroll system as a base registry is more difficult, as it is not in control of the institutions themselves.

The organisation of the IT services also differs institution by institution. All the institutions have some kind of centralised unit that takes care of the common IT infrastructure, including network and Internet connectivity, some basic services such as DNS, email etc. In most polytechnics, IT services are part of the institute administration. In universities, the IT service units are either part of the university administration, like in the polytechnics, or independent institutes. For identity management, having IT services as a part of the university administration appears to make linking the enterprise directory to the student and HR registry easier as the related issues are internal for the administration of the university.

Research is an integral part of the universities’ mission. For identity management, this means that the number of short periodic contracts and the turnover of employees are high; students are recruited as research assistants in a laboratory, and faculty members become post-graduate students. In some universities, up to more than half of the employees were reported to be students at the same time. Thus, attention must also be paid to the design of the identity management for users with two base registries. According to the study, most universities have found that in order to avoid confusion, providing one user account instead of two is preferable for users who are both students and employees.

Polytechnics have applied research in their mission as well, but the tradition is still young and the number of researchers small. The turnover rate of employees is considerably lower in the polytechnics than in the universities. The number of users who are both students and employees is low, consisting typically of just some dozens of users.

4.2. Information Systems Connected to the Identity Management System

Institutions were asked to report the information systems whose identity management currently rely on the information in the enterprise directory. Results are depicted in Figure 1.

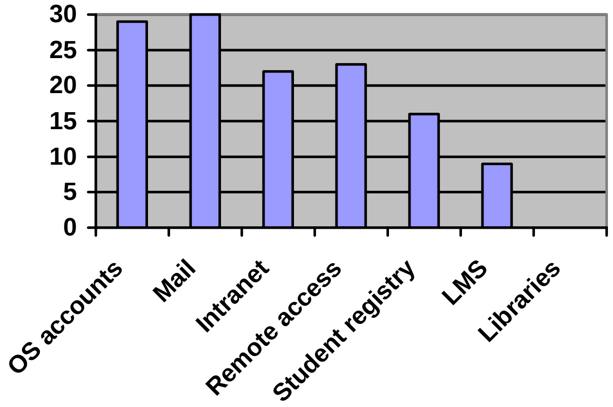

Figure 1. Information systems relying on the enterprise directory.

OS accounts means the operating system (Windows, Unix or Macintosh) accounts provided to the employees and/or students of the institution. 29 of the 30 institutions had the operating system accounts connected to the institutional identity management system. The study also indicated that in the universities, distributed maintenance of Windows and Unix systems is typical. In addition to the systems maintained by the IT services, several institutes take care of their own Windows/Unix environments. This study concerned the systems administered by the institutions' IT service units. The only university in which the OS accounts were not connected to the institutional identity management was the one in which the maintenance of all Unix/Windows systems is taken care of by the institutes.

All the 30 institutions reported that the mail accounts provided by the IT service unit are connected to the institutional identity management. 22 institutions reported that they have institutional Intranet (collection of web pages available only for affiliated users), all of them having it relying on the institutional identity management system. In addition, all the institutions providing remote network access (VPN, dial-up etc) had it connected to the institutional identity management; 23 institutions reported they have one.

The student registry means here a web interface available for students for enrolment to courses, exams and so on. In 16 of the 30 institutions, the students used the username/password in the enterprise directory for authentication in the enrolment services. In the rest, separate usernames/passwords issued by the student administration or some other attributes (for example, surname and the date of birth) were used for authentication.

Learning management systems (LMS) are web-based tools to facilitate learning. There are several commercial, open source and homegrown products in use in Finnish universities [10]. The learning management systems are often maintained by institutes or institutional education technology units. In 9 of the 30 institutions, at least some of the learning management systems rely on the enterprise directory.

The library management system is the information system that, e.g., keeps record on library patrons' loans and reservations. Typically, nearly all students and employees use the institution's library services and have a patron record in the library management system. All the Finnish universities and polytechnics use the Voyager library management system, which has well-documented interfaces for upload and update of patron data. However, at the time of the survey, none of the institutions had linked that to the institutional identity management system. Students and employees were given separate usernames and passwords by the library, and they had to remember to inform the library separately about changes in their personal data, such as the home address.

4.3. Links between Base Registries and the Enterprise Directory

To evaluate the connections between the enterprise directory and the base registries (the student registry and the payroll system), institutions were asked to describe, how they take care of closing user accounts when users leave the organisation. The answers were sorted into three categories: automatic, manual batch processing and manual. Automatic means that no IT service staff intervention is necessary for closing an account. For example, a script is initiated automatically every night to identify and close unnecessary accounts. Manual batch processing means that some automation (e.g., scripting) is in place to assist the IT service staff, but the scripts are triggered manually, possibly also involving other manual operations (such as cutting/pasting text files extracted from the student registry). Manual processing means that the entire process is manual, including locating correct user accounts from the enterprise directory.

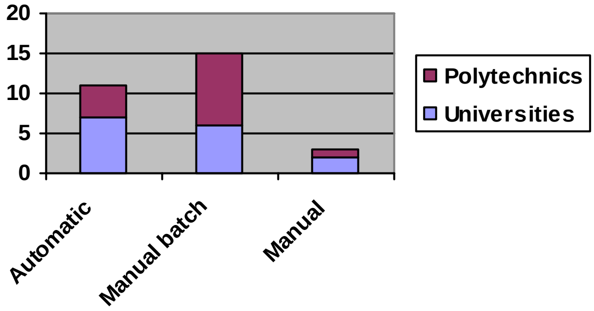

Figure 2. Account closure procedures for students.

The results are depicted in Figure 2. For students' accounts, 11 of the 30 institutions have automatic account closure in place. 15 institutions have manual batch processing, the frequency of which varies from once a week to once a year. 3 institutions use fully manual account closure, based on the notification provided by the student administration. One institution provides only periodic user accounts, which are closed in the end of the period unless renewed by the user.

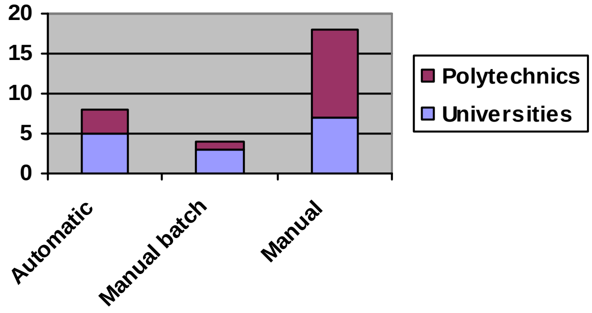

Figure 3. Account closure procedures for employees.

For employees' accounts (Figure 3) the amount of automation was lower. 8 of the 30 institutions had automatic means for account closing, 4 institutions had manual batch processing. 18 of the 30 institutions had no technical tools for closing employees' accounts. Instead, they relied on a notification by the HR department or the supervisor when someone left the organisation or asking the users or their supervisors regularly, if the accounts are still in use. Some organisations with a manual procedure reported that they have problems in getting the notifications. HR departments or supervisors are instructed to inform the IT services, but the organisation is lacking tools for making sure that the instructions are followed.

4.4. Discussion

From the results it can be deduced that information systems maintained by the IT service unit are most likely to be connected to the institutional identity management system. Services provided by the administration of the institution are to follow; student registry by the student administration and intranets provided by the communications administration. Services provided by institutes and libraries are less likely to be integrated to the enterprise directory.

The further away the units are from the IT service unit, the less likely the services utilise the enterprise directory. In the organisation of an institution, institutes and libraries are independent units with longer distance and fewer contacts to the IT services and the university administration. Apparently, the institutes prefer maintaining user identities in their local systems by themselves, although they do not have the facilities, such as the student registry and the payroll system, to support the work.

As Allen [1] has also shown, there may even be a lack of confidence between faculties and the administration in a university. Institutes do not trust the administration to be able to provide them high quality IT services, including services related to user identity. This is a potential barrier preventing institutes from connecting their information systems to the enterprise directory.

Regarding links between the base registries and the enterprise directory, it is evident that the level of integration depends on the number of users and transactions. Automation does not necessarily make sense if the maintenance of an automated system is more time-consuming than doing things manually. From Figures 2 and 3 it can be deduced that fully or partly automated systems are more commonly used in universities, where the number of users and the turnover of employees is larger. A question for future research is where the break-even point lies, where maintenance of an automated metadirectory becomes more efficient than manual updating.

Figure 3 suggests that prompt closing of employees' accounts is not considered a highly important issue. The majority of the institutions rely on manual account closing procedures, which, if not well documented and followed, do not fully guarantee that all users' accounts are closed consistently. From the answers to the study it can be deduced that in universities, a major reason is the lack of the payroll systems' integrity. In institutes, there are employees without written contracts of employment; new employees are hired and periodic contracts renewed, but the written contracts are signed later. In order to use the payroll system as a base registry, organisational processes need to be adapted into the latency. However, it should be beneficial for both the employer and the employee to have the contracts signed in due time, and, thus, the identity management should encourage the heads of the institutes to make sure that the contracts are signed and entered into the payroll system without unnecessary delays.

In polytechnics, the number and turnover rate of employees is low, and, thus, the institutions have considered the automation of account closure processes as a secondary issue. Manual processes are preferred also because several institutions do not have control over their payroll system.

5. Improving Organisational User Administration

Institutional identity management has also been identified as an important issue among information managers in Finnish higher education institutions, and deliberate actions towards improving it has been taken. The issue that was earlier internal to the IT service units and often neglected has now become important, as more institutional and cross-institutional services become reliant on it. The Haka federation, the identity federation of Finnish higher education, has specified the high quality of personal data as a requirement for Identity Providers joining the federation [8].

In order to help institutions in improving their identity management, a set of workshops called "School in User Administration" has been organised. The "School" consists of three workshops for IT service unit staff members, distributed over a time period of one year. The idea is to gather IT staff from several organisations tackling with similar issues, present them some principles and best practices of identity management, and then use the collective pressure of the group to promote progress in the institutions. Practice has shown that the improvement projects are longer-lived in the institutions, if someone outside the institution regularly asks about the progress they are making.

First schoolday 1/2005
Concepts (identity, authentication, authorisation, centralised identity management etc)
Practices (base registries, authoritative registries, roles, unique identifiers etc)
Processes (identity flows, involvement of organisational units etc)
Techniques (metadirectories, LDAP directories, relational databases etc)
CASE homegrown metadirectory (a representative of an institution presents their implementation of an enterprise directory relying on SunOne LDAP and Perl scripting)
CASE commercial metadirectory (a representative of an institution presents their implementation based on Microsoft MIIS product)
CASE RDB (a representative of an institution presents their identity management implementation utilising OpenLDAP as a front-end to a relational database)
First homework given: analysis of the institution's present identity management system
Second schoolday 5/2005
Homework looked through in groups (each institution presents their current identity management system)
Campus Web Single Sign-On (fundamentals, commercial and open source implementations)
Federated identity management (principles and implementations, SAML, Shibboleth)
Identity federation (principles, the Haka federation)
Second homework: setting the goal for institution's identity management system
Third schoolday 11/2005
Homework looked through in parallel groups (each institution presents the goal for their identity management system)
Novell's products for identity management
Eduroam: roaming network access
Other current topics

Table 2. Programme of the School in User Administration.

At the time of writing, two rounds of the "School in User Administration" have been organised. The programme of the second round is outlined in Table 2. During the first and second round, more than 30 institutions have participated the school.

In the "School in User Administration", schooldays are supplemented by homework. As the first homework assignment, each institution is asked to assess the current state of the institutional identity management system. The research results presented in chapter 4 were based on these assessments. The second homework assignment is setting the target for institutional identity management. The target setting is technology-agnostic. The institutions are not asked to fix any particular product they will use; instead, they are asked to make their choices for organisational base registries and authoritative registries for attributes and to decide, which institutional information systems will be connected to the enterprise directory. Furthermore, the organisations are asked to sketch the processes related to the identity flow, starting with what happens in different organisational units, when a new person enters the organisation.

The forerunners in institutional identity management have shown that improving institutional identity management is a several year project. Once the links between the enterprise directory and other registries are built, the work is focused on connecting new information systems to the enterprise directory and deepening the integration of the systems. For example, in one Finnish university, there is a project going on to pass the students' course enrolments from the student registry to a learning management system for authorisation. The work utilises Shibboleth software and CourseID specification for course related roles, both activities of Internet2 [9].

6. Conclusions

As information systems handling personal data have proliferated, the importance of identity management in an organisation has grown. Organisations have set up metadirectories, which take care of synchronising personal data between the enterprise directory and other registries, in order to make the data follow the individuals' role changes in the organisation.

This paper presented the results of a survey on the status of organisational identity management in Finnish higher education. It turned out that services provided by the IT service unit and the institution's administration are most likely connected to the metadirectory. Identities in services provided by institutes and the library are usually managed independently, causing overlapping work and, possibly, the lack of data integrity in the institution as a whole. In the IT service units, economics of scale and links to the institutional base registries make it easier to make sure that the identity information in the enterprise directory is up-to-date.

In an organisation, identity management was not found to be solely a technical issue. The flow of identity information crosses organisation unit boundaries, and different organisational units maintain the information systems, which potentially feed and utilise the enterprise directory. The design of processes and identity flows in the organisation has to be considered as part of the organisational identity management design. A series of workshops called “School in User Administration” was introduced as a way to help organisations to improve their institutional identity management.

References

1 D. Allen. “Information infrastructures, information behaviour and trust”, Proceedings of EUNIS2002, the 8th International Conference of European University Information systems, pp.167–178, (2002).

2 D. Anchan, M. Pegah. “Regaining Single Sign-On Taming the Beast”, Proceedings of the 31st annual ACM SIGUCCS conference on User services, pp.166–171, (2003).

3 B. Bellina (ed). “Metadirectory Practices for Enterprise Directories in Higher Education”, NFS Middleware initiative, (2002). http://middleware.internet2.edu/dir/metadirectories/internet2-mace-dir-metadirectories-practices-200210.htm Referenced 18.4.2006.

4 D. Blezard, J. Marceau. “One User, one password: integrating unix accounts and Active Directory”, Proceedings of the 30th annual ACM SIGUCCS conference on User services, pp.5–8, (2002).

5 S. Clauss, M. Köhntopp. “Identity management and its support for multilateral security”, *Computer Networks*, vol 37, pp. 205–219, (2001).

6 E. Damiani, S. De Capitani di Vimercati, P. Samarati. “Managing multiple and dependable identities”, *IEEE Internet Computing*, vol 7, issue 6, pp.29–37, (2003).

7 D. Gollman. “Computer Security”, John Wiley & Sons, Inc, New York, (1999).

8 Haka Federation. “Service Agreement for Federation Members.” http://www.csc.fi/suomi/funet/middleware/english/ Referenced 18.4.2006.

9 Internet2. “Internet2 middleware initiative”. http://middleware.internet2.edu/ Referenced 18.4.2006.

10 K. Koivu. “Learning management systems in Finnish Universities” (In Finnish), IT-Peda, (2004). http://www.uta.fi/itpeda/Raportit/koko_kartoitus101103.pdf Referenced 18.4.2006.

11 M. Linden. “Organising Federated Identity in Finnish Higher Education”, TERENA Networking Conference 2005, Poznan, Poland, (2005).

12 L. Maltz, P. B. DeBlois. The EDUCAUSE Current Issues Committee “Top-Ten IT Issues, 2005”, *EDUCAUSE Review*, vol 40, no 3, pp.14–29, (2005).

13 L. Patosalmi, K. Salenius (eds). ”Finnish Universities 2000”, Ministry of Education, (2001). http://www.minedu.fi/julkaisut/pdf/Yliopistot_english.pdf Referenced 18.4.2006.

14 Ministry of Education. “AMKOTA database” (In Finnish). Ministry of Education, (2005). http://www.csc.fi/amkota/taulukot2004.html Referenced 18.4.2006.

15 M. Müller. “Identity Economics and Policy for Distributed Systems”, 1st IEEE International Workshop on Grid Economics and Business Models, GECON 2004, pp. 83–90, (2004).

16 I. Stinson, “EUNIS Top Concerns Survey 2004/2005”, (2005). http://www.eunis.org/html3/publications/top_concern_2005/eunis_tc_2005.pdf Referenced 18.4.2006.

Publication 2

Mikael Linden, Pekka Linna, Mika Kivilompolo, Janne Kanner. Lessons Learned in PKI Implementation in Higher Education. Proceedings of the 8th International Conference of European University Information Systems EUNIS, 2002. 246–251

Lessons Learned in PKI Implementation in Higher Education

Mikael Linden, Pekka Linna, Mika Kivilompolo, Janne Kanner

Center for high-performance computing and networking CSC, Finland
mikael.linden@csc.fi
pekka.linna@csc.fi
mika.kivilompolo@csc.fi
janne.kanner@csc.fi

Abstract

A joint project for Finnish universities and polytechnics has studied the applicability of the public key infrastructure (PKI) and smart cards in higher education institutes. The nine pilots in the project have provided practical experience on the implementation of PKI and services relying on it. The project has identified motives for PKI deployment. Interdependencies of PKI and other topics such as user administration and inter-institutional use of resources have been addressed. The project has summarised its experiences to seven conclusions.

Keywords: PKI, smart cards, security

1. Introduction

Cryptography has been used for hundreds of years when passing secret messages between parties through an unreliable channel. Traditional cryptographic algorithms use the same cryptographic key for encrypting and decrypting messages; the method is called symmetric cryptography. A new era of cryptography started in 1976, when Diffie and Hellman [2] discovered asymmetric cryptography (aka public key cryptography), in which a network user has two distinct keys, a public key and a private key. In order to make it available for everyone the user publishes his public key. The private key, on the other hand, shall be carefully protected from disclosure. The usage of the key pair depends on the asymmetric algorithm used. In the popular RSA algorithm [15] the public key is used for encrypting messages, and the messages encrypted with it can be decrypted only with the private key and vice versa.

Public key cryptography as such is not enough. A method for ensuring the true owner of the private key is needed. The objective of Public key infrastructure (PKI) is to establish a binding between a public key and the identity of the person or object possessing the corresponding private key. This is being done with a certificate, which is a digitally signed statement made by a trusted third party about the ownership of the private key. The certificate binds a public key to the identity of the holder of the related private key.

When not in active use, the private key is usually protected by a password and stored on the hard disk of the workstation, providing only limited security. A prominent enabler for PKI is a smart card, which functions as a tamper-resistant storage for the private key of the cardholder. Smart card is a credit card sized computer having enough computing power for running the decryption algorithm that utilises the private key. Because the private key is stored and even used in the on-board microprocessor, it can never be revealed to attackers such as Trojan horses potentially occupying the workstation. Smart card is typically protected with a personal identification number (PIN) to prevent possible misuse.

Public key infrastructure makes it possible to authenticate a network user without a password or any other secret information shared by the user and the authenticating system. Commonly used network security protocols such as Transport Layer Security (TLS) [1], Secure Shell (SSH) [19] and IP Security Architecture (IPSec) [6] already support PKI in authenticating the user. In addition to encrypting messages, PKI provides also non-repudiation services implemented by a digital signature. For instance the S/MIME protocol [14] implements digital signatures and encryption for confidentiality, authenticity and integrity in electronic mail.

2. The national PKI in Finland and the FEIDHE project

In Finland the public sector has been a driving force for PKI implementation. In 1996 the government stated, that electronic identification of a citizen belongs to the infrastructure of the information society [10]. A national PKI was implemented and Population Register Centre was nominated as the certificate authority (CA), that is the trusted party issuing certificates for citizens. The private key was stored in a smart card; a chip was embedded to the identity card issued to citizens by the Police. The first FINEID (Finnish Electronic Identity, [13]) cards were issued in December 1999.

Launch of FINEID was noticed in universities as well, and people responsible for network security started considering the use of FINEID card to improve the reliability of authentication in the university network. Instead of having separate projects in each organisation, a joint project for universities and polytechnics was established. National student unions were involved, because the student cards issued to students by the unions were considered as a potential place for the chip. The goal of FEIDHE (Finnish Electronic Identification in Higher Education) was to investigate the applicability of the public key infrastructure and smart cards in higher education institutes. The project was chartered in June 2000, and it ended in March 2002.

3. Piloting PKI

Running pilots in the participating institutes was considered as an essential method for reaching the goals already in the beginning of the project. Member institutes of the project were encouraged to apply for pilots, which were independent projects driven by individual organisations. The role of the FEIDHE project was to co-ordinate the pilots i.e. to ensure that the pilots together had comprehensive coverage of the PKI application areas and to provide an inter-institutional communication channel for experiences and ideas the pilots had. The FEIDHE project also organised basic PKI training, made an inventory on the products available on the market, and arranged financial aid for the piloting institutes from the ministry of education and the ministry of transportation and communication.

The project set four goals for piloting. A natural goal was to find out how PKI and the applications relying on it should be technically implemented in practice. The pilots were asked to document their implementations in order to make it possible for the others to follow them. The pilots also gathered data about the expenses of the implementation work, including the components that are available on the market or for free and the amount of work that needs to be done in order to get a working implementation.

In the university networks a key player that can be easily forgotten is the user. Replacing passwords by a smart card and introducing new services on it means a significant change to the way people have been using networks for years. A separate study on the usability of a PKI relying on smart cards was done to find out the bottlenecks from the user perspective. Among other things usability inspection and testing in a laboratory and contextual inquiry in the real environment were carried out.

These three goals served the ultimate goal, which was the comparison of the benefits of the system and the costs of its implementation and maintenance. A large-scale implementation of PKI in a higher education institute is clearly a significant investment, and a comprehensive understanding of whether or not it is worth of it is desirable beforehand.

During the FEIDHE project nine pilots took place, all of them having something in common and something different from the others. Most pilots used the FINEID issued by Population Register Centre, but being independent of the certificate authority, however, was considered important. PKI was utilised mostly for authentication in common network security protocols such as Transport Layer Security (TLS), Secure Shell (SSH) and IPSec/IKE, but in one pilot digital signature was integrated into one of the processes in the financial administration of the university. The pilots had students, teachers and other staff members as the pilot group. In most pilots the number of pilot users was between 10 and 50, the biggest one had about 650 users.

Four pilots took place in universities and four in polytechnics. One pilot was organised by CSC, the company maintaining the Finnish research and higher education network. The external funding for the pilots was about 225 000 Euro, the rest was covered by the ordinary IT-budgets of the institutes. Eight man-years were used in the pilots and 16 in the project in total.

4. Conclusions in FEIDHE

The FEIDHE project has summarised its experiences on PKI, smart cards and related issues in a few conclusions [4]. The conclusions and related proposals of action are provided to the management of higher education institutes and the ministry of education in order to support their decision-making.

Conclusion 1: *The basis of PKI has proved to be working, and in the future authentication of users can be based on it. However, implementations relying on smart cards still have some shortcomings.*

The cryptographic principles of PKI have been a subject for intensive research, and severe flaws have not been reported. PKI and certificates have been adopted in common network security protocol standards, and standards on the client side architecture make it possible for the implementations to interoperate. Products utilising PKI and smart cards are entering the market.

Yet the implementations available have shortcomings. Support for smart cards in Unix and Linux workstations is inadequate and only a few smart card readers have drivers available [7]. However, open source projects are working to improve the situation [11, 20]. For workstations running Microsoft Windows there are commercial products to choose from. Unfortunately the products are not yet mature from the usability point of view, and the end users are hampered by complicated installation procedures or error messages, which are difficult to understand and may require understanding of PKI [17].

The de facto standard for the architecture of a workstation with a smart card reader is PC/SC, which specifies the three software components needed [12]. The smart card resource manager implements the support for smart cards in general, and the reader handler is a driver needed for each smart card reader model used. The service provider is a middleware component enabling an application, such as a web browser, to interface a smart card with certificates. In a FEIDHE pilot ten teachers were asked to install a smart card reader and the three software components at the computers at their home. Despite of the written installation instructions tailored for them only three teachers succeeded at the first attempt [8]. Thus, the readers should be installed not by the end users but by the IT support until the products are mature enough from the usability perspective. That is difficult if the cards are used at home e.g. for distant working.

Windows 2000 and its successors have built-in smart card support for certain smart card vendors and PKI can even be utilised for smart card logon [9]. However, FEIDHE project has experienced the Microsoft's implementation of the smart card logon cumbersome, because it has requirements on the certificate contents. For example the certificates in a FINEID card don't fulfil the requirements. Yet the FINEID and other compliant cards can be used for workstation logon, but an additional certificate needs to be installed in the card, causing extra work for the user and the network administration.

Conclusion 2*: There are problems with the security of public workstations. Related safety precautions and liability issues need to be solved before a large-scale deployment of PKI and smart cards in classrooms.*

Smart cards and PKI provide increased security for authentication, making it possible to implement more sensitive services to the users in the network. On the other hand, sensitive services provided are potential targets for attackers if the security of the system is compromised.

A smart card is a tamper-resistant container for the private encryption keys, and in an appropriate implementation of a smart card the private keys can be considered to be safe. The workstation utilising the smart card, however, is seldom controlled completely by the user, and it is very difficult for the end user to track all the software running.

An intruder, such as a worm or a Trojan horse could misuse the smart card and cause significant harm and damage to the user. For example smart cards are commonly blocked after entering three false PIN codes consecutively. A simple intruder could enter a random PIN code to the card three times, causing the card to be blocked. A complicated and much more dangerous intruder would alter the data sent to the card for encryption with the private key. As a result the intruder would have a document that the user has signed unintentionally.

The security of a workstation can be improved by using a smart card reader with a PIN-pad so that the PIN code entered by the user bypasses the insecure workstation. However, an intruder is still able to tamper the data that is intended to be signed by the smart card. A smart card reader equipped by both a PIN-pad and a display would be necessary, causing the complexity and the cost of the reader to increase. In order to sign data with complex encoding, such as entire Microsoft Word documents, a sophisticated terminal would be needed, which may have security flaws in turn.

In higher education institutes there are a lot of workstations that are not controlled continuously by the administrators. Virus shield software may provide adequate protection against common viruses, but a malicious user can e.g. use a security flaw of an operating system to install an intruder in a workstation in a classroom. Actions to protect the workstatios from malicious software and hardware need to be studied. The liability issues have to be addressed for the case that the protection fails and an intruder causes losses for the users or some other party. The institute may have responsibilities as the administrator of the workstation. The users have to be informed about the risks they have as well.

Conclusion 3: *The deployment of smart cards and PKI should be done step by step. At first the user administration of the institute needs to be centralised, so that the user has a single identity in all the services on the network. Distributing smart cards to the users is the final step.*

The usability study made in FEIDHE proved that users expect to have a large number of services available for the card. Users don't benefit from a smart card if it is used for replacing a password in some services, but passwords are still needed in other services. The card is used if it facilitates the user in the daily life. Using a smart card makes sense, if all the usernames and passwords can be replaced by smart card authentication. [17]

Replacing all passwords is challenging, because in Finnish higher education institutes a user usually has several distinct usernames and passwords in separate services. For example, a user may have username *linden* in the internal web pages of the university, username *mlinden* in the Unix environment of the department and username *mikael* in the Windows domain of the laboratory. Nothing binds the three usernames together. From the system point of view, *linden*, *mlinden* and *mikael* are three distinct users in three independent systems.

To implement smart card authentication, a means for mapping a certificate to a username needs to be established. The easiest way is to include the username in the content of the certificate; this is the way Windows 2000 smart card logon is implemented. In an alternative implementation the mapping of certificates and usernames is done in the back-end system. For example certificates and usernames can be considered as attributes of a person in an LDAP (Light-weight Directory Access Protocol, [18]) directory of the institute. The latter is a more flexible implementation because it enables the use of certificates whose contents the institute cannot affect on. One example of such a certificate is the FINEID card.

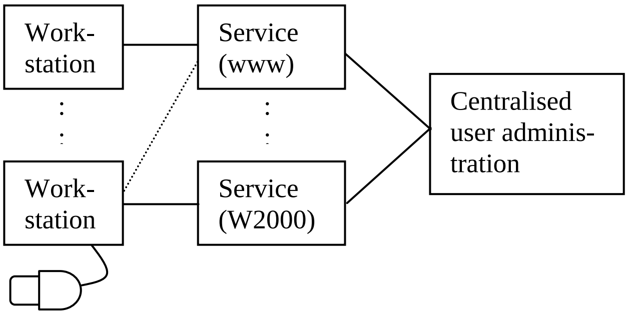

Figure 1. Centralised user administration.

In principle the mapping between users and certificates could be done independently in each of the services provided. However, maintaining the mapping of certificates and users is time-consuming and may need some manual work in the IT helpdesk of the institute. In order to minimise overlapping work, it makes sense to do the mapping in one centralised place. The role of the centralised user administration system is to keep track of all the network users and the authentication mechanisms such as passwords and certificates associated to them (Figure 1). When the users need to be authenticated, the services can rely on the user administration, making implementation of smart card authentication easier in existing and new services. For example, the services can utilise the LDAP directory of the institute in order to find out, to which user the presented certificate belongs.

Centralised user administration was found an important enabler of services relying on PKI, but it has other advantages as well. Centralised user administration reduces overlapping work in the network services available in the institute. The users are more satisfied if they are able to use a single username and password in all the services. Furthermore, it makes sense to synchronise the user administration to other databases, such as to the student register of the institute. Synchronisation of databases makes it possible to automatically add or delete the user accounts when a user enters or leaves the organisation, which increases the security in turn. However, centralisation of user administration is not only a technical problem but also an organisational problem. In the academic world organisational units, such as departments and laboratories, tend to be willing to preserve certain independence in information systems as well.

An obvious pitfall to avoid is the too smart card centric view to PKI, even though people not so familiar with the technology may consider PKI as “the smart card thing”. The focus of PKI implementation in higher education is not in smart cards, but in integrating the certificates in the user administration of the higher education institute. *Attention should be paid on implementing the structural and procedural things of user administration so that certificates can be used instead of passwords in authentication.* Smart cards, certificates, client software in a workstation etc are components that are commercially available, and they are not the primary matters to concentrate on. Consultation and even products, such as metadirectories, are available for user administration as well, but the processes have to be tackled by the organisation anyway. Having implemented the related modifications to the user administration the smart cards readers can be installed in the workstations and smart cards distributed to the users.

Conclusion 4: *Deploying PKI in a higher education institute requires practical experience and training for the network administration and IT support. Thus it is favourable to provide services on PKI for a small user community at first.*

Most of the staff members in the network administration of the higher education institutes are not yet familiar with smart cards and PKI. A considerable amount of education is required before the staff members are experienced enough for implementing and maintaining the related modifications and for providing support to the end users. The lack of experience may be even a bigger problem in an institute than the lack of funding for PKI deployment.

A convenient way to get some early experiences is to deploy smart card based services for a small number of users at first. For example the network administration may decide, that strong authentication is at first introduced to people using the student administration system, because student records contain sensitive data.

An alternative way for getting experiences is to provide smart card readers and related software to the staff members who are potential users for off-campus services. For instance the applications for Academy of Finland, the national organisation for research funding, can be signed in the web using the FINEID card. Providing smart cards and related accessories to staff members whose research work is funded by Academy of Finland does not require modifications in the institute’s own services, but makes it still possible to get some experience on the subject.

Conclusion 5: *Each higher education institute should consider the choices they have in PKI implementation and their benefits and costs. A common smart card for all the institutes is not necessary.*

In the beginning FEIDHE considered specifying a special smart card to be used in higher education. For students the chip would be integrated in the student card and for staff members in the badge they have. In practice specifying a card that fulfils the needs of all the 49 higher education institutes in Finland was found challenging because of the differing requirements. Some institutes wanted to use the card also for purchases and accessing buildings, some institutes already had a campus card with an electronic purse. When the focus of the project moved from the card to the user administration of the institute, specifying a card became unessential.

The institutes deploying PKI have several alternative ways to choose between. The institutes can either use an existing smart card or specify a smart card of their own. Besides FINEID card there are a few smart cards with certificates to be launched for public in Finland. Few banks are going to issue a debit card with certificates. Some cities have plans for a smart card for the city dwellers. If the smart cards are technically compatible and the certificates are considered trustworthy enough, there should be no reason for not accepting those certificates in the services provided by the institute as well.

A significant cost of PKI deployment is formed by the smart cards and certificates issued. A partnership with some external party may benefit both sides. For example the costs of the smart cards for students could be shared with a bank issuing the certificates. The bank could in turn be eager to make all the new students to drop in the bank office to get a smart card. Partnership seems more applicable for the cards used by students. The cards for staff members need to be paid by the institute anyway like other tools needed for daily work.

In FEIDHE a separate study among students was made on the card and its properties [5]. In the study students were asked, what kinds of smart cards and services on it they would like to use. Using the card for getting student discount was considered as the most interesting property. That is for what the current student card is used. Ability to use the card in libraries and public transportation was also important, and small payments and building access in the campus were listed as well. A common denominator for the results was that the services related to daily life as a student were considered natural. The study encourages the institutes to establish partnerships with the public sector.

If the institute decides to issue cards of its own, the PKI can be either outsourced or operated by the institute itself. Even in Finland there are several commercial certificate authorities issuing certificates for smart cards. The acceptance of the certificate in off-campus services depends on the quality of the certificate. It is desirable that at least the other higher education institutes trust on the certificates issued.

Conclusion 6: *In order to benefit from the reduced costs and increased quality of services provided by PKI, a higher education institute needs to carefully develop its services and processes.*

Replacing passwords by strong authentication based on certificates is relatively straightforward if the user administration of the institute is properly implemented. Using strong authentication makes it possible to introduce more sensitive services to the network. An even more interesting enabler for new services is the digital signature that can be implemented by a smart card with certificates.

The non-repudiation implemented by a digital signature can be used to replace handwritten signatures in travel expense reports, book-keeping and varying other applications, making it possible to replace the last step that still has to be done on paper by a digital substitute. Forms on the paper can be replaced by forms on the web, and the signature can be made by entering the PIN code to the smart card. The amount of routine work decreases as printed documents need not to be handled any more and digital documents can be handled and tracked faster and more easily. According to the Directive of the European Parliament on a Community framework for electronic signatures [3], an advanced electronic signature made by a qualified certificate shall be considered equal to a hand-written signature, if it is created by a secure-signature-creation device.

Implementing a digital signature as a means to improve university administration is a challenging task. A too technology-oriented view to the problem should again be avoided. Implementing a digital signature is mostly reforming the processes in the university administration; what kind of steps an affair has to go through to be completed. Usually smoothening these processes would cause significant cost-reductions even without a digital signature and PKI.

Conclusion 7: *Using inter-institutional network resources requires national decisions on practices and technology used and national co-ordination of development in the user administration of the institutes.*

Higher education institutes have developed their information systems independently. The way the systems are implemented has been an internal issue for each institute, and different solutions have been used. Each institute has had its own user administration systems.

Inter-institutional use of network resources is in increase. Users of network resources do not necessarily represent the same organisation as the provider of the resource. For example students from different universities may attend a virtual course provided by one university, and the course may utilise a web-based learning environment with user authentication. Traditionally the username and password are generated separately for each student, causing administrative work for the institute and one more username and password for the student to remember. The need for a more convenient arrangement increases, as the use of network resources across organisation boundaries becomes more popular.

From the user point of view an optimal solution would be the ability to use the same credentials such as usernames, passwords and certificates in all the institutes providing courses to the student. This can be achieved by inter-institutional user administration, in which the user data and credentials are stored and maintained in the user's home institute and used by all the institutes in which the student is taking courses.

A prominent technology for implementing inter-institutional user administration is LDAP. Each institute would set up an LDAP directory containing all the network users in the institute, and the other organisations use the directory in authenticating the users and in retrieving other relevant information. Implementing inter-institutional user administration, however, requires common decisions on the practices used, including specification related to the LDAP schema and the responsibilities of different parties.

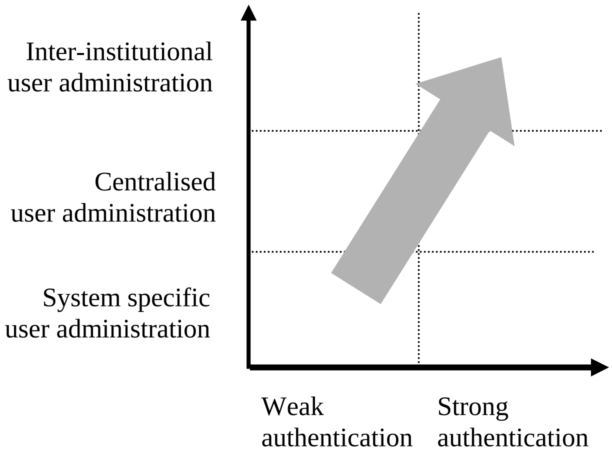
Inter-institutional user administration
Centralised user administration
System specific user administration
Weak authentication
Strong authentication

Figure 2. The relation between authentication and user administration [16].

A vulnerability of inter-institutional user administration is authentication. The risk of password authentication grows as the number of services increases; there are more places in which the password can be compromised, and once compromised, the password can be misused in several services. A more secure authentication mechanism, such as a certificate or an authentication ticket, is needed. The relation between authentication and user administration is sketched in Figure 2. Most of the institutes are in the lower left corner today. The arrow demonstrates the ultimate goal of strong authentication in inter-institutional user administration.

5. Summary

A joint project for Finnish universities and polytechnics has studied the applicability of PKI and smart cards in higher education institutes, and found the emerging technology promising in user authentication, non-repudiation and encryption services. An institute benefits from PKI in increased security, and digital signatures can be used to smoothen the administration of the institute as well.

Instead of smart cards, the focus of PKI deployment should be in the user administration of the institute, making it possible to modify existing services and implement new ones to be used with PKI and smart cards. As the inter-organisational use of network resources becomes popular, PKI can be used as a technology to meet the challenges for network security.

Acknowledgements

We want to express our gratitude for co-operation and support to our colleagues in FEIDHE project and its pilots.

References

[1] T. Dierks, C. Allen. “The TLS Protocol“, *Internet Engineering Task Force*, RFC 2246, (1999).

[2] W. Diffie, M. Hellman. “New Directions in Cryptography”, *IEEE Transactions on Information Theory*, **volume IT-22**, pp. 644-654, (1976).

[3] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[4] Henkilön sähköinen tunnistaminen yliopistoissa ja ammattikorkeakouluissa. “Julkisen avaimen järjestelmän käyttöönotto korkeakouluissa. HSTYA-projektin muistio korkeakoulujen ylimmälle johdolle ja opetusministeriön virkamiehille” (in Finnish), *HSTYA-loppuraportti*, (2002).

[5] T. Jurvanen. ”Sirukorttikonseptin tutkimus” (in Finnish), *Consumer Compass – Kuluttajatieto Oy*, available also https://hstya.funet.fi/loppuraportti/kayttaja/cc_raportti2.pdf.

[6] S. Kent, R. Atkinson. ”Security Architecture for the Internet Protocol”, *Internet Engineering Task Force*, RFC 2401, (1998).

[7] S. Koskinen. ”HSTYA-pilotin loppuraportti” (in Finnish), *Helsinki University of Technology*, http://www.hut.fi/atk/hstya/hstya-loppuraportti.html (referenced 6th May, 2002).

[8] Lahti polytechnic. ”Lahden ammattikorkeakoulun HSTYA-pilottiprojekti. Loppuraportti” (in Finnish), http://www.lpt.fi/lamk/ajankohtaista/hstya/lahden_ammattikorkeakoulun_hstya.htm (referenced 6th May, 2002).

[9] Microsoft Corporation. “Smart Card logon white paper”, http://www.microsoft.com/windows2000/techinfo/howitworks/security/sclogonwp.asp (referenced 6th May, 2002).

[10] Ministry of Finance, Ministry of the Interior, Ministry of Transportation and Communication. “Henkilön sähköinen identiteetti ja henkilökortti” (in Finnish), (1996).

[11] The MUSCLE project. “MUSCLE – Linux Smart Card Development”, http://www.linuxnet.com/ (referenced 6th May, 2002).

[12] PC/SC Workgroup. “PC/SC Specifications 1.0”, http://www.pcscworkgroup.com/ (referenced 6th May, 2002).

[13] Population Register Center. ”The electronic ID card”, http://www.fineid.fi/ (referenced 6th May, 2002).

[14] B. Ramsdell. “S/MIME Version 3 Message Specification”, *Internet Engineering Task Force*, RFC 2633, (1999).

[15] R. Rivest, A. Shamir, L. Adleman. “A Method for Obtaining Digital Signatures and Public-key cryptosystems”, *Communications of the ACM*, **volume 21**, pp. 120-126, (1978).

[16] Uninett. “Greater NOrdic MIddleware Symposium (GNOMIS)”, http://www.uninett.no/info/seminar/gnomis/ (referenced 6th May, 2002).

[17] Usability Laboratory at the University of Tampere. “Käytettävyyden arviointi HSTYA-projektissa” (in Finnish), available also https://hstya.funet.fi/loppuraportti/kayttaja/tauchi_raportti.pdf.

[18] M. Wahl, T. Howes, S. Kille. “Lightweight Directory Access Protocol (v3)”, *Internet Engineering Task Force*, RFC 2251, (1997).

[19] T. Ylönen, T. Kivinen, M. Saarinen, T. Rinne, S. Lehtinen. ”SSH Protocol Architecture”, *Internet Engineering Task Force*, work in progress, (2002).

[20] J. Yrjölä, T. Teräs, A. Tapaninen, O. Kirch. ”OpenSC”, http://www.opensc.org/ (referenced 6th May, 2002).

Publication 3

Mikael Linden, Inka Vilpola. An Empirical Study on the Usability of Logout in a Single Sign-On System. Proceedings of the 1st International Conference in Information Security Practice and Experience. Lecture Notes in Computer Science 3439. Springer-Verlag, 2005. 243–254

Publication 4

Mikael Linden. Towards Cross-organisational User Administration. Informatica, Volume 27, Issue 3, 2003. 353–359

Towards Cross-organisational User Administration

Mikael Linden
CSC, the Finnish IT Center for Science
mikael.linden@csc.fi

Keywords: User administration, authentication, authorisation, cross-organisational services

Received: June 6, 2003

The increase of personal services on the web and the co-operation between organisations have made it necessary to find ways to identify network users regardless of which organisation they are representing. New middleware technologies for user authentication and authorisation are being developed and deployed. This paper outlines the problem of cross-organisational user administration and presents related new technologies and activities in the academic world. Although the paper uses higher education as an example, the results can be generalised to cover cross-organisational services in other kinds of institutions as well.

1 Introduction

User administration is considered to mean keeping track of the information system users and their privileges. User administration covers both technology in use and administrative processes deployed in the organisation.

The concepts of identification, authentication and authorisation are relevant for user administration. Their interrelation is clarified in Figure 1.

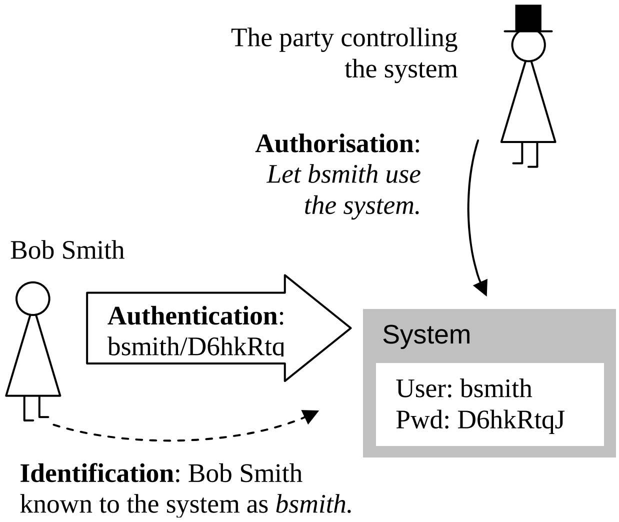
The party controlling the system
Authorisation: *Let bsmith use the system.*
Bob Smith
Authentication: bsmith/D6hkRtq
System
User: bsmith
Pwd: D6hkRtqJ
Identification: Bob Smith known to the system as *bsmith.*

Figure 1. Concepts of identification, authentication and authorisation.

In a distributed environment, the identity of an object is represented by an identifier. In daily life various kinds of identifiers are used in distinguishing between people. Names are the most common identifiers, but they are not very useful as two persons may have the same name. In information systems, the traditional unique user identifier is the username (*bsmith*). Social security numbers are also widely used, although they are not assigned by the organisation in question but by the government. In universities other common identifiers for people are student numbers and employee numbers. A more detailed description of identifiers in universities has been done in Internet2 [8].

Identification and authentication of users are two interrelated concepts. When a service authenticates a user, it obtains assurance about her identity. A common way to authenticate a human user is to ask her to enter a password. The use of passwords is considered as weak authentication, as passwords can be guessed, sniffed, shoulder-surfed or just found on a piece of paper under the keyboard. There are also stronger ways to authenticate a user, such as one-time-passwords and public key infrastructure (PKI).

Authorisation means deciding, who is allowed to access a system (such as a web service) and which operations she is allowed to do in it. Authorisation is done by the party controlling the system. It can be done on individual level by maintaining a list of the identifiers for the authorised users. However, in most cases authorisation is based on the role of the user. An example of role-based access control (RBAC) is that only students are allowed to enroll in an exam of a university course, and only staff is allowed to check, who have enrolled in an exam.

Traditional view of networking has been a set of services, which have been interconnected by the network. Middleware is a layer of abstraction between the applications and the network infrastructure. It covers technologies like remote procedure call (RPC), quality of service, distributed computing (such as Grid) and so on.

One aspect of middleware is administering users and their privileges on services in the network (Figure 2). On one hand it covers identification and authentication of the network users, on the other hand also the mediation of their roles and other attributes that are necessary for deducing what the users are authorised to do in the network.

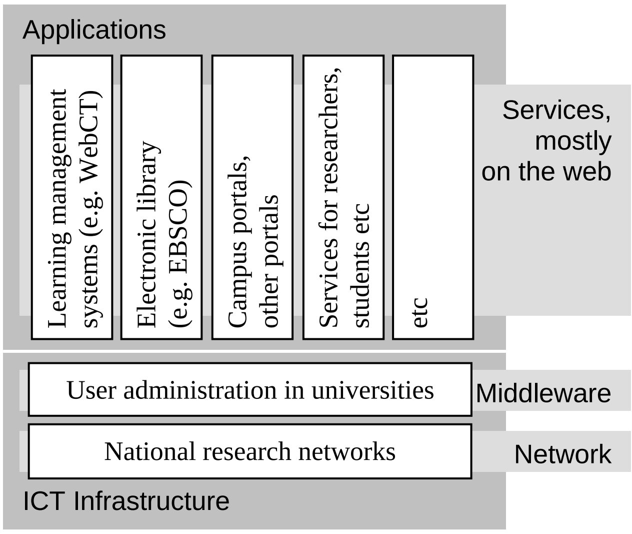
Applications
Learning management systems (e.g. WebCT)
Electronic library (e.g. EBSCO)
Campus portals, other portals
Services for researchers, students etc
etc
Services, mostly on the web
User administration in universities
Middleware
National research networks
Network
ICT Infrastructure

Figure 2. User administration is a middleware component between the applications and the network.

Formerly the network services were provided mostly by the university in which the user was studying or working. As the co-operation of universities increases, the user may not necessarily belong to the same organisation that provides the accessed service. The user, for example, can be a researcher that is accessing a national research portal or a student studying a distant course provided by another university. Most of these services need to be aware of the identity and/or the role of the user in her home organisation.

2 Scope of the User Identity

In an organisation the scope of the user identity can be threefold. The identity can be scoped for only one specific service, or the user may have the same indentity in all the services in the organisation. It is even possible to use the same identity in services outside the organisation. The scope of the identity and its relation to user authentication is sketched in Figure 3.

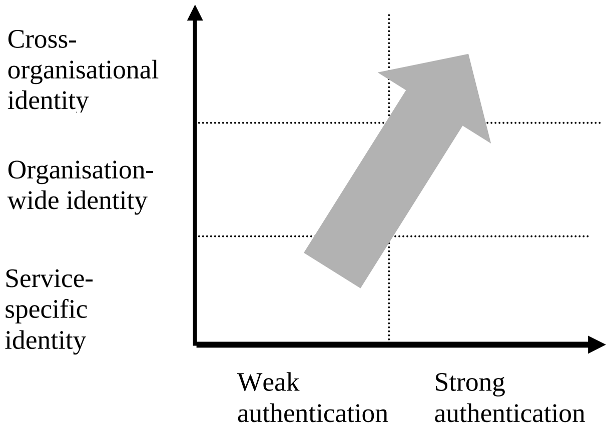
Cross-organisational identity
Organisation-wide identity
Service-specific identity
Weak authentication
Strong authentication

Figure 3. Scope of the user identity and the required reliability of user authentication. [6]

2.1 From Service-Specific Identities to Organisation-wide Identities

In a university an average user is usually authorised to use several information systems, for example workstations and servers in Unix and Windows environments, web based services such as university portals, learning management systems (LMS), dial-up services etc. If the user has different identities in each service, she probably has to remember several username/password pairs in her daily life (lower left corner of Figure 3). In one service Bob Smith is known as *bsmith* and in another as *bobsm*, and the passwords in the services are different unless Bob has synchronised them by himself. If the user administration of the information systems relies on service-specific identities, introducing a new personal service on the network means giving a new username/password pair to the users.

As services in the network proliferate, administration of user identities causes a significant amount of work both for the organisation and the user herself. Replacing the service specific identities by one organisation-wide user identity for each user in the organisation (the middle row of the figure) reduces overlapping work and is also comfortable from the usability perspective. The user has one single username/password that is used in all the services that she is authorised to use in the university.

In other words, organisation-wide identity separates the administration of identity from the administration of authorisation; granting access to a new service does not anymore mean issuing a new service-specific identity to the user. Instead it means authorising an existing user with a known username to use the new service.

The use of an organisation-wide identity is also motivated by information security. When a user leaves the organisation, for example when a student graduates, her user accounts in all the services in the university should be inactivated. In contrast to opening an account, the user is not usually motivated to actively take care that her user accounts are closed as she leaves. Closing all the service specific user accounts is a considerable task unless the user has one organisation-wide identity.

Once organisation-wide identities are introduced, it makes sense to use some time in integrating the user administration to other databases in the organisation, such as to the student registry and the payroll system. If the number of users entering and leaving the organisation is large, manual work and latency can be reduced if the accounts are automatically closed right after the person has left the organisation.

Integration of user account databases and other databases introduces the concept of a metadirectory, which is a directory bringing together the strategic directories that the organisation has. A property of a metadirectory is that once a piece of information is changed in some database, the related changes are mediated to all the other relevant databases in the organisation. For example, as a student graduates, the event is propagated from the student registry to the user administration to close her user accounts, to the library to close her patron files there, to the alumni database to introduce a new alumnus and so on.

There are different technologies available for user administration in a university. Relational databases, which have been connected to student and employee databases, are used widely. When a new student is added to the student registry, a new user account is automatically created in the user administration database. Directories based on Light-weight Directory Access Protocol (LDAP [13]) have also become popular. Companies, such as Novell and Microsoft, are in the market with their enterprise directory products.

The problems faced in the deployment of organisation-wide identities are not only technical but organisational. Administrative processes in the organisation have to be justified to ensure smooth operation. For instance, if the user account is closed immediately after the working contract ends and the person is removed from the payroll system, the new contract has to be made in time if the employment still continues. Otherwise the user's account is closed and she is not able to do her work.

Co-operation between different organisational units inside the administration of a university and between the administration and the faculties is needed for example in the integration of student registry and user database. Sufficient level of trust between organisational units is necessary, which is challenging as shown by Allen [1].

2.2 Using Network Services Across Organisational Boundaries

So far the discussion has been limited to using services inside an organisation. However, co-operation between organisations is increasing, and as a result the user of a service does not necessarily belong to the same organisation as the service.

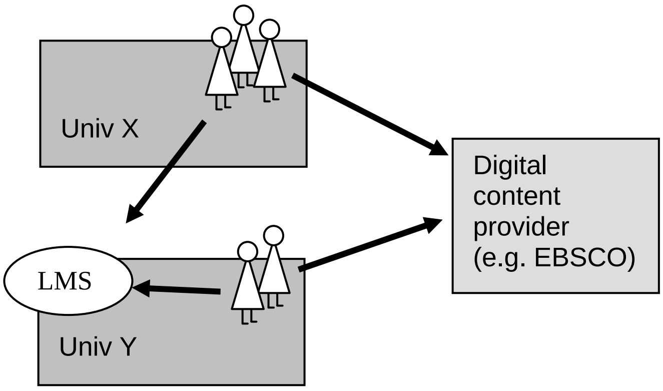

Figure 4. Cross-organisational use of network services.

For example, a student from university X ("origin site") may attend a course provided by university Y ("target site"), and the course may use some web based learning management system (LMS) such as WebCT (Figure 4). The target site somehow has to identify and authenticate the user, and obtain assurance of her authorisation for the service she is accessing. To avoid assigning new identities and issuing new usernames for the user, her identity should be mediated from the origin site to the target site. This is called cross-organisational identity, or federated identity in short (top row in Figure 3).

However, it is not always necessary to uniquely identify the user. In some contexts, it is sufficient to make sure the user is authorised to access the service. For example, the university libraries may have subscribed certain digital content to all the researchers and students in the university. For the content provider (such as EBSCO, a provider of digital contents for university libraries, Figure 4), it is enough to know, that the user accessing the service is either a student or a researcher of the university. From the data protection point of view the content provider should not even get the identity of the user, only her role in the university.

2.3 Identification and Authentication of Users

The need for stronger authentication increases as the scope of user identity gets larger. As the user has the same identity in various network services in her organisation and even across organisational boundaries, the risk of an authentication failure gets bigger. There are more trusted components in which a security vulnerability can cause the security to fail, and once impersonation becomes possible for an attacker, there are more places in which the identity can be abused. Thus, deploying cross-organisational identities increases the demand for strong authentication (the arrow to the upper right corner in Figure 3).

There are different ways to implement strong authentication. Some European governments have plans on launching an identity card for the citizens. The identity cards contain a chip, which utilises PKI in authenticating the user for public and private network services. The chip can be inserted in a mobile phone as well, removing the requirement for an external smart card reader. Smart cards and PKI can be utilised for strong user authentication in the universities as well. Experiences on deployment of PKI based on smart cards are documented for example in [12].

Single sign-on is a commonly referenced concept related to user authentication. For the user, single sign-on means the ability to authenticate only once, and then have access to all the resources available without any further authentication. Single sign-on architectures have been studied for example by Clercq [3].

3 A Model for Cross-organisational Use of Personal Services

This chapter introduces a model for cross-organisational use of personal services. The model contains three entities (Figure 5): the origin site, the target site and the user in question.

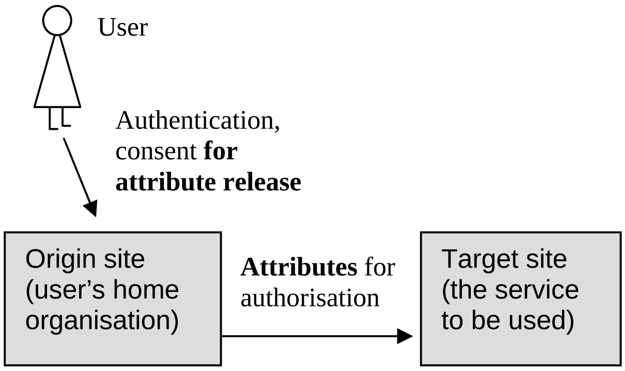
User
Authentication, consent **for attribute release**
Origin site (user's home organisation)
Attributes for authorisation
Target site (the service to be used)

Figure 5. Entities in cross-organisational use of personal services.

3.1 Origin Site

The origin site is the entity that assigns an identity to a user. The identity is represented by an appropriate identifier, such as a user name, which is unique in one domain. Some architectures use identifiers that are globally unique (for example the phone numbers used for identifying a subscriber in the public switched telephone network), in other architectures federated local identities are enough (for example, the identity federation in the Liberty Alliance project to which we will return in Chapter 4). From the data protection point of view, federated local identifiers are preferred, because global identifiers make it easier to aggregate personal information from different sources, causing a violation of privacy.

If global user identifiers are used, a method for implementing global uniqueness is to introduce hierarchy to the namespace. Each institution administrates its local namespace, and some global unique identifiers such as domain names are used to distinguish between organisations. EduPerson [4] suggests that a new attribute eduPersonPrincipalName is introduced in higher education. Bob Smith, for instance, could be known as *bsmith@univ.edu*.

A drawback of hierarchy in the namespace is that once a person is for example a student in two universities, she has automatically two identities. In most cases, this is not a problem, as she probably is acting in some role in one of the two universities, such as as a distant course student in order to include the course in her studies in university X. However, in certain circumstances the two identities can be problematic or at least confusing for the user herself.

Revoking and reassigning unique identifiers in cross-organisational user administration is as problematic as in intra-organisational user administration. If Bob Smith leaves his university, can his unique identifier *bsmith@univ.edu* be later assigned to a Bill Smith starting his studies at the university? If yes, how can it be prevented that the "new" *bsmith@univ.edu* gets access to the information the previous one has left for example to a learning management system he has used?

The origin site is not only responsible for administrating the unique identifiers, but also other attributes belonging to the user. These include her name and other contact information, such as phone number and email address. If some of these change, the user has to remember to update her contacts only to the origin site, and the changes can be mediated automatically to the targets. The origin site also maintains attributes expressing the user's relationship to the home organisation, such as the information that she is a student, professor etc.

A special set of attributes are the credentials used for authentication, including for example passwords and certificates. Maintaining appropriate means for user authentication is the responsibility of the origin site. Some services may have higher requirements for the reliability of the authentication, making it necessary to maintain several credentials for one user; less sensitive services can be used anywhere, more sensitive only on a workstation with appropriate equipment such as a smart card reader.

3.2 Target Site

The target site is the organisation that controls the service the user wants to access. The target site can be, for example, another university whose learning management system is used in some distant course. In other words, a university can act both as a origin site and a target site. The target site can also be some national level organisation such as a national portal for researchers or students, or some commercial content provider, such as EBSCO.

It is expected that the target site wants to control who is able to access the service. The target site authorises the users based on the attributes provided by the origin site. For example the student portal lets only students access the service.

3.3 User

The user is a member (student, staff, faculty, etc in the context of universities) of an origin site. She uses the services provided by target sites and has access only to the services permitted for her.

The European Union Directive (95/46/EC) on data protection requires that in most cases a data subject has to give her unambiguous consent for dissemination of her personal data. User consent for transmission of personal information from the origin site to the target site is needed. If the user is not willing to release attributes that are necessary for the target site, access may be denied or granted only to some lower service level. If the target site gets only information about the role of the user (such as that she is a student at university X) but the identity of the user is not disclosed, the disseminated data is not considered as personal and problems related to data protection become easier.

4 Requirements for Cross-organisational Use of Services

This chapter introduces requirements for an architecture based on the model presented. The requirements incorporate an agreement about the protocol used in communications between the entities, trust between them, the schema used for attributes exchanged by the origin and target sites, and the security infrastructure used in securing the communications. The agreement is made between the entities involved in cross-organisational transactions, forming a community called a federation.

4.1 Protocols Used in the Communications

The traditional protocol for transferring personal information in the Internet is LDAP [13], that is based on X.500 directories. LDAP is commonly used in white page directories, which can be used like phone books to find contact information for people. LDAP is also widely deployed in user administration inside organisations, and products like Novell eDirectory and Microsoft Active Directory support it.

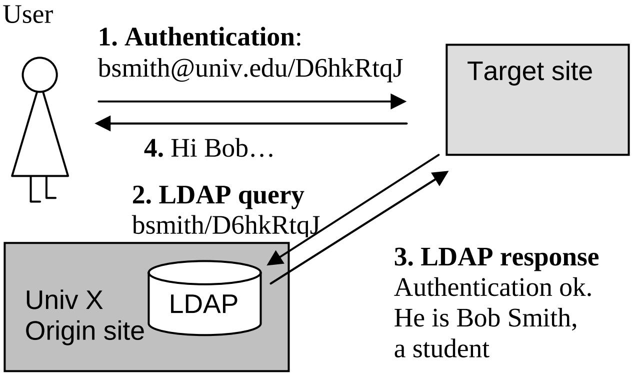

Figure 6. Use of LDAP in cross-organisational user administration.

LDAP can be used for cross-organisational use of services as depicted in Figure 6. The user (Bob Smith) gives his unique identifier (*bsmith@univ.edu*) and password (D6hkRtqJ) used in the origin site to the target site. The correctness of the password is checked against the LDAP directory of the origin site, and the directory provides attributes (e.g. Bob's name and role as a student) to the target site.

However, use of LDAP in cross-organisational user administration has a drawback. As long as authentication is based on a shared secret (such as a password) Bob has to reveal his password, a most sensitive piece of information, to the target site. This causes two risks:

1. If the security of the target site is not properly taken care of, Bob's password can be compromised. For example, if the target site uses basic authentication on top of plain HTTP (not HTTPS) in communications with Bob's web browser, his password is transmitted to the target site in cleartext and it can be sniffed from the network. The origin site has little chances to ensure that the security in each target site is up-to-date.

2. If the architecture above becomes a standard practice and dozens of services start to use it, Bob has no real chance to deduce which service is trustworthy and which is not. Entering the password to any untrusted service is risky. A fake service, whose only intention is to gather passwords from careless users, would probably be a success for a cracker.

Kerberos protocol has been a traditional solution to the problem. New protocols overcoming the problem have been introduced on the WWW. The authentication of the user is always done in the origin site, which provides assertions about the user's identity or other attributes to the target site. As Bob's password is never passed to the target site, a compromise in target's security does not reveal the password, and the damage is restricted to the particular target site. On the other hand, Bob is always authenticated by the familiar authentication server in his home organisation, and he can be told not to provide the password to any other web server.

The Shibboleth protocol specified and implemented by Internet2 is a notable example of such a protocol [9]. The protocol utilises SAML (Security Assertion Markup Language) and SOAP (Simple Object Access Protocol) in the communications between origin and target site. After piloting in some universities in the United States, the first versions of the open source implementation have been released. Attributes of the user are passed to the target site by the Shibboleth protocol, and the target makes the access control decision based on them. The implementation of Shibboleth also provides a mechanism for the user to give her consent for attribute release.

PAPI (Point of Access to Providers of Information) is another protocol used in cross-organisational use of resources [2]. The protocol implemented by RedIris is commonly used for accessing electronic resources in the Spanish higher education.

There are also activities outside the academic communities. The Liberty Alliance has defined a protocol for federating identities between organisations [11]. The focus of the Liberty Alliance project is to get rid of the several identities and related username/password pairs that a user has in electronic services in the Internet, without introduction of a centralised architecture and a globally unique identifier. In the Liberty architecture, the user is authenticated by an identity provider (origin site) and the identity is then federated to service providers (target site), providing a single sign-on experience to the user. In public, the decentralised Liberty protocol is considered to be a challenger for the Passport protocol, whose architecture is centralised around Microsoft.

4.2 Trust between the Entities

In the federation the target sites have to trust the origin sites, which maintain the identity and attributes for the users and the credentials necessary for authentication. The security of the user administration of the service relies on the assertions that the origin site has provided about the users. Thus, the user administration of an organisation needs to be implemented properly before the organisation can enter the federation as an origin site. For instance, the origin site has to ensure that the user account of a certain person is closed when she leaves the organisation.

Also the origin sites have to trust the targets to properly handle the attributes released by the origin. A specially sensitive user attribute is the password used for authentication, if the origin or the user sends it to the target site as cleartext. The architectures presented above, where the user is always authenticated by the origin site, lower the required trust considerably because the passwords never reach the target site.

The user is concerned about her privacy, and she has to trust the origin site that it will not release attributes to the target site without her consent. Even if the user gives her consent for attribute release, only attributes necessary for the target site may be released. The user also has to trust the origin that the log files, which may contain sensitive information about services the user has accessed, are not used to violate her privacy. In most cases, the user privacy is protected by the data protection legislation.

Agreements between origin and target sites are expected to ensure a certain minimal level of security controls implemented by the sites. To avoid many-to-many relationships between the origin and target sites, the federation agrees on the minimal requirements for joining organisations. There may be several federations for services with varying sensitivity; for example, the accuracy of assertions on the user attributes for students is probably lower in library services than in health care services.

In Liberty Alliance, the federation for trust establishment is called a Circle of trust and in the Shibboleth project a Shibboleth club. The requirements for an organisation joining inCommon, the Shibboleth club formed in Internet2, are drafted in [10].

4.3 Schema for the User Attributes Exchanged

The schema describes the user attributes exchanged in the federation. It should cover the syntax and semantics of the attributes, including the vocabularies. The schema should provide attributes for identification, authentication, and authorisation of users.

A lot of schemas have been specified for the directories in the Internet. The basic set of attributes have been defined in Internet standards and are widely used in the phonebook-like white page directories. Attributes such as the given name, surname, postal address, email address, phone number and user password and certificate are specified in [14, 15].

However, in higher education there are requirements that the Internet standards do not fully cover. Most of them are related to attributes necessary for authorisation, because authorisation is usually based on the user's role in the organisation, and relevant roles vary from organisation to another. Usually organisations extend the schema with their own attributes, whose syntax and semantics are specific for the organisation. Enabling cross-organisational use of services, however, requires that the federation agrees on certain basic set of attributes required for authorisation in the target sites.

In the United States, Educause has defined a schema called eduPerson [4], which contains attributes specific for higher education. In eduPerson a new attribute for authorisation is eduPersonAffiliation, which expresses the person's relationship to the organisation. The controlled vocabulary contains values student, faculty, staff, employee, alumn, member, and affiliate. One person may have several roles, for example a post-graduate student in a laboratory has probably values student, faculty, employee, and member. One of them can be promoted to the primary one. European higher education has also had some interest for a similar schema [19].

The attribute eduPersonAffiliation provides a coarse basis for authorisation, as some services are provided only for students, some (such as the previous example of EBSCO) to all members, and so on. On the other hand, it opens up the problem of defining the semantics for each value. For instance, does 'student' cover only students aiming at a degree or should further education students, open university students, etc, be counted in as well?

The need for more fine-grained information about the role of a person in the organisation and the national differences in higher education have caused academic communities in many countries to specify attributes of their own, for example in Swizerland [16] and in Norway [5]. The national schemas present new attributes whose semantics utilise vocabularies maintained by national bodies, such as national statistical offices (for example in a vocabulary '311' means 'doctor of theology'). The higher education institutions already use the codes internally in the student registries.

4.4 Security Infrastructure

A security infrastructure, such as a public key infrastructure (PKI), is required to ensure the authenticity and integrity of the messages exchanged. The origin site and the target site require certificates for mutual authentication and the integrity check of the assertions exchanged. The certificates and SSL/TLS protocol are also used for authenticating the origin and target sites to the user.

For the time being, personal certificates are not widely used, and the authentication of the users cannot be based on PKI on a large scale. Passwords and other weaker means are used instead. However, as the authentication of a user is a local matter for each origin site, the use of strong authentication is not restricted by any design choice. Instead some services may require authentication that is stronger than passwords.

There are several commercial Certificate Authorities (CA) available, and in higher education some universities and research networks have also established a CA of their own. A small number of CAs trusted by the federation is expected to be used for server certificates in the origin and target sites.

5 Initiatives Going On in Higher Education in Europe

Intuitively, the problem of user identification and cross-organisational use of services appears to belong to the higher education institutions, because the users are usually students or employees in some institution. In Europe, the activities, however, are not driven by European University Information Systems association (EUNIS) but by the association of national research and education networks (TERENA). To ensure that the work done in national research networks fulfils the requirements for cross-organisational user administration, discussion and exchange of information between the two associations would be helpful.

In TERENA, related work is done in a specific Task Force TF-AACE (Authentication and Authorisation Coordination for Europe) [18]. TF-AACE is a gathered group of people from individual research networks, who have their own projects, e.g. in Spain (RedIRIS), Netherlands (Surfnet), Switzerland (Switch), Norway (Uninett) and Finland (Funet). TERENA has also trans-atlantic co-operation with Internet2, which develops the Shibboleth protocol and eduPerson schema and has also other related activities.

Switch has been the forerunner for Shibboleth in European research and education network. The AAI (Authentication and Authorisation Infrastructure) project [17] has also specified a schema for attributes used in Swiss higher education. The Norwegian FEIDE project has a schema for LDAP directories used in Mellon o Moria, the architecture designed for cross-organisational use of personal services in Norway [5].

In Finland, the HAKA project, a common project for Finnish higher education, has started pilots for cross-organisational user administration. In the pilots, Shibboleth protocol and funetEduPerson, the Finnish equivalent to eduPerson, is used for accessing services in the portal of the Finnish Virtual University, the Finnish Virtual Polytechnic and the Finnish Electronic Library. More information is available in [7].

6 Conclusions

Demand for middleware that mediates user identities and attributes between services inside an organisation and between organisations has increased. Driving forces are the growing number of personal services in the network, increasing co-operation between organisations, and requirements for flexible and easy use of services without compromises in the information security and privacy.

This paper outlined a model for cross-organisational use of personal services and the requirements implied by the model. In European universities, there are activities aiming at building an infrastructure for cross-organisational use of personal services. The challenges, however, are not only technical but also political and cultural, requiring a new kind of co-operation and trust between organisations and organisational units.

References

[1] D. Allen, “Information infrastructures, information behaviour and trust”. Proceedings of EUNIS2002, the 8th International Confrence of European University Information systems. pp.167–178, (2002).

[2] R. Castro-Rojo, D. R. López. “The PAPI system: Point of Access to Providers of Information”. Proceedings of TERENA Networking Conference, (2001).

[3] J. D. Clercq. “Single Sign-On Architectures”. InfraSec 2002, LNCS 2437. pp. 40-58, (2002).

[4] Educause. “eduPerson Object Class”. http://www.educause.edu/eduperson/

[5] FEIDE project. http://www.feide.no/index.en.html

[6] Greater Nordic Middleware Symposium. “GNOMIS”. http://www.uninett.no/arrangement/gnomis/

[7] HAKA project. http://www.csc.fi/suomi/funet/middleware/english/index.phtml

[8] Internet2 Middleware Initiative. “Identifiers, Authentication, and Directories: Best Practices for Higher Education”, (2000). http://middleware.internet2.edu/internet2-mi-best-practices-00.html

[9] Internet2/MACE. “Shibboleth Project”. http://shibboleth.internet2.edu/

[10] N. Klingenstein. “Draft Club Shib outlines”, (2002) http://shibboleth.internet2.edu/docs/draft-internet2-mace-shibboleth-club-shib-guidelines-01.txt

[11] Liberty Alliance Project. http://www.projectliberty.org/

[12] M. Linden, P. Linna, M. Kivilompolo, J. Kanner. ”Lessons Learned in PKI Implementation in Higher Education”. Proceedings of EUNIS2002, the 8th International Confrence of European University Information systems. pp.246-251, (2002).

[13] RFC 2251. “Lightweight Directory Access Protocol (v3)”. Internet Engineering Task Force, (1997).

[14] RFC 2256. “A Summary of the X.500(96) User Schema for use with LDAPv3”. Internet Engineering Task Force, (1997).

[15] RFC 2798. “Definition of the inetOrgPerson LDAP Object Class”, Internet Engineering Task Force, (2000).

[16] The Swiss Education and Research Network. “Authorization Attribute Specification”, (2002). http://www.switch.ch/aai/docs/AAI_Attr_Specs.pdf

[17] The Swiss Education and Research Network. “Authentication and Authorization Infrastructure”. http://www.switch.ch/aai/

[18] Trans-European-Research and Education Networking Association. “TF-AACE: Authentication, authorisation coordination for Europe”. http://www.terena.nl/tech/task-forces/tf-aace/

[19] Trans-European-Research and Education Networking Association. “TF-LSD: LDAP Services Deployment”. http://www.terena.nl/tech/task-forces/tf-lsd/

Publication 5

Mikael Linden. Organising Federated Identity in Finnish Higher Education. Computational Methods in Science and Technology, Volume 11, Issue 2, 2005. 109–118

Organising federated identity in Finnish higher education

Mikael Linden

CSC the Finnish IT Center for Science, P.O. box 405, FI-02101 Espoo, Finland
e-mail: mikael.linden@csc.fi

Abstract: Finnish higher education has been an early adopter of federated identity in Europe. The Finnish Haka federation is deploying Shibboleth, federating software by Internet2. This paper describes the federation as an organisational entity and explains how privacy issues are taken into account in its policy. Differences between the Haka federation and some other federations are pointed out. The main service areas for federated identity in Finnish higher education are also presented.

Key words: identity management, federated identity, privacy

1. INTRODUCTION

User administration means keeping track of an information system's users and their privileges. In an information system, a user identity is an abstraction of a person in the real world, and it is a collection of attributes describing her. Issues like management of user identities, authenticating users and authorising them to use services are all parts of user administration.

Traditionally, the maximum scope of a user identity has been only one organisation. The identity has not been shared with other organisations. If the user has used services outside her home organisation (for example, her employer or school), she has had separate usernames and passwords for each service. However, as the networking of organisations has become more common, it has become a subject of interest to share (*i.e.*, federate) user identities between organisations. In a federation, an end user only has the credentials (*e.g.*, username and password) her home organisation has given to her, and there is a specific middleware service that federates her attributes from the home organisation (called Identity Provider) to the service she is using (called Service Provider).

A federation is an association of organisations that come together to exchange information, as appropriate, about their users and resources in order to enable collaborations and transactions [1]. The federation, consisting of Identity Providers and Service Providers, has agreed on policies and practices necessary for carrying out the task. Some of these are of a mostly technical nature (such as the protocols used for communication and schemas for syntax and semantics of attribute exchange), some of them are more political (how to make the involved organisations trust each other) and some are legal (how the privacy of the end user is ensured as her personal data is disseminated between the organisations).

Shibboleth is a SAML-based middleware protocol specified by Internet2. Since the open source implementation became available in 2003, it has been deployed by higher education in several countries. In the United States, there are federations already using Shibboleth such as InCommon [1] and InQueue [2] and Australian higher education has shown interest in it [3]. In Europe, Swiss higher education has been the forerunner for Shibboleth. In the United Kingdom, projects funded by JISC are aiming at the deployment of a federation running Shibboleth. In addition, higher education in some other European countries has interest in Shibboleth.

In Finnish higher education, the development of the Haka federation has its origins in the year 2000, when the FEIDHE project focused on personal certificates on smart cards as a tool for strong authentication of end users. However, smart cards did not break through, and as an effect, the project recommended that its followers focus on organisational user administration rather than strong authentication [4]. Having identified the problems of LDAP in cross-organisational user administration, federating software was considered to be an interesting choice [5].

Several national research networks have developed architectures of their own, such as PAPI (Spain), Athens (UK) and FEIDE (Norway). In Finland, we had no resources to implement a protocol of our own. As designing and implementing a security protocol is difficult, we preferred adaptation of existing federating software. The Shibboleth architecture was sound and had the resources of Internet2 behind it. Therefore, it was easy to follow the direction chosen by SWITCH [6] and adopt Shibboleth as the federating software of Finnish higher education. The first Shibboleth pilots started in Spring 2003, and the pilot federation became operational in December 2003.

In February 2004, the Haka project ended and the proposed deployment of the Haka federation, which runs Shibboleth as the federating software [7]. CSC, the Finnish IT Center for Science, started to prepare the federation as a common infrastructure for universities and polytechnics in Finland. The production-level federation was formed in May 2005.

This paper focuses on the organisational elements of the Haka federation. The paper starts with the most important use-scenarios identified for federated identity. Chapter 3 discusses the organisational models for federations and presents the motivation for the choice made by Haka. Chapter 4 presents relevant parts of European data protection legislation from the federated identity point-of-view and how these regulations are taken into account in Haka. Chapter 5 discusses the quality of institutional identity-management and Chapter 6 concludes the paper.

2. USE SCENARIOS FOR FEDERATED IDENTITY IN FINNISH HIGHER EDUCATION

Different kinds of services can be identified as potential users of federated identity. To motivate the rest of this paper, this chapter introduces the four main service categories for federated identity in Finnish higher education.

2.1. Library services

Nowadays, researchers in institutions of higher education do not have to go to the premises of a university library to read scientific journals. Instead, the researchers use electronic services, such as electronic journals and databases, provided on the web by the journal publishers. University libraries pay licence fees to the publishers for making the journals available to the students and researchers in the institution. Typically, libraries intend to licence the journals for students, faculty and supporting staff in the institution and for other regular and registered users on-site [8]. At present, the access control of the journals is usually implemented by configuring the IP address space of the campus in the publisher's service.

IP address-based access control has known problems. It does not actually authenticate the end user; instead, the authorisation to use the service is based on the place where she is using the service. Legitimate users are not allowed to use the service outside the campus IP address space (*e.g.*, at home)[1]. On the other hand, illegitimate users, such as roaming users[2] or other users not considered as students or faculty members at the institution do have access, although, according to the licence terms, the material is not necessarily licensed for them. Furthermore, the authorisation is very coarse and there is no easy way to implement fine-grained access control. For example, the libraries might want to licence some more expensive material only to faculties in a certain department or to the participants of a certain course in the university.

For publishers, authorisation is not the only use for an identity federation. The publishers may like to develop their service further by providing end users with customisation. For example, computer science researchers would, perhaps, always like to see a list of the latest publications in the well-known LNCS publication series of Springer as they browse to SpringerLink. Thus, the publisher needs to get some persistent identifier of the user to which the user profile can be attached in the service[3]. In order to achieve this in its ScienceDirect portal, Elsevier Inc. has already joined the InCommon Federation.

In Finland, the libraries in higher education traditionally co-operate widely in licensing electronic journals. The Finnish Electronic Library consortium is the centralised organisation negotiating the licence agreements with publishers. Furthermore, the consortium has recently deployed a portal (Metalib, a product of Ex Libris Ltd.) that constitutes a common interface to the dozens of publishers with which the libraries have licence agreements. The portal uses services of the Haka federation to authenticate the user and provide her with customised services.

Furthermore, the Finnish libraries also have a common Library Management System (Voyager, a product of Endeavor Inc.), which, for instance, keeps track of library patrons' loans in a library. The web interface (WebVoyage), used by patrons for reviewing and renewing their loans, presently uses library card numbers for user identification. In an ongoing pilot project in Finland, Shibboleth is being integrated into WebVoyage to replace its current user identification system.

2.2. eLearning services

Utilising ICT for learning enhancement has been a subject, not only from the technical, but also from the pedagogical point of view. Several tools have been used, including video-conferencing, multimedia *etc*. The web has also become a commonly used environment for eLearning, and various web-based services have been developed, from simple web-based tools to fully-fledged learning management systems. Many of the eLearning services are interested in the identity and role of the end user.

There is a large number of commercial and open source learning management systems. In Finnish universities, the most widely used ones are WebCT, BlackBoard, Optima and R5 Vision [11]. The maintenance of learning management systems is not so well organised as the use of library services. In some institutions, the laboratories have their own installations of their learning management systems; in other institutions, there are some centrally-operated learning management systems that belong to the institutional IT infrastructure maintained by the university. Some initial discussion has been had about a national service centre for the

[1] VPN connections or dedicated proxy servers (such as EZproxy, http://www.usefulutilities.com/) are commonly used to circumvent the limitations of IP address based access control.

[2] VPN based roaming model is the only one giving a roaming user an IP ad-dress from her home institution [9].

[3] The eduPersonPrincipalName or eduPersonTargetedID attributes of the widely used eduPerson schema [10] can be used, for instance.

main-tenance of learning management systems for better efficiency. However, many lecturers consider the tools they use in teaching as part of their academic freedom.

Considering the aforementioned, it is not a surprise that the user administration of learning management systems is versatile. In some learning management systems, the students register to the system by themselves and get yet another username/password pair to remember. If the institution has a centrally operated learning management system, it is more likely to be coupled to the enterprise directory of the institution's IT department, allowing end users to use the same username/password pair they also use in other IT systems.

In Finnish higher education, it is possible to take courses from a neighbouring institution. Nowadays, the visiting students get local user accounts in the institution they are visiting, making cross-institutional user administration unnecessary. In other words, user administration of learning management systems is typically an institutional, not an inter-institutional issue, and there is little use in joining institutional learning management systems to the national Haka federation. Instead, in order to serve the user administration of learning management systems, IT departments are preparing to set up institutional light-weight federations, serving mostly laboratories inside the institution. These institutional federations may also use the Shibboleth technology, as it is easier to maintain only one middleware infrastructure[4]. In an institutional federation, the bureaucracy is easier because, for data protection, personal data is not disseminated between two organisations.

Having a national federation in place opens new business models for eLearning. The eLearning service need not be installed and maintained in the institution, and yet, it can utilise the user administration of the institution's IT department. In order to achieve economics of scale, there can be separate service centres that maintain learning management systems for several institutions. Furthermore, an institution can licence some specialised eLearning material for a small group of students; for example, to the participants of one individual course. For authorisation purposes, the participation of a student on a course can be expressed as a separate attribute that the institution's IT department provides to the eLearning service[5].

In Finland, several learning management systems have been, or are being integrated to Shibboleth, including WebCT (University of Helsinki), A&O (Tampere University of Technology), Moodle (University of Kuopio) and Optima (University of Oulu). First experiments are about to start on passing the students' course enrolment as an attribute to the learning management systems using Shibboleth.

2.3. National services for end users in institutions of higher education

In addition to eLearning and libraries, nationally centralised services are potential users of federated identity. Nationwide services are typically provided to a subset of end users that spans a large number of higher education institutions. Theend users can be, for example, students or researchers in any of the higher education institutions. As there has not been a national authentication and authorisation infrastructure in place, the services have either issued local usernames/passwords for end users or have not provided personal services to end users at all.

The Academy of Finland is a public body providing funding for research projects in universities. The funding application form has been made available electronically, and the Academy has issued usernames and passwords to the researchers for filling the applications. As the applicant has filed the application, it is circulated to specialists in other universities in order to get expert opinions on it. The use of the Haka federation instead of local usernames makes the application submission and circulation process easier for end users as well as for the Academy.

YTHS (Finnish Student Health Service) is a foundation serving all the masters degree students in Finnish universities. Presently, YTHS has no personal services on the web, as there has been no means to authenticate the 140 000 customers. YTHS would be interested in providing some basic services on the Internet. These services could include, for example, appointment reservation for the first-year-students' health examination or other functions that require no medical expertise.

2.4. Application service providers

Outsourcing applications is becoming common also in higher education. The universities in Finland are government agencies and are involved as the state corporation makes outsourcing decisions to reduce costs and increase administration efficiency. The first group-level outsourcing contracts made by the State Treasury cover electronic circulation of invoices and travel-expense administration. The application services are provided by large Finnish IT companies.

The Finnish state administration has 120 000 officers, 30 000 of which are staff and faculty in universities. Not all of these officers are involved in the circulation of invoices, but typically, most of them have travel expenses. Presently, user administration in the outsourced services is done manually, while some more advanced organisations have scripting in place to synchronise user databases with the enterprise directories. User authentication and authorisation in outsourced services is clearly a customer for identity federation, although it couples the identity federation of higher education to user administration issues in other Finnish government agencies.

[4] Shibboleth Identity Provider, version 1.3 is going to have multi-federation support in it.

[5] The CourseID working group (http://middleware.internet2.edu/courseID/) of Internet2/MACE has specified how a person's role can be expressed as an attribute with respect to a given course offering.

3. THE ORGANISATION OF A FEDERATION

As defined in the first chapter, a federation is a set of organisations who have decided to co-operate in order to authenticate and authorise end users across organisational borders. In order to put the co-operation into practice, the organisations pick up and deploy some middleware technology, such as Shibboleth. In other words, a federation is an organisational, not a technical entity[6]. This chapter discusses how to organise a federation.

As the authentication and authorisation of users is an essential part of computer security[7] and the processing of personal data is regulated in the European Union, it is necessary to have written agreements between the federation participants defining related obligations and responsibilities. Furthermore, as the federation collects fees from the federation members to cover its costs, it also exists as an economic entity. There must be some kind of an organisation that signs the necessary agreements and deals with the accounting for incomes and expenses in the federation.

This paper identifies two ways to organise a federation. The InCommon and SWITCHaai federations have been organised as a service provided by a central organisation, such as InCommon LLC or SWITCH. The alternative would be to organise a federation as a consortium.

3.1. A federation as a service provided by an organisation

Having the federation organised as a service means that an organisation joining the federation signs a bilateral agreement with the operator of the federation (Fig. 1). In a way, the operator becomes a centre of a star, having bilateral agreements with all the organisations in the federation. In Switzerland, the operator is SWITCH, the maintainer of the national research and education network, a foundation of the governing bodies of Swiss universities. In the US, InCommon is a limited liability company dedicated for the provision of federation services.

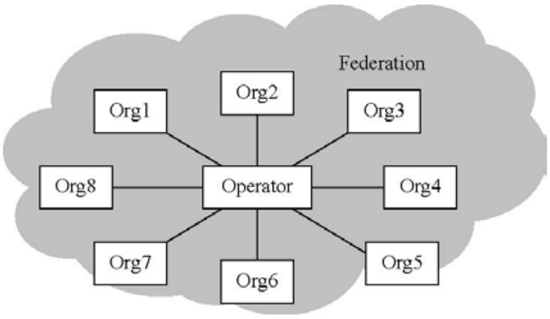

Fig. 1. Federation as a service provided by the federation operator

A benefit for organising the federation as a service is that no new organisation needs to be established for the federation. The joining organisations and the operator sign an agreement specifying the responsibilities of the two parties, and the federation is a collection of bilateral agreements between the operator and the participants. From a participant's point of view, all the other participants of the federation are subcontractors for the operator of the federation. If the participants of the federation have, for example, claims for each other, they have to discuss these with each other *via* the federation operator.

The downside is that organising the federation on top of bilateral agreements is not strictly consistent with the definition of a federation, which considers a federation as a set of organisations. As the centre of the star of agreements, the role of the operator becomes essential and demanding, for example, replacing the federation operator means, in practice, tearing down the federation and building a new one.

The business of the operator is inevitably to develop the federation service to make it more and more attractive and satisfying for the customers. The operator needs to deeply understand the requirements and, on the other hand, the limitations the federation participants. In higher education, the needs are typically driven by service providers like libraries, eLearning, etc. The limitations are set by the IT departments of the institutions and typically consist of issues like the quality of the institutional identity management systems or problems in linking organisational person registries to each other.

3.2. A federation as a consortium

Alternatively, a federation can be organised as a consortium (Fig. 2) that is, by definition, an agreement, combination or group (as of companies) formed to undertake an enterprise beyond the resources of any one member [13]. In that sense, a consortium is quite close to what we are looking for. In a consortium, organisations sign a multilateral agreement to become members. Having signed the consortium

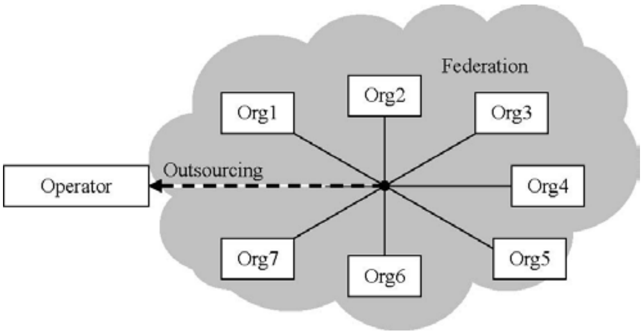

Fig. 2. A federation as a consortium

[6] To distinguish the organisational and technical parts of federated identity, SWITCH has called the technical aspect (servers, configurations, *etc*.) Authentication and Authorisation Infrastructure (AAI).

[7] According to the definition by Gollmann [12], computer security deals with the prevention and detection of unauthorised actions by the users of a computer system.

agreement, the organisations have direct contractual relationships and can make claims directly on each other.

The consortium would need a service centre that coordinates the federation. In higher education, it would probably make sense to place the service centre in some existing institution for higher education, for example, in its IT department. The secretaries of the consortium would be employed by the institution in question. At minimum, the consortium could be just an outsourcing organisation, buying the technical operations of the federation from commercial organisations.

3.3. The organisation of the Haka federation

In Finnish higher education, the two alternative ways to organise the federation were considered. Following the way SWITCHaai had chosen, the higher education institutions preferred organising the federation as another service provided by CSC, the maintainer of the national research and education network Funet. The most significant reason for that was minimising additional bureaucracy; there was no interest in forming yet another body for taking care of the common IT infrastructure in Finnish higher education. This was also the reason for not choosing to found a separate limited liability company, like InCommon in the United States.

CSC had been an active participant in developing the federation. As Funet was already a service provided by CSC, having the Haka federation as another service provided by CSC is not surprising. CSC, in turn, has the option to outsource some parts of the federation operations. For example, at the moment, CSC has no 24 hour support for servers such as WAYF (Where-Are-You-From, a Shibboleth server used by the end user for picking up her Identity Provider), which may become necessary as the use of the federation is increased.

Choosing the consortium would have meant that the institutions would have established the consortium and placed its administration in some existing IT department in a university. Most probably, the administration would have consisted of only one part or full time employee, who takes care of the consortium's administration and financing, of taking new members to the consortium and of outsourcing contracts for all technical issues in the federation. These would include issues like the maintenance of federation metadata and WAYF server, organising a helpdesk and courses for people in higher education institutions and so on. As there is little commercial supply for federated identity at the moment, the subcontractor would probably have been CSC, at least in the beginning.

The organisation of the federation is depicted in Fig. 3. As the federation is organised as a service operated by CSC, which is not a higher education institution itself, it becomes vital to set up mechanisms that make sure the operator has contacts to the daily life of federation users in institutions of higher education. To ensure that the requirements and limitations related to the federation are communicated to CSC, the federation has an Advisory Committee. The committee consists of representatives for the institutions' IT departments (4 persons), eLearning consortia (Finnish Virtual University and Virtual Polytechnic, 2 persons) and a library consortium (Finnish Electronic Library, 1 person) of Finnish higher education. CSC also has a representative on the committee. Participating in related events in higher education (such as gatherings of IT department employees, eLearning people, *etc*.) and personal contacts help the operator adjust to the needs of the customers.

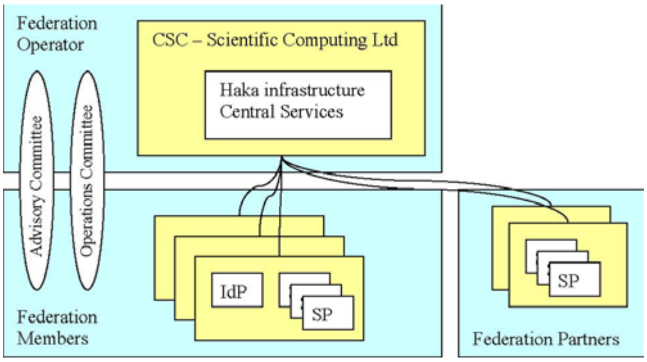

Fig. 3. Organisation of the Haka federation is similar to SWITCHaai

3.4. The service agreement of the Haka federation

The Haka federation is a service provided by CSC as defined in the service agreement of the federation [14]. CSC, the operator of the federation, defines the terms of the service in the agreement's appendices. These can change over time. The Advisory Committee of the federation acts in an advisory capacity and represents the members of the federation. The meetings of the Advisory Committee are prepared and convened by the operator. In the service agreement, the Advisory Committee is defined as the authoritative body for a set of issues, such as accepting federation partners or members other than institutions of higher education. However, the committee's main role is advisory only, and the operator makes final decisions on the terms of service. If federation partners are not satisfied with the service, they always have the ultimate right to terminate the service agreement, or threaten to do so.

Like in SWITCHaai, the Haka federation has two categories for federation's participants; federation members and partners. Higher education and research institutions may join the federation as members and become both Identity Providers and Service Providers. Federation partners, such as library content providers, may only become Service Providers. As the service agreement of the Haka federation is signed between the federation operator and the participant, from the federation participants' point-of-view, the federation is a service provided by the operator and the other participants in the federation are subcontractors for the operator. In the agreement, it is made explicit that the contents of the service agreements are equal for each federation member.

The section defining indemnification is modest. Neither party is liable for damages caused due to bad quality of the service such as its downtime or weak performance. Federation participants refrain from claims on each other. Other sanctions defined in the agreement were considered sufficient for all parties. If the operator has quality problems, the federation participants do not have to pay fees for the time - period in question. If a participant has a problem, the operator is allowed to stop providing the service to it. The ultimate consequence is the termination of the agreement.

It is clear that the service terms, including indemnification, are not very strict in the Haka federation. Having CSC, a non-profit company owned by the Ministry of Education, as the federation operator is far different from a commercial company. The operations of the Haka federation are based not only on the service agreement, but also on the trust higher education institutions have in CSC, which has been their partner for decades. A service agreement with a commercial company would be much stricter, as the nature of a commercial company is to try to minimise the costs and maximise the income from their services.

4. PRIVACY ISSUES IN A FEDERATION

As a member of the European Union, Finland has implemented the EU Data Protection Directive in the national legislation. The Finnish Personal Data Act restricts the way personal data may be processed by the Identity and Service Providers of a federation. This chapter points out the parts of the directive that affect especially on attribute release in a federation. The chapter also presents related means that have been implemented in the Haka federation policy.

The privacy related mechanisms in the Haka federation differ from SWITCHaai. In Switzerland, there is also cantonal privacy legislation in which not all details are similar. As Finland has consistent data protection legislation, the federation preferred to also cover detailed mechanisms for privacy in its procedures; centralising certain privacy-related check-ups in the federation reduces overlapping of work (which the technical staff usually considers boring). The other alternative would have been to leave the privacy issues uncovered and up to each federation participant to take care of.

Liberty Alliance has made an extensive study of European legislation and its effect on federated identity [15]. Although the study focuses on the Circles of Trust, *i.e.*, federations utilising Liberty technologies, the issues are, for the most part, applicable for Shibboleth-based federations as well.

Article 2 of the data protection directive defines personal data as information that relates to an identified or identifiable natural person. Processing of personal data is defined as any operation or set of operations which is performed upon personal data, such as collecting, storing, disseminating and so on. It is clear that user accounts in an Identity Provider are personal data, and, therefore, the Identity Provider processes personal data. The Service Provider processes personal data only if the attributes provided by the Identity Provider and other records collected by the Service Provider relate to an identified or identifiable individual[8]. As the attribute release takes place directly between the Identity and Service Provider, the operator, in turn, never processes end users' personal data in a federation running Shibboleth as the federating software.

4.1. The purpose of processing personal data

Dependency on the purpose of processing personal data is fundamental to privacy laws in Europe. According to the Data Protection Directive, *(Article 6) Member states shall provide that personal data must be (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.* Liberty Alliance has not covered this aspect in its document [15].

In Finland, universities and polytechnics are public organisations as defined in the Universities Act and Polytechnics Act. The mission of universities and polytechnics is also specified in the acts; in short, it is research and education, with the polytechnics emphasising more applied aspects. Identity management is a supportive function in higher education institutions. Thus, according to the Universities and Polytechnics act, the purpose of processing personal data in institutional identity management systems is supporting research and education. Personal data may not be processed (for example, disseminated) in institutional identity management systems for purposes incompatible with that.

The Haka federation has addressed the purpose of processing personal data in its policy. The purpose of the federation is simply "to support higher education and research institutions". Only organisations having services compatible with this purpose are accepted to the federation. For institutions of higher education that act as Identity Providers or Service Providers this is not a problem. For organisations providing services to higher education, such as library content providers, this is not a problem either. On the other hand, services like Internet gambling that are clearly not supporting research and education and may not join the federation. Some organisations are partly compatible with the purpose; for example, the services related to applying for student loans at KELA (the Social Insurance Institution of Finland) can join the federation, but the services related to maternity allowance cannot. In borderline cases, it is up to the Ministry of Education to draw the line.

[8] The United Kingdom Information Commissioner emphasises identifiability as a contextual issue [16]. In the physical world, individuals are distinguished from others typically by names and addresses; in the on-line world, for example, by tracking cookies and pseudonyms.

Dependence on the purpose of the personal data processing makes European privacy legislation different, for example, from the legislation in the United States. In the United States, higher education is co-operating with the e-Authentication project of the Federal government in order to enable end users in higher education to use their credentials for authenticating to government services as well. According to the Data Protection Directive, this appears not to be possible in Europe. Government services, such as social security, taxation, etc, are not supporting research and education. This incompatibility can be seen as an obstacle when bridging the United States and European federations together in the future.

4.2. The relevance of attributes

According to the Data Protection Directive *(Article 6) Member states shall provide that personal data must be (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.*

In an identity federation, Identity Providers are not allowed to release and Service Providers are not allowed to collect attributes that are irrelevant for the service in question. The relevance of attributes depends on the service; for a student loan service, the Social Security Number is probably a relevant attribute, as the SSN is used for identifying individuals in government services. For a learning management system, the SSN is probably irrelevant.

From the data protection perspective, the optimum is that no personal data is processed at all. In higher education, there are several services (such as the article databases licensed by libraries or WLAN roaming access) which are typically not interested in the end user's identity but on her authorisation to the service. The authorisation may be derived from the end user's attributes (for example, faculty members are authorised to use the library database or WLAN network). If an individual cannot be identified, the Personal Data Act is not applied at all to the attribute release.

The Haka federation's policy documents define responsibilities for ensuring that only the relevant attributes are released to the service. The administrative contact of the federation participant signs a request and sends it to CSC before CSC adds the new service to the federation metadata. It is a responsibility of the federation participant's administrative contact to make sure that all the attributes in a service are relevant. In a higher education institution, the administrative contact is typically the information manager of the institution. He or she knows the local circumstances and is, unlike CSC, competent to deduce the relevance of attributes for the service in question.

4.3. Informed consent

According to the directive, an individual's consent is the basis for processing personal data. For Identity Providers, among other things, release of attributes is considered as processing of personal data. For Service Providers, collecting attributes that identify an individual is processing personal data, no matter if the attributes are provided by an Identity Provider or by the end user herself. *(Article 7) Member States shall provide that personal data may be processed only if:*

(a) the data subject has unambiguously given his consent;

(b) processing is necessary for performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the data subject which require protection under Article 1(1).

Some activities in an identity federation could probably fall in a category other than (a). However, the Finnish Data Protection Ombudsman gave advice that the consent of an individual should always be considered as the primary way for making the release of personal data legitimate. Furthermore, according to Article 11, the subject of the data must, in any case, be informed about to whom and for what purposes his/her personal data is going to be released. This can be done conveniently when asking for his/her consent.

It is worth noting that the user's consent overrides neither the requirement for the compatibility of the purpose of processing personal data nor the requirement for the relevance of attributes released. Only relevant attributes may be released and only to services supporting higher education even if the end user has given her consent for the release of attributes.

The policy documents of the Haka federation mandate that the Identity Providers always ask the user when her personal data is released to a new Service Provider for the first time. The consent is asked after the Identity Provider authenticates the end user but before the end user's web browser is redirected back to the Service Provider. If the user denies the release of attributes, the Shibboleth message exchange does not continue.

A Privacy Policy is a document that the Service Provider maintains and that contains the information required by the Article 11. The federation operator gathers and distributes the Privacy Policies' links as a part of the federation metadata. To make the end user's consent an informed one, the Identity Provider is responsible for providing an end user with the link to the Privacy Policy of the Service Provider.

Thereby, the end user is able to read the Privacy Policy before he consents to the release of attributes.

4.4. How Shibboleth fulfils the privacy requirements

Shibboleth provides excellent tools for covering the three issues presented above. The Attribute Release Policies (ARP) provide the means for controlling to which services the attributes are released. In the Shibboleth implementation, there are two kinds of ARPs. Site ARPs are maintained by the Identity Provider and they permit or deny attribute release for any end user. Additionally, each end user may have her personal User ARP. The two ARPs are conjunctive; both the Site and the User ARP (if existing) have to permit attribute release to a certain Service Provider to make the attribute release take place.

Compatibility with the purpose of processing personal data (Chapter 4.1) can be ensured by making sure that the Site ARP does not permit the release of any personal data to a Service Provider incompatible with the purpose of the federation ("to support higher education and research institutions"). The site ARP can also be used to make sure that only relevant attributes are released to a given Service Provider (Chapter 4.2). In the Haka federation, Site ARPs are maintained by the federation operator and distributed to Identity Providers as part of the federation metadata.

The end user's consent (Chapter 4.3) is stored as a User ARP. When the user accesses a service for the first time, the Identity Provider asks her permission for attribute release and writes a relevant entry to her User ARP file. Having given her consent once, the user is not interrupted by the dialogue again when she uses the service the next time. However, the end user can be provided a separate tool for viewing and modifying the ARPs she has in force at any time.

As presented in Chapter 4.3, user consent does not override the requirement for compatibility and relevance of processing personal data. In Shibboleth, this is ensured by requiring that both Site and User ARP must permit the attribute release.

5. THE QUALITY OF INSTITUTIONAL IDENTITY MANAGEMENT

It has become evident that many institutions of higher education have problems with the quality of data in their institutional enterprise directories. User accounts are not systematically closed as students graduate. The links between the student registry, human resources registry and the enterprise directory are missing. The institutions of higher education that have gone through the project of improving the situation have found that it takes several years to fix an institutional user administration. In addition, the project is not only about technology but also about streamlining workflows in the organisation.

Previously, the quality of institutional identity management was an internal issue for each institution. However, in an identity federation, the user attributes, whether of good or bad quality, are visible not only to the Identity Provider itself but also to the Service Providers in the federation. From the Service Provider point-of-view, having Identity Providers with varying qualities of institutional identity management is a problem. Service Providers are questioning what the benefit is of the identity federation if they are not able to trust on the users' attributes provided by the Identity Providers.

Like the FEIDE federation in Norway, the Haka federation has made it a mandatory requirement for an institution joining the federation as an Identity Provider that its enterprise directory has high-quality data in it. Changes in the base registries (student and HR registry) have to be reflected to the enterprise directory. Releasing only high-quality-data to Service Providers has been considered as a high priority issue in the federation. As an Identity Provider joins the federation, it makes a self-audit in its identity management under the supervision of the federation operator. As an output, a doument describing the principles of the institutional identity management is published in the web.

In order to support institutions of higher education in the development of their institutional user administration, CSC has run a series of workshops called "the school in user administration". In the workshops, best practices have been introduced and new products presented. During the workshops, the participants have been asked to make an assessment of the present user administration system in their home organisation and to set the goal for its development.

6. CONCLUSIONS

Although driven by development of protocols such as Shibboleth, federated identity is not only about developing technology. An identity federation must be given an organisational shape as well. The policy documents of a federation have to be in place, defining requirements and best practices for organisations in the federation. Federation policy has to take into consideration the relevant privacy legislation and integrate the obligations to the organisation and procedures in the federation.

This document presented how the Haka federation, the identity federation of Finnish higher education, had come to the decision to organise the federation as a service provided by CSC, the Finnish IT Center for Science. The service agreement and controls over privacy and attribute quality in the federation were also introduced.

Acknowledgements

Acknowledgements to Thomas Lenggenhager for providing background information on the Swiss privacy legislation.

References

[1] InCommon Federation. InCommon glossary http://ww.incommonfederation.org/glossary.cfm Referenced 2.5.2005.

[2] InQueue Federation. http://inqueue.internet2.edu/ Referenced 2.5.2005.

[3] International Middleware Event. Australia Position Paper. http://www.jisc.ac.uk/uploaded_documents/Australia_Posit io nPaper.doc Referenced 2.5.2005.

[4] M. Linden, P. Linna, M. Kivilompolo, J. Kanner, *Lessons Learned in PKI implementation in Higher Education*. Proceedings of EUNIS2002, the 8th International Conference of European University Information Systems, Portugal, 246-251, 2002.

[5] M. Linden, *Towards Cross-Organisational User Admi nistration*. Informatica 27, 353-359 (2003).

[6] SWITCH Authentication and Authorization infrastructure. Architecture Evaluation. January 2003. http://www.switch.ch/aai/pilotdocs/Arch_Eval_v10.pdf

[7] The Finnish Haka Project. Conclusions and Proposals of Action. February 2004. http://www.csc.fi/suomi/funet/middleware/english/HAKA final_report.pdf

[8] The Ligue des Bibliothèques Européennes de Recherche. LIBER Licensing Principles for Electronic Information. http://www.kb.dk/liber/news/981116.htm Referenced 2.5.2005.

[9] *Trans-European Research and Education Networking Association*. Terena Technical Report TF-Mobility. Inter-NREN roaming. Final Report. 2004. http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/TF-MobilityfinalReport.pdf

[10] Educause. "eduPerson Object Class". http://www.educause.edu/eduperson Referenced 2.5.2005.

[11] K. Koivu, Learning management systems in use in Finnish universities, June 2004. Available in Finnish: http://www.uta.fi/itpeda/Raportit/koko_kartoitus101103.pdf

[12] D. Gollman, *Computer Security*. John Wiley & Sons, Inc, New York, 1999.

[13] Merriam-Webster's Online Dictionary. http://www.britannica.com/dictionary Referenced 2.5.2005.

[14] Haka Federation. Service Agreement for Federation Members. http://www.csc.fi/suomi/funet/middleware/english/ Referenced 2.5.2005.

[15] Liberty Alliance Project. Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation. February 2005. http://www.projectliberty.org/specs/Circles_of_Trust_Lega lFramework_White Paper_322200522576.pdf

[16] The UK Information Commissioner. Data Protection Act 1998. Legal Guidance. http://www.informationcommissioner.gov.uk/cms/Docume ntUploads/Data%20Protection%20Act%201998%20Legal %20Guidance.pdf Referenced 2.5.2005.

Lic Tech Mikael Linden is a post-graduate student in Tampere University of Technology, focusing his studies on identity management. At CSC the Finnish IT Center for Science, he is coordinating the deployment and operations of the Haka federation of Finnish higher education.

Publication 6

Mikael Linden, Viljo Viitanen. Roaming Network Access Using Shibboleth. Selected papers of Terena Networking Conference 2004. http://www.terena.org/publications/tnc2004-proceedings/

Roaming Network Access Using Shibboleth

Mikael Linden*, Viljo Viitanen†

* CSC, the Finnish IT Center for Science
mikael.linden@csc.fi

† University of Helsinki
viljo.viitanen@helsinki.fi

Abstract

There are activities aiming at abling users to dock to a wireless or wired network while visiting organisations outside the premises of their usual connection to the network. These activities, known as roaming access to network, are usually based on well-known technologies, such as RADIUS, IEEE 802.1X, VPN or HTTP redirection. On the other hand, there are applications, usually on the web, that are supposed to be accessed across organisational boundaries. The required infrastructure, known as identity federation, takes care of user authentication and authorisation in the participating organisations. Federating software, based, for example, on XML and SOAP, is being developed in the Internet and academic communities.

This research combines the two and implements roaming access to network on Shibboleth, a federating software developed in Internet2. As a result, a unified model was achieved for authentication and authorisation both for network and application access. The architecture makes role-based authorisation easy and provides a single sign-on while preserving the user's privacy. A practical experiment is going on at the University of Helsinki.

Keywords: roaming access, federated identity, Shibboleth

1 Introduction

Network users want using network services to be all the more comfortable. On one hand, this means the users want to have the network connection easily available everywhere while moving around. On the other hand, the users expect applications on the network to be able to provide more personal and tailored services to them. The services, whether they are the applications being accessed or the network connectivity itself, need to be able to recognise the user's authorisation to use the service. Usually, authorisation is based on the user's authenticated identity and the attributes describing her characteristics. The process of keeping track of information system users and their privileges is called user administration.

Typically, the user has one home organisation that she has dealings with and that usually provides most of the services available for her. The home organisation is often the user's employer, school, teleoperator etc. A cross-organisational service means that the service is provided by an organisation other than the user's home organisation. For authentication and authorisation, cross-organisational services need cross-organisational user administration.

Terminology in the area is still young, and varying concepts are being used. In this document, the user's home organisation is called Identity Provider [TFAA04]. The Identity Provider is responsible for authenticating the user and is also the primary source for the user's attributes. The organisation that provides the actual service is called Service Provider. The Service Provider is expected to rely on the authentication done and attributes released by the user's Identity Provider.

Chapter 2 introduces common technologies for a cross-organisational network and application access, which are then compared in Chapter 3. In Chapter 4, the architecture for combining network and application access is introduced. Chapter 5 presents the practical experiments being conducted at the University of Helsinki. Chapter 6 concludes the paper.

2. Cross-organisational Access Technologies

A cross-organisational service may be either network access for roaming users in a visited organisation, or application level access, for example, to a service on the web. Next, technologies to implement cross-organisational network and application access shall be shortly introduced.

2.1. Network Access

Network access is the service that provides a network connection to a user when she is roaming outside her home organisation. A generic architecture is presented in Figure 1. The user can connect to the Service Provider's docking network using either a wireless (WLAN) or a wired link. The Network Access Controller[i] controls the docking network and prevents an unauthenticated user's traffic out of the docking network. In order to authenticate the user, the Network Access Controller consults the user's Identity Provider (i.e.

[i] In [TFMO04], the component is called Access Control Device; here, the word "network" is added to distinguish it from application access.

her home organisation) to deduce if network access should be granted to the user. The Identity Provider has an Authentication Server and a back-end database of its users. Although omitted from the figure, each organisation can typically act both as a home organisation for its local users and a visited organisation for roaming users coming from other organisations.

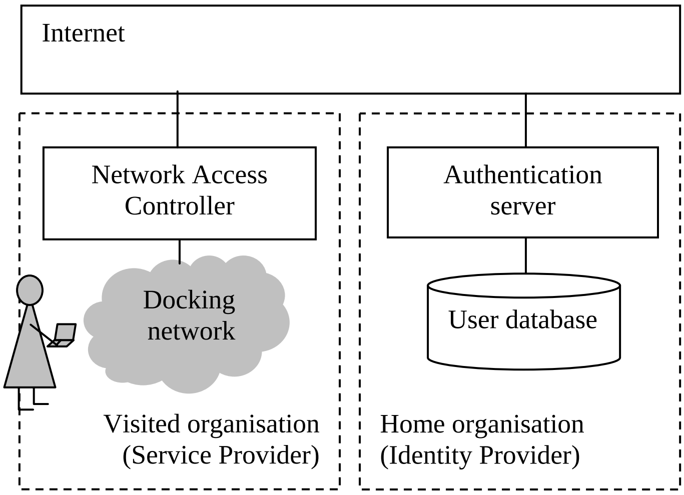
Internet
Network Access Controller
Docking network
Visited organisation (Service Provider)
Authentication server
User database
Home organisation (Identity Provider)

Figure 1. The generic architecture for roaming access to network.

Terena's TF-Mobility group has defined requirements for roaming network access [TFMO04c] and investigated technologies used in academic communities in Europe [TFMO04]. The three most widely used solutions are shortly introduced below.

IEEE 802.1X is a layer 2 authentication protocol that a Network Access Controller uses to authenticate a roaming user. Together with EAP (Extensible Authentication Protocol) and a hierarchy of RADIUS proxy servers, it can be used to validate the user’s username and password against her Identity Provider. The user gives her username in the format of *username@domain* and based on the domain name, the RADIUS proxies are used for relaying the authentication request to the correct Identity Provider. The user's credentials (usually the password) are passed to the Identity Provider on EAP. In European higher education, roaming based on 802.1X is used for example in the Netherlands.

Web Redirection is another roaming solution based on a hierarchy of RADIUS proxies. Instead of using 802.1X, the Network Access Controller presents to the user a web dialog, prompting her to enter her username and password, which are then validated against the Identity Provider’s RADIUS server. For the user, access from the docking network to the rest of the network is granted only if the Identity Provider responds that the credentials were successfully validated. Web Redirection is used in roaming, for example, in Finnish higher education.

VPN based roaming solution does not require a hierarchy of RADIUS proxies. Instead, the Network Access Controller has a list of all the Identity Providers' VPN gateways, which are the only hosts outside the docking network to which the Network Access Controller allows traffic. It is then up to the VPN gateway in the user's home organisation to authenticate the user and route her traffic to the Internet.

The administrational overhead of the extensive list of VPN gateways can be simplified by attaching all the VPN gateways to a single or a small number of networks, and configuring the address space of the networks to each Network Access Controller. Adding a new Identity Provider would then require no modifications to any of the Network Access Controllers. The solution is known as CASG (Controlled Address Space to Gateways) and described in detail by Terena’s TF-Mobility [TFMO04b]. VPN based roaming is used in Swiss higher education.

2.2. Application Access

Accessing cross-organisational applications means using an application level service provided by a Service Provider situated somewhere in the Internet. Typically, applications for a large user base are provided on the web, or may have a web front end for them (such as videoconferencing). Thus, application level access technologies, known as federating softwares[ii], are mostly designed for the web, Kerberos being the most well known exception.

Unlike network access, federating softwares do not have widely deployed protocols on top of which to run. There are implementations utilising web redirects, embedding tickets in the URL fragments, hidden web forms and cookies, but no single standard has emerged. Most prominent technologies, such as SAML (Security Assertion Markup Language), are built on XML and SOAP.

A group of organisations co-operating to administer user access to cross-organisational services is called a federation [TFAA04], which consists both of Identity Providers and Service Providers. To put the co-operation into practice, the federation decides to use some federating software (or develops one of its own).

In academic community, federating software and federations using them are typically aimed at protecting library and e-learning services. The United Kingdom has had the Athens federation [ATHE04] running for years. In Spain and Norway, the national research and education networks have developed the PAPI [PAPI04] and FEIDE [FEID04] systems, respectively. In the Netherlands, Surfnet is promoting A-select [ASEL04] also for cross-organisational transactions.

[ii] From telecommunications perspective, a federating software is a protocol which both the Identity and Service Provider have implemented. From a service developer’s point of view, it is a middleware service that provides user authentication and authorisation service to the application.

There are, however, some technologies that have acquired international use. Shibboleth [SHIB04], the federating software by Internet2, is being used or piloted in the academic world in the United States, Canada, Australia, Switzerland, Finland and the United Kingdom. Outside academic communities, there are commercial organisations developing their federating software, such as Liberty [LIBE04] and WS Federation [WSFE03].

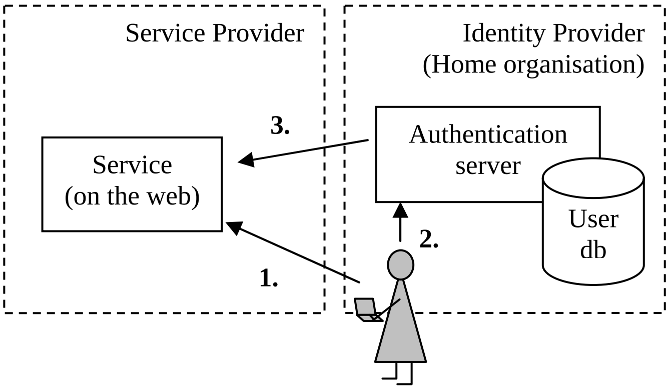

Figure 2. Cross-organisational application access.

Although varying implementations are available, a typical federating software architecture is depicted in Figure 2. The user wants to access a web service outside her home organisation (1. in the figure). At first, the user selects her Identity Provider to whose web server she is then redirected for authentication (2.). Having authenticated the user, the Identity Provider provides the user's attributes to the Service Provider (3.). Based on the attributes, the service decides if the user is authorised to use the service.

Requirements for a federation are listed, for example, in [LIND04]. In addition to a federating software, a federation needs to agree on the syntax and the semantics of the attributes released, on a security infrastructure such as PKI for authenticity and confidentiality of the message exchange and on the arrangements to establish mutual trust between the organisations in the federation. As personal data is processed in the federation, attention should be paid to not compromising the user's privacy when releasing the attributes. For example, the EU directive on data protection [EC95] stipulates that only attributes relevant for the service may be released, and usually only with the user’s consent.

3. Comparison of Network and Application Access

Network and application level access have several things in common and some differences as well. In network access, the basic scene is that the user, while roaming outside her home organisation, wants to connect to the network. In application access, the user is perhaps physically in her home organisation, but wants to use services provided by some other organisation. However, nothing prevents a roaming user from accessing remote applications as well.[iii]

Application access technologies typically pay a considerable amount of attention to releasing user attributes properly from the Identity Provider to the Service Provider. In a minimal setup, the only attribute released to the service could be, for example, some role information, such as "the user is a computer science student at the University of Helsinki", that is enough to let her use an article database licensed only for the computer science department. In that case, the identity of the user is hidden from the service, following the EU’s data protection directive. A sophisticated service, such as a service for applying as a visiting student to a course in a neighbouring university, probably needs to get a large set of attributes about the applicant and her background in her home organisation (for example: her name, mail address, phone number, target degree, study subject, major, number of credit units so far etc). Unlike application access technology, network access technologies are typically not designed for passing user attributes from the Identity Provider to the Service Provider. On the other hand, if the RADIUS hierarchy is used, the user's identity is, nevertheless, revealed to the Service Provider, because the user's Identity Provider needs to be derived from the username that is in the format of *username@domain*[iv].

Roles are user's attributes that describe her relationship to her home organisation. Role-based authorisation, studied, for example, by Sandhu et al [SAND96, SAND01], relies on the user's role on deciding what services are permitted for her. In a large organisation, such as a university with thousands of users, role-based authorisation is attractive, reducing the complexity of user administration tasks.

Federating software with fine-tuned means for passing user's attributes to the Service Provider provides comprehensive means for role-based authorisation. Limiting access to a service (such as access to the network or to an article database licensed by a university library) to some smaller subgroup (such as staff and students of one university department) is easy and is up to the Service Provider. However, network access technologies, which have limited support for attribute release, leave authorisation actually to the Identity Provider. The Service Provider grants access, if the Identity Provider validates the user's credentials

[iii] In the case where the authorisation to an application is based on the client's IP address, it is worth noticing that VPN roaming solution is the only one in which the user gets an IP address from her Identity Provider's address space. In academic communities, databases licensed by libraries typically use authorisation based on the client's IP address.

[iv] Tunnelled EAP, such as PEAP or EAP-TTLS, can, however, be used so that the username is passed in a tunnel to the Identity Provider. Outside the tunnel, only the user’s domain is visible to the Service Provider for relaying the authentication.

successfully. In fact, authorisation is implicit; the user is authorised to access the network if she has a user account in an Identity Provider.[v]

4. Combining Network and Application Access Technologies

Maintaining two overlapping infrastructures for network and application access is ineffective. A single infrastructure for cross-organisational user administration could serve both network and application level access control. Maintaining and supporting one infrastructure for both network and application access would save work and costs for both Identity Providers and Service Providers. The next part introduces a model on how roaming access to network can be implemented on top of Shibboleth federating software. The model and its benefits and downsides are then compared to the models in Chapter 2.

4.1. Roaming Architecture on Shibboleth

The architecture of roaming access to network on Shibboleth is depicted in Figure 3. Shibboleth is a web based protocol that uses browser redirects to pass the user to her Identity Provider for authentication. After a successful authentication, the Service Provider uses SOAP to retrieve the user's attributes from the Identity Provider. As this paper is not intended to be an in-depth-introduction to Shibboleth, readers are encouraged to refer to Shibboleth architecture [SHIB04c] for description of the protocol and Shibboleth distribution [SHIB04b] for its implementation and deployment.

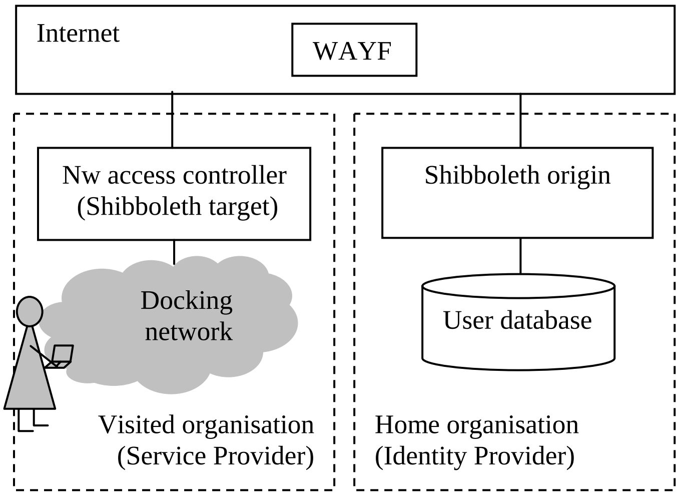

Figure 3. The architecture of roaming access to network on Shibboleth.

The three Shibboleth servers: the Shibboleth origin, the Shibboleth target and the Where Are You From (WAYF) are run on web servers and maintained by the Identity Provider, the Service Provider and the federation, respectively. The Shibboleth origin is the Identity Provider's ordinary Shibboleth server and, from its perspective, network access is just another service for which it provides user authentication and attributes. The Shibboleth origin authenticates the user and communicates with the organisation's user database to supply the Shibboleth target with the user's attributes. The WAYF is the central server that is run by the federation and provides the user a simple drop-down list of all the Identity Providers in the federation.

The actual "shibbolisation" of roaming access to network is done by integrating the Shibboleth target and the Network Access Controller, the component that prevents unauthorised roaming users from accessing the network. The Shibboleth target is the peer of the Shibboleth origin, retrieving attributes of the authenticated user using SAML and SOAP protocol.

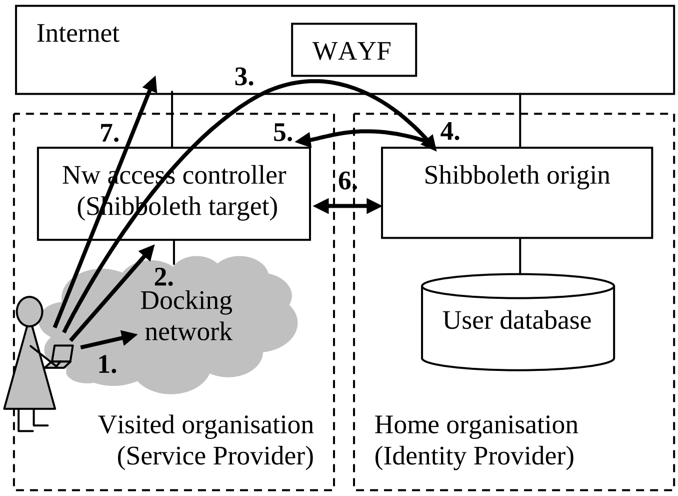

Figure 4. The message exchange in roaming access to network on Shibboleth.

Figure 4 describes the message exchange when a roaming user enters the docking network in a visited organisation.

1. The user activates her client device, connects to the docking network (for example, by activating her WLAN card or by plugging in to an ethernet socket) and gets an IP address via DHCP. However, the Network Access Controller initially blocks all her traffic in and out of the docking network, except the traffic to the TCP port 443 (SSL) of the WAYF and all the Shibboleth origin servers in the federation.
2. The user launches her web browser. The Network Access Controller, which has a web server with Shibboleth target components[vi] in it, captures the user's initial HTTP

[v] TF-Mobility's requirements document [TFMO04c] states that roaming access should be available for all users authorised for Internet access in any home organisation, but visited organisations may want to have more fine-grain authorisation.

[vi] In its current Apache implementation, the Shibboleth target consists of an Apache module and a daemon process running in the same machine.

request. As the web server's main page is protected by Shibboleth, the Shibboleth target is activated and first redirects the user to the WAYF.

3. In the WAYF server the user selects her Identity Provider from a drop-down list. The WAYF server redirects the user to the Shibboleth origin server of her home organisation.
4. The Shibboleth origin authenticates the user, for example, with a username and a password, which are provided to the origin by the user on a web form over HTTPS. The way the authentication takes place is up to the Identity Provider and the federation.
5. After a successful authentication, the Shibboleth origin redirects the user's browser back to the Shibboleth target with a SAML assertion containing a Shibboleth handle.
6. The Shibboleth target uses the handle to acquire the user's attributes from the Shibboleth origin. Communication takes place directly between the Shibboleth target and origin and uses SOAP and SAML.
7. Based on the user's attributes, the Network Access Controller decides if the user is authorised to access the network. If access is granted, it changes the firewall rule so that the traffic can flow between the client and the network.

Roaming access on Shibboleth does not have any specific needs for the client device. A web browser with support for SSL and HTTP redirect, a network interface card and DHCP client is sufficient.

For the visited and the home organisation, roaming access on Shibboleth requires that they are part of a federation which has made necessary agreements for trust establishment, organised the WAYF server etc. In addition, the Identity Providers' Network Access Controllers have to know the IP addresses of the WAYF and the Shibboleth origins in the federation.[vii]

4.2. Comparisons and Remarks

The Shibboleth based roaming architecture and the three roaming architectures presented in Chapter 2 have some common characteristics and also differences, which are summarised in Table 1.

Like the web redirection model, the Shibboleth model relies on capturing the user's HTTP connections in the Network Access Controller. To get access out of the docking network, the user has to open her web browser to initiate the authentication process. However, in Shibboleth, the user's web browser communicates directly on HTTPS with the Identity Provider, whereas in the web redirection model the communication with the Identity Provider is done by the Network Access Controller on top of RADIUS.

Table 1. Comparison of Shibboleth and the three roaming architectures.

Property	802.1X	Web redirect	VPN	Shibboleth
Uses HTTP connection capture		X		X
Uses RADIUS proxy hierarchy	X	X		
End-to-end security for credentials, e.g., user passwords	X		X	X
User identity not revealed to the visited network	(x)		X	X
The Network Access Controller has to know the Identity Providers' IP addresses (or use CASG)			X	X
All traffic routed through the Identity Provider			X	
Vulnerable to MAC address spoofing		X		X
(x): If tunnelled EAP is used, user identity need not be revealed to the visited network.				

Like in VPN and 802.1X models, the connection for user authentication is an end-to-end connection between the client device and the Identity Provider and, thus, the user's password is never available in cleartext to the visited organisation or any other intermediary, making trust establishment easier. However, in 802.1X and web redirection models, the user's identity is usually revealed to the visited organisation, because the RADIUS hierarchy needs the domain part of the username to route the authentication request to the Identity Provider. In VPN and Shibboleth models, neither the user's identity nor the password need to be revealed to the visited organisation, thus preserving the user's privacy.[viii]

Like the list of gateways in the VPN model, the Network Access Controller must have an extensive list of the Identity Providers' Shibboleth origins and the WAYF's IP addresses to which unauthenticated traffic is allowed in the SSL port 443. The hole in the firewall is required for letting the Shibboleth origin authenticate the user directly. However, once the authentication is done and the Network Access Controller allows the user to access the network, the traffic

[vii] Here it is assumed that the Shibboleth origin authenticates the user by itself. If the Shibboleth origin redirects the user to a separate login server for authentication, its IP address has to be configured to the Network Access Controller as well.

[viii] However, to investigate abuse, logs in the Shibboleth origin and target can be merged to reveal user identity.

need not be routed through any gateway in the Identity Provider. On the other hand, the CASG proposed for the VPN model can be applied for Shibboleth as well.

Like the web redirection model, the Shibboleth model is vulnerable to a MAC address spoofing attack. Neither of the two models provides a link layer traffic encryption or an integrity check, making it possible for an attacker to hijack the MAC and IP address of a legitimate user, for example, right after she has left the wireless network. The attack is made by reconfiguring the victim's MAC address to the attacker's client device, requiring skills and special tools from the attacker [TFMO04, p. 20].

Shibboleth uses WAYF for deducing the user's home organisation. In 802.1X and web redirection, the RADIUS protocol and the hierarchy of RADIUS proxies carry out the task; the user's home organisation is derived from the user's username that is in the format of *username@domain*.

A practical remark is, however, that usually different people are responsible for the network and the applications in an organisation. The network people are not necessarily familiar with application level authentication and authorisation technology. For the network people, it may be easier to deploy a technology, such as RADIUS or VPN, that they are already familiar with.

4.3. Benefits and Downsides

A benefit of the Shibboleth model is that it separates the authentication and the authorisation from each other. Authentication is always done by the Identity Provider, and the Service Provider is not involved in it. What the Service Provider has to do to let authentication happen is just to let the user communicate with her home organisation on SSL. Authorisation, in turn, is solely up to the Service Provider, based on the roles and other attributes released by the Identity Provider. The Service Provider can, for example, decide to prioritise the users with role "staff" in places where there is only a limited amount of network capacity available.

Another benefit of Shibboleth is that it unifies the network and application level access architectures, considering network access as just another shibbolised service. Maintenance and support for overlapping architectures becomes unnecessary. Furthermore, the user is able to enjoy a single sign-on, because the authentication takes place when she accesses the network, and she then has an existing session with her Identity Provider's Shibboleth origin. The existing session makes reauthentication unnecessary if the user later accesses another shibbolised service.

A downside of the Shibboleth model is that the technology is not as widely known and deployed as the other models utilising protocols that have been used for years. Besides Shibboleth, there are also other application level access technologies being used and developed, such as Liberty, whose interoperability may require extra effort. As a technology for fine-grained application level access, Shibboleth also needs a more complex federation with related trust fabrics underneath.

Another downside of Shibboleth is the scalability and security issue raised by the maintenance of the extensive list of Shibboleth origins in the federation. It can be, however, partially overcome with CASG.

5. Practical Experiments

To get practical experience, the Shibboleth based roaming architecture has been implemented and piloting started in the University of Helsinki. The shibbolised Network Access Controller was connected to the HAKA pilot federation, the federation of Finnish higher education that uses Shibboleth as the federating software. However, there were no modifications to Shibboleth implementation as the federation in use is just a configuration issue for the Shibboleth target. The architecture should be easily adapted to other Shibboleth federations as well.

5.1. Background Information of the University of Helsinki

The University of Helsinki is the largest university in Finland, with 39 000 users. The university has four campuses in Helsinki, the main one located in the centre of the city. There are also 6 other universities and several polytechnics in Helsinki.

HUPnet, Helsinki University Public network, has been available for the staff and the students of the University of Helsinki since 2001. Currently, HUPnet covers about a third of the university buildings in Helsinki, and the coverage is increasing as more base stations are installed. HUPnet also has ethernet sockets available for wired use. On an average day, there are about 50 different users connecting to HUPnet.

Situated in the heart of Helsinki, the university has been deliberate to open HUPnet for roaming users. There have been concerns that there would be considerably more roaming users coming in than going out, causing the cost to accumulate to the university. However, the university could open HUPnet to some limited user group, for example, to the staff and the faculties of other universities. Allowing access for staff and denying it from students requires role based authorisation, which is not supported by the web redirection roaming model. As the University of Helsinki has been active on Shibboleth deployment, it has now been integrated to roaming access as well.

5.2. Implementation

In the implementation, the Network Access Controller runs in a Debian Linux machine (Figure 5). When a user enters the docking network, a DHCP server gives her an IP address that belongs to a virtual LAN that the Network Access Controller separates from the Internet. Initially, the Iptables configuration of the Network Access Controller is configured to block all traffic from the user's IP address to the Internet, except the TCP traffic in port 443 to the Shibboleth origins in the federation.

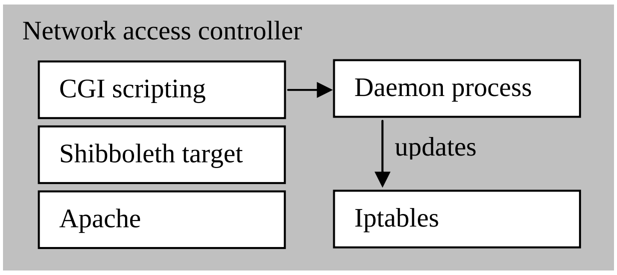

Figure 5. The shibbolised network access controller of HUPnet.

There are Shibboleth target components installed in an Apache web server that runs on the Network Access Controller. When the user opens her web browser, the Network Access Controller captures the web browser's initial HTTP request and provides the initial front page of HUPnet as the HTTP response. The user is asked if she is a local user (and to be authenticated against the local user database of the University of Helsinki) or a user from another university (and to be authenticated on Shibboleth).

To initiate Shibboleth authentication, the user enters a directory in the web server that is protected by Shibboleth in the web server configuration. The Shibboleth authentication and attribute exchange take place, and if the user has attributes required in the server authorisation configuration (that is, eduPersonAffiliation value ‘employee’), she is allowed to run a Perl script in the directory. The Perl script calls a daemon process running in the same machine and provides it with the IP address of the user. The daemon process, running with root privileges, makes necessary modifications to the Iptables configuration file of the Network Access Controller in order to let the user access the Internet.

In HUPnet, user authentication is valid for two hours at a time, after which it has to be renewed. A user can also initiate an explicit logout from HUPnet by calling another CGI script that restores the Iptables configuration.

The university of Helsinki is aware of the architecture's vulnerability to the MAC address spoofing attack and has accepted the risk of a successful attack, because all the attacker gains is just unauthorised access to the Internet. If Internet access is what the attacker wants, it can be obtained freely from the many public Internet "hotspots" at the university and there is little need to hack the university’s wireless network. On the other hand, as the attack requires special skills and tools, it is expected that the present architecture is sufficient to prevent ordinary users from getting unauthorised access, and the small number of attackers skilled enough is tolerable.

However, if MAC address spoofing becomes a problem, a sketch has been made of an improvement of making the web browser in the client device poll the Network Access Controller regularly on SSL. As the communication on SSL relies on a shared secret between the web browser and the server, the attacker replacing a client device in the docking network can be recognised and detached from the network. A downside of the improved architecture is that a temporary interference in the wireless network may block the polling and detach the user from the network.

5.3. Current Status and Future Plans

The shibbolised HUPnet has been launched for pilot use. Staff and faculty members are able to roam at the University of Helsinki if their home organisation belongs to the HAKA pilot federation. The source code of HUPnet has been made public and available for other institutions and federations for free as open source in SourceForge [HUPN04].

6. Conclusions

This paper presented an architecture that turns network access into just another service that can be used across organisational boundaries like application level services in a federation. Piloting the implementation that utilises Shibboleth federating software has started.

Combining network and application level access technologies reduces overlapping infrastructure and brings application level features, such as role-based authorisation and single sign-on, available also for network access. As a downside, application level access technologies are not yet so mature as network level access technologies. The architecture has to allow an unauthenticated user’s traffic to a small set of hosts in the Internet, making the maintenance of the service more difficult.

Acknowledgements

We want to acknowledge Sami Keski-Kasari for comments on the architecture and Carsten Borrman for the idea of introducing CASG also to the roaming architecture on Shibboleth. Acknowledgements also to Switch, which has provided lots of high-quality documentation on Shibboleth, and to Internet2 for the Shibboleth software itself.

References

ASEL04 The A-Select Authentication System. Alfa & Ariss b.v. http://www.a-select.org/

ATHE04 The Athens Access Management System. Eduserv. http://www.athens.ac.uk/

EC95 European Communities. Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

FEID04 Felles elektronisk identitet. Uninett. http://www.feide.no/

HUPN04 The HUPnet - Helsinki University Public network. University of Helsinki. http://hupnet.sourceforge.net/

LIBE04 Liberty alliance project. http://www.projectliberty.org/

LIND04 Linden M. 2003. Towards Cross-Organisational User Administration. Informatica 27, 3, 353–359

PAPI04 The PAPI AA Framework. RedIRIS. http://papi.rediris.es/

SAND01 PARK J. S., Sandhu R. 2001. Role-based Access Control on the Web. ACM Transactions on Information and System Security. 4, 1, 37–71.

SAND96 Sandhu R., Coyne E. J., Feinstein H. L.,Youman C. E. 1996. Role-based Access Control Models. IEEE Computer 29, 2, 38–47.

SHIB04 The Shibboleth project. Internet2. http://shibboleth.internet2.edu/

SHIB04b The Shibboleth test and software distribution site. Internet2. http://shibboleth.internet2.edu/release/shib-download.html

SHIB04c The Shibboleth architecture, working draft 01, 25 May 2004. Internet2.

TFAA04 Trans-European Research and Education Networking Association, Task Force Authentication and Authorisation coordination for Europe. Deliverable B.2: AAI Terminology ver 1.0.

TFMO04 Trans-European Research and Education Networking Association, Task Force Mobility. Deliverable G: Preliminary selection for inter-NREN roaming.

TFMO04b Trans-European Research and Education Networking Association, Task Force Mobility. Deliverable E: Inventory of VPN-based Solutions for Inter-NREN Roaming.

TFMO04c Trans-European Research and Education Networking Association, Task Force Mobility. Deliverable C: Requirements definition for inter-NREN roaming. Version 1.4.

WSFE03 Web Services Federation Language. IBM, Microsoft, VeriSign. 2003.