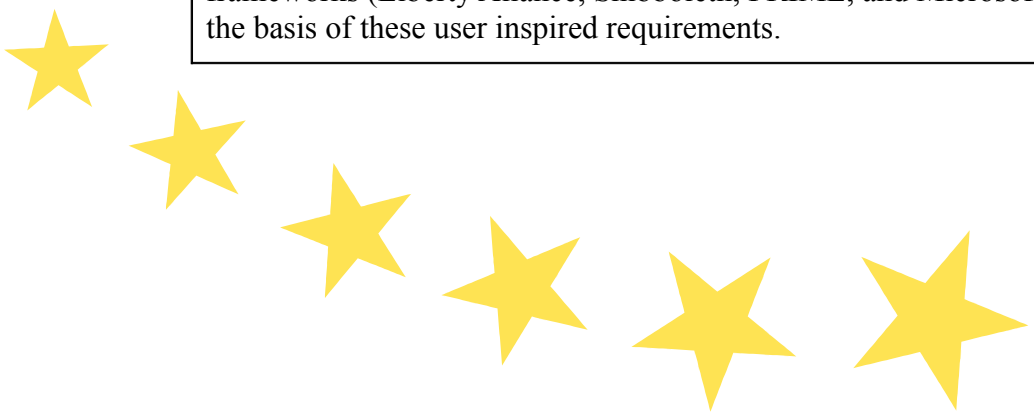
FIDIS

Future of Identity in the Information Society

Title:	"D3.12: Federated Identity Management – what's in it for the citizen/customer?"
Author:	WP3
	Stefanie Poetzsch (TUD)
	Martin Meints (ICPP)
	Bart Priem, Ronald Leenes (TILT)
	Rani Husseiki (SIRRIX)
Editors:	Ronald Leenes (TILT)
Reviewers:	Seyit Ahmet Camtepe (TUB)
Identifier:	D3.12
Type:	Deliverable
Version:	1.0
Date:	Wednesday, 10 June 2009
Status:	Final
Class:	Public
File:	20090506_fidis_D3.12 final 1.0.odt

Summary

This deliverable ventures into the federated identity management (FIM) landscape from the perspective of the individual end user. It provides an overview of features and requirements for FIMs and analyses four FIM frameworks (Liberty Aliance, Shibboleth, PRIME, and Microsoft Cardspace) on the basis of these user inspired requirements.



Copyright Notice:

PLEASE NOTE: This document may change without notice – Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.3	31/08/08	incorporated contributions: Bart Priem (TILT)
0.4	06/02/09	incorporated SIRRIX contrib: Martin Meints
0.5	27/04/09	initial draft: Ronald Leenes (TILT)
0.9	27/05/09	Draft final version Ronald Leenes (TILT)
1	10/06/09	Final version Ronald Leenes (TILT)

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1. Executive summary	Ronald Leenes (TILT)
2. Introduction	Ronald Leenes, Bart Priem (TILT), Martin Meints (ICPP)
3. FIM systems	Ronald Leenes
4. The Customer Perspective + scenarios for Federated IdM	Bart Priem, Ronald Leenes, Martin Meints
5. Concepts and Metrics	Bart Priem, Stefanie Poetzsch (TUD), Martin Meints, Rani Husseiki (SIRRIX)
6. Assessment of Federated IdM systems	Bart Priem (subsections 1 and 2) Stefanie Poetzsch (subsections 3-8) Rani Husseiki (subsections 9-11), Immanuel Scholz (section 6.3.9) Martin Meints (subsection 12)
7. Conclusions	Ronald Leenes

Table of Contents

List of abbreviations

AA	Attribute Authority
AES	Advanced Encryption Standard
CeL	Collaborative eLearning
FIM	Federated Identity Management
FIMS	Federated Identity Management System
HCI	Human Computer Interaction
HS	Handle Service
HTTP	HyperText Transport Protocol
HTTPS	Secure HyperText Transport Protocol
ICT	Information and Communications Technology
ID-FF	Identity Federation Framework
ID-WSF	Identity Web Services Framework
IdM	Identity Management
IdP	Identity Provider
IMS	Identity Management Systems
IP	Internet Protocol
LBS	Location Based Service
OASIS	Organization for the Advancement of Structured Information Standards
PET	Privacy Enhanced Technology
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PRIME	PRivacy and Identity Management for Europe
Rp	Relying Party
SAML	Security Assertion Markup Language
SHAR	Shibboleth Attribute Requester
SHIRE	Shibboleth Indexical Reference Establisher
SOAP	Simple Object Access Protocol
SOSSO	Single Organisation Single Sign On
SSO	Single sign-on
STS	Security Token Services
SSL	Secure Socket Layer
TLS	Transport Layer Security
UAC	User Account Control
WAYS	Where Are You From (Shibboleth context)

1 Executive Summary

Development of Federated Identity Management Systems (FIMS) has taken serious flight in recent years. Enterprises are no longer operating in isolation in their online identity management, but are increasingly realising that they can build 'circles of trust' and depend on identities provided by others as well as by identification, authentication, and potentially authorisation, provided by others and they are willing to provide the same services to their competitors and allies. The benefits of Federated Identity Management Systems for enterprises is relatively clear: each member of the federation wins by not having to set up an entire identity ecosystem and they can ride free on the reputation of others.

FIMS also have potential benefits for the customer, citizen and other kinds of individual end user. Usually, FIM incorporates a single set of credentials that allow the individual to use single sign-on to access services provided by different service providers. This may limit the number of username/password combinations the user has to manage and remember.

Identity management is more than access control to resources, which is the driving reason for enterprises to engage in FIM. Individuals also engage in identity management. They play different roles in life, both offline as well as online, and provide different 'faces' of themselves in these roles and therefore use different partial identities. I am not only a legal academic scholar with a strong interest in privacy and identity management, but also partner of my spouse, compulsive gadget shopper, builder of autonomous lawn mowers, etc. I want to keep these spheres separate. Not everyone needs to know about my shopping habits and affection for autonomous robots. How does this (socially inspired) perspective relate to the enterprise access control to resources perspective?

This deliverable tries to provide an initial answer to this question by developing requirements and metrics to assess FIMS from a user perspective and applying these to a set of existing FIMS.

The document first provides a brief overview of the developments in the identity management landscape. It describes how an evolution from enterprise centric identity silos, towards federated identity management, and more recently towards user-centric identity management can be observed. Next it provides a working definition of Federated Identity Management (Systems).

Chapter three provides a brief justification why we focus our attention in this deliverable on Liberty Alliance, Shibboleth, PRIME, and Microsoft Cardspace, while we could equally have picked other initiatives and systems. The main reason is that these four represent a balanced mix of enterprise centric approaches Liberty and Shibboleth), user centric approaches (PRIME, Cardspace), and a large vendor backed approach (Cardspace).

Chapter four elaborates on the individual (end-user/customer) perspective on FIM. The chapter argues that audience segregation and role playing, convenience and usability, and security are key concerns from this perspective.

Chapter five translates these concerns into specific requirements and metrics that allows the four FIM frameworks to be compared and assessed. An important starting point for assessing the various frameworks is informational self control, both as a goal in itself (to promote and protect autonomy), as well as a instrument to protect individual privacy. Secondly, as identity management, required for access control to resources at least, for many people is not an aim in itself, but rather a means to achieve other goals, we take into account a set of customer adoption requirements. Next, a set of more technical aspects regarding the management of

(partial) identities is distinguished, including authentication management, policy management, history management, context detection and personal data storage. Finally, security on the different levels completes the set of tangible requirements.

Chapter six provides an extensive discussion of the four frameworks along the lines of the requirements which is too extensive to summarize here.

Chapter seven provides a summary of the most salient aspects of the four frameworks as well as a number of comparative observations.

What clearly shows when looking at the four frameworks differ significantly in their approach, focus and maturity. Liberty Alliance and Shibboleth start from an enterprise centric approach, in Liberty's case a federation of enterprises, in Shibboleth's case institution(s) of higher education. The enterprise is the principal party in providing and managing identities. The individual is the (passive) user. PRIME and to a lesser extent CardSpace depart from the perspective of the user as the central actor. Here the individual is really at the steering wheel of her identity management. Both systems allow the user to self create identities, as well as make use of provisioned, certified identities. The user-centricity also shows in the way users can define and negotiate policies regarding personal data disclosure and use.

Liberty and Shibboleth already have an extensive user base and Cardspace, given its Microsoft roots is in an advantageous position. PRIME, which started as a European research project and hence focused on pushing (privacy) envelopes in this respect lags behind. There is no off the shelf PRIME implementation.[1]

Liberty and Shibboleth don't require any download and/or installation on the part of the user. Liberty is a set of standards that can be implemented by technology providers (on the server-side of transactions). Shibboleth consists of a package that can be installed on the service providers IT infrastructure. Both systems provide the user with web based authentication tools. PRIME depends on client and server Middleware for its advanced functionality. This may be an obstacle to widespread deployment and adoption. Cardspace also depends on Middleware, but in this case it is tied in major operating systems (Vista and Windows 7), which facilitates large scale adoption.

With respect to security there are many similarities because most systems use the same underlying mechanisms (SAML), which means they are prone to the same risks. Regarding trustworthiness from the perspective of the user there are significant differences. Liberty Alliance has to rely on the reputation of a potentially diverse large set of identity providers, which may be unfamiliar to the user, as well as relying parties of different stature. Shibboleth currently is mainly implemented in configurations where the user knows the identity provider (his/her university or school) as well as the relying parties which facilitates the trust relation. Trustworthiness in PRIME has different aspects. On the one hand, identity is very much in the hands of the user herself (which should be trustworthy). Also, sophisticated technology (cryptography, anonymous communication) should enhance the (technical) trust level significantly over other approaches, yet trustworthiness here is undermined because the technology is opaque and unfamiliar to most common users. Do they trust technology they don't understand? Cardspace shares PRIME's approach to user-control. Both rely on decentralised storage, which could benefit user trust in the system.

[1] Although the PRIME follow-up project PrimeLife (visit http://primelife.eu) may change this.

2 Introduction

2.1 Scope of this document

This document is directed to an audience of academics, EU policy-makers, experts from technological, social science and legal disciplines and interested citizens. Purpose of this deliverable is to describe federated IdM and what's in it for the end-user, by means of defining relevant concepts and metrics with which we can compare the various IdM projects with respect to privacy and user control. Its focus lies on the interests of citizens and consumers. It contains an overview of a number of the existing federated identity management systems.

2.1.1 IdM evolution[2]

Individuals are right at the center of online identity management, because it concerns the management of their identities, and because decisions are made on the basis of these identities. From an individual's point of view, the concept of identity management therefore not only relates to the access control regarding resources. It also, or maybe even rather, relates to how they are manifested and represented, and how this is aligned to their own perception of their identity. Identity management in this sense strongly relates to role playing and presentation of self. Individuals should be able to act as autonomous individuals, be able to control their reputation, and have insight in the way they are judged by others in a specific context. The online environment facilitates the construction and maintenance of projected and imposed personae. Data can easily be collected and combined into rich personae, transcending the context in which individual bits of information were disclosed. The decontextualisation and combination of data from different sources makes it difficult for individuals to control their different digital personae. This undermines the capabilities for people to control the image they present in different contexts and to segregate audiences online. The need to do so exists online just as it does offline. People engage in different kinds of activities online (e.g. public, commercial, and intimate) and need to be able to construct matching identities that meet the behavioural rules and requirements set by these different environments. Important values such as reputation, dignity, autonomy, judgement, and choice are closely related to the individual perspective on identity management. When people cannot determine or control their identity, they may become overexposed, confused, or discriminated, for example. Human beings have an interest in naming and sorting themselves (Gandy 1993; Raab 2005) and to play different roles. Sometimes they may even need to be anonymous and unidentified (e.g. for purposes of emotional release, relaxation, unpunished criticism, and making mistakes). Individuals appreciate to have a diverse and autonomous life, and need to be able to adapt their identities to the environment they engage in. Even though identity management is not usually the primary goal of the individual, which may explain why many people are not eager to invest time and money in IdM systems (Dhamija 2008), the social values outlined previously warrant the individual perspective to be taken into account in the development of IdM systems.

2.1.2 From identity-'silo's' to federation

Different models for online identity management have been developed in recent history. Traditionally, identities were managed in so-called corporate identity silos. In this model one single identity management environment is operated by a single service for a specific group of

[2] This section is based on the author's contribution to part 1 of the PRIME book (PRIME 2009).

users. Hence, every (online) service had its own identity management system built on their own requirements for authorisation and identification of individuals. From the perspective of users of multiple systems this means that they have to maintain an identity (account) for each and every service they use, which in practice means several sets of passwords and usernames. The "silo-model" is still a dominant model for identity management on the internet. An obvious drawback of this scheme from the perspective of the users are that it requires them to provide the same (personal) information for every new online service. The construction of identities in these systems is guided by rules (implicitly) set by the provider of the service. Each account is identified by an identifier. Sometimes these identifiers can be freely chosen, sometimes they have to satisfy certain rules (e.g., at least one number, 8 characters long), or be a valid email address. Individuals are therefore sometimes forced to create different identities (or rather the identifiers that identify the identity) even when they want to use the same identity across domains. Or, in the case of being obliged to use a valid email address, they may have to use identities they don't want to use for a particular use. As a result of these practices two effects on identity construction are visible: one, difficult to remember identifiers as a result of the rules on identifiers imposed by the service provider, and two a convergence of identities to a limited set of partial identities as a result of the requirement to use email addresses as "usernames". Furthermore, the "silo"-approach has resulted in many identity "one-offs" and an ad-hoc nature of internet identity even though the identities in these silo's can be managed by, for instance, storing passwords and usernames in software (password-managers) on a local computer or on a server (Olsen 2007; Cameron 2005).

A next step in the development of IdM systems has been the development of single organisation single sign-on (SOSSO)(Olsen 2007). Here individuals gain access to different resources (applications, web sites) within a single entity's domain once they are authenticated. Well known in this domain, and underlying many current systems ranging UNIX implementations to the Windows Domain/Active Directory architecture, is Kerberos. This computer network authentication protocol developed at MIT as early as the beginning of the 1980s, makes use of a trusted third party, termed a key distribution center (KDC), which consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS). Kerberos works on the basis of "tickets" which serve to prove the identity of users.

SOSSO systems, in general, slightly alleviate the individual's burden of having to cope with potentially different identities within such a domain. Usually it also limits the individual's capabilities to use different identities within a certain domain (e.g., the association of an account to an email address limits the number of accounts an individual can establish without also obtaining new email addresses). Effects of SOSSO are the collapse of different (social) contexts within a given domain controlled by the enterprise and linkability because the IdM provider can recognize the individual access to the various resources. SOSSO makes coping with enterprise centric IdM easier for the individual within a particular domain (e.g., company), but does not help when multiple domains are involved.

Multi-organisation single sign-on (e.g., Microsoft .Net Passport) aims to solve this problem, as well as lessen the burden of implementing and maintaining IdM systems within each enterprise in a federation (Olsen 2007). In this model, authentication is outsourced to a trusted identity provider (IdP). The IdP identifies and authenticates the user and provides a credential that can be used to access resources from associated service providers. Drawbacks of this model are that the IdP stores the user's data which creates security vulnerabilities. Furthermore, the attendance of one single IdP in all interactions on the Internet creates linkability because the IdP can trace the user after authentication. It also creates a

vulnerability (and convenience) because relying enterprises depend on a single IdP involved in all transactions.

Enterprise centric federated identity management (e.g., Liberty Alliance) addresses the problems related to the dependence on a single IdP in a federation, by allowing any number of IdPs to handle authentication. The user authenticates with any of the IdPs in the federation and subsequently cab access resources at each of the entities in the federation (where the user has proper authorisations). Some federation schemes not only handle authentication, but also allow the transfer of attributes between the federates (Olsen 2007). Federated identity schemes again limit the burden for individuals of having to cope with multiple identities when they want to use a single identity, but do not address the needs of individuals when they want to use different identities for different activities in the federation. The advantages mainly benefit the enterprises which can achieve costs savings arising from a shared scheme based on a standardised, interoperable architecture, and the outsourcing of authentication and IdM to professional identity providers. Federated IdM systems also increase convenience for the user to make use of several different services and make identities portable. Furthermore, they can create opportunities for organisations to ease the process of registration, authentication, and authorisation. In addition, these systems allow for cost saving on the retention and collection of data and can create new business opportunities (see: Olsen 2007).

2.1.3 A definition of Federated IdM

Identity federation is based on a conceptual separation between service providers (SP) and identity providers (IdP) and concerns the arrangements that are made among several organisations and individuals, that let entities use the same sets of identification data, to get access (and authorisation) to the several different (otherwise autonomous) services offered by all the organisations associated with the system of federation. Hence, identity federation aims to make digital (or electronic-) identities usable in different domains. This entails mutual trust establishment between "secured domains of control" which might be associated with different organizations. The cross-domain identification and authorization of users based on single "federated identities" allows those users to seamlessly access services in different domains. On the other hand, it avoids unnecessary redundant user administration by several systems. An important aspect of FIM is that not necessarily one specific Identity provider is needed. From that point of view federated identity management systems can be understood as a trust relationship between so far separate identity management domains and related systems.

Identity federation is a broad concept. It can relate to systems with both a high level of security as to systems with a low level of security. Moreover, federated IdM systems come in the form of user-controlled systems, but are usually controlled by businesses or governments (as in the Dutch DigiD case). In addition, FIM-systems can be 'token-based' or 'anonymous-credential-based', meaning that some systems rely on the mediation of Identity Providers (IdP) between Relying party (Rp) and the user, whereas other systems let the user construct her identity out of anonymous credentials.

However, FIM-systems have in common that agreements, policies, and standards are used to make identities portable. Also, they often rely on schemes of Single-Sign-On (SSO), even though credentials and identities may be stored at different locations, under different conditions.

Combinations of the following features are provided by federated identity management:

- *Identity provisioning*: Based on the registration to one service, respectively identity provider, several services providers are able to generate accounts for that particular user and based on this account to authenticate her.
- *Single-Sign On*: Based on a login to one service, respectively identity provider, the user is also able to user her existing accounts for other service providers.
- *Attribute exchange*: The linkage of several attributes of the user to one digital identity in the domain of one service, respectively identity provider, could be requested from other service providers as well, at least under certain conditions. The exchange of attributes also facilitates authorisation.

From the user's point of view federated IdM makes it more convenient for the user to gain access to several services. It relieves her from the burden of remembering and utilising several account names and passwords, for example. Furthermore, FIM can be beneficial for professional organisations, because data storage and identity distribution can be made more efficient. Moreover, FIM makes it possible to outsource storage of data and provision of identities. Besides these advantages of federated IdM there exist also challenges with regard to privacy and security issues for users' personal data as well as the security goals of the organisations taking part in the federation.

2.1.3.1 Holistic approaches and stand alone technologies

With respect to federated identity management initiatives abound, both on a detailed level as on a conceptual, holistic level. Some systems are developed for a particular area, such as education (such as Aselect for Dutch universities[3]), or (Dutch) public sector (such as DigiD[4]) and (intentionally) have limited applicability. Other systems are intended for large audiences and multiple settings, such as Microsoft Cardspace and Liberty Alliance. In this deliverable we will limit ourselves to the latter, more general systems.

2.1.3.2 What is outside the scope of federation

In recent years a shift from an enterprise centric view to a user-centric view can be observed. Notions, such as `Identity 2.0' (Sxip, Microsoft Cardspace, Higgins, PRIME, etc) belong in this sphere. In these initiatives the IdP is no longer in the centre of issuing and creating identities, but rather the user is. In user-centric identity management the individual's interests are acknowledged in the sense that they manage their own personal data and obtain credentials from identity providers which they can use in their interaction with service providers. Systems based on anonymous credentials even give the user and relying party the opportunity to use identity attributes without the use of a central identity provider (PRIME 2008c). Such systems make it possible to really put the user at the center of IdM, and thus indicates a shift from an enterprise-centric perspective to a user-centric perspective. The user-centric model provides the user more control over the way they present themselves to others. If designed properly, they assure the necessary level of privacy in the online environment.

Although many developments regarding user centric identity management take place, genuine user centric solutions that offer full support for partial identity management are not widespread yet. Also take into account that federated identity management does not necessarily provide support for different pseudonyms or different partial identities. The core feature of federated identity management is building on already existing trust within a federation.

[3] See http://a-select.surfnet.nl/

[4] See http://digid.nl/

2.2 Structure and content of this document

First, we will provide an overview of the systems to be assessed in this deliverable including their background and characteristics. Next a description of the end-user view on IdM will be provided. This overview results in a list of concepts and metrics to be used for assessing the different systems. The main part of the document consists of the actual assessment. Finally some conclusions are provided in the final chapter.

2.3 Relation with other documents

The FIDIS project has produced several deliverables related to identity management systems and that should be consulted to get an overall picture on (federated) identity management.

Notable FIDS deliverables are

- D8.3: Database on Identity Management Systems and ID Law in the EU

  This document consists of two parts. Part A puts forward a structure for a database of Identity Management Systems (IMS). Two designs for a database are laid out: a prototype with 29 fields (section 3) and an extended version with a total of 138 fields (section 4). The prototype has been implemented and is accessible online at http://www.jrc.es/projects/ims/imsintrodb.cfm. This document also includes a user manual (section 5) and the technical specifications for the database (section 6). Records will continue to be added to the database of IMS over the coming months and the document describes the next steps in the development process.

  Part B introduces a database of ID laws, the Identity Law Survey (IDLS). Section 8 provides the context, and section 9 presents the initial structure of the law survey used to build a prototype, available at http://rechten.uvt.nl/idls/. Sections 10-11 outline a revised database structure, and sections 12-14 provide the interface requirements, user manual, and maintenance plan. The aim is to develop a simple and user-friendly database, providing the public with basic information and knowledge on ID-related laws in the EU and North America.

- D3.1: Overview on IMS

  This document provides an overview of existing identity management systems (IMS). Different types, classes and subclasses of IMS are identified, described and illustrated by examples of existing IMS. To get an overview of the variety of existing technical implementations different designs of IMS are presented. Privacy enhancing mechanisms are developed and selected corresponding privacy enhancing technologies (PET) are shown as examples of existing implementations of those mechanisms. Finally an overview is presented of current research and development activities on IMS and conclusions, especially from the FIDIS Network of Excellence.

- Independent Centre for Privacy Protection (ICPP) & Studio Notarile Genghini (SNG): Identity Management Systems (IMS):

  This report presents a multidisciplinary framework for privacy-enhanced identity management (IdM), which includes technical, legal and sociological perspectives for the definition of terms and presents usage scenarios. However, a major focus of the ICPP/SNG comparison study is the analysis of available identity management applications and a survey on expectations with regard to identity management systems.

Outside the FIDIS project there are numerous white papers and papers about federated identity management systems. These will be referenced in the text of the current deliverable.

3 Assessed FIM systems: our choice

As mentioned in the introduction there are many federated identity management initiatives. In this deliverable we can only address a couple: Liberty Alliance, Shibboleth, PRIME, and Cardspace. Our choice is inspired on the following reasons.

3.1 Liberty Alliance

The Liberty Alliance is a relatively old initiative regarding federated IdM. It was established in 2001 by approximately 30 organizations to establish open standards, guidelines and best practices for identity management. Today it continues to focus on these objectives, with a global membership of more than 150 organizations, including technology vendors, consumer-facing companies, educational organizations and governments from around the world, as well as hundreds of additional organizations that participation in Liberty's various open community Special Interest Groups (SIGs).

"The Liberty Alliance Project is an alliance formed to deliver and support a federated network identity solution for the Internet that enables single sign-on for consumers as well as business users in an open, federated way. [...] In a federated view of the world, a person's online identity, their personal profile, personalised online configurations, buying habits and history, and shopping preferences are administered by users, yet securely shared with the organisations of their choice. A federated network identity model will enable every business or user to manage their own data, and ensure that the use of critical personal information is managed and distributed by the appropriate parties, rather than a central authority. The role of the Liberty Alliance Project in all of this is to support the development, deployment and evolution of an open, interoperable standard for federated network identity. The vision of the Liberty Alliance is to enable a networked world in which individuals and businesses can more easily conduct transactions while protecting the privacy and security of vital identity information."[5]

The Liberty project is relevant because it endorses (and sets) open standards and comprises a large community of important ICT vendors and users.

3.2 Shibboleth

The Shibboleth® System is a standards based, open source software package for web single sign-on across or within organizational boundaries. The Shibboleth project was started in 2000 under the MACE (Middleware Architecture Committee for Education), which explains the popularity of Shibboleth in institutions for higher education. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner. The Shibboleth Project, one of the MACE-Internet2 Middleware Initiatives, is developing architectures, policy structures, practical technologies, and an open source implementation to support inter-institutional sharing of web resources subject to access controls.

The Shibboleth software implements widely used federated identity standards, principally OASIS' Security Assertion Markup Language (SAML), to provide a federated single sign-on and attribute exchange framework. Shibboleth also provides extended privacy functionality allowing the browser user and their home site to control the attributes released to each application. Using Shibboleth-enabled access simplifies management of identity and permissions for organizations supporting users and applications. Shibboleth is developed in an

[5] http://www.projectliberty.org/.

open and participatory environment, is freely available, and is released under the Apache Software License.

3.3 PRIME

The PRIME project, an EU and Swiss government funded FP 6 project, aims to develop a working prototype of a privacy-enhancing Identity Management System. Although PRIME does not represent an existing solution on the market, it aims to push the technical envelope regarding privacy-enhancing user-centric identity management far and hence represents 'a standard' to which the other systems can be compared.

"The PRIME Architecture can be seen as a generic architecture that defines a feasible way of bringing multiple complementary technologies from the privacy-enhancing technology (PET) space together with the goal of improving the privacy protection for people that interact over an electronic communication network such as the Internet.

The added value of PRIME with respect to systems developed by other initiatives can be best summarized as follows: 1) PRIME defines methods for establishing trust by data exchange between two parties in a semi-automated way; 2) PRIME strives to reduce a user's need in excessive trust in other parties such as service providers or certifiers regarding proper data handling; 3) PRIME allows a user to make a semi-automated assessment of a service provider that allows her to better judge the trustworthiness of the service provider and thus to make a better informed decision on the release of data; 4) PRIME provides new approaches to the enforcement of agreed data handling policies with a greater degree of expressivity and automation.

The establishment of trust is performed by a mutual release of possibly certified data between two parties. The mutual release of data together with an agreement of data handling policies that need to be applied on those data is called negotiation. The negotiation is to a large extent driven by a new access control policy mechanism developed in PRIME. The data handling policies of PRIME comprise on the one hand aspects that are enforceable by access control and, on the other hand, aspects that are unrelated to access control (privacy obligations). The goal of a negotiation is to allow both involved parties to establish sufficient trust in the respective other party by the provided attribute statements. A wide range of attributes are considered useful for establishing trust. Examples are certified attributes of persons (e.g., as contained in an electronic id card), attributes characterizing organizations (e.g., attributes in a privacy seal), attributes characterizing the assurance state of a data processing system (e.g., integrity, availability of certain enforcement mechanisms), attributes about the reputation of a party (in general their conduct in previous interactions).

The reduction of trust requirements is one of the key goals of PRIME with the goal of putting the user in a better position, thereby reflecting strongly the user-centric approach of PRIME that is directly implemented in the architecture. A key technology for reducing trust requirements is the use of advanced technologies for data exchange.

PRIME builds on top of a powerful anonymous credential system, identity mixer, that operates in a strong model for identity federation in terms of privacy. Such a system allows a service provider to authorize a user without necessarily establishing linkability with other authorizations of this user at this or other service providers. This reduces the possibility of excessive profiling of users by parties they interact with.

A user can assess various properties of a service provider in order to better judge the trustworthiness of the service provider. The assessment is mainly based on assurances that the service provider can communicate to the user on request. Those assurances cover properties

of the organization, its processes, and its data protection system in place, particularly also its individual platforms. Particularly, the availability of certain protection mechanisms, e.g., the availability of a PRIME life-cycle data management system, can be asserted to users. Reputation data can serve as a useful data source for a trust assessment of another (unkown) party as well.

The enforcement of policies for data once they have been released is taken further in the PRIME project when comparing with the state of the art systems. The policies we are referring to are the data handling policies that are agreed for data being released.

The enforcement comprises two parts: The more traditional enforcement of access control constraints using advanced policy mechanisms and also the enforcement of privacy obligations by a new approach of automated enforcement of privacy obligations. The latter has been designed specifically with performance, scalability, and longevity in mind for practical viability."[6]

3.4 Microsoft Cardspace

Microsoft's Cardspace is an initiative from one of the worlds largest software developers with a very big user base. Any development by Microsoft therefore is bound to have an important impact on the identity landscape.

3.5 A brief comparison

The four contenders in this deliverable represent different aims, developers and scopes.

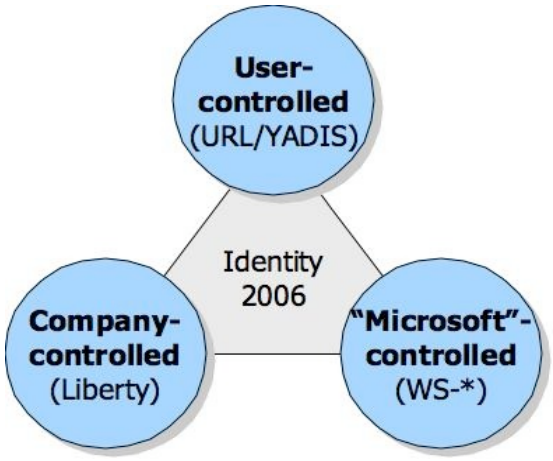


Figure 1: The identity landscape in 2006 according to Johannes Ernst (http://netmesh.info/jernst/Digital_Identity/three-standards.html)

Ernst, on his identity blog distinguishes three pillars of identity management systems in line with the overview of IdM systems provided in the previous chapter. He exaggerates a bit in the picture (see Figure 1), but the main gist seems valid:

“

1. The **company-controlled identity pillar**, which is rooted in the Liberty standards. This pillar is ready-made for corporate adoption: identity is "given" to the individual by the corporation (e.g. the employer), and it is the corporation that decides which identity attributes are managed and shared with whom. Even if the corporation gives

[6] Dieter Sommer, Introduction to chapter 10: The PRIME architecture, The PRIME Book, 2009.

the individual many choices, it is ultimately the corporation who decides whether or not to give those choices to the individual.

2. The **"Microsoft"-controlled identity pillar**. I have put quotes around Microsoft, because on one hand, Microsoft of course does not control WS-* (at least not by itself) which is a major component of this pillar. On the other hand, the adoption of this pillar will be driven by Windows Vista and InfoCard adoption and the particular subset of WS-* that Microsoft has chosen to support (unless of course, somebody built it into Linux or all cell phones ... but so far, I have not heard about an announcement of this kind, so I don't think I'm wrong to identify Microsoft as the major driver here)
3. The **user-controlled identity pillar**, where the individual is fully in control, over identity providers, over attributes, over whether or not to have an identity or how many, over the software to run, and over the feature set associated with their identity. It's most visible sign is the use of URLs to point to people, just like we use URLs to point to companies or documents. This pillar is rapidly coming together in the YADIS community, which essentially facilitates an open marketplace of interoperable identity-related features from which the individual may pick as many or as few as they like."[7]

The enterprise pillar is represented in the current report by the Liberty Alliance (for enterprise centric) and Shibboleth (for 'educational corporation' centric). The Microsoft controlled pillar is represented by Microsoft Cardspace. The user controlled pillar is represented by PRIME.

3.6 Other systems

Higgins is an open source framework that enables users and other systems to integrate identity, profile, and relationship information across multiple heterogeneous systems. Higgins unifies all identity interactions (regardless of protocol/format) under a common user interface metaphor called i-cards. Higgins enables developers to write to a common API for Identity management, rather than needing to support multiple identity management systems individually. Software applications written to Higgins will allow people to store their digital identities and profile information in places of their choice and to share the stored information with companies and other parties in a controlled fashion.[8]

The **Bandit** project is an open source collection of loosely-coupled components to provide consistent identity services. It implements open standard protocols and specifications such that identity services can be constructed, accessed, and integrated from multiple identity sources. Portions of the identity services are an implementation of the Higgins trust framework. The Bandit system supports many authentication methods and provides user-centric credential management. On this base of a common identity model, Bandit is building additional services needed for Role Based Access Control RBAC and for the emission of records to verify compliance with higher level policies.[9]

OpenID is an open, decentralized standard for user authentication and access control, allowing users to log onto many services with the same digital identity. As such, it replaces the common login process that uses a login-name and a password, by allowing a user to log in once and gain access to the resources of multiple software systems.

---

7 http://netmesh.info/jernst/Digital_Identity/three-standards.html

8 http://en.wikipedia.org/wiki/Higgins_trust_framework

9 http://en.wikipedia.org/wiki/Bandit_project

An OpenID is in the form of a unique URL, and is authenticated by the user's 'OpenID provider' (that is, the entity hosting their OpenID URL). The OpenID protocol does not rely on a central authority to authenticate a user's identity. Since neither the OpenID protocol nor Web sites requiring identification may mandate a specific type of authentication, non-standard forms of authentication can be used, such as smart cards, biometrics, or ordinary passwords.

OpenID authentication is used and provided by several large websites. Organizations like AOL, BBC, Google, IBM, Microsoft, MySpace, Orange, PayPal, VeriSign, Yandex, Ustream and Yahoo! act as providers.[10]

[10] http://en.wikipedia.org/wiki/Openid

4 The end-user perspective on FIM

ICT facilitated communications and transactions lack the characteristics of normal face-to-face contact. Because of this, individuals, government, and private enterprises face a significant challenge in the online identification of themselves, and their transaction partners. Especially when it is necessary to be certain about specific characteristics of each other, e.g. for accountability or credibility, identity management systems are of key importance.

Many identity management solutions are being developed by organisations, meeting their own requirements for IdM systems[11], which, as we have seen already used to focus on access control to their resources. Customers and citizens potentially have different and additional requirements because they interact with multiple service providers. This chapter aims to provide a brief end-user perspective on identity management by describing the customer/citizen point of view to identity and identity management, followed by some customer scenarios.

4.1 Role playing and proving claims

In the online environment, identities are being used by customers for several purposes, like gaining access to specific services or for making agreements with others. From an individual's point of view the concepts of identity and identity management relate to more than just getting access to services or proving who they are. Individuals may also relate the use of digital identities to how they present themselves to others and how the resulting representation is aligned to their own perception of self. Customers have an idea of 'who they really are' (which idea is fluid and dynamic), but use several static representations[12] (partial identities) of themselves throughout different contexts and relations.[13] Individuals use several different partial identities throughout life for the sake of playing different roles in life, e.g., of mother, citizen, employee, or consumer[14]. These partial identities are composed of different attributes, and are identified by (potentially different) identifiers (e.g., different usernames/passwords for different services). To avoid confusion and deception, the individual has an interest in aligning, segregating, and controlling, in other words managing their different (partial) identities to maintain consistent relations with others and to synchronise the static representations with her 'real' identity.

It is important that one can effectively prove that the attributes and identifiers provided are valid and thus that the individual actually is who she claims to be (authentication). In the offline world, proving claims is facilitated e.g., by means of the environment (e.g. where we are), self-assigned characteristics (e.g., clothes, physical presence), and credentials provided by others (e.g., driving license, passport). For the online world, people also need means to prove their claims concerning their identity. In comparison to the offline world, this is more challenging online, because online we usually cannot use the traditional trust tokens, such as our passport[15], and because roles and contexts succeed each other more seamlessly and rapidly. Moreover, identities are easily stored, copied, and transferred, which facilitates

[11] And may be concentrated on business processes instead of the user point of view.

[12] Which can be projected by the individual, but can also be imposed, see: Clarke (1994).

[13] FIDIS WP2. (2005). D 2.1: Inventory of topics and clusters (FIDIS Deliverables): FIDIS Consortium. Fidis D 2.1.

[14] Ibid.

[15] Some countries have issued smart-card based identity cards that allow individuals to substantiate their claims. Examples are Spain, Italy, and Belgium. Germany is in the process of issuing a new ID card which can also be used in electronic transactions. See http://www.bsi.bund.de/bsi/reden/20080821EICC_Erice.pdf

identity theft and misuse[16] [17]. The rise of identity fraud in recent years further undermines online trust, which makes it even harder to obtain online services without proper authentication. At the same time, the need for implementing an end-user perspective in IdM system increases: ICTs are being used for an increasing number of purposes, contexts,[18] and applications[19].

The increasing use of ICTs in several contexts has increased the need to know how we represent ourselves online and who we are interacting with. However, whereas role playing and proving claims is obvious in the normal offline world, online identity management seems to be more burdensome and less obvious to consumers.

4.2 Convenience and usability

The online world can be a opaque and incomprehensible place for customers trying to manage their digital identities. For example, one single online session may already require customers to remember and fill-in several usernames (and passwords). Moreover, online services can have extensive policies, requiring customers to scrutinise several statements (in a foreign language, regulated by foreign legislation), before getting access to a service. For the end-user, it is often an impossible task to remember in which circumstances and under what terms they have used a service on the internet. Currently, registration or access to online services often requires superfluous, but compulsory information disclosure (form filling).

Online identity management introduces many hurdles for the end-user, which may lead to users refraining from using certain services or online interaction at all. Online IdM systems may also induce the end-user to behave different from their actual preferences (Berendt 2005). For example, extensive policies prevent customers to read these policies at all (Milne 2004), users forget which agreements they have previously made and they may provide false data when personal data is requested. In addition, when applications are complex, customers may choose to use the default settings, which may not necessarily correspond to their personal preferences or their privacy interests. Ultimately, this can lead to customers making decisions that are detrimental to their own interests (dhamija 2008). The complexity of the online world may add difficulty for customers to actually understand why they should use an application or service (Shostack 2003).

Online identity management is not what individuals care for when they interact with service providers. They engage in online transactions for the sake of transactions, the IdM is a necessary and unavoidable nuisance in many cases. Individuals often lack the interest, means, time, or knowledge to manage their identities in a way that suits their interests. To avoid that customers from engaging online interactions or make wrong decisions, it is important that IdM systems take into account the usability of the system, its default settings, and the eventual use of the system by customers.

[16] See FIDIS D 4.2 on identity fraud.

[17] Cf. for example the phishing activity trends on www.antiphishing.org/, last visited August 11, 2008

[18] Web 2.0. applications, which require more interaction, are being developed both in the field of social media as for government and commercial services.

[19] We are moving to an 'Internet of Things': computing becomes 'ubiquitous' so that individuals in the future may be supported by several devices that are connected to the internet.

4.3 Security (from the user's point of view)

Another aspect of IdM that is of importance to both organisations and consumers is the security of IdM systems. However, motives and advantages for having secure IdM systems differs for end-user and organisation.

IdM systems need to ensure that personal information that is stored in these systems cannot be obtained by unauthorised persons and organisations, for example for criminal purposes. Loss of identity information can have serious consequences for the end-user. First of all, it may lead to economic loss because some digital identities can be used to retrieve money from credit card accounts and bank accounts. Even though a considerable amount of the economic loss resulting from identity fraud is carried by businesses (Brody 2007), the costs in the end of course befall to the customers themselves and even in the short run the individual can still be significantly harmed economically.

Also other adverse effects of identity misuse incur on the individual. Identities can, for instance, be abused for manipulation, deception, gossip, or bullying (Donath 1998). Inadequate security can also lead to reputational damage for the individual, for example when sensitive information becomes available to a broader public or when lost identities are being abused for criminal purposes (Solove 2007). Repair reputation damage is difficult even because it may be difficult to detect by the 'victim' and because removing all damaging information may be extremely difficult in practice due to caches, copies, etc.

Identities are used as a basis of decisions and judgements, e.g. made by the government and commercial organisations like banks. Identities abuse may lead to discrimination and exclusion of services. In the worst case, this occurs without the awareness of the individual. In addition, the burden of proof of undoing discrimination or exclusion lies at the individual, which can require much effort.

Individuals also have an (indirect) interest in the security of IdM systems, because it may increase the general trust in electronic services, and thus improve the possibilities to make use of ICTs for communication and transactions. Trusted and secure IdM can pave the way for more efficient and effective services to the end-user, whereas mass loss of personal data due to insecurity will have a negative affect on the general use and supply of electronic services as a whole. [20]

4.4 Scenarios

Individuals have to cope with many service providers in daily life, both offline and on-line. One can not expect all these service providers to have relevant details about you when the interaction starts, nor is this desirable as we have seen. But in certain situations we expect to be able to authenticate (and sometimes identify) once for different transactions and interactions because we may have the impression that the multitude of service providers in fact is a single entity or a conglomerate of related entities (a federation). In other occasions entities that may appear unrelated to the individual in fact turn out to be related, either as part of a whole, or as part of a federation. The following scenarios describe these, typical, federated identity situations. They are taken from real life and describe the Dutch situation.[21]

[20] Like for instance the loss or mass amounts of personal data at the UK HRMC, or recently, or the recent theft of 41 million credit card numbers, see: http://www.guardian.co.uk/politics/2007/nov/21/immigrationpolicy.economy3 and http://www.nytimes.com/2008/08/06/business/06theft.html (both last accessed August 11, 2008)

[21] More scenarios and an analysis of identity in egovernment, ehealth, education and workplace, can be found in PrimeLife HeartBeat 1.3.3 (June 2009).

4.4.1 Students and academics at work[22]

Dutch students are clients of the *Informatie Beheer Groep* (IB-groep). The IB-groep is the Dutch government agency responsible for student grants administration and management of related student and educational information. Until the early 2000s, the agency was heavily criticised because of slow responses and bureaucratic delays. A strategic reorganisation with a focus on Internet-based delivery of services had to solve these problems.

The IB-groep developed a unique authentication concept using mobile phones and SMS; this channel was selected specifically because students often misplace electronic tokens or other e-solutions, but generally do not lose their mobile phones. The SMS e-authentication concept was offered to DigiD (see 4.4.2), and was subsequently adopted as the Dutch middle-level e-authentication system.

After logging in with DigiD and SMS e-authentication, students have access to their personal online portal (*Mijn IB-groep*) for student loans. The portal also grants access to different processes pertaining to school and higher education affairs and information. Prospective students are offered options to search databases, find courses, and apply for some programmes.

The IB-groep therefore plays a central role in the life of students. However, when they want to access services within their school or university, the IB-Groep is no longer in sight, although it could play a role here. In other words, the IB-Groep is not, or only to a limited extent, part of the 'education federation'

There is a real federation in the educational domain. This federation is facilitated by SURFnet, the Internet service provider for higher education and called the SURFfederation[23].

“The SURFnet Federation will ensure that users can prove their identity by making use of data which this organisation (an educational institution), known as the Identity Provider (IdP), issues and manages for this purpose. The point of departure is the privacy of the user. It is therefore the task of the Identity Provider to determine the user’s identity, and to issue it to the federation, in combination with a number of user characteristics, where appropriate.

In turn, the SURFnet Federation ensures that information and service providers trust the information regarding this identity. This prevents users having to remember multiple login names and access codes, and prevents the organisation having to maintain a large number of technical connections to information and service providers.“[24]

Within the SURFnet Federation authentication and authorisation data are exchanged based on the SAML (Security Assertion Markup Language) standard. [25] The SURFnet Federation is an identity provider based on A-Select technology. Organisations (institutions and other service providers like publishers) can all become member individually.[26]

Depending on the purpose of the connection specific attributes are provided to a service provider. Users in the SURFnet Federation (every student and employee of an institute of higher education and universities) make use of their credentials (username and password) provided by their school or university to obtain services within the federation. Within their

---

22 Based on Arnold Roosendaal's contribution to PrimeLife HB 1.3.3.

23 See: http://federatie.surfnet.nl (last visited: December 2008).

24 See: http://federatie.surfnet.nl/cms/content/view/16/1/lang,en/ (last visited: December 2008).

25 See: http://federatie.surfnet.nl/cms/content/view/96/57/lang,en/ (last visited: December 2008).

26 Valkenburg, Peter/Jurg, Peter (2007). *Identity Management; omgaan met elektronische identiteiten*, The Hague: ICT Bibliotheek, p. 83.

own institute this may be logging into databases, websites and portals. But also outside their own institute they can authenticate (and indeed identify) themselves within the federation. For instance, members may download Journals from publishers, such as Elsevier ScienceDirect on the basis of the same credentials. And also SURFspot, an online software shop run by Surfnet that offers discounted software (such as Microsoft Office and Adobe Illustrator) on the basis of a country wide license agreement with these publishers.

Users are in most cases redirected to their own institute's A-select (the name of the underlying authentication system) login page and after successful login are redirected to the service provider. Depending on the service provider attributes pertaining to the user are provided.

To the individual the scope of the federation is not at all clear. One might assume that all services provided by one's own institute belong to the federation. Due to all sorts of reasons, for instance technical, this is not the case and therefore users have different sets of credentials within their own institute (the author has two sets: the 'SURFnet' credentials as well as a Novell server set, which, for instance is used for email and file sharing. It is not always clear which credentials are requested, which opens the door for identity fraud). Outside one's own institute it is again not always clear that a service provider is part of the federation. Why would students, for instance, assume that Elsevier ScienceDirect is part of a university federation. Again the risks of identity fraud are lurking. It is easy to set up a site regarding something that is remotely associated to (higher) education and spoof the A-select login page to obtain user credentials that can be used for obtaining services.

4.4.2 Doing business with government

In the Netherlands many governmental organisations (but far from all) are part of a federation that is facilitated by GBO.Overheid. The federation is based on DigiD. Associated relying parties, typically public administrations such as municipalities, redirect users for authentication to GBO.overheid which authenticates the claimant and on successful authentication returns a BurgerServiceNummer (‘Citizen Service Number’ or BSN) to the relying party. Claimants that want to obtain an electronic identity, apply for this identity at the DigiD website, which is a service managed by a department of the Ministry of the Interior and Kingdom Relations, called ‘GBO.overheid’.

The DigiD service comprises three assurance levels and hence three different kinds of DigiD’s can be obtained by the claimant. The first and second assurance levels are called ‘DigiD basis’ and ‘DigiD middle’. The third level, ‘DigiD high’, will be filled in by the Dutch electronic Identity Card, called ‘eNIK’, which is currently under construction.

The DigiD basis level grants a claimant access on the basis of only a password and username. For most electronic services this assurance level is regarded sufficient. The middle level provides a higher assurance and currently consists of session-specific login codes that are provided to the claimant by means of text messages on their mobile phone (SMS, Short Message Service). The high level of authentication (the eNIK card) will be based on PKI, but this project is severely delayed.

The base and medium levels of DigiD consists of the BurgerServiceNummer (BSN), which is a unique identifying number for citizens registered in the Municipal Registry. The BSN is used as a key to records pertaining to individuals in other Dutch Authentic Registries (currently there are ten registries). One of these registries is the Municipal Registry, which contains information about residents in a municipality, such as name, last name, marital status, address, residence, and parents and children.

Holders of a DigiD can use the associated credentials to authenticate for electronic government services. DigiD is also used as a digital signature for tax purposes. When a citizen needs to authenticate herself on a municipal website, she is redirected to the DigiD login page and after successful authentication the DigiD site transfers the citizens BurgerServiceNumber to the relying party.

The basic infrastructure for the federation is in place, but all sorts of issues exist. One, not all government agencies are part of the federation. This means one can use one's DigiD in municipality A, but not in B. Secondly, although the DigiD is personal, some service providers, most notably the Tax Authority in 2006, have advised citizens to use someone else's DigiD to complete a service (for instance filing a tax return). This example also shows that delegation, which is a requirement in the public domain (for instance, many people: elderly, businesses, do not file their own tax return, and therefore someone else needs to be able to act as a proxy) is not taken into account in the design.

4.4.3 Moving from work to leisure

An entirely different kind of scenario is one where the different kinds of partial identities come into play. I have a work related identity (my professional career, publications, colleagues) and several private identities (my hobbies, sports, family life, etc). Users engaging in Web 2.0 applications (wiki's, blogs, social networks) will therefore typically engage on different platforms. My professional life is represented on LinkedIn, while my hobby life is represented on Myspace, web forums, such as RC-Technics and MacRumors, etc. Some of these platforms make use of federated identity management solutions, most notably OpenID. The user can use a single set of credentials to access these different platforms. Although it certainly is convenient not having to remember usernames and passwords for all these platforms, but being able to log-in using a single set of (OpenID) credentials, the question here is whether it is sensible to use the same credentials in totally different domains. Using one's OpenID credentials for work and private related platforms introduces issues of linkability that one may want to prevent. The alternative would be to maintain different (OpenID) identities, but this would diminish the advantage of federated IdM.

4.5 Conclusion

In this chapter we have provided a high level overview of desirable features and characteristics of federated identity management systems from the perspective of the individual. We have focused on the need to be able to play different roles in life, also online, and being able to keep these separated which requires identity management systems to move away from formal identities (one's real name) towards token and claim based authentication. Secondly, convenience and usability are important. People want to obtain services. Having to log in or prove certain claims is a mere 'nuisance' on the road to these services. Finally, security is an important aspect to keep in mind from the perspective of the user. IdM deals with people's identities. These can be misused and abused. Security is also important from the perspective of trust establishment and maintenance: only in an environment where a basic level of trust exists between users and service providers can we have serious service delivery.

The scenarios at the end of the chapter have shown that different kinds of federations exist with different characteristics and (trust/security) issues.

In the next chapter we will derive a number of concrete aspects to facilitate comparing the four FIM frameworks selected in the previous chapter.

5 Concepts and Metrics

5.1 Introduction

In order to assess and compare the four identity management frameworks from the perspective of the individual user, we need to have a set of concepts and metrics to guide evaluation. For the purpose of this deliverable we have derived these from literature and the PRIME project.

An important starting point for assessing the various frameworks is informational self control, both as a goal in itself (to promote and protect autonomy), as well as an instrument to protect individual privacy. Secondly, it is important to keep in mind that identity management, required for access control to resources at least, for many people is not an aim in itself, but rather a means to achieve other goals. This provides the source for a set of end-user adoption requirements. Next, a set of more technical aspects regarding the management of (partial) identities can be distinguished, such as authentication management, policy management, history management, context detection and personal data storage. Finally, security on the different levels need to be taken into account.

5.2 Control over an identity through privacy

ICTs have the characteristic to separate the body from the interactions and transactions we have with other people. This makes it difficult to establish trust between the end-user and the organisation they interact with. Moreover, time and space have become irrelevant with the use of ICTs. We can do business online irrespective the direct availability or attendance of others, by using digital representations of ourselves (Lyon 2001). These digital representations, or 'digital persona' are constructed out of identity information (Clarke 1994). Identity information can be used, transferred, and copied on a global scale, which can lead to the existence of scattered digital identities of customers. When such identities are abused, forgotten, out of date, or combined, the end-user becomes vulnerable as this situation could lead to, for example, 'identity deception', 'identity fraud', 'profiling', 'function creep' or 'overexposure'. ICTs and digital persona make the individual 'transparent' in a new way because information can easily flow in and out of contexts and because an information asymmetry can easily originate between the user of identity information and the person whom a digital identity relates to. In other words, customers are not always aware of the use of their digital identities by others (Hildebrandt 2006; Solove 2007).

Because the use and abuse of identities in the online world can have far reaching consequences for the individual (and for society), it is important that the honest use of digital identities is guaranteed. Obviously, IdM systems can have an important function here.[27] Specifically this means that a level of privacy ought to be assured in the design of IdM systems. Privacy and identity are closely connected concepts (hildebrandt 2006). Privacy, for example, has been defined as the possibility of individuals to 'build identities without unreasonable constraints', and to freely project these constructed identities to others (Agre 1997; Goffman 1957). Customers need to use different roles (and thus identities) throughout contexts, to adjust contextual requirements (e.g. to have intimacy, autonomy, team play, and consistency of a relation). And only when the individual can segregate her different identities between contexts and audiences, will it be possible to adjust to the integrity of the context in which she acts Goffman 1958; Nissenbaum 2004). When privacy is assured by IdM systems, the individual can control the information with which she builds her own identities and can

[27] Next to regulation, norms, and the market, cf. Lessig (1999).

deploy identities according to her own needs whenever there is a reasonable possibility to do so.

Informational control (or informational self determination) by the individual is considered to be a major aspect of privacy (Fried 1968; Stalder 2002; Westin 1967), (especially in the information society) and is considered a necessary feature of IdM systems (Cameron 2005). It can be assured on the basis of the following requirements/metrics[28]:

1. *The IdM system's possibilities for providing ex post and ex ante information to the end-user.*

Control of the user over his identity starts with the information an IdM system provides to the user prior to the deployment and construction of a digital identity. The system needs to create end-user consciousness about data processing as to provide the ability to anticipate to data processing. Information provisioning contributes to the perceived fairness of a data processor/IdM system by establishing transparency. Information should, however, not only be provided previous to data processing, but should also be provided *after* identities have been created or used. This relates to the circumstances in which an individual wants to inspect the use and storage of digital identities, but for example also to the situations in which identities are exchanged with other parties in the service chain.

2. *The possibilities for the end-user to choose an identity, and consent to – and confinement of – the use of identities.*

The importance for customers to segregate audiences results in the necessity to choose between the identities he or she uses in a certain context. Moreover, it is important that these different identities are confined and thus are not blended or combined with other identities. Next to the choice between identities and the confinement of the use of these IDs, IdM systems need to (pro-actively) ask for permission to use an identity, to make the data processing legitimate. The end-user, moreover, needs to be able to define by herself the conditions under which organisations can make use of her identity (e.g. scope of use, length of storage, and purposes of use).

3. *Possibilities of alteration and deletion of used identity-information by the end-user.*

Customers that make use of digital identities may occasionally need to be able to delete their online profile. Such a need for 'forgetfulness' is a default setting in the 'offline world' but not in the online world (Blanchette & Johnson 2002). Next to this, it is important that people can alter their digital identities and can correct these identities when they have made mistakes or when the conception of their identity is not aligned (anymore) to their static digital representation.[29] In a sense, the requirement for end-user alteration and deletion follows from the demand to have transparent data processing, because without an instrument for the end-user to change errors and mistakes, information provisioning about the use of identities would have limited value.

5.3 Customer adoption characteristics

To the end-user, identity management is often not a target in itself but mostly a means to, for example, get access to specific services. This means that the adoption of an IdM system by its customers may follow the path of least resistance (Dhamija & Dusseault 2008). Users will not

[28] Abstracted from: Kosta et al (2008); Jutla et al (2005).

[29] This also relates as to how the 'I' can be aligned with the 'implicit me' and 'explicit me', cf. FIDIS WP2. (2005). D 2.1: Inventory of topics and clusters (FIDIS Deliverables): FIDIS Consortium, p. 30

likely put much effort and money in the management of their identities.[30] Because of this, IdM systems must pay attention to the adoption of IdM systems by customers. Especially for the commercial use of IdM, it is likely that the value of an IdM system increases as more customers adopt it[31].

Federated IdM systems are driven by standardisation and a cross-contextual approach towards IdM. Hence, in theory, these systems should be scalable. However, such scalability may be business-oriented only (focused on exchange of identities by businesses), instead of being end-user oriented. Because of this, we define a concept of end-user adoption, which aims at assessing the FIM initiatives on the basis of some metrics that can indicate the likeliness of end-user adoption:

1. *Increasing trustworthiness of the system and its transaction partners*

Trust establishment is a central feature of FIM systems, as the exchange of identifiers and identity attributes obviously requires trust mechanisms between the organisations that join a federation. However, the importance of trust establishment between the end-user and the FIM system and its connected organisations should not be underemphasised. Bearing in mind that on the internet "consumer trust is a key foundation for success" (Tan & Sutherland 2004), and that in FIM systems trust needs to be established in all participants of the federation[32], it is important that consumers are convinced that they are not harmed by the federation as a whole. Of course, trust is a social and cultural matter, but some markers of the quality of the federation, the reliability of its technology, and its measurements against risks, need to provide the end-user insight in its trustworthiness. This counts especially for FIM systems, as, due to their nature, federations will be as strong as their 'weakest link'[33]. Some examples of measures that can establish trust are: seals, mutual authentication, external audits, information provisioning, or dispute resolution mechanisms.

2. *Connection to the skill level of the users, social settings, efforts, and costs*

Currently, it is likely that IdM systems will be adopted when they are easy to download, install, and configure (Dhamija & Dusseault 2008). Bearing this in mind, it seems that IdM systems that are integrated in an OS or browser have an advantage over IdM systems that need to be purchased or downloaded separately (Dhamija & Dusseault 2008). Moreover, when installed, IdM systems need to avoid that the customers are overwhelmed with identity-related choices or warnings, which can lead to unforeseen effects (e.g. people clicking "OK" to all requests) (Dhamija & Dusseault 2008). The user's rationality is bounded (c.f., Acquisti & Grossklags 2005), and excessive choices in the field of identity management do not always lead to a desired outcome (Schwartz 2004).

For the sake of usability, the interface of an IdM system needs to be easy to understand, but should also provide insight in the normal line of operation (consistency), and ideally provides concise and layered policies supported with tutorials. It is a challenge for IdM systems and for the federations in which they are used to provide these features without making identity management a burdensome experience. Because of this, choices in the field of human-computer interaction (HCI) can should support the user and need to make the system

30 Ibid.

31 In other words, a successful FIM system can create a 'network effect', because the more users and organisations join the federation, the value of using the system increases for both users as organisations, cf. Katz & Shapiro (1994).

32 The chain is as strong as the weakest link in federated IdM.

33 One organisation can threaten the trustworthiness of all members of the federation.

adjustable to social settings (e.g. with the use of symbols and language), while keeping in mind the 'cognitive scalability' (Schwartz 2004) of the IdM system as a whole.

5.4 Management of Digital Identities

Attributes of a user, which are operationally accessible by technical means (e.g. personal information stored in data bases), form a *digital identity*. Since each different set of attributes can be regarded as a single digital identity, one user can have several – not necessarily entirely distinct - digital identities.

Creating, managing, manipulating and deleting these digital identities of a user are primary functions of an identity management system. The manipulation of a digital identity includes adding, deleting or changing some of its attributes, such as the postal address, the e-mail address, or the hobbies of the respective user. These attributes can be filled in by the user or – in some cases – automatically configured by the system. For digital identities unique pseudonyms can be used as identifiers. Pseudonyms make it easier to handle and to reuse digital identities.

From a privacy perspective, it is important that personal data disclosed by the user acting under a digital identity, cannot be linked with attributes this user uses with other digital identities. Nevertheless if linkability is given, the identity management system should inform the user and point out which data are linkable, to enable the user to avoid unintended linkage between his digital identities.

5.5 Authentication Management

Federated identity management systems support authentication of users via identity providers and access control to resources of service providers. In contrast to identification, authentication is the verification of a given identity. Verification is operated by showing a certificate and attributes such as a key, a password or by having some privileges. As soon as a user has authenticated herself, she gets access to the service.

A special case of authentication is single sign-on, which enables a user to authenticate herself just once and thereby gain access to the resources of multiple service providers. This feature is usually provided by federated identity management systems.

The standard functions of an identity management system concerning authentication and access control are:

- Support for access management (or enabling single sign-on for each session between the client and the service provider) in order to get access to services of the service provider.
- Support for digital signatures. Digital signatures are digital data, which can be attached to an electronic file or message, and confirm its authenticity and integrity as sent by the user's device, therefore guaranteeing the correctness of data in messages, documents, e-mails or contracts.
- Support for authentication credential management in order to enable the user to manage her login data, e.g. login name, the corresponding password, and the URL of the service provider. Of course the password needs to be kept secret for authentication to work effectively.

5.6 Policy Management

A policy is a guideline concerning disclosure, use and manipulation of data, especially user-specific personal data. These policies are necessary, both for users and for service providers. A special case of a policy is a *privacy policy*, whereby the service provider determines which data he will store for which purposes and to what extent he will make use of these data during the transaction and/or after the transaction has been finished. The possibility of looking at and enforcing these policies is realised by policy management within an identity management system.

Besides this, the policy management gives the user *control* of the use of his personal data, because in each transaction case she can agree or disagree with the use of the data as the service provider suggests it. Therefore, on one side the user determines which personal data she transfers to which service provider for which purpose. On the other side, the service provider also determines which data he needs from a user and how he will use them e.g., how long he will store these data. Only if the policies of the user and of the service provider match each other, data are transferred.

At present policy management can take advantage of standard terms defined by the platform P3P (W3C 2007); P3P makes an automatic recognition whether the user's and the service provider's requirements match.

Furthermore, the policy management should support translation between machine readable policies and the wording presented to users.

5.7 History Management

History management of a federated identity management system logs all transactions with identity/service providers and keeps a record of all personal data revealed. This information is a basis for users' awareness, comprehension, and exercise of their rights concerning privacy. The history management should be able to present the data transferred and the context of its transferral (time, purpose, recipient) to the user. Either the attribute disclosed is stored (e.g. "first name") or attribute and value disclosed are stored (e.g. "John"). In the latter case, the history management contains personal data which may require further privacy protection mechanisms. The history management is not intended to log all data the user discloses, for example there is no logging of content of messages during her interaction with a chat partner (although the messages may contain personal information, if they are interpreted semantically).

5.8 Context Detection

To help the user to handle her digital identities according to her current situation, i.e., transaction partner, activity and history of personal data release (c.f. 5.7), the identity management system should be able to identify the context of the user automatically. The context-detection component of an identity management system should identify contexts within the applications or the services the user interacts with. In case of a context switch, the identity management can act in two ways:

- either it makes some suggestions for further activities to ensure privacy and security of the user (e.g. suggest to use another digital identity), or
- else it takes action autonomously to this end (e.g., based on previously defined preferences of the user).

To enable those features, the system must offer the possibility of specifying contexts and of determining how the user can navigate through them.

5.9 Client-based vs. Server-based Storage of Personal Data

The storage of user specific personal data can be realised either on the user's own computer ("client-based storage") or centralised on a computer which acts as a server ("server-based storage"). In the second case, the computer concerned is typically not under the control of the user but operated by an identity provider. This means that the user needs additional interfaces to access her personal data, and also that she has to trust the identity provider concerned not to misuse her personal data. Trust is especially required with regard to availability of the personal data. In theory, confidentiality and integrity can be realised by the user herself applying cryptographic mechanisms. Server-based storage raises the question of transparency of the transactions using personal data. With respect to federated identity management systems, distributed server-based storage of user's digital identities across several identity providers is also possible.

5.10 Security Aspects of Federation and related FIM Framework

Security of a system needs to be understood in a holistic way. Bruce Schneier (1996) verbalised this as follows: "Security is a chain; it's only as secure as the weakest link."

For Federated Identity Management Systems (FIMS) this means that each of many aspects inside and outside of the federation framework and related communicational infrastructure may define the effective level of security reached, as an adversary will most likely attack the system in its weakest point. In this context we do not need to think about the security of FIMS alone – as FIMS are meant to be used as an authentication infrastructure for many applications and related business or governmental procedures, the security level of these procedures also depends on the security features (according to ISO/IEC 15408 (Common Criteria) also called "security functions") of the FIMS.

In many cases FIMS are implemented as federation framework based on traditional directory services or other (mostly organisation centric) identity management systems. They serve as a source of reference for authentication information provided by a user during an authentication procedure. As a consequence the security of FIMS depends at least on four layers:

1. An infrastructural layer composed organisational directory services including related security infrastructure (layer 1),
2. The federation framework including related communicational infrastructure (layer 2),
3. The security of applications relying of the FIMS, as manipulation of the FIMS principally via the application may be possible (layer 3), and
4. The user in case he is client of one of the organisations participating in the federation, his local client and communication infrastructure (layer 4); (in case the user is member of an organisation he belongs to layer 1)

Examples for this architectural concept are LibertyAlliance and OpenID. The following figure shows architectural layers influencing the security of FIMS with a focus on user activities:

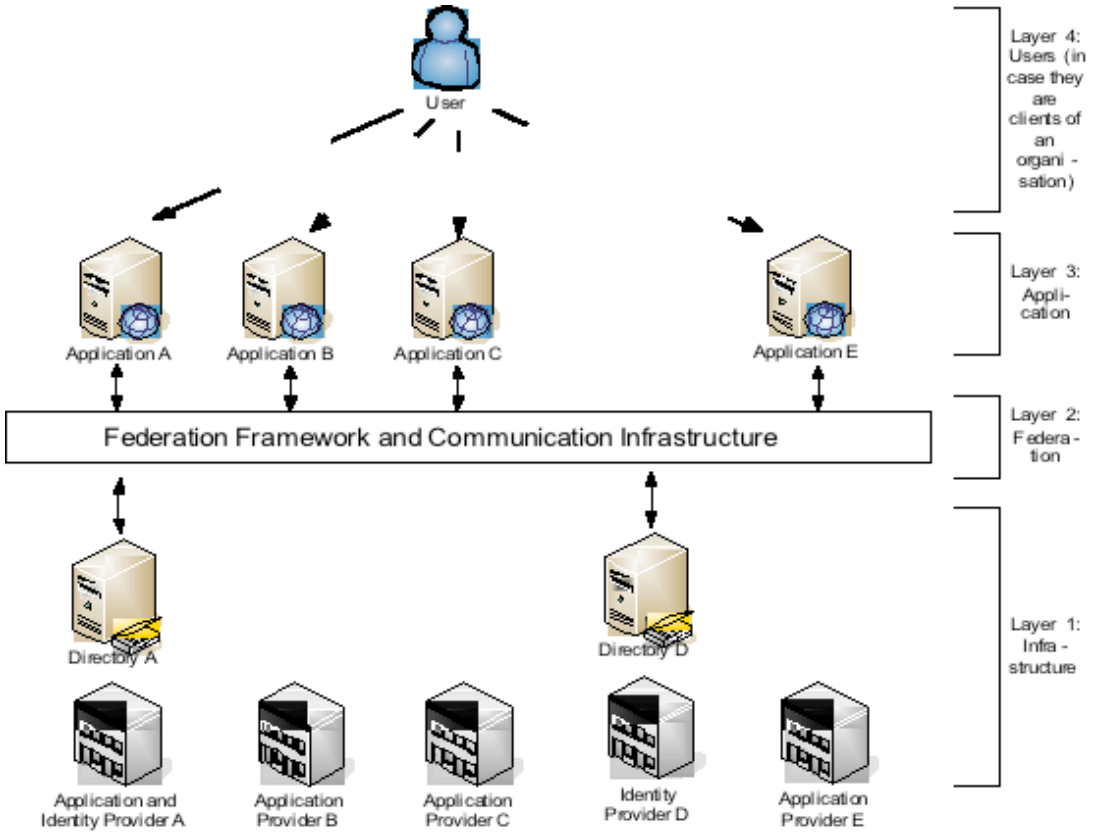


Figure 2: Architectural layers influencing the security of FIMS

The discussion of security aspects relating the user, his client and the various applications (layers 3 and 4) are outside the scope of this deliverable. In this context we refer to existing standards covering related security aspects such as ISO 27002, the Baseline Protection Catalogues issued by the German Federal Office for Information Security[34] and the Common Criteria (ISO/IEC 15408).

In the following section the focus will be put on security aspects of the infrastructural layer of FIMS.

5.10.1 Security Aspects of the Infrastructure (Layer 1)

From the perspective of the operator of procedures, an important requirement for the implementation of an appropriate security level is control, i.e., that the organisation is able

- to establish a management system that checks and adjusts continuously and effectively the activities and results of the following areas of activity
- to define and describe the appropriate (and thus required) security level,
- to describe the related infrastructure; this typically includes: organisational units of the organisation (including employees involved), environmental infrastructure (buildings, rooms an the like), hardware, systems and components including corresponding operating systems or firmware, networking infrastructure and applications involved,
- to carry out a risk assessment, and
- to set up and implement a risk treatment plan, namely required technical and organisational security measures.

[34] See http://www.bsi.de/english/gshb/index.htm

FIMS are meant to be used organisation-spanning without a superordinated entity. As a consequence, no participating organisation alone possesses the control to implement the required security level. In the FIMS context, each organisation is highly dependent on the implemented security level of the other participating organisations in the federation. This situation becomes even more complex if the participating organisations provide more than one security level in their internal IMS.

In any case according to international security standards such as ISO/IEC 27001 (Information Security Management Systems – Requirements) to reach a reliable security level, the participants of a FIMS need

- security policies referring with respect to the FIM to the same (or a very similar) security level;
- connected information security management systems including personnel resources and security processes (e.g., for the maintenance of security concepts, security incident handling and business continuity planning and management);
- a jointly agreed security concept containing
    - A description of the FIMS and related infrastructures
    - A risk assessment
    - A risk treatment plan (organisational and technical security measures)
- contractual agreements ensuring implementation, maintenance, auditing schemes and enforcement of agreed technical and organisational security measures.

Typically, these essential security measures are beyond the horizon of the mostly product-related discussions of security functions of federation frameworks. Nevertheless they are relevant, as examples show in which security considerations also on this layer were a reason not to introduce FIMS, though potential cost savings through Single-Sign-On (SSO) and distributed administration could have been significant.[35]

For an end-user (client of a participating organisation) these aspects are equally relevant, as the security of his authentication information relies on the security of the infrastructure, systems and applications of identity and service providers. The confidentiality, integrity and availability of authentication data stored at the identity provider may be at risk. This leads to an infrastructural security criterion:

> *Security of the infrastructure supporting the federation framework and communication infrastructure needs to be on an appropriate level*.

Traditionally, security and data protection policies of identity providers may be investigated for information concerning this criterion, as these policies provide basic information for the users.

5.10.2 Security aspects of the federation framework and communicational infrastructure (Layer 2)

Federation of identity is performed based on a federation framework that includes an infrastructure for establishing communication between participating organizations. The main aim of identity federation is to enable users of one “security domain” to access services of another domain. For that purpose, protocols are employed to broker information on identities,

[35] See e.g. the U.S. American food service company Aramark, http://www.pcwelt.de/index.cfm?pid=829&pk=60374

identity attributes and authentication credentials as well as sharing federation metadata including security token exchange between Requestors, Identity Providers (IP) and Security Token Services (STS).[36]

Although many federation standards exist, each with different capabilities, they all share common security requirements. We list here Shibboleth (by Internet2), Security Assertion Markup Language (SAML, by OASIS), Liberty ID-FF (by Liberty Alliance) and WS-* efforts for web services (mainly WS-Security, WS-Trust and WS-Federation by IBM, Microsoft, and partners).[37]

There are many aspects in those standardized protocols that can directly or indirectly affect the security of the federation framework. Basically, the message-level authentication and authorization in the federation framework depends on a general security model. For evaluation purposes we propose three criteria: (a) the security model used, (b) the trust model used and (c) security of communications.

5.10.2.1 Security Model

The security model of a federation framework relies on the notion of security tokens, which represent a collection of claims that a user has with regard to authorization to certain services. Security tokens constitute one of the core means for securing the process of authorization of a certain user to a specific service. Typically, security tokens that are initially provided by one STS (that corresponds to one IP in a domain) are used to access web services in another domain, for example, by:

- Getting certified by STS corresponding to the second domain, or
- Obtaining new local security tokens that are valid for authorization to the web service from STS in the second domain, or
- Getting validated by the Resource Provider's STS.

The usage of security tokens depends on the established trust model. However, it is necessary to exchange these tokens between participating parties by means of adequate communication protocols, which entail the requirement of secure communication.

5.10.2.2 Trust Model

Federated trust can be based on different trust models. A trust model typically depends on the different parties and entities contributing to the federation process, namely the STS, the IP, the requestor, and the resource itself. The following figure illustrates the different entities/parties, and the established trust between them.

[36] Federated Identity – Wikipedia (2008) http://en.wikipedia.org/wiki/Federated_identity

[37] Federated Identity Management and Web Services Security, IBM, 2005 http://www.redbooks.ibm.com/redbooks/pdfs/sg246394.pdf

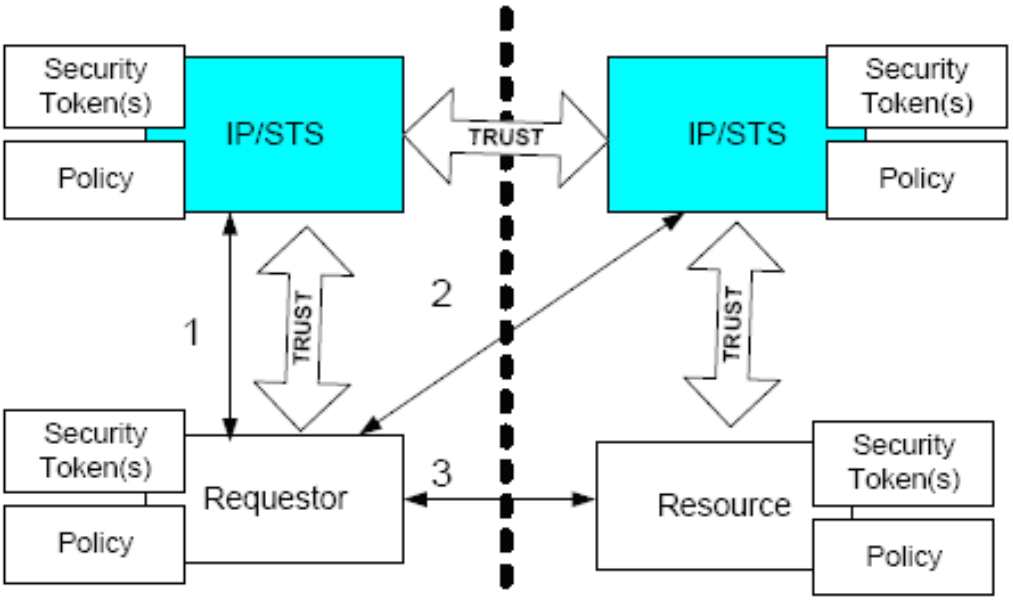


Figure 3: Federation and Trust Model[38]

The requestor trusts the IP/STS of its own realm, and same does the resource with its IP/STS in the second realm. The IP/STS in the different realms trust each other.

Based on this model, different trust topologies can be derived. Basically, they differ in the way security tokens are issued, validated and exchanged by the different entities involved in the process. For example, one approach (shown in figure Error: Reference source not found) requires the requestor to obtain a token from the IP/STS in its own realm, provide it to the IP/STS in the second realm, which then check its validity and exchange it with a token that is valid in this second realm. Using this token, the Requestor would be able to directly access the Resource. Another approach would require the requestor to obtain a token from its IP/STS, supply it to the Resource which then validates the token at its own IP/STS before granting access to the Requestor.

5.10.2.3 Security of communication

The requirement of secure communication between participating parties is important, especially across different domains. The security of communication protocols is crucial to the security and reliability of the overall FIMS since any malicious or involuntary breach of those protocols could have several consequences such as the user obtaining access to a certain service to which she is not authorized, or a user denied access to a service which she is supposedly authorized to access.

Therefore, message exchanged between services should be integrity protected by including the body of the message as well as the headers in the signature. Moreover, encrypted communication is needed (e.g. using transport security protocols).[39]

Moreover, certain parameters used in the protocols need to undergo a strict verification due to their sensitive nature. For example, in an HTTP protocol used by a Web Requestor, the *wreply* parameter including the URL to which responses are directed can be spoofed.

---

[38] Web Services Federation Language (WS-Federation) http://specs.xmlsoap.org/ws/2006/12/federation/ws-federation.pdf

[39] Web Services Federation Language (WS-Federation) http://specs.xmlsoap.org/ws/2006/12/federation/ws-federation.pdf

While attribute service information is usually privacy critical, and should therefore be handled with care, pseudonym service information can include passwords and similar secret information. Their encryption during communication is therefore necessary.

Security tokens must either have an embedded signature for integrity protection or be included in message supporting integrity check mechanisms.[40]

The attacks that can be carried on the communication protocols are mainly: metadata alteration, message alteration, message disclosure, key integrity, security tokens replay attacks, forged security tokens, etc…

5.11 Conclusion

We now have a set of concepts and requirements that allow us to compare and assess the four Federated Identity Management frameworks/systems selected for this deliverable: Liberty Alliance, Shibboleth, PRIME and Microsoft Cardspace.

[40] Web Services Federation Language (WS-Federation) http://specs.xmlsoap.org/ws/2006/12/federation/ws-federation.pdf

6 Assessment of Federated IdM systems

On the basis of the concepts, requirements and metrics discussed in chapter 5, this chapter provides an analysis of the four Federated Identity Management frameworks selected for this deliverable: Liberty Alliance, Shibboleth, PRIME and Microsoft Cardspace. For each of the systems, we will follow the structure adopted in chapter 5. We start with informational self control (to promote and protect autonomy, and as an instrument to protect individual privacy). Secondly, we address end-user adoption requirements. Next, the technical aspects are discussed: the management of (partial) identities, authentication management, policy management, history management, context detection and personal data storage. Finally, security on the different levels in the frameworks will be described.

6.1 Liberty Alliance

The assessment of Liberty Alliance IdM is mostly based on an analysis of documentation, which can be retrieved on the Liberty Alliance website.[41]

6.1.1 Control over identity through privacy

Liberty Alliance (hereafter 'Liberty') recognises that the implementation of its specifications in connection with web-based offerings can lead to privacy and security concerns. Because of this, Liberty provides tools and guidance for more secure, privacy-friendly services[42].

Liberty sees privacy as a "security policy applied to a Principal".[43] The project makes it possible for companies that use Liberty standards to comply with national privacy laws and regulations. However, Liberty does not manage the actual compliance with these laws.[44] Because of this, using Liberty specifications is no automatic guarantee for a certain level of end-user privacy.

Liberty can be considered as a business centric approach to identity management, as it is based on collaboration between organisations and on an implementation of its specifications by these organisations. Moreover, the Liberty perspective on privacy is influenced by the fact that the project itself does not provide products or services to the public, but merely the specifications for standards-based federated IdM. Because of this, Liberty states that companies that implement Liberty specifications are responsible by themselves for compliance with applicable privacy laws[45]. The Liberty Alliance protocol is neutral regarding data protection[46].

With regard to the Liberty Specifications, Liberty made the following decisions:[47]

- to use a decentralize architecture where centralized storage is not necessary;

---

41 See: http://www.projectliberty.org, last accessed on August 13, 2008

42 Liberty Alliance Project. (2003c). Privacy and security best practices (v2.0).

43 In this definition, Principal relates to the individual that discloses her personal information.

44 Liberty Alliance Project. (2003c). Privacy and security best practices (v2.0).

45 Liberty Alliance Project. (2003c). Privacy and security best practices (v2.0)., p.8

46 ICPP/ULD, & SNG. (2003). Identity management systems (ims): Identification and comparison study; referring to: Article 29 Data Protection Working Party. (2003). Working document on on-line authentication services (wp 68). The fact that project was largely composed out of American participants, has raised the attention of the Article 29 Data Protection Working Party in 2003

47 Liberty Alliance Project. (2003c). Privacy and security best practices (v2.0).

- to support and promote the sharing of consumer's attributes based on permission of the user;
- to enable companies to use the best security, while information is transmitted acording to the specifications;
- to include tools that enable companies to respond to consumer interests regarding privacy.

Liberty pays substantial attention to privacy, but some of this attention is based on 'non-normative' guidelines and specifications, which thus are not mandatory for Liberty-implementers. Moreover, the open character of the project makes it difficult to assess its promoted IdM solution, as differences exist in the translation of Liberty Specifications.

In one of its (non-normative) documentations, the 'Privacy and Security best Practices', Liberty recommends that implementing companies should comply with all relevant laws or fair information practices. This statement is supported by an outline of several privacy laws and fair information principles. In addition, Liberty recommends to give individuals: 1) clear notice considering information collection, 2) choice with regard to what personally identifiable information is collected, 3) possibility to review, verify or update consent, 4) reasonable access to view non-propretary personally identifiable information, and 5) the opportunity to provide corrections. Moreover, these recommendations stipulate the need for purpose limitation, timeliness of data, complaint resolution, and security.

As these recommendations should be *considered*, it is up to the implementing organisations to meet them. Customers cannot rely on the compliance with these recommendations.

Ex ante and ex post information to the end-user.

In the ID-FF architecture overview of Liberty (non-normative), it is stated that the identity federation should be predicated upon notice to the user and user consent, of which auditable records should confirm that notice and consent were provided.[48] User notice upon federation (and also defederation) is considered a functional requirement of Liberty identity federation.[49]

Because Liberty does not provide products or services itself, there is no standardized manner for e.g. privacy expressions or icons. Moreover, the Liberty Alliance cannot provide information about the concrete applications in which Liberty specifications are being implemented. Hence, much information provisioning about data processing is at the discretion of Service Providers and Identity Providers. However, the Liberty Alliance website[50], does provide an extensive overview of the project, its specifications, and architecture for example by means of white papers.

Liberty Alliance Specifications do not provide a function for tracking the use of personal data. Such a function has to be decided by the Identity Provider and Service Provider.[51] Moreover, there exists no privacy seal function[52], for privacy-friendly implementations of Liberty.

[48] Liberty Alliance Project. (2003b). Liberty id-ff architecture overview (version 1.2), p.8

[49] Liberty Alliance Project. (2003b). Liberty id-ff architecture overview (version 1.2), p. 16

[50] On www.projectliberty.org, last accessed, August 14, 2008

[51] Cf. ICPP/ULD, & SNG. (2003), p.139

[52] As proposed by Alsaleh & Adams (2006)

Choice and consent (and audience segregation)

Consent is key to Liberty's vision: 'permissions based attribute sharing' is the foundation for its functioning. Specifically, Liberty Alliance requires the consent of a user previous to the *federation* of her identity.

User consent can be automated with Liberty Specifications, for example with a tool that enables users to specify their authorization policies. Such policies would also make it possible to confine the use of personal data throughout 'circles of trust'. Next to this, with Liberty Specifications, customers may adjust their default policy with so-called permission exceptions. Important in this regard is that user privacy preferences should match with SP's policies (Alsaleh & Adams 2006) .

Confinement of identities may be supported by means of Liberty Specifications' support for 'opaque handles'[53], which identifies an end-user by means of an arbitrary set of characters. Opaque handles can make it more difficult to track the end-user when she navigates among Service Providers[54], but should be refreshed periodically. [55] In addition, Liberty Specifications allow the use of an 'Anonymous Identity Protocol'.

With regard to the choice of an end-user to use and confine several identities, the creation of different 'circles of trust' can contribute to the confinement of a user's identity in one 'circle'. Thus, Liberty specifications support the use of multiple identities throughout contexts. In addition, implementations must support the use of pseudonyms and anonymity.[56]

Alteration and deletion

The possibilities for alteration and deletion of personal data/identities is left at the discretion of the implementers of a federation. Identities are stored decentrally at the identity provider, so local conditions determine if alteration and deletion are possible (ICPP/ULD, & SNG. 2003). In addition, users have the possibility to defederate their identities, based on the Federation Termination Notification Protocol, by selecting a 'Defederation link'.[57]

The Liberty solution for federated IdM does not provide the end-user with specific privacy support, as privacy depends on the choices that are made in a specific implementation of Liberty Specification. The various design options can influence the possibilities of privacy breaches (Alsaleh & Adams 2006). Organisations that implement Liberty, can decide by themselves which kind of privacy-framework they will develop and how the guidelines and recommendations are translated. It may not always be clear if organisations provide information by themselves considering the realisation of the (privacy-) recommendations and specifications.

6.1.2 User adoption characteristics

Trustworthiness (from the end-user's point of view)

Customers can decide by themselves if they join a Liberty-enabled 'circle of trust'. The trustworthiness of the federation will be one of the variables on which the user makes her decision to proceed with federation. This trustworthiness is hard to achieve by the Liberty

53 Liberty Alliance Project. (2003b). Liberty id-ff architecture overview (version 1.2).p. 12

54 Liberty Alliance Project. (2003c). Privacy and security best practices (v2.0), p. 19; even some other tracking possibilities have been described by (Alsaleh & Adams 2006).

55 Liberty Alliance Project. (2003b). Liberty id-ff architecture overview (version 1.2).p.24

56 Alliance Project. (2003b). Liberty id-ff architecture overview (version 1.2), p. 16/17; (ICPP/ULD, & SNG. 2003), p. 138,

57 Liberty Alliance Project. (2003b). Liberty id-ff architecture overview (version 1.2), p.27

Specifications only. Hence, trustworthiness will mostly need to be achieved by the implementers of the specifications (reputation, experience, etc.)

The mutual agreements between members of a federation can serve as a trust-establishing mechanism, but it is not likely that customers can assess these agreements.[58] The Liberty Interoperable testing program may provide some trustworthiness for a Liberty implementation, as this program binds the Liberty implementers to a defined quality level.

Even though the user indicates by herself if she joins a circle of trust, much actions in a Liberty federation are 'behind the scenes' and the circles of trust and its characteristics are defined by the organisations that join the federation. In other words, trust levels for Liberty implementations can be different as the technology can be implemented differently and because federations exist out of different organisations.

Efforts, skill level, social settings, costs

The Single Sign-In and Single Sign-off experience of Liberty implementation offers a feasible user experience. The federation of identities is initiated by the service provider or identity provider, which assures that the user does not have to put in much effort in the actual IdM.

The design and interface of the Liberty implementations is a choice of the implementers, so there is no guarantee for a consistent user experience.

There is no need for individuals to download or install additional software to make use of Liberty IdM, as implementation of the specifications is done at the service end. The Liberty Alliance project counts many participants, which assures a high comparative adoption rate for this particular IdM solution. Next to this, the open standards and specifications of Liberty can assure a high level of adoption.[59] Customers can make use of Liberty IdM from several locations, and are therefore not bound to a single device.

It is not sure to tell if customers will understand the idea of liberty-enabled federation and the notion of 'circles of trust', even though the Liberty Alliance website may realise that these concepts and definitions will settle down after a while. The choice to federate identities is left to the user, but without a notion of federation and its underlying architecture, it will be difficult for individuals to make a deliberate identity-decision. Moreover, there may be difficulties for the user to keep track of the identity to which they are logged on inside a certain federation, and the several requests for identity federation may be a overwhelming experience. It is up to the implementers of Liberty to distribute the necessary help functions or manuals to assist the user in the FIM experience.

6.1.3 Management of Digital Identities

Digital identities are represented by different accounts that the user has at different identity providers. If the user agrees to federate her digital identities between an identity provider and service providers, the same account can be used for interactions with various service providers, which belong to the same circle of trust as the identity provider. A *circle of trust* is a federation of service providers and identity providers that have business relationships based on Liberty architecture and operational agreements and with whom users can transact business in a secure and apparently seamless environment." (c.f., Figure 4) Still, the user can have several accounts with one service provider and thereby she decides which account she wants to use when signing on at a service provider. A single organisation can be both service provider and identity provider.

[58] These agreements may be opaque or too extensive to scrutinize

[59] Cf. http://www.projectliberty.org/liberty/adoption, last visited August 14, 2008

Instead of user's actual account identifiers, so-called *opaque user handles* are exchanged between federated providers for referring to a user. Thus, for instance, a service provider will not be able to display a user's identifier from the related identity provider (Liberty Alliance Project, 2005).

6.1.4 Authentication Management

Authentication with Liberty Alliance is based on the SAML standard (OASIS 2008) and organised as follows (Liberty Alliance Project, 2005, pp.38):

1. The user wants to access a protected resource, e.g. she browses to the Web site of a service provider without being authenticated so far.

2. She selects her preferred identity provider to sign in from a list that is presented by the Web page of the service provider.

3. There are three options how the login via identity provider can be realised:

    a) The user is *redirected to the identity provider's Web site* and provides the usual login information there.

    b) By clicking a link on the service provider's Web page a *dialogue box* from the identity provider pops up and login information is required.

    c) The Web page from the service provider contains an *embedded login form* from the identity provider. In this case the user may provide his login credentials in plaintext to the service provider, who controls the source code. This privacy/security risk should be taken into consideration.

4. After successful login procedure, the service provider establishes a session based upon the users' identity federation with the identity provider.

When a user signs in at one provider, he will be authenticated at all members within the same circle of trust and may use the other services without entering authentication information again.

6.1.5 Policy Management

Liberty Alliance does not allow for policy negotiation and enforcement between users and identity/service providers. (Liberty Alliance Project, 2005, p. 8) only gives an overall policy/security note:

"Identity federation must be predicated upon prior agreement between the identity and service providers. It should be additionally predicated upon providing notice to the user, obtaining the user's consent, and recording both the notice and consent in an auditable fashion. Providing an auditable record of notice and consent will enable both users and providers to confirm that notice and consent were provided and to document that the consent is bound to a particular interaction. Such documentation will increase consumer trust in online services. Implementors and deployers of Liberty-enabled technology should ensure that notice and user consent are auditably recorded in Liberty-enabled interactions with users, as appropriate."

Thus, policy management is shifted to local responsibility of identity providers and service providers and is not part of the Liberty Alliance framework.

6.1.6 History Management

Liberty Alliance does not provide any history functionality. Such features may be implemented by identity and service providers directly. However, in this way it is more

difficult for the user to keep track of which data she disclosed when, to whom and for what purpose.

6.1.7 Context Detection

Liberty Alliance supports no automatic choice of a digital identity according to preferences stated by the user.

For exchange of information about users between service providers and identity providers, various subclasses of information and their formats exist, called *metadata and schema* (Liberty Alliance Project, 2005, pp. 22). This defines the context for technical exchange of information about the user:

- *Account/identity* information is an opaque handle to identify the user within a special context, i.e., the handle enables service provider and identity provider to refer to the same user in the context of a transaction.
- The *authentication context* describes which technologies, protocols and processes are used for authentication of users. Such metadata needs to be communicated between service providers and identity providers to ensure interoperability and fulfilment of additional requirements, e.g. legal obligations with respect to how users need to be authenticated.
- The *provider metadata* are data concerning identity providers and service providers, which is required for establishing communication between each other. X.509 certificates or service endpoints are examples for provider metadata.

6.1.8 Client-based vs. Server-based Storage of Personal Data

According to the Liberty Alliance standard, user data are stored on different servers which only contain parts of her data. Therefore different circles of trust exist. The user decides which of her data can be processed by which circles (c.f. Figure 4).

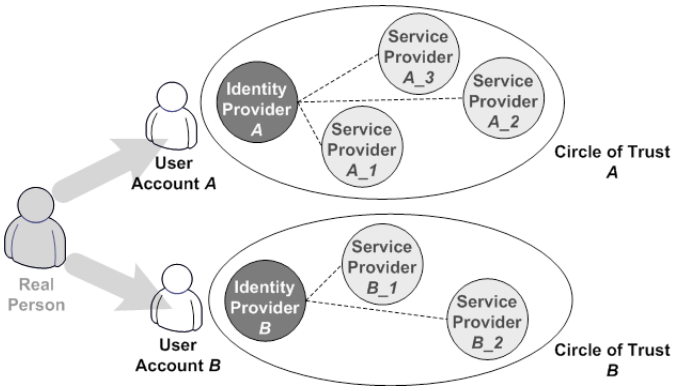


Figure 4: Federated Network Identity and Circles of Trust

(according to Liberty Alliance Project, 2005, p. 6)

6.1.9 Security measures implemented

The "Liberty ID-FF Architecture Overview" specifications document includes some general security guidance that need to be considered by implementers of a Liberty-based FIM architecture. Those guidance notes are mentioned in the form of "POLICY/SECURITY" notes throughout the different parts of the document (Liberty ID-WSF) .

The “Liberty ID-WSF Security Mechanisms” specifications document (Liberty ID-WSF) defines in more detail a set of mechanisms for authentication, signing, and encryption operations performed for communication between entities during identity federation for web service access.

In most identity-based web services, the authorization of a service requestor to access the resource is based on the authenticated identity of the requestor, the resource in question, and an authorization policy (typically enforced at the accessed web service). The authorization process involves several parties (IP, SP, Resource, etc…) to communicate authentication data and metadata by means of “messages” transferred over “channels”. The table below (figure 5) shows the security mechanisms and the correspondent channel or message security requirement.

Security Mechanism	Channel Security	Message Security (for requests, assertions)
confidentiality	required	optional
pre-message data integrity	required	required
transaction integrity	–	required
peer-entity authentication	Identity provide – required Service Provider – required	required
data origin authentication	–	–
non-repudiation	–	required

Figure 5: Security Mechanisms and Channel/Message security requirements (Liberty Specs Tutorial)

Channel Security can be achieved only if the following rules are implemented:

- A Service Provider can authenticate the IdP using IdP server-side certificates.
- Mutual authorization: each Service Provider is configured with a list of authorized IdPs and each IdP is configured with list of authorized SPs.
- Before a user presents personal authentication data to IdP, the authenticated identity of IdP must be presented to the user.

Message Security is achieved by means of digital signatures only if the following applies:

- Digital signatures should use key pairs distinct from those used for TLS and SSL, also suitable for long-term use.
- Request protected against replay and responses checked for correct correspondence with issued requests

6.1.10 Security of protocols

According to the “Liberty ID-FF Protocols and Schema specification” document (Liberty ID-FF Protocols and Schema Specification), the Liberty protocol suite consists of the following protocols:

- **Single Sign-On and Federation:** The protocol by which identities are federated and by which single sign-on occurs.

- **Name Registration:** The protocol by which a provider can register an alternative opaque handle (or name identifier) for a Principal.
- **Federation Termination Notification:** The protocol by which a provider can notify another provider than a particular identity federation has been terminated (also known as de-federation).
- **Single Logout:** The protocol by which providers notify each other of logout events.
- **Name Identifier Mapping:** The protocol by which service providers can obtain (often encrypted) name identifiers corresponding to an identity federation in which they do not participate.

However, this specification document does not define security requirements for those abstract protocols, but rather defer them to Liberty-defined individual protocol profiles defined in another specifications document which is the "Liberty ID-FF Bindings and Profiles specification". Nevertheless, confidentiality, privacy, and authentication mechanisms and a message authorization model are defined as basic and generic security requirements to be fulfilled by the protocols and their deployment environment (Liberty ID-WSF).

Confidentiality and Privacy Mechanisms

Confidentiality and privacy mechanisms are basically concerned with protection of the information communicated between trusted parties and recipients of resource access requests. The required measures to be employed to attain a certain level of confidentiality include *Transport Layer Channel Protection* which mandates integrity and confidentiality of information communicated between peers based on SSL/TLS cipher suites. The document recommends a set of TLS 1.0 cipher suites to be used, and anticipates that AES-based cipher suites will be "widely adopted and deployed". It is also recommended to use certificates and private keys which are distinct from the SSL/TLS certificates/keys for signing and verifying protocol messages. *Message Confidentiality Protection* requirements mandate the use of SOAP message security mechanisms to encrypt the child elements of the message body, and the use of Encrypted Name Identifiers and Encrypted Attributes mechanisms which are also necessary for *Identifier Privacy Protection*.

Authentication Mechanisms

The specifications in (Liberty ID-WSF) define a set of authentication mechanisms (with specific identifiers) which are differentiated according to their ability to provide *Peer Entity Authentication* and *Message Authentication*. The peer entity authentication mechanisms are concerned with either unilateral peer entity authentication, or mutual peer entity authentication, both relying on the inherent security properties of the SSL/TLS protocol, and requiring usage of X.509 v3 certificates for authenticating the peers by demonstrating procession of the key bound to the corresponding certificate. The message authentication mechanisms rely on the integrity properties stemming from the digital signatures applied on the message header and payload. Three mechanisms are defined in this specification which are: "X.509 v3 Certificate Message Authentication" based on the WSS X.509 Certificate Token Profile, the "SAML Assertion Message Authentication" based on the WSS SAML Token Profile, and the "Bearer Token Authentication" which rely on bearer semantics (e.g. SAML bearer tokens).

6.1.11 Other security aspects

Referring to the four layer model introduced in section 5.10 the Liberty framework in addition to layer 2 also covers the layer 1.

The document "Liberty Identity Assurance Framework"[60] covers security requirements related to identity. Participants in the Liberty Framework need to comply to a set of predefined security measures. The quality of the implementation of these security measures is described in four assurance levels. For each assurance level the degree of implementation of the same set of security measures is described. Section 3.7.1 (p. 58) of the "Liberty Identity Assurance Framework" covers infrastructural aspects at the identity provider. This includes:

- Handling and **organisational protection of secrets** (e.g. passwords and PINs)
- **Risk assessment and risk treatment** regarding commonly known attacks in the area of technical **attacks on secrets** (e.g.passwords and PINs) and **systems** (e.g. by introduction of malicious code and out-of-band-attacks)
- Physical and environmental security
- Access control procedures
- Secure storage of secrets (mainly encryption)
- Security relevant event and audit logging, analysis of log data
- Implementation of changeable secrets

[60] Version 1.1, 2008, see http://www.projectliberty.org/liberty/content/download/4315/28869/file/liberty-identity-assurance-framework-v1.1.pdf

6.2 Shibboleth

6.2.1 Control over identity through privacy

Shibboleth is a standards-based, open source software package for web single sign-on across or within organizational boundaries.[61] It was designed for the purpose of providing users of one organisations infrastructure access to online resources from both inside and outside the organisation. Shibboleth 'sits on top' of an organisation's authentication technology and provides a web single sign-on functionality for online resources. It supports the setting up of agreements and interactions between an organisation (the Identity Provider (IdP)) and the resource provider (Service Provider). These agreements can subsequently be used for all new relations with whom an organisation wishes to federate (Internet2, 2008). Predominantly, Shibboleth aims at deployment in universities.[62]

Shibboleth is focused on those institutions that want to federate the identities of their users (students, employees). Because of this, both the initiative for a federation and the approach to privacy depends on the institution's approach (Internet2, 2008). However, Shibboleth emphasizes on user privacy and control over information in the access control arena (Erdos & Cantor 2002). According to the Shibboleth information sheet, the Identity Provider only sends minimal data to a Service Provider, and such data is only sent at the time a user accesses the resource (of the Service Provider), so the service provider does not have to store data about the users (Internet2, 2008).

Shibboleth-based federated administration allows the Service Provider to rely on the administration of user identities and attributes at a users' origin site (the IdP) (Erdos & Cantor 2002). The origin site provides the attributes of a user to the Service Provider, on the request of this Service Provider.

Ex ante and ex post information to the end-user

Information about data storage and disclosure to resource providers in the federation will mostly need to be distributed by the Identity Provider. Shibboleth does not provide a standard interface or user tool which informs and supports the individual, so the use of identities and underlying data need to be communicated by the IdP. Data disclosure will to an extent depend on the local privacy policy of the organisation that construes and issues an identity. How this privacy policy is presented to the individual is left up to the discretion of the IdP.

Choice and consent (and audience segregation)

The amount of choice over identities that an individual has depends on the amount of identity providers that join a federation in which a service provider is present. In theory it is not unlikely that, even though Shibboleth is implemented, a user can only use one identity for the services in a federation, because she joins only one organisation that is federated to a service.

Choice between identities is also related to the contexts in which an identity can be used. As an organisation (the IdP) initiates the identity federation, the amount of resources/service that can be accessed with a certain identity shall be related to the agreements an IdP has made with resource providers and the role and authorization of the user in the 'original' environment (campus, employer, etc.).

---

61 'About Shibboleth', http://shibboleth.internet2.edu/about.html, last accessed August 16, 2008

62 See also the educational scenario in paragraph 4.4.1

The choice over the amount of data sent to a service provider depends on the possibilities for the user to define an 'attribute release policy', which should be the responsibility of the Attribute Authority at the Identity Provider (Erdos & Cantor 2002). However, Shibboleth does not specify how such policies should be stored and managed. Thus, the use of such a policy depends on the decisions made by the implementers of Shibboleth.

Finally, Shibboleth associates a "handle" to a user at the moment she wishes to enter a resource. The use of this handle avoids making it necessary to exchange the user's name (or any other identifying information) between the IdP and service provider. Shibboleth advises not to use an existing user-id as a handle for IdP–SP communication, because this would make it possible to retrieve user's data from examining the handle alone (Erdos & Cantor 2002).

Alteration and deletion

User attributes in a Shibboleth federation are stored at the 'home institution' (the IdP) (Coyle 2007). Hence, alteration and deletion of identities and their underlying data is bound to the policies and requirements from this institution.

6.2.2 User adoption characteristics

Trustworthiness (from the user's point of view)

Because identity federation with Shibboleth is initiated by an organisation with which a user already has a relation with, trustworthiness of the system can be achieved by the reputation of this organisation, their information provisioning about security towards the user, and the agreements they make with the Service Providers that join the federation.

Shibboleth does not have a standard user interface for attribute exchange, and many actions happen behind the scene, which makes it difficult for the user to derive trustworthiness from the technical features of Shibboleth.

Efforts, skill level, social settings, costs

Users do not need to adopt the Shibboleth infrastructure by themselves. Adoption is a task for the institutions that wish to implement the system. Moreover, use of Shibboleths is not complex, as much of the actions are opaque to the user. The complexity of the system happens 'under the hood'.

6.2.3 Management of Digital Identities

In Shibboleth the user is assigned to a so-called *home organisation*, which acts as her identity provider and administers her attributes. Decision whether a user is allowed to access a resource from a service provider is made by the service provider based on values of attributes that are required by the service, e.g. age or affiliation with an organisation.

Various digital identities may be created by allowing different service providers to learn different sets of attributes about a user. An *Attribute Release policy* specifies which attributes and values, known by the identity provider, can be released to service providers (c.f. 6.2.5). Shibboleth allows users to create their own Attribute Release policies and thus to be in control of their digital identities. Otherwise, the identity provider takes on this responsibility.

A user may have a unique persistent pseudonym as identifier at each service provider, thus recognition of the user by the particular service provider is possible. However several service providers are not able to exchange information about this user.

6.2.4 Authentication Management

The workflow for authentication with Shibboleth is visualised in figure 6 and described below (Eduserv 2008; Shibboleth 2005):

1. First, the user wants to accesses a protected resource, e.g. a Web site.
2. The resource redirects the user to *Where Are You From* service of Shibboleth, so that she can select her identity provider. Depending on the policy of the federation, the user may be able to record this preference, perhaps in a cookie, for future use (c.f. 6.2.7).
3. The user's browser is then directed to her identity provider and includes the authentication request from the service provider.
4. The user is authenticated with the help of the identity provider, by whatever means her identity provider deems appropriate for this federation with the service provider (e.g. username/password).
5. After successful authentication, a one-time handle is generated for this session, and the user is returned to the resource at the Web site of the service provider.
6. The resource uses the handle to request attribute information from the identity provider for this user.
7. The identity provider allows or denies the attribute information to be made available to this service provider depending on the *Attribute Release policy*.
8. Based on the attribute information made available, the resource then allows or denies the user access to the resource.

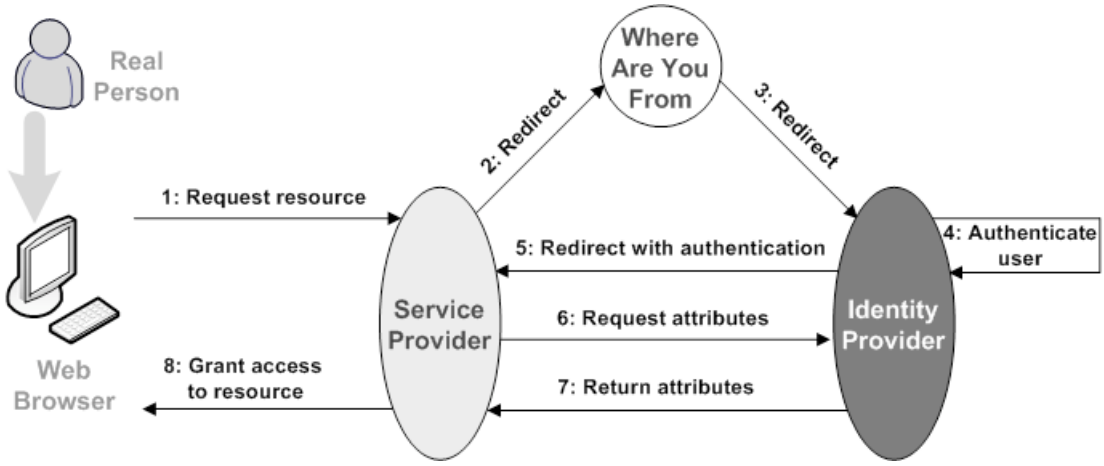


Figure 6: Shibboleth authentication process (according to Eduserv, 2008)

Authentication requests and assertions are made using the SAML standard (OASIS, 2008). For privacy and security reasons, assertions are signed with the key of the identity provider and encrypted with the key of the service provider.

6.2.5 Policy Management

Shibboleth offers *Attribute Release policies* that determine which personal attributes can be released to whom under which circumstances. The Attribute Release policies may be defined either by the identity provider or by the user herself using the Shibboleth Attribute Release Policy Editor (Federation.ShARPE, 2007), for instance. Currently, no management interfaces are available that allow enforcement of the specified policies (Eduserv, 2008).

Service providers can specify *Attribute Acceptance policies* that determine which attributes and values are accepted from which identity providers.

6.2.6 History Management

No information found.

6.2.7 Context Detection

Contexts in Shibboleth are bound to service providers. That is, if a user is known to a service provider, requesting the *Where Are You From* service can be skipped and the authentication process (c.f. 6.2.4) is abbreviated automatically.

6.2.8 Client-based vs. Server-based Storage of Personal Data

Since Shibboleth stores personal data on server-side, the user has to trust her identity provider. The advantage of the server-based storage is the availability of the information without being bound to a client device.

6.2.9 Security measures implemented

Shibboleth has a relatively complex architecture. The current version of the Shibboleth architecture specification is written in the OASIS Security Assertion Markup Language (SAML, particularly SAML2) (SAML 2003).

In fact, Shibboleth implements a selection of the possible SAML assertions (McLeish 2008). Therefore, many of the security strengths of Shibboleth rely on the security considerations of SAML (SAML 2005) For example, in Shibboleth, an SP provides a service to authorization or customization on the basis of a *security context*[63] established by means of SAML browser profile (Shibboleth, 2005b).

Shibboleth, as a FIM architecture, comprises a set of security services that enhance the basic system. A simplified view of the Shibboleth architecture is based on a Service Provider (SP), and Identity Provide (IdP), and a Federation Manager implementing a “Where Are You From” (WAYF) service (Witheridge 2006). At each resource that need to be secured, the corresponding SP includes Shibboleth Attribute Requester (SHAR) and a Shibboleth Indexical Reference Establisher (SHIRE). Users are registered at IdPs that include an Attribute Authority (AA), a Handle Service (HS) and a local authentication system (by which users sign on) (Rixon 2005). The WAYF service is chosen by the SP and can therefore be run by it.

[63] Security context: the semantic union of the message's security header blocks (if any) along with other security mechanisms that may be employed in the message's delivery to a recipient. E.g. security mechanisms employed at lower network stack layers such as HTTP, TLS/SSL, IPSEC, etc (OASIS 2005b).

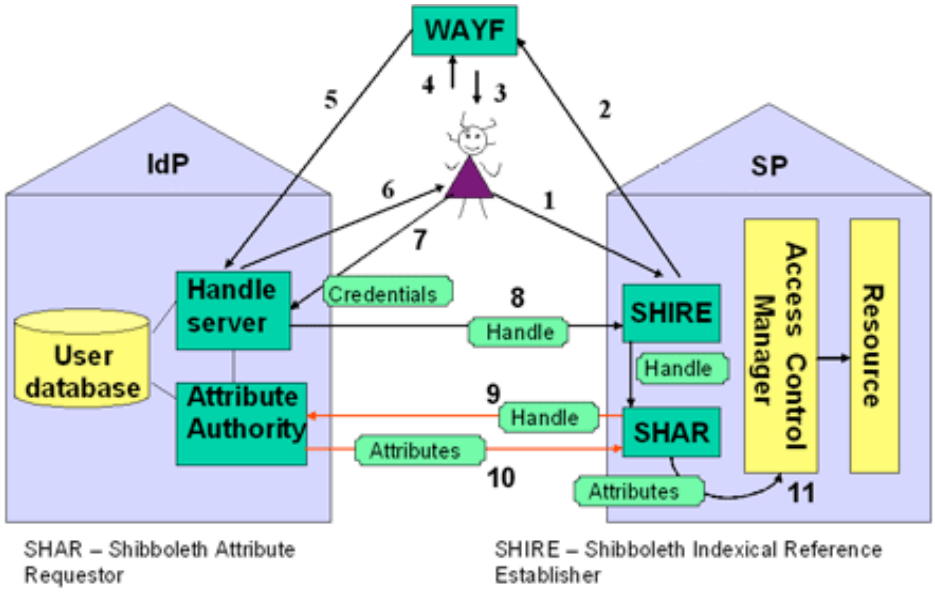


Figure 7: Simplified Diagram of Shibboleth Architecture

As shown in Figure 7, the steps 1 to 8 between the SHIRE, the WAYF and the HS are used to establish a *handle*[64] for a certain user attempting to connect to a service. In steps 9 the SHAR provides the handle to AA which returns (in step 10) a set of attributes based on which the Access Control Manager at the SP can make an authorization decision for the user to access the specific service (Rixon 2005; McLeish 2008).

The security features implemented in Shibboleth can be summarized as follows (Witheridge 2006):

- Message Authentication: based on PKI certificates for mutual authentication of messages exchanged between the IdP and SP.
- Transport Layer Security: based on the SSL/TLS protocols to protect communication between different parties of the architecture.
- Message Layer Security: based on XMLSignature and XMLEncryption for protecting SAML assertions based on which user authentication is communicated from an IdP by means of a user handle.
- Federation Metadata (trust relationships) Protection: based on message and transport layer security between IdP and SP.
- HTTP state management: based on session cookies, providing SSO capability and protected against theft and session hijacking by means of IP address checking.

6.2.10 Security of protocols

Following are the main security aspects of the generic protocols taking place from the time a user attempts to access a service through the service provided, until he is authorized to access the service (Rixon 2005).

1. Determining the user's home site

The site where the user is registered and can sign on using a local password is determined when the SHIRE intercepts the attempt to access the web resource. This initiates the search

[64] A temporary, anonymized and unique reference to the user that is understood by the other services at the user's point of registration.

for a handle, which is typically delegated to the WAYF service. The Shibboleth specification implicitly requires the WAYF service to provide "some means for the user agent to cache the user's selection, perhaps using HTTP cookies…" in order to retain the user's information for future authentications (Rixon 2005).

2. Getting the handle

When a handle is derived by the HS, the latter encodes it in a *SAMLResponse*[65], and applies a digital signature on it. This response is presented to the user within an HTML form as a hidden parameter (base-64-encoded). The form tells the user the kind of security information shared with the SHIRE. The latter validates the signature of the SAMLResponse, e.g. using a "certificate passed along with the [*SAMLResponse*]".

3. Getting the attributes

In steps 9 and 10 of the figure, where the SHIRE and AA exchange handle and attributes by means of SAMLRequest and SAMLResponse, the two entities can use any protocol, but the Shibboleth specification requires support of SOAP 1.1 and HTTPS (it is up to the virtual organization to choose any or none of those two).

4. Precautions

Furthermore, the Shibboleth target deployment guide (Shibboleth 2004) recommends a set of security precautions to be satisfied by the deployment environment for the protocols not be compromised. The recommendations can be summarized as follows:

a) SSL, though optional for target sites, should be used when possible (Federation guidelines should be considered), especially with client machines in order to avoid man-in-the-middle-attacks, and to protect sensitive data.
b) Safeguarding the WAYF service is necessary to avoid attacks during redirection steps, as well as ensuring that rogue targets and origins are not used.
c) Enterprise directory of users require proper security measures on directory acess and population (avoid plaintext passwords).
d) Server platforms should be properly secured, cookies on client machines well protected.

6.2.11 Other security aspects

Shibboleth is relying on the "InCommonFederation"[66] policies, requirements and information. Participants in the Shibboleth federation need to sign a compliance agreement with documents published there. In the section "technical information"[67] also aspects of security are covered, but this is mainly related to the handling of identifiers and the set up and operation of certificate authorities. Aspects of operation systems security, environmental security etc. are not covered in these documents.

[65] XML structure defined by the Security Assertion Mark-up Language

[66] See http://www.incommonfederation.org/

[67] See http://www.incommonfederation.org/technical.html

6.3 PRIME

The assessment of the PRIME-project solution to IdM is mostly based on an analysis of documentation, which can be retrieved on the website of the PRIME-project.[68]

6.3.1 Control over identity through privacy

The PRIME IdM solution aims to develop an IdM system, which is user centric and privacy-enhanced. Because of this, the EU funded research project has the principles of data minimisation and 'maximum privacy' as starting points. During its life span it has developed IdM solutions based on state of the art technologies in the field of privacy enhanced technology (PET).

By default, the PRIME IdM solution makes interactions anonymous, e.g. by concealing network addresses of the user. Moreover, the system relies on the use of various partial identities, cryptography, user policy negotiation, user data tracking, and user assessment of platforms and services. The system uses credentials and, where necessary, makes use of PKI and trusted third parties (Fischer-Hübner & Hedbom 2008).

The PRIME functions with a user-controlled module (that can take over IdM tasks from applications like web browsers) and a module located at the service. PRIME uses a holistic approach to privacy-enhanced IdM, which takes economic, legal, HCI, and social considerations into account. For its legal considerations, PRIME takes the EU Data Protection Directive (95/46/EC) as a starting point.

Ex ante and ex post information to the end-user.

The PRIME console, which is the module located at the end-user's end, aims to inform the user by means of a standard user interface, which handles all privacy-related functionality (Casassa-Mont et al., 2007, p. 25). The interface can take over web-based interfaces so the user has a consistent experience when it concerns IdM.

Prior to data collection, information is provided to the user by the PRIME console with a function that asks if data may be sent to the service provider. This 'Ask Send Data module', functions as a click-through agreement (Pettersson 2008, p. 24). The module indicates the data to be sent, which organisation is the receiver, and the terms and conditions of data sharing (Pettersson 2008, p. 24). Another feature of the console is that it can indicate the integrity of the data receiver, by means of an assurance evaluation.

In PRIME, users can define predefined privacy preferences for certain services. These predefined settings are indicated with icons (e.g. a mask for anonymous, and a face for the situation when data is stored) (Pettersson 2008, p. 28). The different icons inform the user of the kind of identity that is being used in a specific situation.

With regard to information provisioning after data has been collected, it is relevant to mention that the PRIME solution provides a 'data track' function, so the consumer can recall when data is requested and used and which agreements have been entered.

In general, it needs to be mentioned that the PRIME project provides additional information about the operating procedure of PRIME technologies by means of tutorials and extensive documentation. This information gives insight in the working of PRIME applications.

[68] See: http://www.prime-project.eu, last visited August 13, 2008

Choice and consent

Anonymous communication is one of the starting points of PRIME. Because of this, the system allows users to choose in which way they want to present themselves to others, varying from anonymous communication to the use of different partial identities (including pseudonyms). Of course, the kind of identity used and the attributes that are part of this identity, need to be in conformity with the requirements of the service provider. However, assuming that a service provider also uses PRIME technologies, multiple identity-choices are supported. Moreover, the use of (certified) credentials makes it possible to create (trustworthy) identities without a need for superfluous data exchange.

The PRIME console assists in making a choice for a specific identity and negotiates between policies. When the requirements of the user are in harmony with the demands of a service provider, data exchange can take place automatically. If this is not the case, the user will be asked to choose a suitable identity and will need o consent to data use by means of the ASD-module.

Several preference settings can support the user in choosing the right policies and identities for the interactions she engages in. With the use of such preferences, the PRIME console can automatically confine the use of identities in certain contexts.

Alteration and deletion

PRIME software installed at the user end and service end makes data management at the service side possible. The PRIME Architecture gives the examples of 'access control mechanisms' that can enforce the privacy policy subject and 'privacy obligation management', which allowas automatic enforcement of privacy policy aspects (a.g. automatic deletion of data after an agreed period of time) (Casassa-Mont et al., 2007, p. 25). According to the PRIME architecture, the user manages all privacy-related data in a centralized store, which makes it possible to keep track of data disclosure and data access by others (Casassa-Mont et al., 2007, p. 25).

6.3.2 User adoption characteristics

Trustworthiness (from the user's point of view)

PRIME aims to create trust by means of several functionalities in its system, like the possibility to assess the user's platform and the platforms that receive data on their security aspects, e.g. by means of an assurance evaluation function in the PRIME console (Andersson et al 2005, p. 30), and possibility to track the data handling by service providers.

On a higher level, the starting points of the PRIME project contribute to trust establishment, because with anonymous communication and user control as starting points, vulnerability of the end-user will be decreased which increases the trustworthiness of the system and its participating parties. In this regard, the possibility to prove identity-related claims with (anonymous) credentials and cryptography are worth mentioning, as these techniques make it difficult for others to link data or to tamper with identities.

Trust factors that are important for customers that use IdM systems, but which have no direct relation with the technical security of a system like reputation, previous experiences, security seals, and external audits, are present in the PRIME technology by means of the consistent use of the PRIME console. Because this is the interface that handles all data transactions, it functions as a trust-establishing mechanism.

Efforts skill level, social settings, costs

PRIME has not developed commercial applications for IdM. The PRIME project, which is a research project, has however developed several prototypes for example in the field of location based services (LBS), or collaborative eLearning (CeL). The PRIME IdM solution has not been implemented in existing operating systems or web browsers yet, which makes a fast adoption of the technology unlikely at the moment. Moreover, the adoption of PRIME is likely to be affected by the fact that for PRIME adoption, both on the user-side as the service-side, a PRIME module has got to be implemented, which makes it hard to reach critical mass (Casassa-Mont et al., 2007).

PRIME has functionalities that make it possible to automatically or semi-automatically handle the exchange of personal information (Pettersson 2008). Moreover, the use of predefined preferences and identities can improve usability and can speed up the process of IdM (consent and policy negotiation) for an end-user. However, the emphasis on user control and data minimisation can also have a reverse side. First of all, customers may have difficulties to understand the PRIME concepts of, for example, anonymous communication, unlinkability, and credentials-based authentication. Moreover, it may be difficult for the end-user to comprehend when and why different identities actually need to be used. The need for privacy on the internet may become more and more clear to many people, but it is unclear if an average internet user can understand why PRIME is actually the solution to this problem. Fortunately, instruments like the PRIME-tutorial do give some insight in the functioning of PRIME. Moreover, it is an advantage that these tutorials are elaborated in several languages.

For a seamless PRIME-enabled IdM experience, it is necessary that users define preferences and contexts, so the system can act semi-autonomous. However, without these efforts, use of PRIME may be burdensome and even a frightful experience, because warnings and requests for data can succeed each other quite rapidly. Hence, PRIME adoption requires some effort of the end-user. Only when an end-user is willing to invest in using the system, adoption will be achievable.

6.3.3 Management of Digital Identities

The *PRIME Identity Manager* (see figure 8) allows the user to administer her personal data within PRIME and to configure various settings concerning his digital identities. These setting's are called *Preference Sets* (short form: *Presets)* for version 2, respectively *Privacy Preferences* (short form: *PrivPrefs*) for version 3.

The usual process of user's management and usage of her digital identities is handled dynamically by the so-called „Send Personal Data?" – Dialogue. This module intercepts the data flow of a common application and directs it to the PRIME system. PRIME then requests user's input for the handling of the disclosure of her personal data and redirects data to the application accordingly. Thereby the user has the option to choose data for transfer to the transaction partner, e.g. pseudonyms, credentials etc. The user also provides her informed consent via the „Send Personal Data?" – Dialogue.

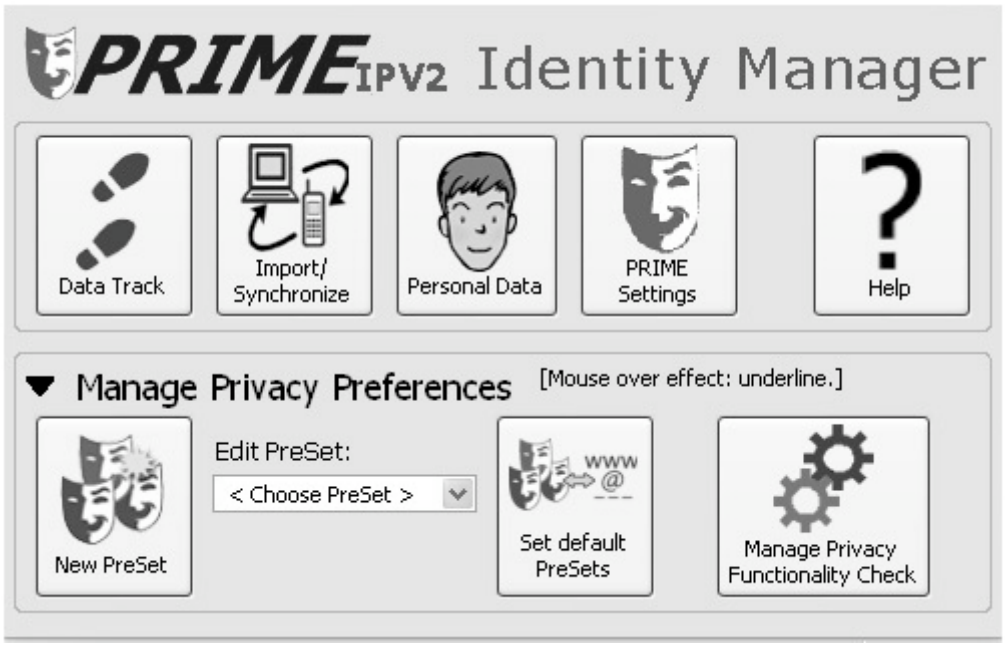


Figure 8: User Interface of the PRIME Identity Manager

6.3.4 Authentication Management

Assuming that both, the user's device and the service provider have installed the PRIME middleware, authentication of the user takes place as follows (Casassa-Mont et al., 2007, pp. 64):

1. The user browses to the Web site of a service provider and wants to get access to a protected resource.
2. In this case, when personal information from a user is required, the PRIME middleware of the service provider sends a request for an identifier of the user (e.g. pseudonym) to the PRIME middleware on the user's device.
3. On the user's device a pseudonym is generated and sent back to the service provider, who checks whether data about this pseudonym is already available in the data base and if authentication based on these data is possible.
4. If this check fails, further information is requested from the user. For each piece of requested data the service provider submits data handling policies that describe the purpose of the data collection (e.g. payment) and related obligations (e.g. deletion of data after defined period of time).
5. The user device checks whether the provided data handling policies from the service provider match the user's preferences and, after positive matching, the requested personal data is sent to the PRIME middleware of the service provider and passed on to the application.
6. Now the user can be authenticated and access to the restricted resource is granted. The PRIME middleware is responsible for enforcing data handling policies, e.g. deleting the data item after a fixed period of time.

6.3.5 Policy Management

In PRIME users state their preferences concerning the handling of their personal data by defining Presets (and choosing PrivPrefs in version 3, respectively). Service providers submit templates for *data handling policies* bound to each requested personal data items. Before a user discloses personal data, both the user and the service provider agree on those data handling policies.

The negotiation process starts with the data handling preferences of the user and the template for the data handling policy presented by the service provider. Preferences set by a user are enforced by comparing each request for personal data by a service provider against the user's statement. Only if the negotiation process succeeds, i.e., there are no conflicts during the comparison or there is an explicit consent of the user, requested personal data is revealed under the agreed policy. The service provider guarantees for enforcement of the data handling policy (Casassa-Mont et al. 2007; PRIME, 2008a).

6.3.6 History Management

The Data Track is the PRIME history feature allowing the user to review all her transactions at different points in time, including any personal data revealed to service providers. Thus, it is possible to reconstruct how much personal data a service provider has accumulated and to estimate if he may be able to draw any unwanted conclusions from that information. The Data Track records are automatically logged during user's interaction with the "Send Personal Data?" – Dialogue and enables her not only to understand which personal data were disclosed, but also to whom, when, and for what purpose.

The graphical interface of the Data Track presented to the user offers different views to her data, as well as search functionality and a help dialogue.

6.3.7 Context Detection

By configuring settings for digital identities, the user explicitly states how personal data shall be handled in different contexts, i.e. concerning different service providers or different activities of the user. So-called *bookmarks* can be used by the user in order to define which pre-configuration of privacy preferences should be applied to which service provider (Bergmann, 2007). Thus, context detection in PRIME version 2 is bound to service providers. Version 3 expands the definition of context to activities, since users can choose between PrivPrefs that focus on the purpose of a transaction, e.g. "anonymous surfer" or "returning customer" (Bergmann et al., 2008).

6.3.8 Client-based vs. Server-based Storage of Personal Data

In PRIME, personal data of users including credentials issued by distinct authorities are stored on client-side. Thus, the user is in control of her data, but always needs access to her client device which is running the PRIME middleware in order to use the identity management service.

6.3.9 Security measures

PRIME security architecture can be viewed from three different perspectives. First, the personal data stored within the secure data storage of each PRIME core[69] is secured with the PRIME policy engine. The second perspective is of the trusted certificates imported into the

[69] Communication entities running the PRIME software are called PRIME core, e.g. the web services on server side, but also a local PRIME core installed at the clients machine.

key stores of the different entities in the PRIME communication model. Finally the third perspective are Basic Authentication passwords to further protect specific web services with privileged access.

6.3.9.1 Policy Evaluation for the Secure Data Storage

Every PRIME core includes a protected data storage for holding personal information. Information can be stored into the storage without policy evaluation, but retrieval of information (disclosure) is

- evaluated by the PRIME policy engine,
- logged in the PRIME Data Track and
- delivered with all data handling policies attached.

The policy language can request the presentation of credentials or other information (e.g., passwords). Credentials are either anonymous Idemix credentials or signatures created with OpenPGP. In the data disclosure process when browsing with a PRIME enabled web browser, the personal data as credentials or passwords are transferred directly between PRIME cores and never gets disclosed to either the client web browser nor the server's web application.

6.3.9.2 Trusted Certificates between PRIME cores

For all communications between PRIME cores and all web service access is done using TLS/SSL and https with server certificates. The connection is only established, when the server certificate is known and trusted to the requesting key store. In case of unknown server certificates to a PRIME client core, a pop-up message informs the user and allows to override the security warning.

Public Key Infrastructures are honoured by the key store and the developer version of PRIME comes with a pre-installed certificate issued by the Technische Universität Dresden as well as scripts and documentation how to create an own Public Key Infrastructure.

6.3.9.3 Privileged Web Services and Basic Authentication

Some Web Services within PRIME have privileged access to the data storage or provide configuration functionality. Most of these Web Services are only required during development or during the server set-up. They are not started by default and have to be activated by specifying an access password.

When accessing the Web Services, Basic Authentication Scheme over https is used to restrict the access. A password can either be set for the whole Web Service or for individual functions in one Web Service API. Should Basic Authentication not be sufficient, it is possible to extend PRIME and perform more sophisticated access control, e.g. by using the PRIME policy engine.

Further details about the security measures for PRIME can be found in (Casassa-Mont et al., 2007 and Camenisch et al 2009).

6.4 Microsoft Cardspace

The assessment of Windows CardSpace is based on an analysis of documentation, scientific papers, and the user interface of the system[70].

6.4.1 Control over identity through privacy

Windows CardSpace ('CardSpace') is a system that does not mandate a single approach to digital identity, but aims at being an 'identity metasystem'. The system is agnostic about the format of the security token that is used, so CardSpace can work with multiple digital identity systems (Chappell 2006). Moreover, CardSpace is open standards based (Malinen 2006). It can not be considered as a Single sign-on system.

CardSpace is designed to meet the 'laws of identity', which have been elaborated by Microsoft's Kim Cameron. These laws of identity amongst others comprise the requirement for user control and consent, minimal disclosure of information, interaction with justifiable parties, and preventing unnecessary correlation handles (Cameron 2005). Hence, several privacy considerations have been taken into account in the design of the system. Moreover, one of the design rationales behind the identity metasystem architecture is that consumers will need to be convinced that the solution improves the consumer privacy landscape (Cameron & Jones 2006).

CardSpace aims at identity management at the end user's machine (Malinen 2006), by providing software that is integrated in its Vista operating system, can be integrated with Internet Explorer and other browsers, and can be used on other operating systems. Some of the features of the CardSpace solution are that it can circumvent the use of passwords and usernames at the *service provider*, that it can 'take over the system' of the end-user, and that it provides comprehensible metaphors for digital identities, called 'InfoCards'.

Ex ante and ex post information to the end-user.

The interface of CardSpace aims to provide a consistent user experience for the handling of digital identities. Its 'Identity Selector', one of the core components of the system, enables the user to make decisions about her digital identities, on the basis 'information cards'. The underlying data of an information card can be scrutinized as well.

The interface gives insight in the information that will be sent to a service provider. Moreover, it has the feature of providing the user an overview of the site information and the certificate that has been issued to the service provider (if any).[71] If the service provider has defined a privacy statement, this will can be accessed in the CardSpace interface. However, the information provided to the end-user is to an extent left up to the service provider and the link to this information does not stand out dominantly in the interface.

When an identity needs to be chosen by the end-user, the interface indicates which InfoCards have been used previously in the interaction with the service provider. Moreover, the user can assess when certain InfoCards were shown to a service provider. After an InfoCard has been selected, however, the user may forget under which identity she has logged on for a service.

---

[70] General information about CardSpace can be found on: netfx3.com/content/WindowsCardSpaceHome.aspx , last accessed on August 15, 2008.

[71] This has been regarded as a privacy-flaw in the system, as several levels of security/trustworthiness come together in the same user interface, cf. Alrodhan & Mitchell (2007).

The interface does not give advice which identity or what kind of identity should be used. However, CardSpace has as a starting point that from the chosen InfoCard only the information is forwarded which has been requested by the service provider.

Next to the fact that a end-user can create her own InfoCards, these can be issued to the end-user by identity providers. Such InfoCards are stored at the user machine, but do not comprise 'non-sensitive meta-information' (Alrodhan & Mitchell, 2007). These issued InfoCards can indicate information about the identity provider, like contact information and token information (Cameron & Jones 2006).

Choice and consent (and audience segregation)

The CardSpace system can be regarded as a user-controlled system, as identity cards are stored at the user's device and because she decides if an identity is being used and which identity this will be. If possible, the consumer can issue her self constructed identity cards. However, when a service provider requires an identity that is assigned by an Identity Provider, the amount of identity-choices will depend on the requirements of the service provider, and the amount of IdPs that can meet these requirements.

Because CardSpace is a meta-system, any type of token/digital identity can be used. This means that the end-user can use identities that are based on different standards. This also means that different levels of security or privacy may co-exist inside the CardSpace metasystem.

CardSpace separates the IdP from the service provider and puts the user in the middle of identity management. So, next to the fact that this system makes it possible to keep identities apart, the IdP and service provider can also be kept apart. However, this does not necessarily have to be the case, as the system supports 'auditing identity providers' as well (Cameron & Jones 2006), which can track the use of a certain identity.

The separation of identities throughout context can be assured by the support for 'unidirectional identifiers' (Cameron & Jones 2006), so that identifiers that are given to service providers cannot be linked to the identifiers given to others.

The CardSpace system is based on proving claims. Identities that are provided to service parties, only exist out of the data that is requested by the service provider, which would make linking of personal data on the basis of superfluous information not possible.

Alteration and deletion

In theory, service providers/relying parties do not need to store data. CardSpace facilitates "data rejection", because the Identity selector in the user interface can remember which identity has been used for a site (Cameron & Jones 2006). This information can be re-supplied on request. Sites thus may discard their information about an end-user.[72]

Digital identities created by an end-user herself can be altered and deleted easily in the interface. But there seems no automated possibility to delete any information at the service provider\relying party, when any information is stored at this point. Identities can be removed from the Identity selector, but this will only remove metadata. It will depend on the characteristics and agreements of the Identity Provider if the actual digital identities will also be removed at the IdP. The terms and conditions under which an IdP issues and creates identities may also influence the end-user's possibilities to alter such identities. In addition, there are difficulties when identities are lost or stolen. In such a case, users need to contact identity providers and relying parties (cf. Chappell 2006).

[72] But it seems that it is up to the service provider to make this decision.

6.4.2 User adoption characteristics

The laws of identity, which were already mentioned in the previous paragraph, also elaborate on the need to have human integration, pluralism, and a consistent user experience implemented in an Identity Management System (Cameron 2005). Hence, they ought to have provided a foundation for the usability and adoption features of CardSpace.

Trustworthiness (from the user's point of view)

Trustworthiness can be realized by means of the standard user interface and consistent representation of digital identities for all IdM decisions. This also counts for the fact that users control the identities used in a service, that they can assess the underlying data of an identity, and that the previous use of digital identities can be checked.

One goal of CardSpace is to have reliable site-to-user authentication (Cameron & Jones 2006). Thus, websites should authenticate themselves to the user. To enable this, CardSpace utilizes the use of high value certificates.[73] It depends on the service parties however, to obtain such a certificate. Parties are not obliged to use certificates, so customers may also be confronted with service providers that do not authenticate themselves correctly. Hence, with CardSpace it is not completely impossible that users interact with malicious parties. This depends on the decisions made by the user (Alrodhan & Mitchell, 2007). On the other hand, with CardSpace, malicious parties would not be able to obtain username and password, as this kind of information is not shared between the 'identity selector' and the service provider.

Service providers and identity providers do not need to establish a preceding 'trust relation', to be able to collaborate through CardSpace. However, it is worth mentioning that IdPs may become aware of the identities of the service providers to which the user attempts to log in (Alrodhan & Mitchell, 2007). When this is the case, IdPs may track the customers, which can be detrimental to the trustworthiness of an IdP (as, the end-user becomes more vulnerable to this IdP).

Increased trustworthiness of CardSpace itself can moreover be derived from the fact that most users have experience with Microsoft products. Moreover, the fact that it has developed a local agent for identity management (in stead of a Microsoft-in-the-middle approach), may enhance the overall trustworthiness of CardSpace (but not the organisations that make use of it).

Efforts, skill level, social settings, costs

The comprehensive user interface of CardSpace makes it relatively easy to operate by aN end-user. The metaphor for digital identities (the InfoCard) is understandable to many individuals, and most people will be able to understand their function, without the necessity of understanding its technical complexity. It is not sure however, if users comprehend that the identity cards do not, by themselves, comprise identity information, but metadata in stead.

Because CardSpace is implemented in the Vista operating system and can be used for multiple other OS', it is likely that the adoption of this IdM system is potentially high. CardSpace has a large potential user base, especially because interoperability with other standards and IdM solutions (e.g. OpenIdentity) is one of its starting points.[74]

The CardSpace interface has several help functions and click-through options, which increases the usability for non-skilled users. It is not sure, however, if and how individuals are going to shop for identities at identity providers, and it may still be difficult for them to

[73] In collaboration with VeriSign, see: Cameron & Jones (2006).

[74] Cf. http://www.identityblog.com/?p=668, last accessed on August 15, 2008

comprehend for example the difference between identity provider and service provider. And even though individuals are relieved from the burden of using passwords and usernames for service providers, it is not clear what kind of authentication procedure is necessary at the IdP. Moreover, it is not clear in which languages the help functions are available to the customers.

Finally, users may also have difficulties with the use of their digital identities on different computers. Even though it is possible to export and transfer the InfoCards (cf. Chappell 2006), users may experience difficulties to do so (especially when self-assigned identities need to be transported, or are created on, for example, public computers). In addition, the need to lock and secure local computers becomes increasingly important, when CardSpace is installed on a device.

6.4.3 Management of Digital Identities

CardSpace distinguishes between two basic types of information cards that represent digital identities of users. *Personal cards* can hold varying personal data, e.g., name, e-mail address, date of birth, or similar. This information is encrypted locally and may be sent to partner websites if necessary. However, the user decides which data should be revealed to the respective service provider. Personal cards are also called self-issued cards since the user has also the role of an identity provider in this case. The second type of cards is called *managed cards*. These represent information (e.g. credit card information) provided by other organisations which act as identity providers and maintain the actual data in their systems, while the user's local managed card contains a link to these data (Microsoft Corporation 2008b).

CardSpace allows the user to define any number of personal cards or acquire managed cards. Each card in consists of

- a unique ID,
- time and date of creation,
- a claim about a set of personal data (*security token*), e.g., name and e-mail address, that form a digital identity of the user,
- digital signature of the identity provider.

The user chooses from her set of cards (digital identities) which data should be revealed to the respective service provider. Thus, service providers can have varying knowledge of the user’s identity.

6.4.4 Authentication Management

The process of authentication with CardSpace proceeds as follows (Microsoft Corporation 2008a):

1. The user tries to access a protected resource of a service provider.
2. The service provider communicates to the user’s client, which *security token* would be required.
3. CardSpace filters users’ cards and finds those that would fulfil the service provider’s requirements. The user selects one of those cards, e.g. a managed card. The selected card does not contain personal data, but specifies which identity provider posseses the required information.

4. CardSpace passes the requirements from the service provider further to the identity provider, who generates a respective security token and sends it back to the user's client.
5. After the user gives his consent, the security token is released to the service provider.
6. Based on the personal information included in the security token, the service provider grants the user access to the resource.

In CardSpace, the user has the option to set passwords for particular cards. Thus, even if others have access to her client device, access to her personal data can be protected.

6.4.5 Policy Management

The user decides how many and which of her cards may be transmitted to service providers. Besides necessary data which is requested by the service provider, optional information can be included. Based on a *privacy policy* that service providers should publish, users may decide to interact with that service provider and to release personal information via cards. There are no rules for format or content of such a privacy policy (Microsoft Corporation, 2007).

In order to specify requirements from the service provider concerning acceptable authentication mechanisms (e.g. trusted identity providers, type of security tokens…), user's device retrieves a service provider's *security policy*. CardSpace matches the requirements from the service provider with the user's cards in order to find those cards, which meet the security policy (Alrodhan, Mitchell, 2007).

6.4.6 History Management

In order to keep a record of all personal data that a user has released to service providers, CardSpace stores a history of usage for each card. This history contains the following information (Microsoft Corporation, 2008c):

- Information about the service provider, who has received a card.
- Time and date when the card was sent.
- Type of data that was sent, but not data itself, e.g. item "date of birth" is stored in the history, but not value "1976-04-01".

History information of a card is not transmitted, when the card is revealed to a service provider.

6.4.7 Context Detection

Context detection in CardSpace is bound to service providers as transaction partners. Due to the history that is stored for each card, users can be informed if a new service provider requests a card (c.f. Figure 9) or if the required identity information of a service provider who already obtained a card has changed and additional data is requested[75] (Microsoft Corporation, 2008c). When the user is asked for personal information from a service provider, whose domain has been visited before, CardSpace automatically suggests the most-used card for that service provider.

[75] If additional data is requested, the user may add this information to the respective card, use another one or create a new card for this service provider.

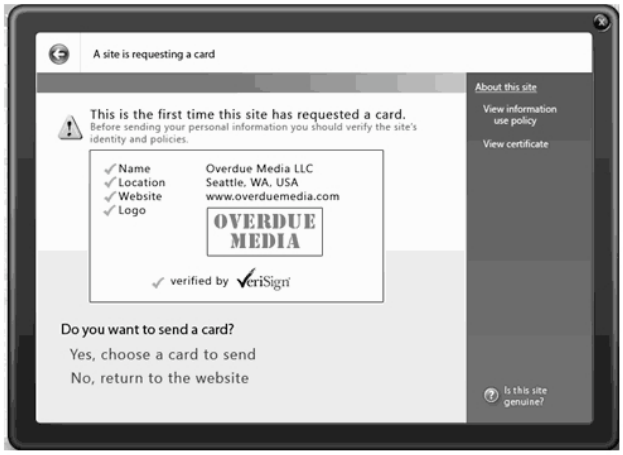


Figure 9: CardSpace Screen when a Service Provider requests a Card for the first time

6.4.8 Client-based vs. Server-based Storage of Personal Data

Contrary to its predecessor Microsoft .NET Passport, CardSpace does not store personal information on a central server. Some data are being encrypted and held client-side, while other data remains on the servers of identity providers. This arrangement defines the de-centralised nature of the CardSpace system.

6.4.9 Security measures implemented

Windows Cardspace security model relies on the idea of Infocards that describe a trust relationship between a user and a security token service (STS). Windows Cardspace employs SAML tokens and is based on WS-Trust, WS-Security, and WS-Policy and WS-SecurityPolicy standards for handling these tokens. Its security is strongly tied to the WS-* efforts led by IBM, Microsoft and Verisign.

WS-Security allows communicating using SOAP messages the security token, which is obtained through the STS of the corresponding IdP based on the WS-Trust standard. WS-SecurityPolicy permits the service provider of web service to express a security policy. WS-MetadataExchange defines a way to exchange service description over the internet.[76]

Windows CardSpace does not depend on the format of the security token obtained from the IdP. Therefore, CardSpace works with legacy digital identity systems, using any type of security token, whether simple usernames, X.509 certificates, Kerberos tickets, SAML tokens, etc.

As default implementation of an STS from Microsoft uses SAML 1.1 assertions as security tokens (Malinen 2006).

A set of security requirements for the deployment have been defined and can be summarized as follows:

- A high-assurance certificate with logotype which provides identity to a user and is used to sign the security token.
- Security Token Service, implemented at the IdP and can process token requests, authenticate users, creates tokens, etc… A policy describes the token capabilities and binding requirements.

[76] Windows CardSpace :en route vers l'identité, http://www.programmez.com/vista/93_vista_windows_cardspace.pdf

- Signed InformationCard per user containing the security token metadata and the user authentication method to the IP.

The security features of the Cardspace architecture are summarized in (Dorrans 2006):

- All communication links are secure.
- Data encrypted in memory until use
- Store is double encrypted and ACLed
- Service provider can be concealed from the Identity Provider
- Signing key for self-issued tokens varies for each SP
- Users can protect cards with a PIN
- CardSpace runs on a private Windows Desktop like UAC in Vista.

6.4.10 Security of protocols

Figure 10 illustrates the protocol between the different entities of the Windows Cardspace model.

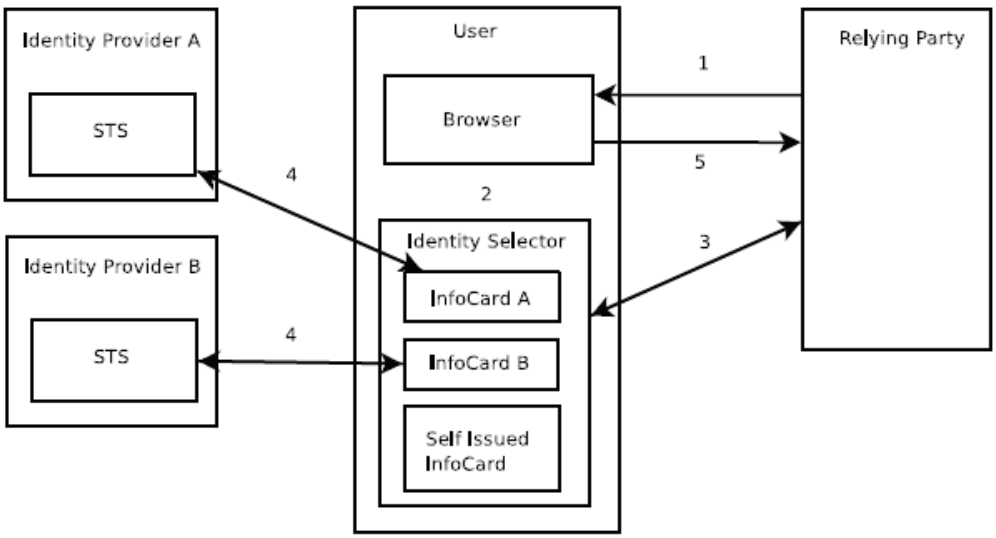


Figure 10: Overview of the Windows Cardspace model Malinen 2006)

The steps of the security protocols involved for acquiring a security token and accessing a service a relying party (Service Provider) are according to (Malinen 2006):

Step1: relying party web site redirects the client to a login page with embedded Windows CardSpace tags. These tags include a number of parameters to be passed to the identity selector, including what information is needed and whether self issued tokens are accepted.

Step2: when user clicks Windows CardSpace authentication button on the web page, the browser's CardSpace support code invokes the identity selector on the client machine.

The identity selector processes the requirements from the relying party and optionally

Step 3: The identity selector can request more specific details about the security policy of the relying party using WS-MetadataExchange. Identity selector then can

decide which InfoCards fulfill the requirements of the relying party and show user a list of choices.

Step 4: user chooses one of the cards and if it is a self issued card, the identity selector will generate a SAML 1.1 assertion as the security token acting itself as an STS. If the card represents an identity at one of the IdPs, the identity selector will request a token using WS-Trust. The tokens that the IdP generates can be of any type the relying party has declared to accept in its security policy in step 1 and optionally in step 3. These third party tokens are treated as opaque binary data by the identity selector. The STS will also generate a proof key for the token and send it together with the token to the client.

Step 5: the browser will use HTTP(S)/POST to send the encrypted token along with proof of possession of the proof key to the relying party. The relying party validates the message and then creates a session for the user.

6.4.11 Other security aspects

A search in the web resulted in no information concerning infrastructural (layer 1 related) security requirements or policies in CardSpace and the Identity Metasystem. Obviously Microsoft in this respect is relying on already existing white papers concerning server and client security[77] on the operation systems level.

[77] See e.g. http://www.microsoft.com/Downloads/details.aspx?FamilyID=90ec8abb-08c7-4706-b730-9a1f9fcf2d9f&displaylang=en

7 Conclusions

This chapter first summarizes some of the salient features of the assessment made in Chapter 6 and then provides some comparative remarks.

7.1.1 Liberty

Liberty can be considered as a business centric approach to identity management, as it is based on collaboration between organisations and on an implementation of its specifications by these organisations. Liberty only provides the specifications for standards-based federated IdM as well as infrastructural components. Liberty itself does not provide services. Regarding privacy and possibilities for users to actively manage their (partial) identities, much is left open to the implementing organisations. They have to adopt the privacy recommendations provided in (non-normative) documentations, such as the 'Privacy and Security best Practices'. Customers can therefore not rely on the compliance with these recommendations.

Digital identities are represented by different accounts that the user may have at different (or the same) identity providers. Liberty provides means for privacy enhanced identity management by offering 'opaque handlers' and allowing for an 'Anonymous Identity Protocol', yet again whether this is implemented in a concrete case depends on the service provider implementing Liberty standards.

Regarding trustworthiness ('circles of trust'), again, much depends on the actual implementations and the reputation of the implementers. In other words, trust levels for Liberty implementations can be different as the technology can be implemented differently and because federations exist out of different organisations.

Liberty does not require users to download or install additional software: Liberty is server based.

Authentication in Liberty is based on SAML. Liberty Alliance does not allow for policy negotiation and enforcement between users and identity/service providers. Concrete policy management is left to the identity providers and service providers.

Liberty does not provide history management, nor context detection. User Data are stored on different servers, each containing only partial data.

The Liberty specifications provide ample attention to security aspects, both on an abstract (e.g., in Liberty ID-FF Architecture Overview) level, as well as on a more concrete level (e.g., (Liberty ID-WSF)).

7.1.2 Shibboleth

Shibboleth is a standards-based, open source software package for web single sign-on across or within organizational boundaries that 'sits on top' of an organisation's authentication technology and provides web based single sign-on functionality for online resources. Shibboleth comes from academia predominantly aims at deployment in universities, contexts in other words, where users and (identity and service) providers 'know' each other and also have off-line relations.

In Shibboleth the user is assigned to a so-called *home organisation*, which acts as her identity provider and administers her attributes. Typically, the user will have only one identity for the services in a federation.

Shibboleth allows users to create data handling policies (Attribute Release policies) and thus provides a certain level of user control over their digital identities.

Because identity federation with Shibboleth is initiated by an organisation with which a user already has a relation, trustworthiness of the system can be achieved by the reputation of this organisation, their information provisioning about security towards the user, and the agreements they make with the Service Providers that join the federation.

Authentication requests and assertions are made using the SAML standard. For privacy and security reasons, assertions are signed with the key of the identity provider and encrypted with the key of the service provider. Many of the security strengths of Shibboleth rely on the security considerations of SAML

7.1.3 PRIME

The PRIME IdM solution aims to be a user centric and privacy-enhanced identity management system. PRIME, by default makes use of anonymous interactions, e.g. by concealing network addresses of the user. Moreover, the system promotes the use of various and different partial identities, makes use of advanced cryptography, allows for user policy negotiation, provides user data tracking, and user assessment of platforms and services.

At the core of the PRIME infrastructure is the PRIME Middleware, which in order to provide the functionality mentioned above, has to be implemented on server and client alike. The PRIME IdM solution has not been implemented in existing operating systems or web browsers yet, which makes a fast adoption of the technology unlikely at present.

The PRIME console (*PRIME Identity Manager)*, which is the module located at the end-user's end, aims to inform the user by means of a standard user interface, which handles all privacy-related functionality. The interface can take over web-based interfaces so the user has a consistent (and trusted) experience when it concerns IdM. The *PRIME Identity Manager* allows the user to administer her personal data within PRIME and to configure various settings concerning his digital identities.

PRIME allows users to specify and negotiate data handling policies. The *PRIME Identity Manager* checks whether the provided data handling policies from the service provider match the user's preferences and, after positive matching, the requested personal data is sent to the service provider. Before a user discloses personal data, both the user and the service provider agree on those data handling policies. The service provider's Middleware guarantees for enforcement of the data handling policy.

In PRIME, personal data of users, including credentials issued by distinct authorities, are stored on client-side.

7.1.4 Microsoft Cardspace

Windows CardSpace ('CardSpace') is a system that does not mandate a single approach to digital identity, but aims at being an 'identity metasystem'.

CardSpace allows the creation multiple (partial) identities, represented by Infocards. It distinguishes two basic types of information cards. *Personal cards* can hold varying personal data, e.g., name, e-mail address, date of birth, or similar. This information is encrypted locally and may be sent to partner websites if necessary. However, the user decides which data should be revealed to the respective service provider. Personal cards are also called self-issued cards since the user has also the role of an identity provider in this case. The second type of cards is called *managed cards*. These are provided by identity providers.

Cardspace aims to provide a consistent user experience for the handling of digital identities. Its 'Identity Selector', one of the core components of the system, enables the user to make decisions about her digital identities, on the basis of the 'information cards'. The underlying information of a information card can be scrutinized as well. CardSpace's comprehensive user interface makes it relatively easy to operate by an end-user. The metaphor for digital identities (the InfoCard) is understandable to many individuals, and most people will be able to understand their function, without the necessity of understanding its technical complexity.

The user decides how many and which of her cards may be transmitted to service providers. Besides necessary data which is requested by the service provider, optional information can be included. Based on a *privacy policy* that service providers should publish, users may decide to interact with that service provider and to release personal information via cards. The interface gives insight in the information that will be sent to a service provider. Moreover, it has the feature of providing the user an overview of the site information and the certificate that has been issued to the service provider (if any). In order to keep a record of all personal data that a user has released to service providers, CardSpace stores a history of usage for each card.

Trustworthiness is taken seriously in Cardspace. Worth mentioning here is the fact that trust is approached as a mutual concept. Not only individuals have to authenticate, but also websites should authenticate themselves to the user. Trustworthiness is also enhanced by means of the standard user interface and consistent representation of digital identities for all IdM decisions.

Trustworthiness of CardSpace is enhanced by the fact that most users have experience with Microsoft products.

Because CardSpace is implemented in the Vista operating system and can be used for multiple other OS', it is likely that the adoption of this IdM system is potentially high.

User data are encrypted and held client-side, while other data remains on the servers of identity providers.

Windows Cardspace security model relies on the idea of Infocards that describe a trust relationship between a user and a security token service (STS). Windows Cardspace employs SAML tokens and is based on WS-Trust, WS-Security, and WS-Policy and WS-SecurityPolicy standards for handling these tokens. Its security is strongly tied to the WS-* efforts led by IBM, Microsoft and Verisign.

7.1.5 General remarks

What clearly shows when looking at the four frameworks differ significantly in their approach, focus and maturity. Liberty Alliance and Shibboleth start from an enterprise centric approach, in Liberty's case a federation of enterprises, in Shibboleth's case institution(s) of higher education. The enterprise is the principal party in providing and managing identities. The individual is the (passive) user. PRIME and to a lesser extent CardSpace depart from the perspective of the user as the central actor. Here the individual is really at the steering wheel of her identity management. Both systems allow the user to self create identities, as well as make use of provisioned, certified identities. The user-centricity also shows in the way users can define and negotiate policies regarding personal data disclosure and use.

Liberty and Shibboleth already have an extensive user base and Cardspace, given its Microsoft roots is in an advantageous position. PRIME, which started as a European research

project and hence focused on pushing (privacy) envelopes in this respect lags behind. There is no off the shelf PRIME implementation.[78]

Liberty and Shibboleth don't require any download and/or installation on the part of the user. Liberty is a set of standards that can be implemented by technology providers (on the server-side of transactions). Shibboleth consists of a package that can be installed on the service providers IT infrastructure. Both systems provide the user with web based authentication tools. PRIME depends on client and server Middleware for its advanced functionality. This may be an obstacle to widespread deployment and adoption. Cardspace also depends on Middleware, but in this case it is tied in major operating systems (Vista and Windows 7), which facilitates large scale adoption.

With respect to security there are many similarities because most systems use the same underlying mechanisms (SAML), which means they are prone to the same risks. Regarding trustworthiness from the perspective of the user there are significant differences. Liberty Alliance has to rely on the reputation of a potentially diverse large, and to the user unfamiliar, set of identity providers as well as relying parties of different stature. Shibboleth currently is mainly implemented in configurations where the user knows the identity provider (his/her university or school) as well as the relying parties which facilitates the trust relation. Trustworthiness in PRIME has different aspects. On the one hand, identity is very much in the hands of the user herself (which should be trustworthy). Also, sophisticated technology (cryptography, anonymous communication) should enhance the (technical) trust level significantly over other approaches, yet trustworthiness here is undermined because the technology is opaque and unfamiliar to most common users. Do they trust technology they don't understand? Cardspace is in the same ball-park as PRIME with respect to user-control. Microsoft has learned from the objections to central data storage by Microsoft in their .NET Passport project and instead currently uses decentralised storage. This should enhance user trust in the system. The entire Cardspace environment lives under Microsoft's umbrella. To most this is a comforting idea, to some it is not.

This is not the place to make verdict regarding the suitability or unsuitability of any approach. The deliverable aims to provide an overview of a number of different Federated Identity Management Systems to show that this is a field in flux where different approaches co-exist and co-evolute, hopefully in a direction that benefits the individual end-user as well as the federations.

[78] Although the PRIME follow-up project PrimeLife (visit http://primelife.eu) may change this.

8 Bibliography

(Alrodhan & Mitchell, 2007) Alrodhan, W. Mitchell, C., 'Addressing privacy issues in CardSpace', *Third International Symposium on Information Assurance and Security*, 2007, pp. 285-291.

(Agre 1997) Agre, P. E. (1997). Introduction. In P. E. Agre & M. Rotenberg (Eds.), Technology and privacy: The new landscape. London: The MIT Press

(Alsaleh & Adams 2006) Alsaleh, M., & Adams, C. Enhancing consumer privacy in the liberty alliance identity federation and webservices framework

(Andersson et al 2005) Christer Andersson, Jan Camenisch, Stephen Crane, Simone Fischer-Hübner, Ronald Leenes, Siani Pearsson, John Sören Petterson, Dieter Sommer: Trust in PRIME. In Proceedings of the 5th IEEE Int. Symposium on Signal Processing and Information Technology, Athens, Greece, December 2005.

(Aquisti & Grossklags 2005) Alberto Aquisti & Grossklags, J. Privacy and rationality in individual decision making. IEEE Security & Privacy, January/February, 24-30.

(Berendt 2005) Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: Stated preferences vs. Actual behaviour. Communications of the ACM, 48(4), 101-106.

(Bergmann et al., 2008) Bergmann, M., Crane, St., Fischer-Hübner, S., Pettersson, J., 'Human-Computer Interaction', *PRIME Book (version 1)*, 18 July 2008, pp. 357-388, to appear.

(Bergmann, 2007) Bergmann, M., 'User-side IdM Integrated Prototype V2', *Public Deliverable D11.2.b*, 30. March 2007.

(Blanchette & Johnson 2002) Blanchette, J.-F., & Johnson, D. G. (2002). Data retention and the panoptic society: The social benefits of forgetfulness. The Information Society, 18, 33-45.

(Brody 2007) Richard G. Brody, Elizabeth Mulig, and Valerie Kimball. Phishing, pharming and identity theft. Academy of Accounting and Financial Studies Journal, 11(3), 2007.

(Camenisch et al 2009) Jan Camenisch, Dieter Sommer & Ronald Leenes (eds) The PRIME Book, to appear in 2009.

(Cameron 2005) Kim Cameron. The laws of identity. Technical report, Microsoft Corporation, 2005.

(Cameron & Jones 2006) Kim Cameron & Jones, M. B. Design rationale behind the identity metasystem architecture: Microsoft.

(Casassa-Mont et al., 2007) Casassa-Mont, M., Crosta, St., Kriegelstein, T., Sommer, D., 'PRIME Architecture V2' *Public Deliverable D14.2.c*, 29. March 2007.

(Chappell 2006) D. Chappell, Introducing windows CardSpace: Chappell & Associates.

(Clarke 1994) Roger Clarke, The Digital Persona and its Application to Data Surveillance. The Information Society

(Coyle 2007) K. Coyle. "Identity Crisis." The Journal of Academic Librarianship 33(4).

(Dhamija 2008) Rachna Dhamija and Lisa Dusseault. The seven flaws of identity management: Usability and security challenges. IEEE Security and Privacy, 6(2):24–29, 2008.

(Donath 2004) Judith Donath and d. boyd. Public displays of connection. BT Technology Journal, 22(4):71–82, 2004.

(Dorrans 2006) Barry Dorrans, An Introduction to CardSpace, Charteris plc http://idunno.org/presentations/webdd/An%20Introduction%20to%20CardSpace.ppt

(Eduserv, 2008) Eduserv, 'What is Shibboleth?'. Online available http://www.eduserv.org.uk/aim/shibboleth (last access 15 August 2008)

(Federation.ShARPE, 2007) 'Shibboleth Attribute Release Policy Editor', October 2007, Federation.ShARPE, 2007. Online available http://www.federation.org.au/twiki/bin/view/Federation/ShARPE (last access 15 August 2008)

(Erdos & Cantor 2002) Erdos, M. and S. Cantor. "Shibboleth-Architecture DRAFT v05."

(Internet2, 2008) 'Shibboleth', Internet2, 2008. Online available http://shibboleth.internet2.edu/ (last access 15 August 2008)

(Fischer-Hübner & Hedbom 2008) Simone Fischer-Hübner & Hans. Hedbom (eds.), PRIME WP 14.1. (2008). Framework v3 (No. D14.1.c): PRIME Consortium.

(Fried 1968) Fried, C. (1968). Privacy. The Yale Law Journal, 77, 475-493

(Gandy 1993) Oscar H. Gandy. The Panoptic Sort. A Political Economy of Personal Information. Critical Studies in Communication and in the Cultural Industries. Westview Press, Boulder, San Francisco, Oxford,, 1993.

(Goffman 1958) Erving Goffman. The presentation of self in everyday life. Garden City, New York: Doubleday Anchor Books.

(Hildebrandt 2006) Mireille Hildebrandt. Privacy and identity. In E. Claes, A. Duff & S. Gutwirth (Eds.), Privacy and the criminal law. Antwerpen: Intersentia

(Jutla et al 2005) Jutla, D. L., & Bodorik, P. (2005). Sociotechnical architecture for online privacy. IEEE Security & Privacy, 29-39

(ICPP/ULD, & SNG. 2003). ICPP/ULD, & SNG. Identity management systems (ims): Identification and comparison study.

(Katz & Shapiro 1994) Katz, M. L., & Shapiro, C. (1994). Systems competition and network effects. The Journal of Economic Perspectives, 8(2), 93-115.

(Kosta et al 2008) Eleni Kosta, Dumortier, J., Ribbers, P., Fairchild, A., Tseng, J. C., Liesebach, K., et al. (2008). Requirements for privacy enhancing tools (Deliverable D1.1.d): PRIME Consortium,

(Lessig 1999) Lessig, L. (1999). Code and other laws of cyberspace. U.S.: Basic Books.

(Liberty Alliance Project, 2005) 'Liberty ID-FF Architecture Overview', Version: 1.2-errata-v1.0, Liberty Alliance Project, 2005. Online available http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications (last access 11 August 2008).

(Liberty ID-FF Architecture Overview) Liberty ID-FF Architecture Overview, Liberty Alliance project http://www.telenor.com/rd/idm/liberty-idff-arch-overview-v1.2.pdf

(Liberty ID-WSF) Liberty ID-WSF Security Mechanisms http://xml.coverpages.org/LibertyIDWSF-SecurityMechanismsV20-03.pdf

(Liberty Specs Tutorial) Liberty Specs Tutorial http://www.project-liberty.org/liberty/content/download/423/2832/file/tutorialv2.pdf

(Liberty ID-FF Protocols and Schema Specification) Liberty ID-FF Protocols and Schema Specification

http://www.projectliberty.org/liberty/content/download/2197/14625/file/draft-liberty-idff-protocols-schema-1.2-errata-v3.0.pdf

(Lyon 2001) David Lyon. Surveillance society; monitoring everyday life. Buckingham: Open University Press.

(Malinen 2006) Jussi Malinen. Windows CardSpace (pp. 7): Helsinky University of Technology. http://www.tml.tkk.fi/Publications/C/22/papers/Malinen_final.pdf

(McLeish 2008) Simon McLeish, Installing Shibboleth, https://spaces.internet2.edu/display/SHIB/InstallingShibboleth

(Microsoft Corporation, 2008a) 'About Information Cards and Digital Identity', August 2008, Microsoft Corporation, 2008. Online available http://msdn.microsoft.com/en-us/library/ms734655.aspx (last access 15 August 2008)

(Microsoft Corporation, 2008b) 'Introducing Windows CardSpace.', Microsoft Corporation, 2008. Online available http://msdn.microsoft.com/en-us/library/aa480189.aspx (last access 20 August 2008)

(Microsoft Corporation, 2008c) 'Windows CardSpace. Frequently asked questions.', Microsoft Corporation, 2008. Online available http://windowshelp.microsoft.com/windows/en-us/help/7dc9c520-9d16-473d-b21b-413ac7226fb61033.mspx (last access 20 August 2008)

(Microsoft Corporation, 2007) 'Identity Selector Interoperability Profile V1.0', April 2007, Microsoft Corporation, 2007.

(Milne 2004) Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. Journal of Interactive Marketing, 18(3), 15-29.

(Nissenbaum 2004) Helen Nissenbaum. Privacy as contextual integrity. Washington Law Review.

(OASIS, 2008) 'OASIS Security Services (SAML) TC', OASIS, 2008. Online available http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security (last access 14 August 2008)

(OASIS 2005) Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V1.1
http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf

(OASIS 2003) Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1

http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf

(OASIS 2005b) Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0
http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf

(Olsen 2007) Thomas Olsen, Tobias Mahler, Clive Seddon, Vicky Cooper, Sarah Williams, Miguel Valdes, and Sergio Morales Arias. Privacy & identity management. Technical report, Senter for rettsinformatikk, 2007.

(Pettersson 2008) Pettersson, J. S.. Hci guidelines: The PRIME Consortium.

(PRIME, 2008a) 'Advanced Tutorial v3', March 2008, PRIME, 2008. Online available https://www.prime-project.eu/tutorials/devto (last access 11 August 2008)

(PRIME, 2008b) 'General Public Tutorial v2', March 2008, PRIME, 2008. Online available https://www.prime-project.eu/tutorials/gpto (last access 11 August 2008)

(PRIME, 2008c) 'Framework V3' 17 March 2008, PRIME 2008. Online available https://www.prime-project.eu/prime_products/reports/fmwk/pub_del_D14.1.c_ec_wp14.1_v1_final.pdf (last access 22 May 2009).

(Raab 2005) C.D. Raab. Perspectives on 'personal identity'. BT Technology Journal, 23, 2005.

(Rixon 2005) Guy Rixon, Review of Shibboleth, Version 0.1, 2005 http://www.ivoa.net/internal/IVOA/IvoaGridAndWebServices/shibboleth-review-v0.1.html

(Shibboleth, 2005) 'Shibboleth Architecture' Working Draft 02, 8 June 2005. Online available http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-tech-overview-latest.pdf (last access 11 August 2008)

(Shibboleth, 2005b) Shibboleth Architecture Protocols and Profiles http://shibboleth.internet2.edu/docs/internet2-mace-shibboleth-arch-protocols-latest.pdf

(Shibboleth 2004) Shibboleth Target Deployment Guide, Shibboleth Version 1.2.1, 2004 http://www.switch.ch/aai/docs/shibboleth/internet2/1.2/deploy-guide-target1.2.1.html

(Shostack 2003) Shostack, A. "people won't pay for privacy," reconsidered (pp. 5).

Schneier, B., *Applied Cryptography*, Addison-Wesley, New York 1996.

(Schwartz 2004) Schwartz, B. The tyranny of choice. Scientific American.

(Solove 2007) Daniel J. Solove. The Future of Reputation. Gossip, Rumor, and Privacy on the Internet. Yale University Press, New Haven, 2007.

(Stalder 2002) Felix Stalder. The failure of privacy enhancing technologies (pets) and the voiding of privacy. Sociological Research Online, 7(2);

(Tan & Sutherland 2004) Tan, F. B., & Sutherland, P.. Online consumer trust: A multi-dimensional model. Journal of Electronic Commerce in Organizations.

(W3C, 2008) 'Platform for Privacy Preferences (P3P) Project', W3C, 2007. Online available http://www.w3.org/P3P (last access 20 August 2008)

(Westin 1967) Alan Westin. Privacy and freedom. New York: Atheneum.

(Witheridge 2006) Neil Witheridge, MAMS&the Identity and Access Management (IAM) Suite, http://cd-docdb.fnal.gov/cgi-bin/RetrieveFile?docid=1976&extension=ppt