Network Identity

Kai Kang
Helsinki University of Technology
Networking Laboratory
kkang@cc.hut.fi

Abstract: This paper is concerning on modern Network Identity issues, emphasizing on network identity management, implementation and architectures. Two most popular approaches are introduced, while the Liberty Alliance's concept is emphasized in details. The contribution of Finnish companies is also mentioned at the end part.

Keyword: identity, circle of trust, federated identity, smart card

1. Introduction

Identity is an essential characteristic of human being. It encompasses all the elements that make each human being unique but also all the characteristics that enable membership to particular groups.

Network Identity (NI) is the context-sensitive identity, attributes, rights, and entitlements, all maintained within a policy-based trusted network framework. [1] Examples of it can be Email address, customer name, PIN, credit card number, social security number, passport, even DNA and Retinal scan results of an individual!

Managing Network Identity describes the software infrastructure and business processes for managing the life cycle and usage of an identity, including those attributes, rights, and entitlements. [1]

Nowadays the NI evolution presented us 3-phase infrastructures, which were

- Identity Linking with Mutual Content,
- Identity Circle of Trust,
- Federated Network Identity Services.

As for last phase Federated Identity services, there we have two major approaches,

- Microsoft Passport
- Liberty Alliance

I analyzed the two approaches in chapter 2, and the rest of my paper is arranged with chapter 3 Technical architectures and chapter 4 Status in Finland.

1.2 Five drivers for the Network Identity

•Financial Driver

The need to contain and control costs while expanding channels of business, regardless of location of end user. [1] Network Identity infrastructures will reduce the costs of doing business because the duplication of the same profile can be reduced. Thus lower overhead drive business and organizations backing Network Identity.

•Legislation Driver

And generally public regulations will always protect consumer privacy and govern the sharing of personal information. Governments are legislating laws protecting personal information from being shared without permission.

Network Identity offers a fully configurable functionality that an enterprise can use to meet its privacy and security needs and as a yardstick to measure the legislated compliance. Enterprises that respect customers' privacy gain trust from their customers.

•Trust driver

Modern business activities will result in losing trust, and it is inevitable.

However, properly structured Network Identity environments will enable a possible solution for that, because it is by definition built on trust, security, and privacy, in which users' privacies are always under protection and their information are shared with permission at several levels of trust.

•Security driver

Because we are coming towards a world of data-driven devices, in which environment security is more critical than ever.

Network Identity systems enable user recognition at security basis.

•Technology driver

The need for more flexible, standardized, and context-based forms of managing identity that is application-independent. Implementations must support a wide range of devices.
Network Identity enables truly secure and easy services without duplication of the same infrastructures.

1.3 Basic Network Identity Services

Many network identity services mechanisms have been used. Here are some basic and most frequently used ones: [2]

- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Remote Authentication Dial-In User Service (RADIUS)
- Lightweight Directory Access Protocol (LDAP)
- Microsoft's Active Directory
- Novell Directory Services (NDS)
- Public Key Infrastructure (PKI)

Each service has its specific functions field. But they also interact with each other.

1.4 Network Identity Evolution Roadmap

There are 3 phases exist in the Network Identity Evolution Roadmap, they are:

Phase 1. Identity Linking with Mutual Content

In this stage, the sharing of 'user identity between merchants' is enabled. This sharing is done through mutual consent between the consumer and merchants; however, each merchant requires a unique identity profile in order to operate business activities. Consumers are directly connected with merchants but also know other merchant services. [1]

Phase 2. Identity Circle of Trust

This stage is dominated by of the "Circle of Trust" concept, where the consumer and merchants rely on Identity Providers as trusted sources for identity information. The consumer can choose to engage directly with merchants or by the help of an Identity Provider. The Identity Provider manages the identity profiles on behalf of both sides. [1]

Phase 3. Federated Network Identity Services

This stage is the most advanced. It represents a network of Circles of Trust, where identity is shared among trusted Network Identity Providers. While the Circle of Trust model in phase 3 offers consumers and merchants greater value in federating the circles among themselves. Federation of identity gives consumers the ability to freely move in-and-out of Circles of Trust to access their desired services. [1]

2. Network ID management approaches

There are two major Network Identity Management approaches, which are

Microsoft's .Net Passport
Liberty Alliance approach

2.1 What is Microsoft's .Net Passport?

Microsoft’s .Net Passport is a "universal-login" service provided by Microsoft since July 1999 that allows users to log in to many websites using one account. It is a key part of Microsoft's .Net strategy. [5, 6]

Passport comes in two flavors: sign-in and wallet. A customer needs a sign-in account to use Microsoft's consumer services, including Hotmail, MSN and Windows Messenger. If you have a Hotmail or MSN account, you already have Passport: now by using Hotmail or MSN address and password it will be ok at sites that require a Passport sign-in. [11]

The Passport wallet service enable customers buy online without re-entering profile information at every participating site; it's similar to Amazon.com's one-click shopping. Currently, however, only few Microsoft external sites use the Passport sign-in and wallet. [11]

2.2 What is the Liberty Alliance?

ü A business alliance, formed in Sept 2001 with the goal of establishing an open standard for federated identity management

ü Global membership consists of consumer-facing companies and technology vendors as well as policy and government organizations

ü The only open organization working to address the technology, policy and business issues of federated identity management [2, 10]

Nowadays over 150 diverse member companies and organizations nowadays including: [2]

q Governmental organizations
The U.S. General Services Administration, the U.S. Department of Defense

q End-user companies

q System integrators

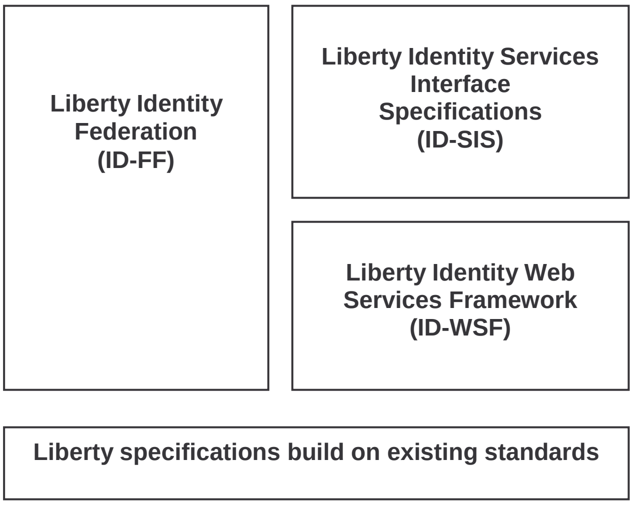
q Software and hardware vendors

3. Technical Architecture

Varies approaches had been introduced and implemented; here I choose the Liberty Alliance’s model for this discussion.

3.1 The Liberty Model architecture

Can be described as: [3]



Liberty Identity Federation (ID-FF)

Liberty Identity Services Interface Specifications (ID-SIS)

Liberty Identity Web Services Framework (ID-WSF)

Liberty specifications build on existing standards

Liberty Identity Federation Framework **(ID-FF):** ID-FF provides the mechanism for single sign-on and linking of separate accounts within a group of service providers in a circle of trust. [3]

Liberty Identity Web Services Framework **(ID-WSF):** ID-WSF provides an infrastructure for identity-based web services through aspects such as permission-based sharing of users’ attributes, discovery of additional identity-based services, allowing for user security profiles, and support for differing types of client devices. [3]

Liberty Identity Services Interface Specifications **(ID-SIS):** ID-SIS is a collection of specifications for interoperable identity-based service formats made possible by ID-WSF. [3]

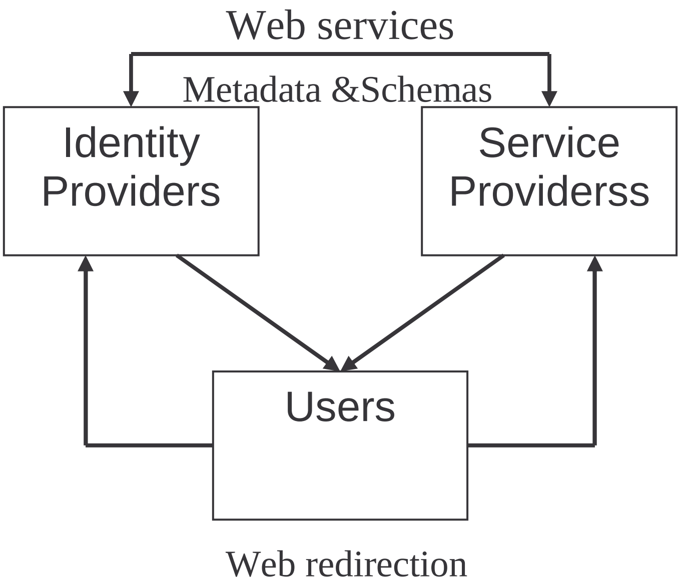
Liberty specifications build on **existing standards** include: [3]

SAML WAP

HTTP
WSS
WSDL
XML Enc
XML
SSL/TLS
SOAP
XML-DSIG

3.2 ID-FF infrastructure

While looking into the ID-FF infrastructure [4], we have the basic architecture as:



The overall architecture is composed by three architectural components as: Web redirection, Web services and Metadata and schemas.

Their functions [4] can be defined as:

Web redirection	Enables Liberty-enabled entities to provide services via today’s user-agent-installed base.
Web services	Protocol profiles that enable Liberty entities to directly communicate.
Metadata and schemas	A common set of metadata and formats used by Liberty-enabled sites to communicate various provider-specific and other information.

4. Status in Finland

Network ID Product pioneer: ***SETEC***
Famous for its **smart cards**

- In 2000 the world's first payment card based on EMV&PKI technology
- In 1999 developed the world's first, PKI SIM card
- In 1998 launched SIM card with a Wireless Internet Browser.
- In 1995 first in the world to develop a PKI smart card with 1024-bit keys.

World Telecommunications leader ***NOKIA***

- June 2004 **Nokia** and Sun Microsystem co-published a new white paper “Deploying Mobile Web Services using Liberty Alliance’s Identity Web Services Framework (ID-WSF) ” [7]
- One of the ten member companies offer Liberty Alliance interoperable products (passed the conformance tests)
- In Sept 2001 **Nokia** was one of the founders of the **Liberty Alliance,** board member and key impetus [8]

5. Conclusions

The Network Identity is a very important concept within modern e-commerce society; regards of the question “how to manage identity”, many discussions and implementation had been performed. And the most evolved one is the Federated Network Identity Services.

As for the Identity Management Standardization, the war between Microsoft and the Liberty Alliance appears to be intensely, and will never end. However, more and more support had been gained by the Liberty Alliance time by time. I believe these progresses are build upon the open model concept and great efforts contributed by the alliance members. However, the reasons should also include the public hate of the monopolization and the security weakness [9, 11] within the Passport technology.

As for status in Finland, in this science and technology motivated nation, many Network Identity related progresses had been achieved in company basis. Among them, the SETEC and NOKIA play key roles. One works as the most successful supplier and developer for better NI applicable solutions, while another works for the open standard of the federated NI management.

Reference

[1] “Strategic Implications of Network Identity” by Sun Microsystem
http://wwws.sun.com/software/whitepapers/webservices/wp-identity.pdf

[2] “Gaining Control of Your Network Identity Infrastructure” by Stuart Bailey, CTO of the Infoblox Company

[3] “Whitepaper: Benefits of Federated Identity to Government” by Tanya Candia and Sigaba
https://www.projectliberty.org/resources/whitepapers/Liberty_Government_Business_Benefits.pdf

[4] “Liberty ID-FF Architecture Overview” by Thomas Watson from IEEE-ISTO
http://www.projectliberty.org/specs/draft-liberty-idff-arch-overview-1.2-errata-v1.0.pdf

[5] “Passing Passport” By Earl Perkins from Meta Group by February 5, 2002
http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2844846,00.html

[6] Microsoft Corporation
http://www.microsoft.com

[7] “Deploying Mobile Web Services using Liberty Alliance’s Identity Web Services Framework (ID-WSF)” by Nokia and Sun
http://www.projectliberty.org/resources/whitepapers/Nokia_Sun_A4_2806.pdf

[8] “Nokia and industry leaders launch Liberty Alliance Project,a network identity initiative”
http://press.nokia.com/PR/200109/835073_5.html

[9] “Critical bug found in Microsoft Passport, Passwords were easy to nick” By Staff at the Newsdesk on Thursday 08 May 2003
http://www.theinquirer.net/?article=9392

[10] “Network Identity and the Liberty Alliance Project” by Marc Hamilton and Ismet Nesicolaci from Sun Microsystem

[11] “Everything You Ever needed to know about Microsoft Passport”
http://www.freepctech.com/pc/xp/xp00188.shtml