Network Identity

Kai Kang

27th October 2004
Outline

• Introduction
  – Definition
  – Five drivers
  – Basic services
  – Roadmap

• Network Identity management approaches
  – Microsoft Passport
  – Liberty Alliance

• Technical architectures

• Status in Finland
  – SETEC
  – NOKIA
Introduction

What is Network Identity?

It is the set of attributes that describe profiles of an individual in the Internet.

like:

Email address, customer name, PIN, credit card number, social security number, Passport, even DNA, Retinal Scan ....
Formal Definition

by Sun Microsystem

Network Identity (NI) is the context-sensitive identity, attributes, rights, and entitlements, all maintained within a policy-based trusted network framework.
Network Identity Drivers

• Financial
• Compliance and Legislation
• Trust and Privacy
• Security
• Technology
## Basic Network Identity Services

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Objective</th>
<th>Interfaces</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>Domain names</td>
<td>IP address</td>
<td>naming service</td>
</tr>
<tr>
<td>DHCP</td>
<td>MAC address</td>
<td>IP address</td>
<td>IP network connectivity</td>
</tr>
<tr>
<td>LDAP</td>
<td>User identity</td>
<td>Policies</td>
<td>Enforcement of access rights</td>
</tr>
<tr>
<td>PKI</td>
<td>User name</td>
<td>Public key</td>
<td>Encryption/Decryption for data security and session verification</td>
</tr>
<tr>
<td>RADIUS</td>
<td>User</td>
<td>User attributes and access rights</td>
<td>Control over authorized use of network resources</td>
</tr>
</tbody>
</table>
Network Identity Roadmap

Figure 1
Network Identity Infrastructure
Source: Liberty Alliance Website
Network Identity Management approaches

Microsoft’s .Net Passport (centralized)
Liberty Alliance (Federated)
Centralized Model

Figure 2
Centralized concept
Source: Liberty Alliance Website
Open Federated Model

Figure 3
Open Federated concept
Source: Liberty Alliance Website
Microsoft’s .Net Passport

Microsoft’s .Net Passport is a "universal-login" service launched 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.

Microsoft's NET Passport has more than 200 million active accounts and handles more than 4 billion authentications per month.

Adam Sohn
Product Manager
Platform Strategy Group at Microsoft
Participating companies that use Passport technology
Liberty Alliance

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

Liberty Alliance Provides the technology, knowledge and certifications to build identity into the foundation of mobile and Web-based communications and transactions.
Membership categories

Over 150 diverse member companies and organizations nowadays including:

- Government organizations
  - The U.S. General Services Administration,
  - and the U.S. Department of Defense
- End-user companies
- System integrators
- Software and hardware vendors
Liberty Alliance Board Members
Technical Architectures

Varies technical approaches for the implementation of Network Identity, here I choose the Liberty Alliance’s model
Liberty NI Architecture

Liberty Identity Federation Framework (ID-FF)
Enables identity federation and management through features such as identity/account linkage, simplified sign on, and simple session management

Liberty Identity Services Interface Specifications (ID-SIS)
Enables interoperable identity services such as personal identity profile service, contact book service, geo-location service, presence service and so on.

Liberty Identity Web Services Framework (ID-WSF)
Provides the framework for building interoperable identity services, permission based attribute sharing, identity service description and discovery, and the associated security profiles

Liberty specifications build on existing standards (SAML, SOAP, WS-Security, XML, etc.)
Figure 5
ID-FF Basic Architecture
Source: Liberty Alliance Website
Figure 5. Passport's architecture
Source: Microsoft Corporation
Status in Finland
Network ID Product pioneer

SETEC

Famous for it’s 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)”

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