SASSO: Personal Identity Provider on Mobile Phone

NTT Information Sharing Platform Laboratories

Kenji Takahashi
What is SASSO?

• SASSO stands for Strong Authentication for Single Sign On
• SASSO means “pebble” in Italian
• SASSO is written as 颯爽 in Japanese, meaning “gallant, dashing, smart, jaunty”
• SASSO represents one’s identity
Market trends in Japan

• Advanced mobile services have been deployed and widely accepted
  – Broadband – 3G available nationwide, HSDPA (up to 3.6 Mbps), …
  – Built-in security – PKI, biometrics, NFC, …
  – Advanced applications – payment, search, SNS, DTV…
  – From voice to data
  – Flat rate

• Also fixed broadband services have been pushed down
  – ADSL 40.6%, FTTH 28.2%
  – NGN will be available soon

• Identity management is an integral part of the future converged world
  – Advanced personalized data services to play the bigger roles
  – Subscription as a basis of identity
  – Subscription as a basis for one-stop service offering
Problems: Strong authentication needed everywhere

- Passwords are often said to be insecure, but are still used everywhere
- Strong authentication has been proposed but not used as widely as desired because...
  - It may require the acquisition and installation of new hardware and/or software
  - People forget (or hate) carrying it
  - It may not be compatible with PCs that users want to use
The Emperor’s New Security Indicators

A study of online banking customers reveals that they entered their passwords even if:

- HTTPS indicators were missing => 100%
- “Site authentication” images were missing => 92 %
- A security warning page was presented => 53%

Solution: SASSO

- Enable single sign on to a PC with the strong authentication capabilities of a mobile phone
  - e.g. NTT DoCoMo’s FirstPass, an authentication service
- No installation or cable or footprint on PC
- Standards-based approach avoids incompatibility
- User centric approach
Slide show demonstration
Login Page

Click on the "Sign On" button.
Login Page
Launch IdP application
Login Page

Please enter your Mobile Phone IdP's URL.

https://mobile-idp.ntt.jp/abel
Notification of authentication request
PIN code authentication
Send SAML assertion
Welcome page
Sequence flow
Relay Server
Performance
Typical sequence flow

PC  IdP (Mobile Phone)  SP

Request for service

AuthnRequest

Authentication on mobile phone

Response with SAML assertion

Provide service

Verify response

IdP discovery
IdP Discovery

PC  IdP (Mobile Phone)  SP

Request for service

Prompt for URL of user’s IdP on mobile phone

URL of user’s IdP on mobile phone

AuthnRequest

Response

Provide service

Verify response

Copyright(c)2007 NTT Corporation. All Rights Reserved.
Enabling Mobile Phones to act as Servers

Problem
• PC cannot access mobile phone by HTTPS directly

Solution
• Mobile phone accesses the relay server
• Relay server maintains the connection
• PC accesses the mobile phone through the relay server
Sequence Flow

PC  IdP (Mobile Phone)  Relay Server  SP

Request for service

AuthnRequest

Connect

Relay AuthnRequest to appropriate IdP

Initial authentication

maintain connection

Response with SAML assertion

Provide service
IdP URL

Statically allocated IdP URL

https://mobile-idp.ntt.jp/abe
https://mobile-idp.ntt.jp/itoh

Common part
(relay server URL)

Distinct part
(e.g. username)

Dynamically allocated IdP URL

https://mobile-idp.ntt.jp/14ety38r

Common part
(relay server URL)

Distinct part
(random string)
Performance
Prototype System Configuration

PC

WWW browser

OS

NTT DoCoMo mobile phone

IdP i-appli

i-appli API

J2ME CLDC

OS

Relay server

Relay Servlet

Tomcat

J2EE

OS

SP

SP JSP

Liberty Alliance SP middleware

OS

Legend:

Newly developed component for SASSO

Conventional component

Copyright(c)2007 NTT Corporation. All Rights Reserved.
## Performance

### Specifications of mobile phone

<table>
<thead>
<tr>
<th>Model</th>
<th>NTT DoCoMo F903i</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>SH-Mobile G1</td>
</tr>
<tr>
<td>Communication speed</td>
<td>384 kbps</td>
</tr>
</tbody>
</table>

### Processing time of IdP on mobile phone

<table>
<thead>
<tr>
<th>Process</th>
<th>Time [seconds]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication</td>
<td>3</td>
</tr>
<tr>
<td>Digital signing</td>
<td>3</td>
</tr>
<tr>
<td>Other</td>
<td>0.4</td>
</tr>
</tbody>
</table>

Copyright(c)2007 NTT Corporation. All Rights Reserved.
Future

- Mobile attribute provider capability
- Multi-protocol interoperability
  - OpenID, CardSpace, etc...
- Home identity center for net-connected appliances
- Adoption for VRM (Vendor Relationship Management)