2007 IDDY AWARD WINNER

Case Study:

NTT's SASSO Turns a Mobile Phone into a Personal Identity Provider

The Company

The NTT Group—reorganized in 1985 from a government owned utility to a privately held corporation—has led the development of telecommunications in Japan for more than a century. The major companies that comprise the NTT Group continue to accommodate the emerging needs of the ubiquitous broadband society in the 21st century, while fulfilling their social mission in each business field in an increasingly competitive global market environment.

The Application

Mobile C2B

> "Liberty's open standards, upon which SASSO is based, are platform-independent, collaboratively developed, vendor-neutral, and are licensed royalty free. These base standards allow vendor innovation, which is illustrated so well in SASSO, while preventing vendor lock-in. This is free market enterprise in its finest form."
>
> **Brett McDowell,**
> Executive Director,
> Liberty Alliance,

The Challenge

As the use of mobile phones explodes and consumers use them for purposes once exclusively the domain of PCs, security becomes an increasingly important concern. Mobile phones have the potential to enable strong authentication to Web sites without the use of cumbersome add-on hardware. Such an approach would also sidestep the need to be tethered to a single ubiquitous platform.

The Solution

NTT has tackled this issue head on with SASSO, a strong authentication solution that turns a mobile phone into a personal identity provider.

"Our technology employs mobile phones and open standards to strike the tough balance between security and privacy concerns on the one hand, and usability on the other—two necessities in the modern world," said Dr. Kenji Takahashi, a senior research engineer and supervisor at the NTT Information Sharing Platform Laboratories in Tokyo, Japan.

SASSO also represents an important step in the evolution of client identity capabilities. New smart identity clients like SASSO will play an increasingly active role in identity operations for their users, replacing the prevailing "dumb browser" approach.

What SASSO represents is so significant that it was recently honored by the Liberty Alliance with a 2007 IDDY Award for the most outstanding proof of concept.

Addressing the Obstacles to Widespread Strong Authentication

To best understand SASSO, it's important to step back and look at where strong authentication on the mobile platform currently stands.

Usernames and passwords have been used as authentication methods for a long time. However, phishing has become a huge problem: Personally identifiable information (PII) is at more risk than ever before.

Therefore, many business sites are using stronger authentication methods such as one-time passwords (OTP). However, to use OTP methods, a site owner has to distribute special hardware tokens to every user, and that cost is not negligible. Carrying tokens all the time is also inconvenient for users—this is often referred to as the "token necklace" problem.

Mobile phone terminals have naturally received attention as portable security devices. There are some commercial systems that use mobile phone terminals as an OTP software token or connect a mobile phone terminal to a PC with USB cable and use it as a hardware token.

SASSO takes this one step further, enabling a mobile-based strong authentication mechanism based on the preeminent standard for federated identity—SAML 2.0.

The Technical Approach

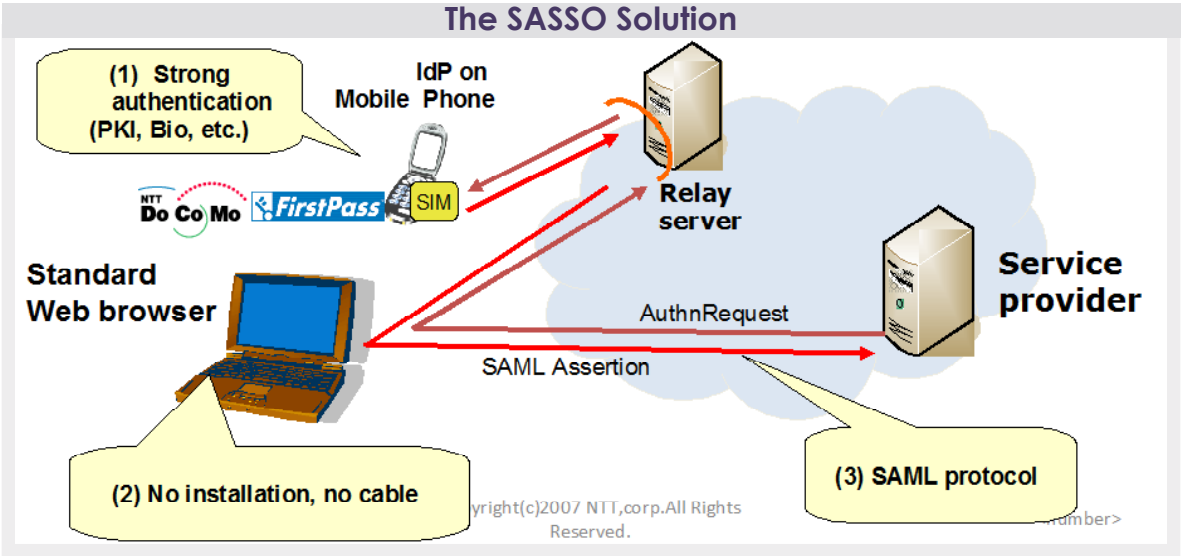
NTT's SASSO model implements a mobile phone terminal as an Identity Provider (IdP) as defined by SAML 2.0. The mobile phone IdP authenticates the user and asserts this fact to online Service Providers (SPs). Once a user is authenticated by his/her own mobile phone, the IdP on the mobile phone issues SAML assertions signed by a private key on its USIM and sends that assertion to the various SPs that the user interacts with—thereby enabling SAML-based SSO to those SPs. (Importantly, the solution is not restricted to SPs accessed with the mobile phone.)

As in "ordinary" SAML SSO procedure, no additional software or hardware are required for users' PCs.

SASSO's Key Differentiators

- SASSO, installed on mobile phone, enables the user to single sign-on to a PC with strong authentication.
- No installation or cable or footprint on a PC is necessary.
- It deploys SAML 2.0, an industry standard-based approach.
- It makes the user the IdP.

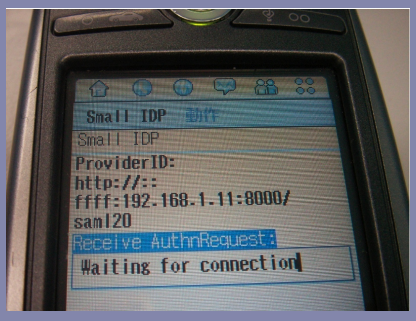
The SASSO Solution



The User's Experience

From the user's point of view, how SASSO works is simple:

1. User accesses an SP, let's say an online bank. The user inputs their personal IdP URL when prompted to do so by the bank (this is similar to the OpenID model, the difference is that in SASSO the URLs may be dynamically generated).
2. User's PC browser is redirected to a Web page saying that phone IdP authentication is taking place.
3. User launches their personal IdP on their phone. Phone IdP receives request from the bank that the user be authenticated.
4. User is prompted by the phone IdP that the bank is requesting they be authenticated. User is asked for consent to proceed.
5. Phone IdP authenticates user (likely by PIN).
6. User's PC browser is redirected back to the bank with an authentication assertion from the phone IdP.



Fundamentally, the SASSO sequence is the same as that of the ordinary SAML 2.0 SSO procedure, but the IdP software is running on the mobile phone terminal, not on a server computer over a network. Therefore, initial authentication can be performed directly between the user and IdP, instead of through the network.

When a user accesses the SP from their PC to receive a service, the SP redirects the user to the IdP on the mobile phone to authenticate the user (typically through a network hosted relay server). If the user has not been authenticated yet, the IdP on the user's mobile phone authenticates the user. At a minimum, a PIN code can be input using a keypad. If the mobile phone has its own security feature, like fingerprint authentication, that can also be used for initial authentication to the IdP.

Then the IdP on the mobile phone creates an SAML assertion and signs the assertion with the private key of the mobile phone. One of the mobile phone carriers in Japan ships USIMs with digital certificates and key pairs, and some mobile phone terminals can use USIMs for digital signing. An authentication response that has the issued SAML assertion is sent to the SP through the user's PC by the HTTP POST method. Then the SP verifies the authentication response.

If the verification is successful, the SP provides the service to the user. Using key pairs in the USIM has security and usability merits. In terms of security, because UICC is a tamper resistant device the private key is stored safely. As for usability, a user can use the same key pair even if the user changes the mobile phone model.

Why Do Open Standards Matter?

SASSO is designed to be "plug and play" and to support universal interoperability among SPs. Importantly, SASSO presumes no special capabilities of SAML IdPs or desktop PCs. Such devices act just as they do in "normal" SAML SSO, so SASSO creates no special interoperability challenges.

Why Is SASSO Important?

- **Strong Authentication**
  By leveraging the mobile phone, SASSO leverages a more and more ubiquitous "what you have" factor for strong authentication. What's more, as the IdP is actually on the phone, the user retains complete control over how their identity information is released, e.g., to which SPs and when.

- **Convergence of Models**
  A client-based IdP is similar to the personal cards model of Microsoft CardSpace. Additionally, as the user initiates discovery of their personal IdP at the SP through the presentation of a personal URI, SASSO shares some aspects of the OpenID model. As such, SASSO demonstrates an interesting convergence of the OpenID, CardSpace and SAML styles of user-centric identity management.

- **Client Evolution**
  Clients are evolving to be "identity aware," actively assisting users as they engage in identity operations, rather than acting as passive conduits for identity attributes as do today's browsers. In one sense, SASSO is just another point of client identity evolution—along with Liberty Alliance's Advanced Client, whose specifications extend user-controlled identity management functionality to client devices such as cameras, handhelds, laptops, printers, and television set-top boxes. The specifications are part of Liberty's roadmap to deliver an open and interoperable end-to-end digital identity management framework that provides security and privacy protection across all networks and devices. The Advanced Client relies on ID-WSF 2.0 (Liberty Web Services) which includes support for WS-Addressing and WS-Security specifications.

Key Benefits to Business Organizations

- Mitigating security risks and increasing opportunities for deploying security sensitive services by deploying strong authentication
- Lower costs for and shorter time to deployment
- Better customer retention rate

Key Benefits to End-Users

- Higher confidence due to strong authentication and privacy friendliness
- Greater customer satisfaction due to the ease of use
- Better control of users' identity information by the users themselves

Moving towards the Future

SASSO is currently targeted to the mobile industry by leveraging the FirstPass Digital Authentication Service of NTT DoCoMo, but the solution can be applied to any segment and region where strong authentication is required.

In the future, Dr. Takahashi indicates that that SASSO will embrace:

- Identity attribute capability, e.g. The mobile IdP providing profile information to SPs as appropriate.
- Multi-protocol interoperability—OpenID, CardSpace, etc…
- Home identity center for net-connected appliances

Winning an IDDY Award

IDDY Award nominations are evaluated based on criteria that include the benefits applications deliver to users and organizations; the ROI the application is demonstrating; and how the solution may successfully address identity issues such as reducing identity theft, meeting regulatory requirements or providing users with increased security and privacy protection. The program includes an emerging applications category to showcase up-and-coming Liberty-based applications and proof-of-concepts that are driving the next generation of secure and trusted digital identity management solutions.

For more information on the IDDY Awards and how to apply, contact Russ Deveau at russ@projectliberty.org

About Liberty Alliance

Liberty Alliance is the only global identity organization with a membership base that includes technology vendors, consumer service providers and educational and government organizations working together to build a more trusted Internet by addressing the technology, business and privacy aspects of digital identity management. The Liberty Alliance Management Board consists of representatives from AOL, Ericsson, Fidelity Investments, France Telecom, HP, Intel, Novell, NTT, Oracle, and Sun Microsystems. Liberty Alliance works with identity organizations worldwide to ensure all voices are included in the global identity discussion and regularly holds and participates in public events designed to advance the harmonization and interoperability of CardSpace, Liberty Federation (SAML 2.0), Liberty Web Services, OpenID and WS-* specifications.