Standardization Activities of the Liberty Alliance

Teruko Miyata†

Abstract

This article provides an overview of the Liberty Alliance, which was established to create open global standards for federated identity management technology and related business guidelines, and surveys its activities, achievements, and current progress.

1. Introduction

The Liberty Alliance Project ("Liberty Alliance") was founded in 2002 to establish open, international standards-based specifications for federated identity management technology and related business guidelines [1]. This international standardization organization currently has over 150 participating companies and organizations from around the world. This article provides an update to the April 2003 article in NTT Technical Review [2].

2. Federated identity management technology

Federated identity management technology refers to technology for managing several identities and linking them to their various Web sites in a safe and secure way. It relieves the rise in the number of accounts that an individual must manage as the number of Web services grows. Here, identity refers generally to any information that identifies an individual, such as user account information for a system. To implement federated identity management, the concepts of an Identity Provider (IdP), a service provider (SP), and a federated ID [3] are introduced. IdP is a structure that provides unified management of authentication information. SP is a web site that provides a service, such as an e-commerce site. The concept of a federated ID refers to how a relationship is created between the IdP ID and the ID managed by the SP by generating a random string called a pseudonym.

† NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan
E-mail: lap@lab.ntt.co.jp

3. Liberty Alliance standardization activities

To establish these international technical standards for federated ID management, the Liberty Alliance is releasing them in four major phases (**Fig. 1**). Phase 1 covered "single sign-on" (SSO), Phase 2 extended the SSO standard in Phase 1 and transformed it so it was based on user-authorized attributes. In Phase 3, ID-FF was adopted by OASIS (Organization for the Advancement of Structure Information Standards) for SAML v2.0 (security assertion markup language v2.0), extending the attribute-exchange functions and specifications for linking to various types of Web services. Phase 1 and 2 specifications have been completed [4], and preparation for freezing the final specifications for Phase 3 is proceeding. Below, this article gives an overview of the architecture that the Liberty Alliance has settled on ("Liberty Architecture") and reports the current progress of Phase 3. It also introduces a particular Web service example for the regular exchange of personal information in digital broadcasting. Finally, it discusses future activities in terms of NTT's strategy and Phase 4.

4. Overview of Liberty Architecture

The Liberty Architecture is composed of three main components and is based on SAML and SOAP (simple object access protocol) (**Fig. 2**).

- **Identity Federation Framework (ID-FF):** Specifications for the most basic set of functions required

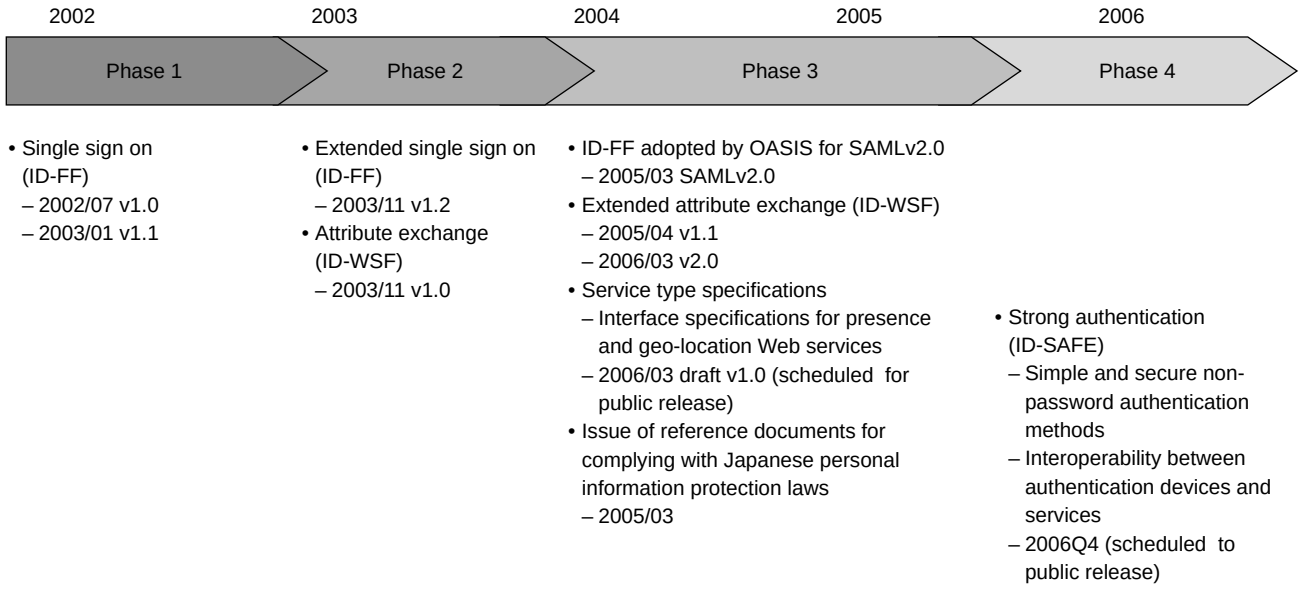

Fig. 1. Liberty Alliance specification phases.

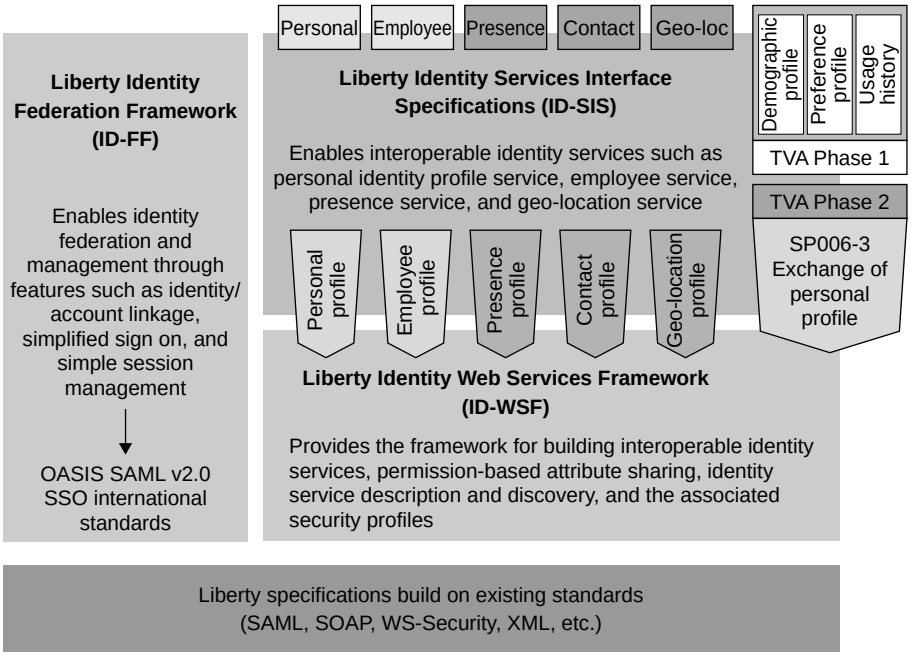

Fig. 2. Position of Liberty architecture and TVA specifications.

for implementing SSO, such as ID federation. ID federation, SSO, and single log-out were finalized in Ver. 1.1. Ver. 1.2 enabled links between IdPs as well as IdP anonymous authentication.

- **Identity Web Service Framework (ID-WSF):** Set of specifications for exchanging user attributes with sites providing Web services. Personal information is shared with the service site based on permission from the user. Identity services can also be discovered and used.
- **Identity Service Interface Specifications (ID-SIS):** Set of specifications for the actual service interface for implementing Web services based on ID-WSF. It prescribes specifications for providing personal information or employee information (in the case of a corporate service) as a Web Service

based on an actual identity. In particular, the data service template (DST) interface of ID-WSF is essential in ID-SIS. ID-SIS can be standardized for each service. At the Liberty Alliance, model DST specifications for handling various services have been provided within the ID-WSF specification set. Attribute information can be exchanged based on the ID-WSF framework by using a DST to create a new service interface.

5. Phase 3 (2004–2005)

Liberty Alliance activities from 2004 to 2005 were called Phase 3. The main objectives for the technical specifications of each component were achieved. The use of the Liberty Alliance ID-FF specification set for SSO in OASIS SAML v2.0 technology is expected to boost efforts to make SSO an international standard and also to gain wider adoption. In the ID-WSF specification set, new specifications regulating personal data management were added for social network services. In the ID-SIS specification set, three new Web service interface specifications were published (for presence, geo-location, and contact-book services), adding to the existing personal data and employee data specifications. Finally, in response to the enactment of the new personal information protection law in Japan, which took effect in April 2005, "Liberty Alliance and Japan's Personal Information Protection Act" [5] was released.

6. Adoption of Liberty ID-WSF as a personal information exchange specification for digital broadcasting

The Liberty Alliance is conducting liaison activities, collaborating with standardization associations in each industry, and supporting the adoption of Liberty specifications. In 2004, it made a liaison agreement with the TV-Anytime Forum (TVA) [6], [7]. Most members of TVA are European broadcasters and vendors, and TVA is creating international standards for new broadcast services incorporating links to telecommunications and local storage of broadcasts. Standards adopted by TVA have already been referenced by the European Telecommunications Standards Institute (ETSI) and by the Association of Radio Industries and Businesses (ARIB). NTT is participating in both the Liberty Alliance and TVA and is establishing itself in a leadership position in technical and business areas in both associations. Through this liaison agreement, TVA has adopted the Liberty Alliance ID-WSF v1.0 specification set, standardizing the exchange of viewer attributes. Furthermore, ETSI has decided on this viewer attribute exchange specification (TVA Phase 2 SP006-3) as an ETSI standard (ETSI TS 102 822-6-3, released Jan. 2006) [8]. In practical terms, the three profiles already specified by TVA (viewing usage profile, viewing preference profile, and demographic data profile) will be managed and shared using the Liberty Alliance ID-WSF v1.0 scheme.

7. Future activities

In the final Phase 4, the Liberty Alliance will establish a group to investigate strong authentication methods against "phishing" and ID theft and will push forward work on interoperability between authentication devices and services. NTT will continue to take part in Liberty Alliance standardization activities.

References

[1] Liberty Alliance: http://www.projectliberty.org/
[2] K. Terada and K. Takahashi, "Activities Targeting the Standardization of the Liberty Alliance," NTT Technical Review, Vol. 1, No. 1, pp. 94-96, 2003.
[3] Y. Koga, T. Miyada, and K. Takahashi, "Trends in Management of Personal Information and 'Liberty Alliance', the Association for Standardization of Information Sharing," Journal of the Institute of Electronics Information and Communication Engineers, Vol. 87, No. 6, pp. 504-507 (in Japanese).
[4] Liberty Alliance Specifications: http://www.projectliberty.org/specs/
[5] "Liberty Alliance and Japan's Personal Information Protection Act," http://www.projectliberty.org/jp/resources/lib-JapanPIPAct-ja.pdf (in Japanese).
[6] TV-Anytime Forum: http://www.tv-anytime.org
[7] M. Kawamori, "Recent Activities of the TV-Anytime Forum," NTT Technical Review, Vol. 4, No. 3, pp. 77-80, 2006.
[8] http://webapp.etsi.org/exchangefolder/ts_1028220603v010101p.pdf

Teruko Miyata
Senior Research Engineer, NTT Information Sharing Platform Laboratories.
She received the B.S. and M.S. degrees in mathematical science from Ochanomizu University, Tokyo, in 1991 and 1993, respectively. She joined NTT Laboratories in 1993. Her current field of interest is identity management business and technology.