Standardization Trends in Identity Management Technologies

Hiroki Itoh† *and Teruko Miyata*

Abstract

We introduce the latest standardization trends in identity management (IdM) technologies and schemes for achieving interoperability among several IdM technologies currently being considered, such as SAML, OpenID, and InfoCard.

1. Identity management

As the number of web applications increases, users are having to set up more and more online digital identities. In terms of protecting user security and enabling service providers to ensure that their services are compliant with security requirements, the administrators and the users must carefully manage user identities throughout their life cycles from creation to termination. In practice, the identity life cycle consists of three aspects—*authentication* (managing the use of applications), *authorization* (managing access to resources), and *attributes* (information associated with users, such as names, addresses, and credit card details)—together with various actions such as the creation, provision, updating, and termination of identities. There has recently been growing interest in identity management (IdM) technologies such as the ones used to federate web applications like software as a service (SaaS).

Technologies for managing user identities across multiple web applications can be classified as either single sign-on (SSO) technologies or attribute exchange technologies. In the former, the authentication procedures for different applications (from various service providers) are aggregated by an authentication provider (identity provider) and services are provided to users on the basis of the authentication results issued by the identity provider. In the latter, user attributes are shared between identity and service providers.

At the moment, the main SSO technologies are SAML (security assertion markup language) [1], [2], OpenID [3], and InfoCard [4], and the main attribute exchange technology is ID-WSF (Web Services Framework) [2], [5]. For each of these technologies, some industry groups have been set up to decide the specifications and encourage use of the technologies (**Fig. 1**). SAML, OpenID, and InfoCard technologies are all chiefly targeted at IdM in web applications. Their characteristics are outlined below.

(1) SAML has a strong affinity for web services and exploits the convenience of authentication tokens (XML (extensible markup language) documents representing the authentication results) on the assumption that user identities are circulated securely among specific services.

It has been introduced into many existing services, and since user identities can be mutually referenced among services, it is also described as a cooperative IdM scheme.

(2) OpenID allows user identities to be shared openly by expressing their identifiers in a globally unique identifier such as a URL (uniform resource locator).

(3) InfoCard is a user-friendly visual technology for implementing a *card selector* in user terminals to make it easier for users to perform identity management. The CardSpace implementation by Microsoft Corp. has been provided as standard in the Internet Explorer web browser since version 7 and/or in the Windows Vista operating system.

In this article, we discuss the latest trends in IdM

† NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan

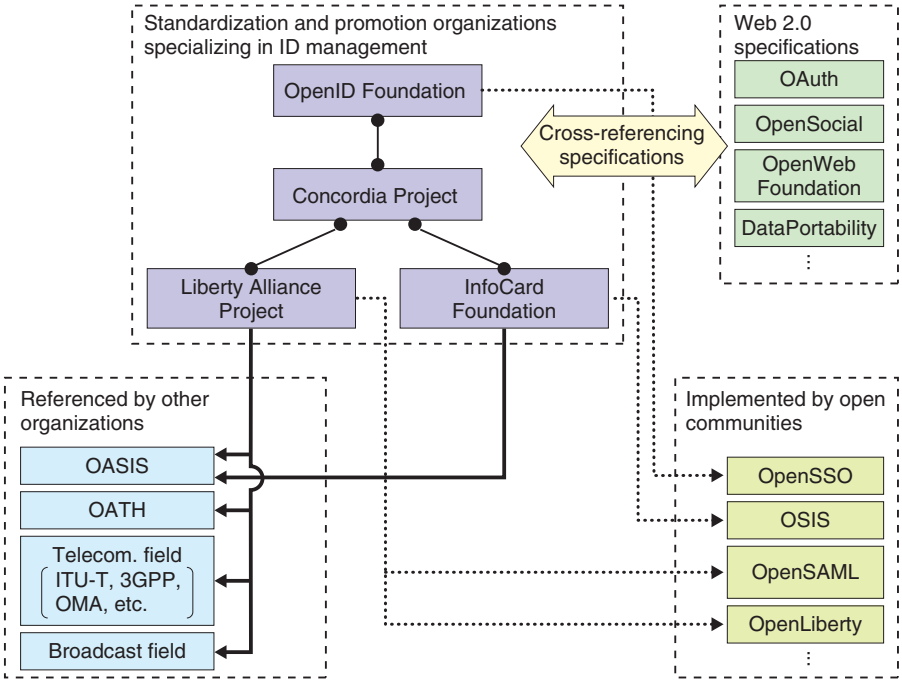

Fig. 1. Groups related to IdM.

technologies by introducing standardization trends of SAML and ID WSF centered on the activities of the Liberty Alliance Project (Liberty Alliance) [2], the trends in IdM technology theory at ITU-T (International Telecommunication Union, Telecommunication Standardization Sector), and the trends in open communities, such as the Concordia Project, which are investigating ways to interconnect IdM technologies.

2. Previous trends in the Liberty Alliance

The Liberty Alliance was established in 2001 with the aim of drawing up international standard specifications and business guidelines for cooperative IdM technologies. Today, it is an international standards organization with the participation of over 150 businesses, groups, government organizations, and other entities from all over the world. Its activities are mainly concerned with *authentication* and *attribution* (**Fig. 2**), two out of the three aspects mentioned above. The current situation regarding these two aspects is as follows:

(1) SSO

The Liberty Alliance used to regulate the Identity Federation Framework (ID FF), but ID FF has developed into SAML v2.0, which is now regulated by the Organization for the Advancement of Structured Information Standards (OASIS). The Liberty Alliance is still involved in discussions related to SAML with regard to the provision of implementation guidelines and the like.

SAML v2.0 is also referenced by ITU-T. In the form of Recommendation X.1141, it has been referenced in numerous drafts related to IdM in current discussions. The trends in IdM technologies at ITU-T are summarized in section 3.

(2) Attribute exchange

Two of the main Liberty Alliance specifications for the implementation of attribute exchange are ID WSF and ID-SIS: ID-WSF specifies communication schemes among servers and ID SIS specifies the interface (XML schema) of individual services.

The Liberty Alliance is currently making efforts to draw up standards that cover profiles customized by SAML and ID WSF for use as an e-government platform (eGovernment Profile), an Identity Assurance Framework that guarantees the strength level of authentication results among web applications [6], and an Identity Governance Framework for managing federated identities [7].

The third IdM aspect mentioned above, *authoriza-*

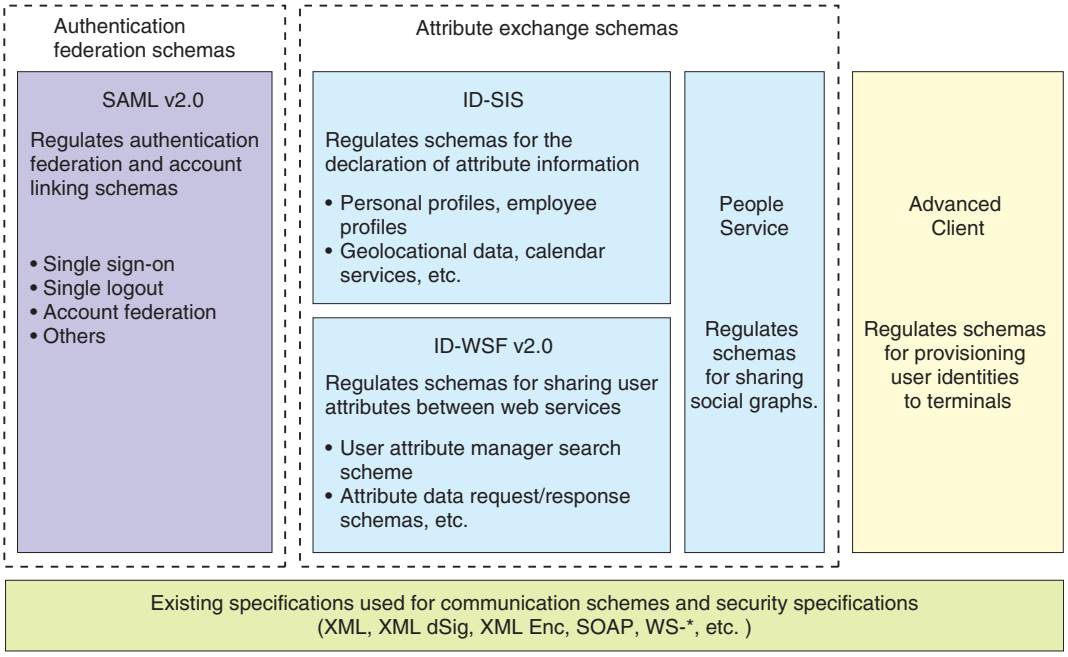

Fig. 2. Framework of IdM specifications prescribed by the Liberty Alliance.

tion, generally makes reference to other existing specifications such as XACML (extensible access control markup language) [8], which is specified by OASIS.

3. Trends in IdM technologies at ITU-T

At ITU-T, documents such as Recommendations related to IdM are mostly prepared by two investigative committees called Questions. These are Q16/13 (Question 16 in Study Group 13), which is investigating security and IdM in future networks including Next Generation Networks (NGNs) and mobile networks, and Q10/17, which is investigating IdM architectures and security mechanisms.

The main Recommendations and other documents (including draft documents) produced by these two Questions are listed in **Table 1**. In this article, we introduce the trends of discussions related to Q16/13, which are driving forward the preparation and completion of drafts related to IdM in NGNs.

The discussion of IdM in NGNs started in July 2006, when active discussions were held with a large agenda, and agreement was reached on the draft Recommendation Y.IdM sec (NGN identity management security) [9].

Then, in parallel with the submission of numerous contributions from many countries, there was active discussion of the main trends for existing standardized technologies.

As a result, the scope of investigations into IdM in NGNs (i.e., the importance of a *framework*) was advocated, and, taking this as a guideline for the construction of NGN IdM, the revised Recommendation draft Y.IdMsec was agreed in September 2007 and three documents were scheduled to be prepared on the topics of *requirements*, *use-cases*, and *mechanisms*.

An NGN IdM framework document was produced on the basis of this agreement with reference to earlier discussions and existing technologies. Then, at a meeting in January 2009, it was approved as ITU-T Recommendation Y.2720 (NGN identity management framework) as the first stage of Recommendations related to IdM in NGNs.

This framework document specifies the relationship between the functional requirements and architecture of NGNs and the concepts of IdM in NGNs and explains the roles of attributes, identity federation, and identity providers related to the management of attributes and security risks. This document is useful as a checklist of items to be consulted when IdM structures are investigated in NGNs.

In the future, based on this Recommendation

Table 1. Main ITU-T Recommendations (including drafts) related to IdM.

ID management recommendations (including drafts) in Q10/17 (as of Feb. 2009)

Recommendation No.	Recommendation name	Scheduled agreement date	Editor (affiliation & country)
Y.2720	NGN identity management framework	Approved (Jan. 2009)	Richard Brackney (DoD, USA), Takashi Egawa (NEC, Japan)
Y.NGN IdM Requirements (draft)	NGN identity management requirements	May 2009	Martin Dolly (AT&T, USA) Enhui Liu (Huawei, China) Anthony Rutkowski (Verisign, USA) Ray Singh (Telcordia, USA)
Y.NGN IdM Mechanisms (draft)	NGN identity management mechanisms	Sep. 2009	Takashi Egawa (NEC, Japan) Zachary Zeltsan (Alcatel-Lucent, USA)
Y.NGN IdM Use-cases (Technical Report) (draft)	NGN identity management use cases	May 2009	Martin Dolly (AT&T, USA) Paul Knight (Nortel, USA) Ray Singh (Telcordia, USA)

ID management recommendations (including drafts) in Q10/17 (as of Feb. 2009)

Recommendation No.	Recommendation name	Scheduled agreement date	Editor (affiliation & country)
X.1250 (draft)	Capabilities for enhanced global identity management trust and interoperability	2009 (Reconsideration to gain approval in May 2008 and redetermined in Feb. 2009)	Anthony Rutkowski (Verisign, USA), Jiwei Wei (Huawei, China)
X.1251 (draft)	A framework for user control of digital identity	2009 (redetermined in Feb. 2009)	Sangrae Cho, Seung-Hun Jin, Michael McIntosh (ETRI, South Korea)
X.eaa (draft)	Entity authentication assurance	2010	Richard Brackney (DoD, USA)
X.idm-dm (draft)	Common identity data model	Oct. 2009	Anthony Nadalin (IBM, USA) , Paul Knight (Nortel, USA)

Y.2720, three further documents are planned as Recommendation drafts—a requirements document (Recommendation draft Y.NGN IdM Requirements), a mechanism document (Recommendation draft Y. NGN IdM Mechanisms), and a use-case document in the form of a technical report (draft Y.NGN IdM Use-cases). Efforts are being made to submit papers as contributions to assist in the progression of these drafts into Recommendations.

4. Latest applications of IdM technologies

The Liberty Alliance is making progress in global use centered on business systems, government systems, and telecommunications providers. In business systems, the NTT DATA employee system cooperates with the authentication systems of an external service (an airline's online booking system). In government systems, in accordance with the provisions of the US General Services Administration, information systems for government agencies must use SAML as the IdM scheme [10]. Efforts are also being made with regard to cooperative IdM among e-government systems in Europe, and many examples of one-stop services can be seen in e-government systems aimed at civilians. In the field of telecommunications, France Telecom and Deutsche Telekom use cooperative schemes for their customer services, while in the NTT Group, the SSO scheme is used between NTT Communications (for the open computer network (OCN)) and NTT Resonant (for goo, a portal service). Another SSO scheme is also used in

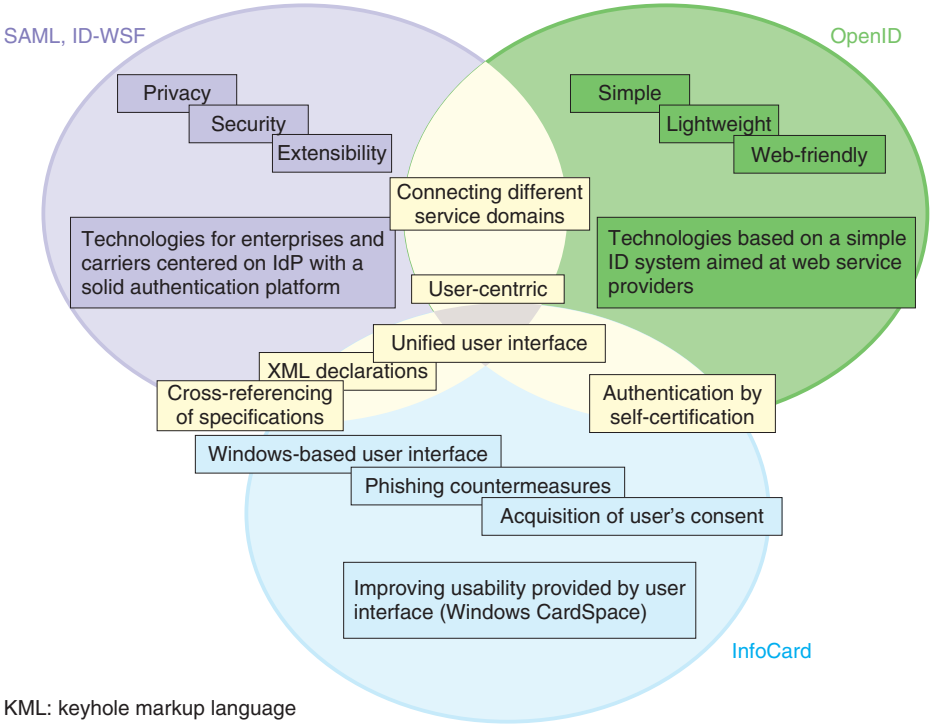

Fig. 3. Relationships among the main IdM technologies.

NTT DOCOMO (for My docomo, imode.net, and DCMX mini).

Below, we introduce two examples of efforts related to the development of applied technology at NTT Information Sharing Platform Laboratories.

(1) Advanced Client

The Advanced Client is a specification for implementing IdM on mobile terminals. It was drawn up in 2007 by building on the ID WSF specification.

In a terminal compatible with the Advanced Client, user identity is managed on a secure chip such as a trusted platform module or user identity module. This specification consists of functions for the distribution of user identities to terminals and the distribution of user identities needed for external control (provisioning functions) and proxy authentication provider functions that operate on the basis of the distributed user identities to allow users to log into applications compatible with the Advanced Client and allow the terminal to take the initiative in attribute exchanges.

(2) MD SSO

Multi-device single sign-on (MD SSO), which is based on the ID WSF specification, was drawn up in 2008 as a guideline for implementing ID information transfer among multiple mobile terminals. By sharing attribute information and user authentication contexts among MD-SSO-compatible terminals, it is possible for a single user to use a web application seamlessly across multiple terminals. For example, a user can start viewing a video-on-demand service on his mobile phone while traveling home and can continue viewing the same content on his IPTV (Internet protocol television) equipment after he gets there.

The drafting of MD SSO was led by NHK Science & Technical Research Laboratories and NTT Information Sharing Platform Laboratories, and the prototypes were built by NTT Cyber Solutions Laboratories.

5. Interoperability among IdM schemes

Centered on the schemes introduced in this article, various different IdM schemes are currently entering the market and spreading. Their specifications have been designed for different use cases, so the optimal scheme should be selected for each IdM-using service. For example, the IdM schemes discussed in this article can be regarded as having mutually complementary characteristics, as shown in **Fig. 3** [11].

However, now that efforts are being made to create

new services through the fusion of multiple services, it is becoming necessary to make services built on different IdM schemes that cooperate with one another. Moreover, each IdM scheme prescribes a number of extension specifications for purposes such as adapting to use-cases that are different from those originally considered in the design stage. As a result, the differentiating features of the individual IdM schemes shown in Fig. 3 are now becoming less apparent. In the future, the implementation of different IdM schemes is expected to obstruct cooperation among web applications just as web application cooperation becomes more active.

The Concordia Project (an open community established in 2006) is studying how to solve this problem by investigating interconnection schemes for multiple IdM schemes. NTT Information Sharing Platform Laboratories is playing an active role in this project. In addition, a study is being conducted into combining the activities of the Liberty Alliance and the Concordia Project and establishing a new group that encompasses all the other groups currently involved in identity management technologies.

References

[1] http://saml.xml.org/
[2] T. Miyata, "Standardization Activities of the Liberty Alliance," NTT Technical Review, Vol. 4, No. 5, pp. 51–53, 2006. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200605051.pdf
[3] http://www.openid.org/
[4] http://informationcard.net/
[5] http://www.projectliberty.org/
[6] http://www.projectliberty.org/resource_center/specifications/liberty_alliance_identity_assurance_framework_iaf_1_1_specification_and_associated_read_me_first_1_0_white_paper
[7] http://www.projectliberty.org/resource_center/specifications/igf_1_0_specs
[8] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml
[9] T. Hariu, T. Miyata, and Y. Oshima, "Recent NGN Security Standardization Trends in ITU-T," NTT Technical Review, Vol. 5, No. 12, 2007. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200712gls.html.
[10] http://www.cio.gov/eauthentication/documents/EAuthFederationArchitectureInterfaceSpec.pdf
[11] E. Maler, "The Venn of identity," http://www.xmlgrrl.com/blog/archives/2007/03/28/the-venn-of-identity/

Hiroki Itoh
Researcher, Ubiquitous Computing Project, NTT Information Sharing Platform Laboratories.
He received the B.S. degree in applied physics from Tokyo University of Science, the M.E. degree in applied physics from Tokyo Institute of Technology, and the MOT (Master of Management of Technology) degree from Tokyo University of Science in 2002, 2004, and 2009, respectively. He joined NTT Information Sharing Platform Laboratories in 2004. His current research interests are security and usability of user interfaces (e.g., web browsers, mobile phones, and other electronic gadgets) and his current work is standardization and technology incubation of identity management.

Teruko Miyata
Senior Research Engineer, Secure Communication Project, 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.