The Kantara Initiative— A New Organization for Identity Management Technology

Hiroki Itoh†

Abstract

This article provides an overview of a new organization called the Kantara Initiative, which aims to act as a bridge between existing identity management (IdM) standardization organizations by proposing methods for interoperability between IdM technologies such as SAML, OpenID, and InfoCard.

1. Introduction

Identity management (IdM) technologies have been attracting much attention recently for use in linking multiple software-as-a-service (SaaS) products such as web applications. IdM currently covers many technologies and activities such as security assertion markup language (SAML), OpenID, and InfoCard, the Concordia Project, which is an open community for discussing interoperation among IdM technologies, and related initiatives at the NTT Information Sharing Platform Laboratories. An overview of IdM management technologies was given in a recent NTT Technical Review article [1].

2. Kantara Initiative

2.1 Founding

NTT Information Sharing Platform Laboratories created a prototype and conducted demonstrations based on IdM technology interoperability use cases resulting from the Concordia project. In April 2009 at the RSA Conference USA 2009, we demonstrated interoperation between SAML and OpenID in collaboration with the Nomura Research Institute and Oracle Corporation [2]. However, that organization did not encompass activities required for consultations regarding technical standardization such as requirements definition, specification creation, and compatibility testing for implemented applications. In response, the Kantara Initiative [3] was established in June 2009 as a new organization to address these and other issues.

2.2 Range of activities

The Kantara Initiative is an open community for collaboration among seven organizations involved in IdM technology (**Table 1**) that is intended to promote the assurance of security and privacy in the use of online services through the use of IdM technology. It will be involved in studying IdM-related technologies, creating guidelines for issues such as privacy assurance, and presenting lectures. The results of its discussions and studies will be published by the organization as white papers and other documents independent of technical specifications. The Kantara Initiative is not expected to create technical standards. Any technical standards arising from its work will be submitted as drafts to existing standards organizations such as OASIS (Organization for the Advancement of Structured Information Standards) or IETF (Internet Engineering Task Force). This is because, in view of the number of companies and organizations that have already created technical specifications and the fact that there are already conflicts between them, the Kantara Initiative has decided on the approach of proposing methods of interoperation among compet-

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

Table 1. Kantara Initiative founders.

Concordia Project	A non-profit organization studying methods for interoperation between IdM technologies such as SAML, OpenID, OAuth, and Information Card.
Liberty Alliance	A standardization organization performing work such as defining technical standards related to IdM technology, security evaluations, and interoperability testing for implementations based on technical standards.
openLiberty	An open community implementing open source software based on Liberty Alliance specifications.
DataPortability Project	A non-profit organization studying methods for interoperability between services that utilize user information on the Internet.
Information Card Foundation	A non-profit organization promoting the spread of a digital identity card called the "Information Card" on the Internet.
Internet Society	A non-profit organization providing leadership for Internet-related activities such as standardization, education, and policy-setting. Lower branches of the Internet Society structure include the IETF and the Internet Architecture Board.
XDI.org XDI Public Trust Organization	A non-profit organization for identities that can be used safely and securely over long periods by individuals and companies, are based on the extensible resource identifier scheme, and are independent of network or protocol.

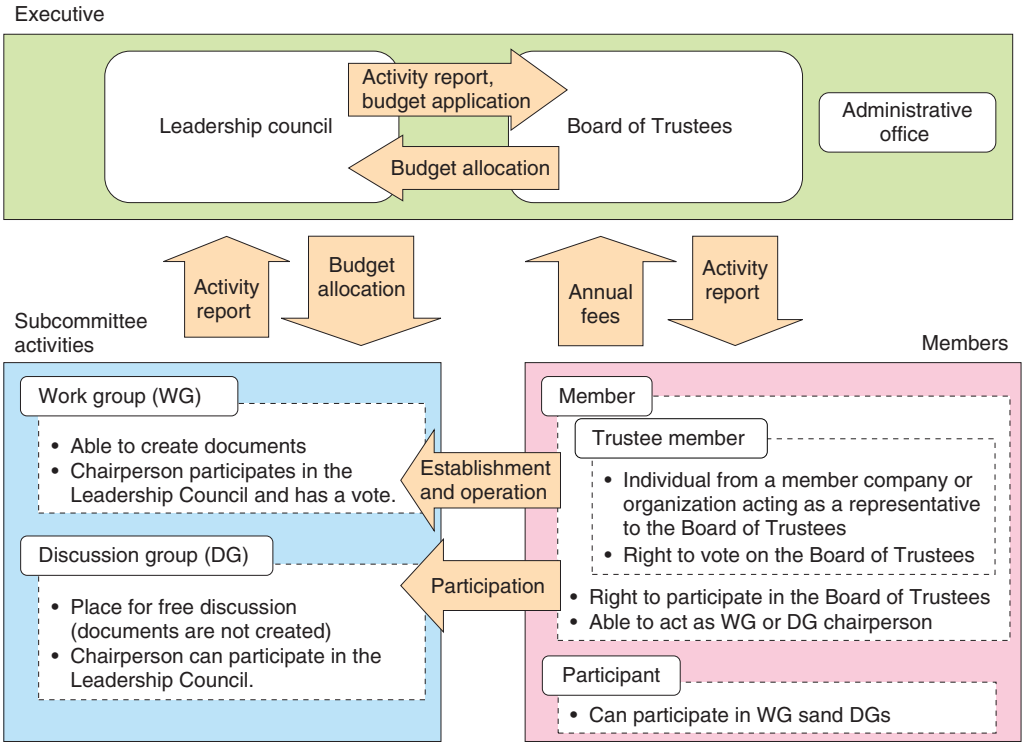

Fig. 1. Organizational structure of the Kantara Initiative.

ing solutions.

Note that the Kantara Initiative will take over control of the activities of three existing projects, Liberty Alliance, Concordia Project, and openLiberty, which will disband as of the end of December 2009.

2.3 Organizational structure

The organizational structure of the Kantara Initiative is shown in **Fig. 1**. Actual activities of the organization will be carried out mainly in subcommittees,

which will be divided into two types: Working Groups (WG) and Discussion Groups (DG). WGs will perform tasks such as producing documents and submitting technical specification drafts to other organizations, which DGs will not be authorized to do. This setup was chosen to cope with differences in intellectual property rights (IPR) policies and enable participants concerned with such issues to participate in DGs more easily with lower entry barriers in a *birds-of-a-feather* style. Both Members and Participants (described below) may participate in subcommittees, but the chairperson of each subcommittee must belong to a corporate Member company.

There are three types of membership in the Kantara Initiative: Trustee Member, Member, and Participant. Trustee Members are selected as representatives of Trustee Member corporations/organizations, and as such have a vote on the Board of Trustees, as described below. A Member refers to an individual acting as a representative of a Member corporation/organization; he or she is permitted to act as a subcommittee chairperson and participate in meetings of the Board of Trustees. Participants who do not belong to a Member corporation/organization may become subcommittee members and may participate in subcommittee activities if they agree to the IPR policy according to subcommittee regulations, but there are differences between Participants and Members, such as Participants not being permitted to act as subcommittee chairpersons.

The Management Executive of the organization consists of the Leadership Council and the Board of Trustees. The Leadership Council (currently 19 people) consists of one representative of each subcommittee and two representatives from the Board of Trustees, while the Board of Trustees (currently 16 people) consists of two representatives from each Trustee Member corporation/organization and two representatives from the Leadership Council.

The Leadership Council will perform tasks such as approving the results of subcommittee activities for publication and drafting subcommittee budgets, while the Board of Trustees will simply approve or reject. This setup is intended to allow independent operation of subcommittees and prevent undue intervention in subcommittee activities by the Board of Trustees or Trustee Member companies.

2.4 Plans for activities in Japan

Two subcommittees, the Japan Workgroup [4] and the Japan Discussion Group [5], have been convened to carry on the activities developed earlier in Japan under the Liberty Alliance.

The Japan Workgroup was established to hold events, write white papers, translate specification documents, and perform other activities to increase the awareness and spread of IdM technologies within Japan. The chairperson is Kenji Takahashi from NTT Information Sharing Platform Laboratories, the vice-chairperson is Toshihiro Suzuki from Oracle Japan Inc., and the secretary is Takashi Shitamichi from Sun Microsystems Japan.

The Japan Discussion group was established to provide a place for discussion related to IdM technologies in Japan using email lists, a Wiki, and other means.

These two subcommittees will continue the relationships built in the Japan SIG (special interest group) of the Liberty Alliance and have indicated their intention to cooperate with the OpenID Foundation Japan.

2.5 Other subcommittee activities

As of December 18, 2009, the Kantara Initiative subcommittees consisted of 15 WGs and 5 DGs, either already established or in the process of being established, and it was gradually establishing its place as a forum for discussion. Along with the Concordia Discussion group mentioned earlier, the Identity Assurance WG (IAWG) [6], which is currently studying specifications for an Identity Assurance Framework (IAF) [7], is also becoming a pillar of activity within the Kantara Initiative.

2.6 IAF overview

The IAF is a standard document that defines the requirements for (1) “Levels of Assurance” for ID data, (2) a unified basis for aspects such as authentication methods that must be met by all providers for each level of assurance, and (3) procedures for third-party IAF compliance testing, in order to simplify processes when linking IDs between different Web Services operators, such as mutual confirmation of the reliability of information. The work of deciding and finalizing the IAF is currently being done by the IAWG within the Kantara Initiative.

The objective of the IAWG is to establish a framework for auditors approved by the IAWG to test compliance in both directions between Web Services providers and authentication servers, as shown in **Fig. 2**.

The IAF represents the continuation of the work in the EAP Trust Framework 1.0 [8], established in January 2005 by the E-Authentication Partnership

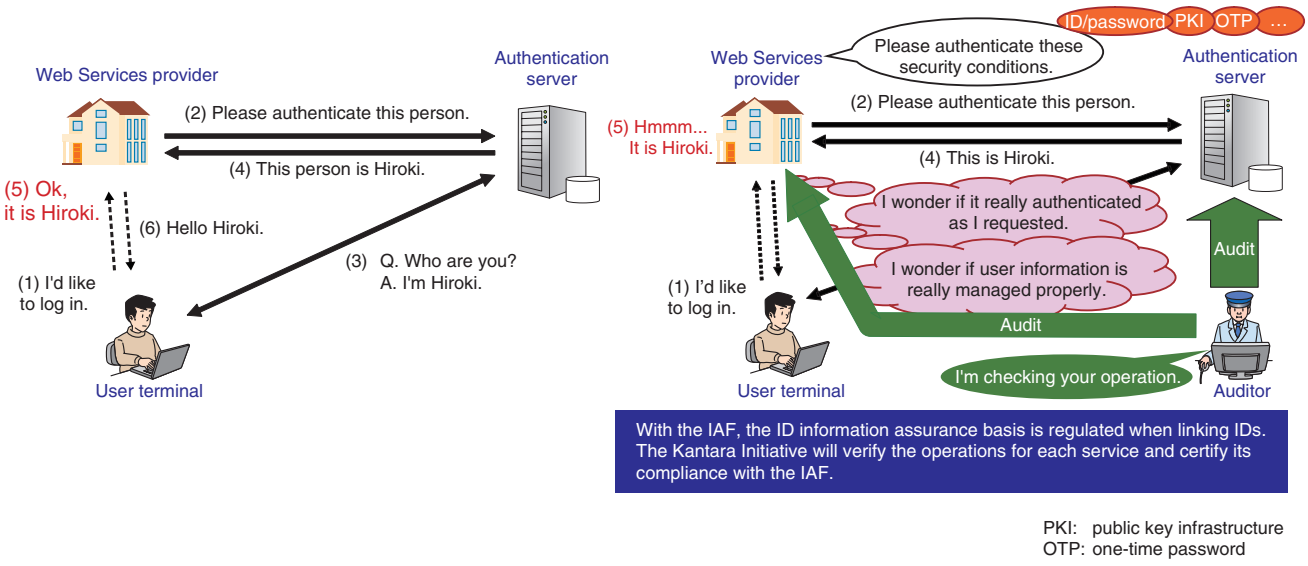

Fig. 2. Overview of IAF.

Table 2. Assurance levels regulated by IAF.

Level	Overview
AL1	Service requires almost no confidentiality or reliability. Corresponds to operations like login for e-commerce and other sites.
AL2	Service requires confidentiality and reliability. Corresponds to registration or change of name, address, etc. on a website.
AL3	Service requires a high level of confidentiality and reliability. Requires reliability of a level provided by multifactor authentication using software tokens, hardware tokens, or one-time passwords. Corresponds to services such as trading on a securities company website.
AL4	Service requires an extremely high level of confidentiality and reliability. Requires reliability of a level provided by multifactor authentication using hardware tokens. Corresponds to the handling of confidential data such as medical information.

(EAP) in the USA, and the Credential Assessment Framework 2.0 [9] (CAF 2.0), a level-of-assurance evaluation standard established in March 2005. EAP was absorbed into the Liberty Alliance in September 2007 and its activities moved to the Identity Assurance Expert Group [10] of the Liberty Alliance, which created the IAF. IAF 1.1 was released in June 2008, and as of August 2009, work on IAF 2.0 was in progress, with partial drafts having been released. Now, with the inauguration of the Kantara Initiative, this work is being reorganized under the IAWG.

The IAF regulates assurance-level (**Table 2**) compliance requirements, including: (1) requirements that service providers must satisfy, (2) requirements that services provided by such organizations must satisfy, and (3) requirements that must be satisfied when an organization issues user-authentication information. These assurance levels are defined in the M-04-04 [11] guidelines for electronic authentication in federal government facilities, regulated by the USA Office of Management and Budget for the Executive Office of the President, as well as the NIST 800-63 [12] guidelines for electronic authentication, regulated by the USA National Institute of Standards and Technology.

The IAWG is currently working on IAF specifications and also studying ways in which authorization testing programs for the framework could be put into practice.

Note that the USA General Services Administration

and the USA financial industry are actively promoting standardization of IAF regulations, so they are expected to be widely provided to groups such as ITU-T x.eaa, ISO WD 29115, the Financial Services Technology Consortium, and the Healthcare Information Technology Standards Panel.

3. Outlook for IdM technology standardization

IdM technology, which is currently still in an introductory phase with providers, will become extremely important in the Concordia discussion group and in activities in Japan and elsewhere, as mutual operation between service businesses expands in the future. The activities of these subcommittees are open and anyone can participate, so it is hoped that there will be greater participation and more active discussion in the future.

References

[1] H. Itoh and T. Miyata, "Standardization Trends in Identity Management Technologies," NTT Technical Review, Vol. 7, No. 6, 2009. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200906gls.html
[2] http://projectconcordia.org/index.php/Planned_Scenarios_for_RSA_2009
[3] http://kantarainitiative.org/
[4] http://kantarainitiative.org/confluence/display/WGJ/Home (in Japanese).
[5] http://kantarainitiative.org/confluence/display/DGJ/Home
[6] http://kantarainitiative.org/confluence/display/idassurance/Home
[7] 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
[8] http://eap.projectliberty.org/docs/Trust_Framework_010605_final.pdf
[9] http://www.idmanagement.gov/eauthentication/documents/CAFv2.pdf
[10] http://www.projectliberty.org/liberty/strategic_initiatives/identity_assurance
[11] http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf
[12] http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

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 Science, 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 research interests are security and usability of user interfaces (e.g., for web browsers, mobile phones, and other electronic gadgets) and his current work is standardization and technology incubation of identity management.