# Activities Targeting the Standardization of the Liberty Alliance

*Kenji Terada*†*, and Kenji Takahashi*

**Abstract**

With the increasing popularity of the Internet, various types of personal information (usernames, passwords, usage histories, *etc.*) are being created, shared, and utilized on diverse websites. The Liberty Alliance is a standardization organization that establishes technical specifications designed to link these scattered forms of personal information and share it safely and efficiently in the from of an "Identity" that expresses all aspects of the individual. As of February 2002, the Alliance had 159 member companies from diverse backgrounds, including telecommunications (*e.g.*, NTT and NTT DoCoMo), vendors (*e.g.*, Sun Microsystems), and finance (*e.g.*, VISA International).

## 1. Identities linked on the Internet

A user's "Identity" on the Internet plays an important role in terms of enabling that user to comfortably and safely access personal services suited to his or her own tastes and usage style. At the moment, however, commonly used identity management and application technologies present the following problems.

1. Lack of interoperability
   An inordinate number of identity-related technologies and services without interoperability results in complex user information management and operations.
2. User anxiety regarding security and privacy
   There is distrust regarding unauthorized collection and use of personal information and anxiety about dependence on closed technologies.
3. Excessive concentration of personal information
   The concentrated collection of personal information by specified organizations is inhibiting healthy development of the industry.

In order to resolve these problems, the Liberty Alliance is studying technical frameworks for open and secure distributed (linked) identity management and applications that also offer a high degree of interoperability (Fig. 1). The Liberty Alliance framework can be applied to a variety of authentication domains (gatherings of cooperating companies and organizations that accommodate authentication results) in keeping with the usage scene (Fig. 2).

The Liberty Alliance is conducting activities according to goals set for specific phases. Already, specifications for a single sign-on technology, the target of the first phase, are complete, and are now available to the public (ver. 1.1). Currently, the Alliance is working on technical specifications for the second phase, "Sharing of Personal Information based on User Authorization," with plans for completion by the middle of this year.

## 2. Phase 1: Single sign-on

Technical specifications for the first phase of the Liberty Alliance's activities achieve "single sign-on" to allow a user to access multiple services with a single authorization. Already, major vendors such as Sun Microsystems and Hewlett Packard have expressed their support for the Phase 1 specifications. The main features of these specifications are as follows.

- Because this method links identities managed by various providers, it is possible to take advantage of the individual initiatives of providers and avoid the risk of privacy invasion through central manage-

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

ment of identity information.
- Users can access applications through standard Web browsers.

The goal of the specifications is to enable the use of single sign-on technologies from a wide range of terminals to allow applications even from mobile phones, which have limited resources, by introducing Liberty Alliance proxies on the network side.

## 3. Phase 1 (single sign-on) mechanisms

The framework for the first phase, single sign-on, is made up of the user, the service provider, and the identity provider (IDP). The service provider is a company or organization that actually provides the user with various services, while the IDP is one that links user identities and performs authorization. Once the user has signed on to the IDP, he or she can access the services of service providers connected with that IDP without having to sign on again (Fig. 3).

First, as preparation, the user links the identity at the IDP with the identity at the service provider. An alias is used in both cases, so that the user's true identity cannot be leaked from one provider to the other; this ensures that privacy is protected and that the

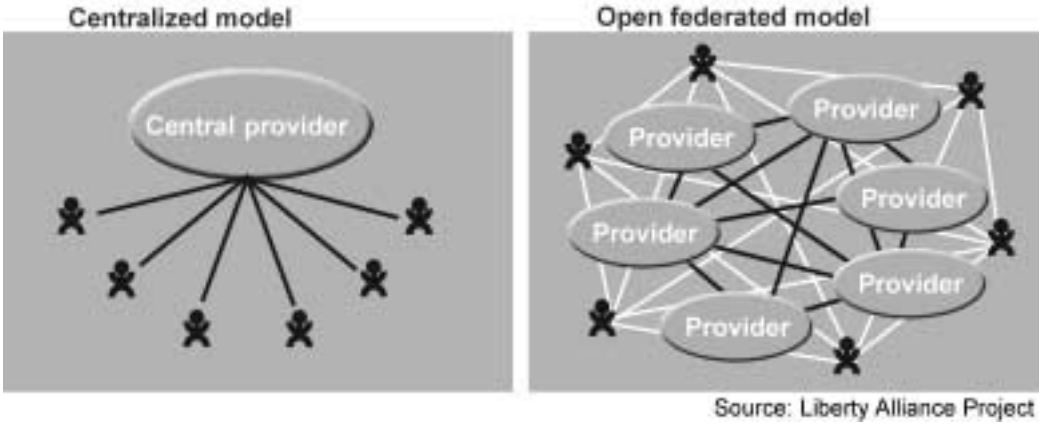



Fig. 1. Identity management model.

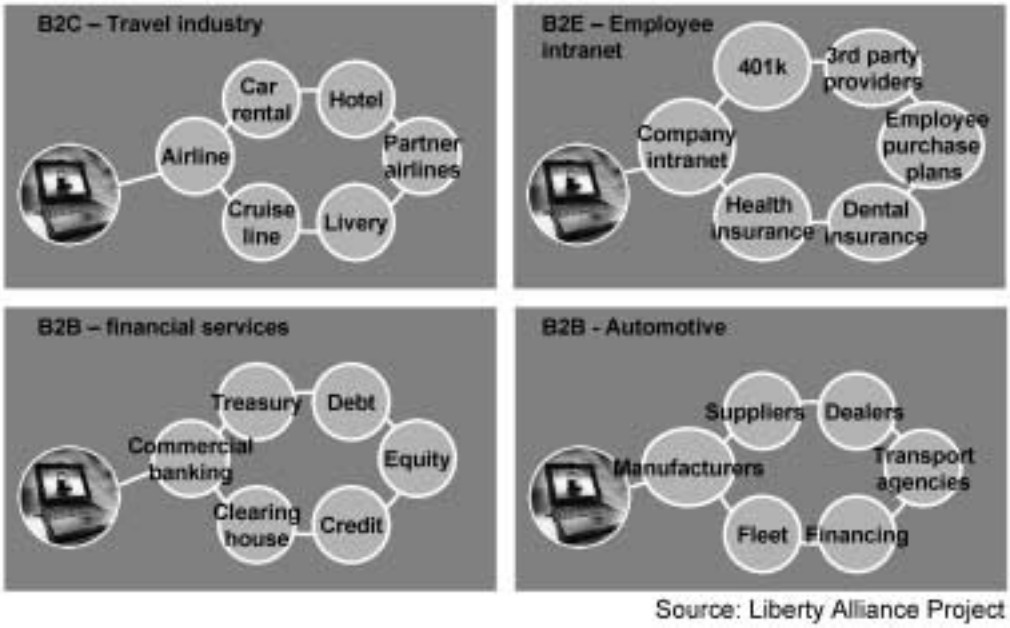



Fig. 2. Examples of trust domains.

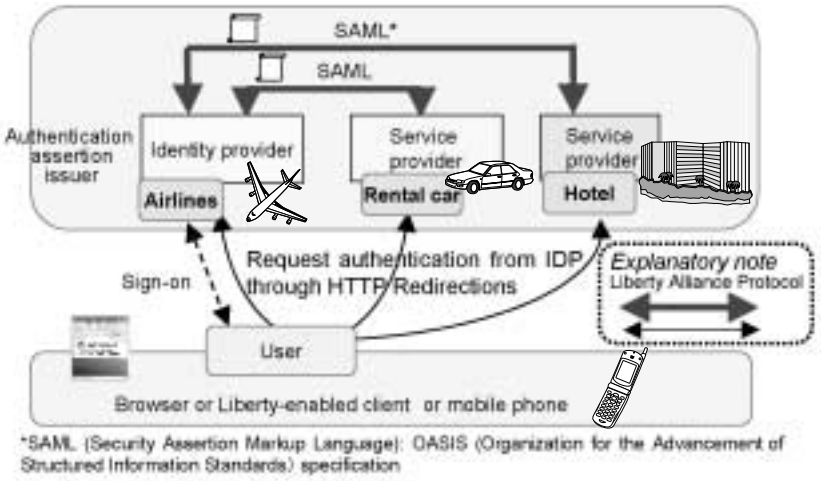



Fig. 3. Sketch of Liberty Alliance single sign-on.

independence of the service provider is maintained. Next, the user carries out authentication processing for the relevant service providers. The following are some of the more common processes involved:

(1) The user signs on to the IDP (single sign-on).
(2) The user requests services from the service provider.
(3) The service provider requests authentication from the IDP through redirections.
(4) The user's authentication ticket is passed from the IDP to the service provider.
(5) The user begins using the service provider's service.
(6) If the user wants to user another service provider, steps (2) to (5) are repeated.

## 4. Toward Phase 2 (sharing of personal information)

In Phase 2, the Alliance will establish technical specifications for sharing personal information (names, contact numbers, addresses, *etc.*) among service providers. Furthermore, Liberty Alliance functions will become accessible across differing authentication domains.

When Phase 2 comes to fruition, users will be able to access personalized services from a variety of service providers without having to input the same personal information over and over again. Meanwhile, service providers will have a greater opportunity to cooperate with other service providers to offer even more personalized services to a greater number of users.

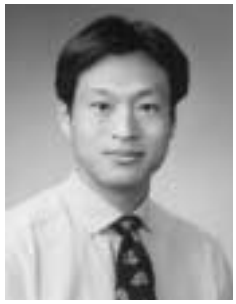
## 5. Status of NTT Group participation and activities

Two companies from the NTT Group—NTT and NTT DoCoMo—are participating in the Liberty Alliance. NTT, in particular its laboratories, proposes specifications and develops technologies that take advantage of newly established ones.

## References

[1] http://www.projectliberty.org/

**Kenji Terada**
Research Engineer at Proactive Platform Project, NTT Information Sharing Platform Laboratories.
He received the M.E. degrees from Japan Advanced Institute of Science and Technology, Ishikawa, Japan, in 1998.
Mr.Terada is a member of the Institute of Electronics, and Communication Engineers. He received the Best Paper award at the 5th Pacific Rim International Workshop on Multi-Agents.



**Kenji Takahashi**
Senior Research Engineer, Supervisor at Proactive Platform Project, NTT Information Sharing Platform Laboratories.
Currently he is leading several R&D projects for, such as, indentity managment and ubiquitous computing technologies.
Since joining NTT, he has been actively participating in many international industrial consortium and standardization activities, including CommerceNet, IETF and Liberty Alliance.
Dr. Takahashi received the Ph.D degree in Computer Science from Tokyo Institute of Technology.