

A Concept of Interoperable Authentication Framework for dynamic relationship in Identity Management

Seung-Hyun Kim*, Seung-Hun Jin*, Hyung-Jin Lim**

* *Electronics and Telecommunication Research Institute (ETRI), Daejeon, Korea*

** *Financial Security Agency, Seoul, Korea*

{ayo, jinsh}@etri.re.kr, Dream.hjlim@gmail.com

Abstract— The Identity Management (IdM) is a technology for systematically managing an entity's identity. There exist several kinds of IdM technology and are complicated to present a method for intersection and integration among them. It is also difficult to provide a consistent level of security because of mutually different certification mechanisms and strengths even in case of using a same IdM technology. Although authentication technologies manage the important role in the security, the IdM technologies describe a correlation with the authentication technologies in the abstract and general level. They do not well present how to request the necessary authentication technique and how to be offered as any kind of authentication type.

This paper presents a method that provides an integration of the IdM technologies through the common authentication framework. The framework is able to configure dynamic CoT (Circle of Trust) according to each authentication technology. It also offers a consistent experience to the users not limited to a specific CoT. If a user passes a specific authentication level, the user can be offered an important service from non-trusted CoT which has a different IdM technology. Namely, the proposed framework provides the CoTs to integrate with dynamic relationship in the Internet level.

Keywords— Circle of Trust, Dynamic relationship, Identity Management, Interoperability

I. INTRODUCTION

Identity Management (IdM) is a technology for systematically managing an entity's PII (Personal Identifiable Information) and life-cycle. IdM is largely divided into centralized, federated, and user-centric type. These types are required to provide consistent identity life-cycle management in common. But the existing centralized/federated types specify a specific IdM scheme and a strict entity relationship. They have too limited position and it is hard to expand dynamically. On the other hand, the user-centric type is very suitable for dynamic extension. Although the type has various authentication schemes, it is difficult to convince that the scheme is performed properly. Even if each entities use

the same IdM technology, because of the different authentication methods, it raises problems of the authentication strength, convenience and so on. In case of centralized and federated IdM, its security relies on the identity provider. Therefore the trust relationship is limited to the CoT. In case of user-centric IdM, it manages users' identity to the Internet level by establishing a dynamic trust relationship between the entities. However the trust relationship is limited because a relying party cannot convince the security of an identity provider. Integration of the IdM technologies is also difficult in case of a different types and a different authentication schemes.

We have been developed a single protocol to cover the various authentication mechanisms by extending the SASL authentication mechanism. It provides the user the negotiation in a single protocol format. In this paper, we extend this concept and implementation. Therefore we propose a framework not only manage the authentication technologies not involved in the ID management but also exceed the CoT within the ID management scheme. The proposed authentication framework applies to the ID management to provide universal and static/dynamic trust domains (CoT), as well as support for various authentication levels and services which can be negotiated. Regardless of the interoperability and the ID management scheme, the proposed framework can be applied to integrate with ID life-cycle management, security (strong authentication), authentication technologies, as well as negotiation which includes security level mapping between the entities which have different characteristic(ex. ID management scheme and authentication methods).

This paper is consisted as follows. In chapter 2, we introduce the status of the ID management technology and the authentication framework, and will emphasize the need of the cooperation between them. In chapter 3, we explain the concepts and schemes for the proposed authentication framework and then offer a detailed message, the protocol. Chapter 4 enumerates the related works and the last we give a conclusion and future research in chapter 5.

II. BACKGROUNDS

Figure 1 shows the latest trend of IdM framework areas and multi-factor authentication, and also represents their relevance. The sites make the transition from the traditional authentication frameworks to the ID management framework or to the strong authentication framework. Although the ID management technologies and strong authentication technologies maintain their domains, the proposed authentication framework works closely with each other and leads the synergy effects [1,2,3,4].

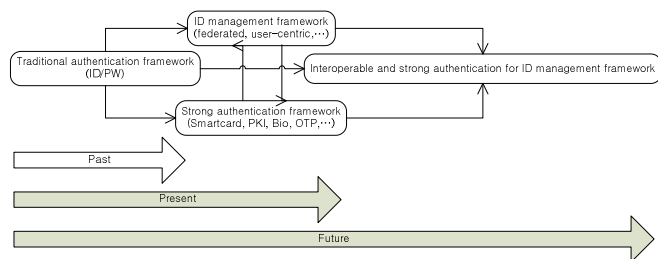


Figure 1. Transition of IdM framework area and multi-factor authentication

From the perspective of the evolution of the ID management framework, existing ID management technology was oriented to the protocols such as SAML and WS-FED, the service profiles, metadata for the maintenance of the entity relationship. Recently, the IAF (Identity Assurance Framework) [19] and IGF (Identity Governance Framework) [20] from the Liberty Alliance has expanded to consider the ID life-cycle. But they describe the association with the authentication scheme in the abstract and general level, and do not provide how the authentication technologies are requested and provided.

Even if the user passes the same authentication technology, there have different security levels (ex. Password strength of id / pw). However it is out-of-scope in the traditional ID management scheme. Even if the user has the same ID management technology [5,6,7,8,9,10], it may provide completely different security levels and user experience based on the authentication scheme. It also causes the confusion while the integration and the use. ID management technology considers the security of the protocol level, but the authentication process and authentication methods were out-of-scope.

However recent hacking trends are not focus on the vulnerability of protocol for the ID management, but the vulnerability of the user terminal which uses the service. It means, although the ID management scheme that provides the convenience and reliability, sophisticated attacks such as MITM (Man In The Middle), MITB (Man In The Browser) [22] are still vulnerable to the ID management framework itself and limit to provide a reliable level of authentication for the ID management framework. To guarantee the reliable level of authentication, we should consider how to provide strong authentication while not undermine the convenience of the ID management framework [11,12].

Evolution of the authentication strength is able to reduce or block the mentioned threat of sophisticated attacks. However, to adopt these authentication technologies in the

actual application service, we have to define how to link these technologies and the user's identity in the ID management technology. While independent of the ID management, the authentication technologies evolve to the mature frameworks which provide stronger authentication (ex. smartcard, PKI, bio, OTP) to the entity or resource. However, in the view of the main purpose of the strong authentication technologies is the reliable verification of the electronic identification, the authentication technologies are required to define the terms of cooperation with various ID management framework [1,2,3,4]. Maintaining the security level of reliability for the user depends on the authentication technologies and methods. The ID technology needs to consider the integration of certification and authentication.

To meet the security requirements of existing applications, it is needed to consider the current infrastructure and the available authentication services. It also needs to define the organized security level and apply the appropriate authentication mechanism. If the authentication framework applies only to one ID management technology or for a specific authentication technology, it will be reduced the actual utilization. Therefore, it is required that the authentication framework is general-purpose and can be applied to the multiple ID management schemes. Interoperable expansion is needed to accommodate the traditional ID management cycle to provide a reliable level of authentication. Finally, the framework enables a more reliable level of security by combining the ID management and strong authentication.

To summarize, an authentication framework must satisfy the following conditions to work with ID management technology.

- Association with ID life-cycle and credentials life-cycle
- Seamless transition and integration with traditional authentication infrastructure and ID management infrastructure
- Guideline for the security level of services
- Common authentication methods and procedures for ID management technology
- Various ID management services which do not referred to the ID management standards.
- Common UX (User eXperience) without regard to ID management

III. PROPOSED SCHEME

A. Basic Concepts

This paper presents measures to meet the above requirements from the point of view about the interoperability, life-cycle, security, and so on. Through a consistent and independent UI, messages format, and the protocol, it provides the interoperability regardless of the authentication methods and ID management technologies (ex. SAML, CardSpace, OpenID). It also provides a flexible framework for authentication methods and ID management schemes to add/delete/change easily. In addition, without infringing on a range of existing ID management technologies, it covers the remaining part to apply easy integration. It runs an authentication procedure according to the policy of life-cycle

management, and provides various operations for the ID lifecycle. According to the authentication level, the user negotiates with the service provider about the authentication method for a service. For the authentication methods, it can support from id/pw to OTP and multi-factors.

This paper is largely based on the modeling for the type of authentication technologies and basic requirements. Therefore we need to classify security levels for each authentication technology which are not mentioned in the ID management schemes. Also, in order to perform the negotiation which is one of the features highlighted in this paper, it requires systematic mapping for the service level and authentication technology. This paper presents the warranty coverage with a simple combination of LoA (Level of Assurance).

It is hard to expand the content of a token in ID management schemes. Therefore we think the significant contribution is that authentication framework covers this expansion. To do this, this paper provides various authentication levels whether with the support of ID management technology by mapping LoA and the services. The biggest contribution of this paper is to present a common authentication framework for the integration of the ID management schemes. It has the ability to configure dynamic CoT for each authentication technology, and provides a variety of experience to the user cause of not limited to the specific CoT. Even a not trustful user from an ID management CoT, if the user passes high-level authentication in other CoT, the user can be served the services. In other words, it combines a dynamic relationship at the Internet level with the confidence.

B. Framework

Proposed authentication framework is consisted as follows.

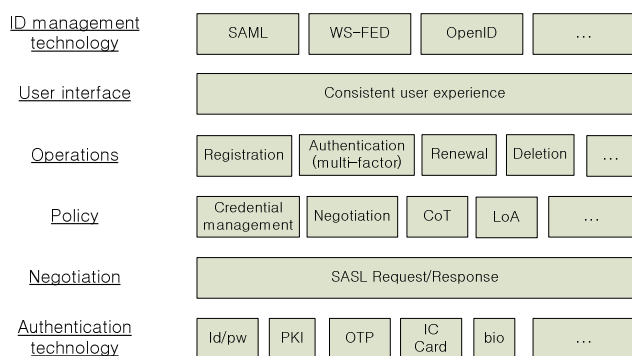


Figure 2. Proposed authentication framework

The following describes each layer.

- ID management technologies; proposed authentication framework can provide the services independent from the applied ID management technology. It interprets the authentication methods for each ID management scheme, and then generates a token through the authentication process. The token may include user's identity information, authentication information/levels, and so on.

- Consistent UI; It provides the same user experience regardless of the authentication technology, multi-factor, and ID management technology. The user is able to perform the same task in the same screen when the user visits any site which uses different ID management technologies or authentication technologies.

- Features; Life-cycles for ID management and credential (id/pw, certificate, bio, OTP) are organized as modular type. Therefore each site is able to select the favorite ID management technology and authentication methods. Over the traditional id/pw and PKI, the proposed framework manages not only stronger authentication such as OTP and bio but also multi-factor authentication. It supports everything for this layer, but the site determines what the technologies use.

- Policy; this layer manages the policies for negotiation, CoT configuration, lifecycle management, and so on. Similar to the metadata in SAML, it manages the supported services and required security level for the supported services. By specifying the other trust-able domain in point of authentication service, it is able to configure the CoT which is set dynamically based on the authentication method.

- Negotiation; this layer defines a protocol that specifies the service level and the LoA to meet the agreement for the appropriate security level with the user, the identity provider, and the relying party. The user selects a desired level from the presented levels, and forwards the issued authentication token for satisfying the security level. Depending on the relying party's policy, where the user can be issued is determined dynamically.

After verified in the relying party of low LoA, the user may want to access the relying party of higher LoA. In this case, the user has to proceed with the negotiation process again because the existing LoA is not valid for the access. Conversely, to prevent this troublesome process, the user can negotiate with higher LoA at first and deserve a service without additional negotiation process.

- Authentication technologies; Authentication technologies are optionally applied to satisfy the level of the relying party. It also means that the user logs in the identity provider with the following authentication methods, as well as manages the authentication information.

C. Architecture

The authentication framework presented in this paper aims to configure the dynamic CoT regardless of ID management technology. Existing CoT is based on the trust relationship, and uses the same ID management scheme. Also the authentication levels are dependent on one or two mechanisms defined on the identity provider on the CoT. If the proposed authentication framework is applied, however, a service provider is able to trust an identity provider dynamically without having to a specific authentication protocol or authentication mechanism. The user just issues an authentication token from the trust-able identity provider and passes to the service provider. In case of

multi-factor authentication, the user does not need to sign up for the identity provider which supports all of the following authentication methods. Among the identity providers which the service provider trusts, the user chooses the identity provider to get each authentication token.

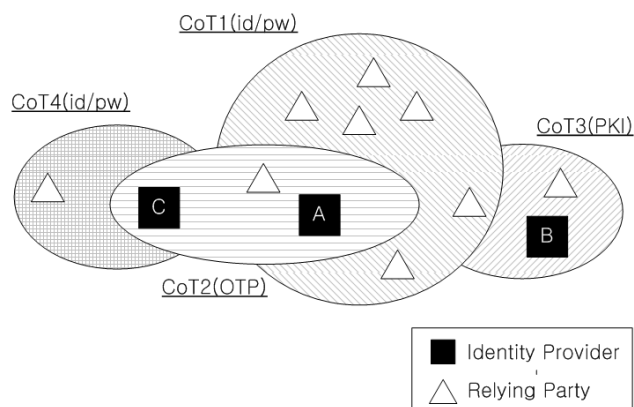


Figure 3. Virtual service environment for the proposed authentication framework

Figure 3 shows the virtual service environment. Various CoTs in the figure mean that it is trusting environment go beyond the kind of ID management technology. For example, various ID management technologies can be used in the CoT1. However every entity in the CoT1 trusts the identity provider 'A'. The identity provider 'A' supports the ID management technology which is used by the relying parties in the CoT1. When the relying party requires an authentication through their own ID management technology, the identity provider 'A' is able to handle the request. The identity provider 'A' returns the id/pw-type token with the corresponding ID management protocol.

If the relying party requires the same level of authentication technology, the user can use a preferred identity provider. It is similar to the OpenID and the CardSpace, but it does not dependent on a range of ID management technologies. For example, if the relying party requires OTP authentication token, the user can select the identity provider 'A' in the CoT2 or the identity provider 'C' in the CoT4. If the user has an account on the identity provider 'C' in the CoT4, the user receives an token after authenticating the identity provider 'C'. In other case, the relying party want an OTP token, but the relying party may specify a list of identity providers or a specific identity provider. It is similar to the federated approach, but the proposed scheme can expand the trust range at easy. And it does not depend on the ID management technology.

For multi-factor authentication, an existing identity provider has to provide all the necessary authentication technology. In addition, multi-factor authentication is optional in the identity provider and relying party itself can not require the function. It was not existed how to express multi-factor authentication and message structure to receive multiple authentication types at once. However, proposed authentication framework has the structure of the message

format to express a multi-factor authentication. For example, identity provider 'A' located in the CoT1 and CoT2 can provide both the id/pw and OTP as multi-factor. The identity provider 'A' has an own OTP authentication system, so it can verify the presented OTP token. Or the identity provider 'A' can verify the OTP token in the form of TTP(Trusted Third Party).

Not only the case to support multi-factor authentication in an identity provider, but also several identity providers may participate in the creation of a multi-factor token. When the relying party want to serve both id/pw and OTP as multi-factor authentication, the user requests a id/pw token to the identity provider 'A' and an OTP token to the identity provider 'C'. Then the user integrates these received tokens and sends it.

IV. RELATED WORKS

A. Existing authentication frameworks

There already exist the multi-factor authentication frameworks such as the authentication sharing framework (ITU-T, x.sap-3, South Korea) [1], the ID sharing framework such as SAML [14], and the distributed authentication framework (Singapore) [9]. These models provide a service in the form of trusted third party. Therefore, if the additional authentication features are required, these models are able to negotiate through their frameworks.

In case of the authentication sharing framework and the distributed authentication framework, main purpose is to provide the multi-factor authentication service. In case of the identity sharing framework, however, main purpose is to perform the effective ID management. It also performs the multi-factor authentication service in addition. The major difference between the frameworks is that whether the framework vets the user's identity directly, or the framework only verifies the multi-factor authentication. The identity sharing framework is the former, and the authentication sharing framework is an independent framework for the identity verification.

B. SASL

SASL (simple authentication security layer) is an authentication framework for providing authentication and data security services in connection-oriented protocols via replaceable mechanisms. It provides a structured interface between protocols and mechanisms. The resulting framework allows new protocols to reuse existing mechanisms and allows old protocols to make use of new mechanisms. The framework also provides a protocol for securing subsequent protocol exchanges within a data security layer. [24]

Basic SASL protocol begins from the server passes the list of authentication technologies to the client. When the client selects one of the authentication technologies in the list, they perform the authentication process through the selected authentication technology. If the server requests an additional authentication, the server passes the authentication request after the previous authentication process.

The SASL is not associated with the ID management technologies. There only exist how to authenticate with the

authentication mechanism, but it does consider neither how to register and manage the authentication mechanism nor how to combine with the ID management technologies. In the SASL, the negotiation means that the client is able to select an authentication technology among the server list of authentication technologies. Although the authentication technology has different level of security, it is not mentioned in the SASL.

It does not deal with the negotiation by indicating the service level for each authentication technology, either. In case of the multi-factor, the client cannot know how strong level the server requires until the end of the protocol. The client doesn't know what authentication technologies are to be conducted in any order. Because the SASL goes to the next authentication only after the current authentication is verified successfully.

V. CONCLUSIONS AND FUTURE WORKS

The existing ID management frameworks describe abstract and general level for the association with the authentication technology. So they do not present how to request the necessary authentication technology but also how to be provided the authentication token. Even the same authentication technology, there are various levels of security exist such as password strength of id/pw authentication. But these descriptions were out-of scope in the ID management. However, the recent hacking mostly uses the vulnerability from the user terminal not the level of protocol which relates with the ID management. It is still vulnerable to the sophisticated attacks, and limited to provide a reliable authentication in the ID management framework itself. Therefore, to provide a reliable level of authentication, it should consider how to provide more strong authentication in the range of not undermine the convenience to the ID management framework. In addition, it is largely dependent on the authentication methods to maintain the reliable security level (assurance) which the user requires. Therefore the ID management technologies need to consider the integration of related authentication technologies.

In this paper, we present a common authentication framework to integrate the ID management technologies. Proposed authentication framework is able to configure the dynamic CoT for each authentication technology, and provides the user a variety of experience. Regardless with the ID management technologies, the user may receive the valuable services from the trust-less CoT if the user passes the high level of authentication. In other words, the proposed framework combines the dynamic relationship in the Internet while providing the confidence.

Although this paper presents the concept, we need to define the detailed contents mentioned in the paper and implement the proposed framework. At first, we should define the detail items which correspond to each of the layer mentioned in the chapter 3. Authentication protocol, message format, policies, and the operations to manage the ID lifecycle must be defined. In addition, we must define how to

map the LoA and the services. Proposed authentication framework uses the FAME [21], however we have to expand and classify it more effectively for providing the service suitable for the LoA.

ACKNOWLEDGMENT

This work was supported by the IT R&D program of MKE/KIAT[2007-S-601-03, User Control Enhanced Digital Identity Wallet System]

REFERENCES

- [1] Hyung-Jin, Lim and Hee-won, Shim, "X.sap-3, The management framework for OTP-based authentication service", ITU-T SG17/Q7, Feb, 2009.
- [2] Yongjin Lee, Hyung-Woo Lee, Yunsu Chung, and Kiyoun Moon, "X.ott, : Authentication framework with one-time telebiometric template", Feb. 2009.
- [3] ITU-T, X.842, "Information technology - Security techniques - Guidelines for the use and management of trusted third party services", Recommendation X.842, ITU-T, Oct. 2000.
- [4] ITU-T, X.842, "Information technology - Security techniques - Specification of TTP services to support the application of digital signatures", Recommendation X.843, ITU-T, Oct. 2000.
- [5] NIST, "Electronic Authentication Guideline", Recommendations of the National Institute of Standards and Technology, America Feb. 2008.
- [6] "Evidence of Identity Standard", Department of Internal Affairs, New Zealand, Jun. 2006.
- [7] Australian Government Information Management Office, "National e-Authentication Framework", Jan. 2009
- [8] e-Government Strategy Framework Policy and Guidelines, "Assurance", Version 2.0, Sep.
- [9] NAF Security Guidance For E-Government, "National Authentication Framework Call-For-Collaboration", Oct. 2008.
- [10] Liberty Alliance Project, "Identity Assurance Framework - Service Assessment Criteria", Feb. 2004.
- [11] Hiltgen, A. Kramp, T. and Weigold, T, "Secure Internet banking authentication", Security & Privacy, IEEE, Apr. 2006.
- [12] Wayman, J.L, "Biometrics in Identity Management Systems", Security & Privacy, IEEE, Apr. 2008.
- [13] R. Oppinger, "Microsoft .net passport: A security analysis", Computer, 36(7):29-35, 2003
- [14] N. Ragouzis et al., Security Assertion Markup Language (SAML) V2.0 Technical Overview". OASIS, Feb. 2007
- [15] Marc Goodner and Anthony Nadalin, "Web Services Federation Language (WS-Federation) V1.2", OASIS, Mar. 2009
- [16] Organization for the Advancement of Structured Information Standards (OASIS), <http://www.oasisopen.org/home/index.php>
- [17] David Chappel. "Introducing Windows CardSpace", <http://msdn.microsoft.com/library/enus/dnlong/html/IntroInfoCard.asp>, Apr. 2006.
- [18] David Recordon and Drummond Reed, "OpenID 2.0: a platform for user-centric identity management", Proceedings of the second ACM workshop on Digital identity management, Nov. 2006
- [19] Russ Cutler, "Liberty Identity Assurance Framework V1.1", Liberty Alliance, 2007
- [20] Liberty Alliance, "Identity Governance Framework V1.0", Liberty Alliance, 2008
- [21] A Nenadic, N. Zhan, J. Chin, and C. Goble, "FAME: Adding Multi-Level Authentication to Shibboleth", '06. Second IEEE International Conference on e-Science and Grid Computing, Dec. 2006
- [22] Philipp Guhring, "Concepts against Man-in-the-Browser Attacks", <http://www2.futureware.at/svn/sourcerer/CACert/SecureClient.pdf>, 2006
- [23] Myers, J, "Simple Authentication and Security Layer (SASL), IETF, 1997
- [24] A. Melnikov and K. Zeilenga, "Simple Authentication and Security Layer (SASL), IETF 4422, 2006