A model for Interoperability among Authentication Systems

AHMED TALLAT  HIROSHI YASUDA

Abstract—conventionally, service providers have to manage their own authentication systems individually and independently without interoperation among them. Lack of the interoperability causes certain serious problems. In this paper, we clarify the requirements for the interoperability, and propose a model, where three independent players, that is, service provider, identity provider and authentication agent, cooperate and communicate with one another.

Keywords: authentication; interoperability; identity provider; password

I. INTRODUCTION

Authentication is a mandatory building block for security of the society. Currently, public service providers such as governments, banks, service providers on the web and so forth provide authentication functionality individually and independently. This indeed causes multiple serious problems, and establishing interoperability among multiple authentication systems could be a solution to the problems. First, from the providers’ point of view, individual investment in authentication systems would be avoidable costs if the interoperability were provided. From the customers’ point of view, without interoperability, they are required to register their identities per services, and the risk of leakage of the identities multiplies as the number of services increases.

SAML [2] is a specification of internet protocols to realize the functionality of single-sign-on. It provides some extents of the required interoperability, but is still insufficient. In fact, SAML require certain pre-trust relation among service providers and identity providers, and such relation cannot be always assumed in the open environment where entities do not know each other beforehand.

BioAPI [1] is another attempt to realize interoperability among authentication systems based on biometrics, in which applications are for access control whereas biometric devices are for both registration and authentication of users. However, in reality, registration and authentication could be performed by different entities. For example, in the case of ATM, banks register customers’ identity information in its database and an ATM authenticates the customers.

In this paper, we clarify the requirements for the interoperability, and propose a model, where three independent players, that is, service provider, identity provider and authentication agent, cooperate and communicate with one another.

II. INTEROPERABILITY

A. Players

By interoperability of authentication, we mean that service providers (SPs) take advantage of results of authentication procedures performed by identity providers (IdPs). An IdP retains identity information of users, and performs authentication procedures on behalf of SPs. On the other hand, an SP owns service resources, and provides users with conditional access to the resources. In the reality, most of the existing SPs play the role of IdP by themselves, and run their own authentication systems only for their use. Even worse, no interoperability among these authentication systems is provided.

In order to solve the problems caused by lack of the interoperability, including those stated in Section I, we should consider a model of the interoperability assuming that SPs and IdPs are independent entities that cooperate and communicate with each other. Furthermore, in addition to SPs and IdPs, we introduce the third independent player, namely authentication agents (AAs). An AA is an entity that provides interfaces for authentication to users. An existing example of AAs is the companies that operate ATM placed in convenience stores in Japan. Such companies have contracts with multiple banks, and customers of the banks can deposit and withdraw money using the same ATMs.

B. Advantages of Interoperability

Interoperability by the aforementioned model provides the following advantages.

1) Improvement of Security for Identity Information

The user can have his identity information registered in the most trustworthy IdP, instead of putting his identity information in multiple SPs. This reduces the possibility of information leakage to unauthorized third parties.

2) Reduction of Users’ Costs

There are three types of users’ costs: registration costs, authentication costs, and management costs. However, the authentication platform can reduce the registration costs by managing identity information in one place [9]. It is also possible to reduce the authentication costs by achieving a Single-Sign On [2] environment where it is only one time that users need to be authenticated by an IdP. It also can reduce management costs by lessening identity information for authentication.

3) Reduction of Service Providers’ Costs
Because IdPs and AAs cooperatively perform authentication on behalf of SPs, SPs do not have to own their authentication systems, and do not owe investment to construct and expense to maintain authentication systems. Furthermore, SPs are released from the burden to keep customers identification information secure [8][9].

C. Important Functionality for Interoperability

A platform to realize the interoperability must support the following functionality.

1) Common Measures for Assessing Security Levels

Although SPs have no control over authentication processes, they must know the security levels of authentication performed by IdPs and AAs. For SPs to evaluate the security levels of multiple IdPs and AAs, common measures of security levels should be determined and publicized. Therefore, the measures must cover at least the following factors of authentication.

- Registration procedures (see RFC 3647 [5], for example)
- Authentication technology (e.g. PKI, Biometrics, Password)
- Security of stored identity information (e.g. Tamper-resistant module, firewall)
- Auditing procedures (see RFC 3647 [5], for example)

2) Trust among players

From the SP’s point of view, all of IdPs and AAs are not necessarily trustworthy. In the open environment, however, an SP is likely to receive information informing authentication results by those IdPs and AAs that was unknown to the SP. Thus, the SP has to not only verify the alleged security levels of the received information but also determine whether or not their claims are trustworthy (e.g. cross recognition [6]).

III. Our Model for Interoperability

This section is devoted to a brief description of the interoperability model that we propose in this paper. This model defines three important phases named Registration Phase, Authentication Phase, and Entitlement Phase (Figure 1).

A. Registration Phase

In this phase, the user (Claimant) registers his/her identity to an IdP that he/she voluntarily selects. The IdP verifies that his/her claimed identity is correct according to its registration policies. As a result of the registration procedures, the Claimant acquires authorized token and the IdP does reference. Examples of the pair (token, reference) are (private key, public key), (token device such as SecureID, account on server), (finger print, template) and so force.

B. Authentication Phase

In Authentication Phase, the Claimant accesses interfaces provided by AAs to prove his/her identity. The Claimant generates identity proof from his/her token, and sends it to the AAs. The proof can be a password, a digital signature, an output of the token device, a scanned image of the registered finger prints and so forth. On receipt of the proof, the AAs either verify it based on reference that the AAs have received from the IdPs or transfer it to the IdPs, who verify it. The result of the verification is included data named endorsement and issued to the Claimant.

In addition to the verification result, the endorsement includes information regarding the security levels of the authentication event described according to the common measures (2.C.1), and also is signed by the AA and/or the IdP involved in the event. To verify the signature, certificate of the AA and/or IdP is accompanied by the endorsement. The certificate is associated with the policies of its issuer, and the policy describes trustworthiness of the AA and/or IdP.

C. Entitlement Phase

In Entitlement Phase, the Claimant presents the endorsement and the certificate that he/she has received in Authentication Phase to SPs, who at least verify: the authentication procedure was completed successful; the alleged security level of the authentication supports the requirements of the SPs; the involved AA and/or IdP are trustworthy; the information included in the endorsement and the certificate is not subject to tampering; and the endorsement is fresh.

IV. Implementation and Future Work

We have made a list of detailed requirements for the data to be generated and exchanged among the players, that is, token, reference, endorsement and certificate. As a next step, we have started the task to define an XML schema to encode the data. Finally, we will develop prototypes of the SP, IdP and AA systems that cooperate with each other based on the XML-encoded data.