Poster: Multi-Sign-on; Authentication collecter

Takashi Ishizuka
Kanagawa Institute of Technology

Hajime Iwata
Kanagawa Institute of Technology

Manabu Okamoto
Kanagawa Institute of Technology
Shimo-ogino 1030 Atsugi-shi
Kanagawa, Japan

Abstract— **Strong security is required now. To authenticate users more secure we use not only passwords but also biometric identification, IC card and PKI certification. Especially strong authentication is necessary for the site handling money or personal information. However a burden is big for the sites using strong security. In this paper Service Provider (SP) can use plural Identity Provider (IdP) for strong authentication and need no functions of authentication on SP itself. A user can select IdPs as he like it. Each IdP provides authentication score to SP through a user and user needs to get score beyond the value SP decided. We utilize Single Sign-on protocols for exchanging authentication score between servers.**

Keywords—Authentication , Two-Factor Authentication , Single sign-on

I. Introduction

Strong security is needed. Now almost all Service Providers (SP) such as SNS, Web mail or E-commercial use password for authentication. However SPs handling money or personal information such as e-bank need strong security. They use two-factors authentication [1]. E-bank SP distributes one time password token machine for users and when a user login the SP he inputs one time password on the display on that machine.

SPs that do strong authentication have to bear big cost for strong security. It gets great cost for the purchase and the distribution of devices of bio-metrics or one time password token. Small SPs cannot do it. And user who use plural SPs have to get plural token machine. It is also a burden for users.

In this paper we propose multi-sign on using multi-IdPs. It is a kind of multi-factor authentication. SP need no authentication devices and functions and SPs can use plural IdPs jointly. Users can select IdP freely. Each IdP has his "authentication score" depending on his authentication strength. A user needs to get score beyond the value SP decided.

II. Relyaed Work : Single Sign On

We are going to use Single sign-on (SSO) protocols for exchanging authentication score between servers. SSO is a mechanism whereby a single action of user authentication enables a user to access multiple web services without needing to enter multiple sets of credentials. One of them, OpenID [2] is an open standard. When a user uses a service provider (called Relying Party (RP) in the OpenID glossary), RP redirects the user to IdP (OpenID provider (OP)) and OP authenticates the user and brings him back to OP with an authentication response. OP then confirms the response and authenticates the user. Figure 1 shows basic sequence for authentication.

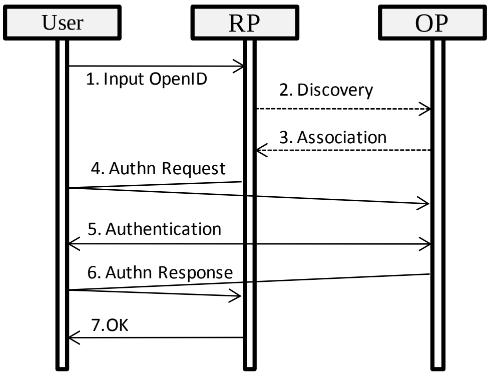


Figure 1. OpenID sequence.

Basically SSO is intended that plural SPs are available by receiving one certification from one IdP. But we are going to use it for multi-sign on. In other word our proposal is that one SP is available by receiving plural certifications from plural IdPs.

In our proposal a user repeat authentication between SP and IdPs and get response including "authentication score" and if total of score is beyond the value SP decided a user can be authenticated on SP.

III. Proposed Method

In this paper we propose multi-sign-on using plural IdPs on SSO protocols. It is useful for strong security. IdP can set authentication strength appropriate to the contents. We call it "authentication score". SP also can set total score necessary for login.

We assume that a user have accounts of plural IdPs and SP and can use them anytime. Each IdP have each authentication method for user authentication. Some IdP may use ID/password and some IdP may use bio-metrics and some IdP use IC-Card. These IdPs have each "authentication score" appropriate to the strength of authentication method. These scores is decides with the agreement of all IdPs. For example ID/password is "10" score and bi-metrics is "30" and IC-Card is "50" score. This score means level of assurance and can refer to NIST. But we can set it in greater detail than NIST.

SP is a site which a user want to use. We assume that SP and IdPs trust each other and access any time each others.

And we assume that we use Single-Sing on protocol for our proposed method such as OpenID. In this paper we assume that we use OpenID.

Figure 2 shows sequence of our proposed method.

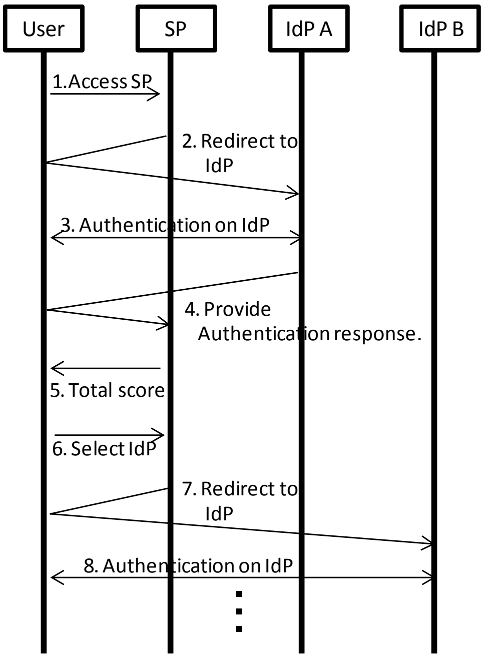


Figure 2. Sequence of proposed method.

1. A user accesses the SP that he want to use. He knows score that he need to login.
2. A user move to an IdP he select. A user can select IdP freely. (Actually he push the IdP button (icon) in figure 4 and he is transferred redirect to the IdP.)
3. A user is authenticated by the IdP. IdP provides autentication method based on its policy.
4. IdP provides certification of authentication with “authentication score” for SP. SP receive the certification and check it and add the score to the total.
5. A user repeat 3 and 4 until he get socre more than SP need. Actually SP is acted as “Authentication Collector” such as Figure 3. If total score is beyond the value SP need then a user can login the SP. A user can know his score on browser such as Figure 4.

Of course certification from IdP to SP include sign of IdP. Any other security is also kept by single sing on protocol.

We can also use single sing on protocol for exchange authentication score in 4. Single sing on protocol include attribute exchange. OpenID has OpenID AX[3]. Especially OpenID Connect [4] can use OAuth at the same time and use both identity token and access token for exchanging attributes. To make it simple we denote one arrow in 4 but actually we need some sequences between IdP and SP for exchanging tokens and some attributes includes “authentication score”. SP can get “authentication context” from each IdP in attribute exchange. “Authentication context” tells SP how to authenticate the user on the IdP or “authentication score” itself.

In our simplest implementation environment, we use OpenID sReg and input “authentication score” in “postcode” parameter and exchange it between IdP and SP.

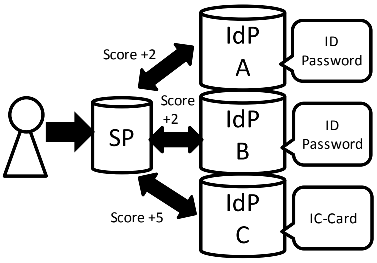
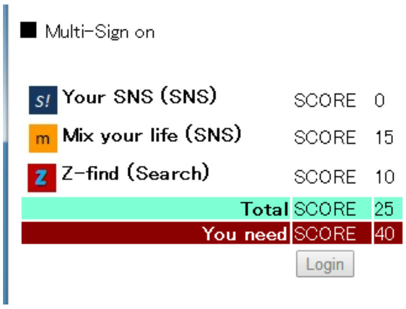


Figure 3. Authentication Collector.



■ Multi-Sign on

S! Your SNS (SNS)	SCORE	0
m Mix your life (SNS)	SCORE	15
Z Z-find (Search)	SCORE	10
Total	SCORE	25
You need	SCORE	40

Figure 4. Total score on browser.

IV. Advantages

In this section, we describe advantages of our method.

Usability: A user need to be authenticated plural times by plural IdPs. When plural method is needed such as password, bio-metrics and IC-Card , a user have to have all devices for these method. But we can unify IdPs freely. A user needs not to have plural onetime password token.

Efficiency: SP need no functions and devices for multi-sign-on. IdP can provide his authentication certification for plural SPs. Users who wants to use SP need to access the IdP for authentication and the IdP may get big number of access and the IdP may be able to earn advertisements. And plural SPs can share the same IdP authentication method and it is very effective about a development cost.

Security: SSO sequence that we use for exchanging authentication response and authentication score in our method is exactly same as standard method and then security of protocol is same as standards.

V. Conclusion

In this paper, we proposed multi-sign-on using plural IdPs which have original authentication method and provide authentication certification for SP including “authentication score”.

References

[1] “The Case for Mobile Two-Factor Authentication”, DeFigueiredo, Dimitri, IEEE Security and Privacy, vol.9 No.5, pp.81-85,2011.

[2] OpenID, http://openid.net/foundation/.

[3] OpenID AX, http://openid.net/specs/openid-attribute-exchange-1_0.html

[4] OpenID Connect, http://openid.net/connect/.