Liberty IdP Selector MRD - Marketing Requirements Document for IdP Selector

Version: **1.0**

Filename: liberty-idp-selector-mrd-v1.0.doc

Editors:

Philippe Clement, Orange-France Télécom

Contributors:

Shin Adachi (NTT)
Fulup Ar Foll (SUN)
Joni Brennan, IEEE-ISTO
Ingo Friese (Deutsche Telekom)
Joao Girao (NEC)
Britta Glade, IEEE-ISTO
Gael Gourmelen (Orange-France Télécom)
Jonas Hogberg (Ericsson)
Mikko Laukkanen (Telia Sonera)
Paavo Lambropoulos (Telia Sonera)
Rob Lockhart, IEEE-ISTO
Søren Peter Nielsen (Danish Government IT and Telecom Agency)
Ken Salzberg (Intel)
Paul Simons (Nortel)
Sreeram Thirukkonda (Fidelity Investments)
Colin Wallis (New Zealand Government Technology Services)

Abstract:

This document aims to precisely describe requirements and use cases in which Identity Providers affiliated with users are efficiently presented to the user, with an IdP Selector Agent or not.

This Market Requirements Document (MRD) has been developed by the IdP Selector subteam of Liberty Alliance to capture the business requirements for IdP Selection. Liberty Alliance is making this MRD publicly available to the industry at large for review and consideration. This publication does not constitute a commitment by Liberty Alliance, explicit or implied, to develop technical specifications in full compliance with the requirements herein, now or in the future.

Notice

Liberty Alliance Project
Licensing Administrator
c/o IEEE-ISTO
445 Hoes Lane
Piscataway, NJ 08855-1331, USA

112 **Table of Contents**

113

1 Introduction

The authentication of a Principal by a Service Provider (SP) follows a chronology relying on three intangible main steps:

1. Selection of the IdP

2. Authentication of the Principal

3. Access of the Principal to the SP

1.1 Selection of the IdP

This first step leads to a user friendly determination of the best IdP to use to authenticate the Principal. It can be done:

a) directly on the SP User Interface (UI) or

b) with the help of an IdP Selector Agent (ISA).

1.2 Authentication of the Principal

When the authentication is done directly on the SP User Interface (UI), the problem is solved by http redirection. When the authentication is done with the help of an IdP Selector Agent (ISA), the behavior of the ISA must follow generic rules to communicate with the SP and the IdP.

1.3 Access of the Principal to the SP

This third step is triggered when authentication is started from the SP.

2 Context

When a user wants to access a personalized service at an SP, he must first authenticate. The number of Identity Providers is growing, and the choice of one of them can be complicated for a user.

A few initiatives, including OpenID v2, JanRain, the common domain cookie (Liberty and SAML), the LECP (Liberty) or ECP (SAML) and identity selectors (CardSpace, Higgins, JanRain, etc.) , try to resolve the choice of the Identity Provider by providing the Service Provider a means to determine the IdP that can authenticate the user.

Some of these initiatives (e.g., identity selectors) don't take into consideration specific authentication means (implicit authentication, strong authentication, etc.).

See [LibertyGlossary] for definitions of the acronyms used in this document that are not defined in Section 10.

3 Use Cases

3.1 Assisted Discovery of Identity Provider Based on Preferred IdP (Principal and SP Negotiate Which IdP to Use)

3.1.1 Main Description

The goal of this UC is to guide the Principal through the authentication phase when the Principal has described his preferred IdPs.

3.1.2 Business Justification

SP ability to support multiple IdPs with priority or preferences set by Principal.
IdP ability to extend its exposure toward more SPs.
Principal ability to define a preferred IdP for his convenience.

3.1.3 Details

Title/ID	Assisted Discovery of Identity Provider Based on Preferred IdP
Pre conditions	1. SP can delegate the authentication to many IdPs, and among them IdP A and IdP B. 2. Principal has an identity at IdP A and IdP B. 3. SP is able to detect IdP A as the preferred IdP for Principal. 4. SP does error handling.
Constituents	Principal, IdP A, IdP B, SP
Use case	1. Principal is browsing SP and want to access a personalized zone. 2. SP detects that IdP A is the preferred IdP for Principal, and that IdP A is in its list of potential IdPs. 3. SP requests IdP A to authenticate Principal. 4. IdP A authenticates Principal and returns an assertion to SP.
Alternate course of action 1	This alternate course of action begins at step 4 of the main Use Case. 4. Authentication is not possible with IdP A. 5. IdP A returns a failed message to SP. 6. SP does not authorize the Principal to access the requested personalized zone.
Post condition 1	Principal is not authenticated and his claim to access is rejected.
Alternate course of action 2	This alternate course of action begins at step 6 of alternate course of action 1. 4. SP detects that IdP B is able to authenticate Principal. 5. SP requests IdP B to authenticate Principal. 6. IdP B authenticates Principal and returns an assertion to SP.
Post condition 2	Principal is authenticated at IdP B and enters his personalized zone at

	SP.

3.2 Assisted Discovery of Identity Provider in Case of Non-Existence of Preferred IdP (Principal and SP Negotiate Which IdP to Use)

3.2.1 Main Description

The goal of this UC is to guide the Principal through the authentication phase when the Principal has NOT described his preferred IdPs. In this case, the SP sets its own priorities for the IdP selection, and can filter potential IdPs, or ask the Principal directly for an IdP name.

3.2.2 Business Justification

SP ability to present or order potential IdPs according to its business priorities.

3.2.3 Details

Title/ID	Assisted Discovery of Identity Provider in Case of Non-Existence of Preferred IdP
Pre conditions	1. SP can delegate the authentication to many IdPs, and among them IdP A, B… Z). 2. Principal has an identity at IdP A and IdP B. 3. SP does error handling.
Constituents	Principal, IdP A, B…Z , SP
Use case	1. Principal is browsing SP and want to access a personalized zone. 2. SP shows a list of all the potential IdPs (A, B…Z) accepted by SP and asks Principal to choose. 3. Principal chooses IdP A. 4. SP requests IdP A to authenticate Principal. 5. IdP A authenticates Principal and returns an assertion to SP.
post condition	Principal is authenticated with IdP A and can access his personalized zone.
Alternate course of action 1	This alternate course of action begins at step 2. 2. SP shows Principal a selected sub-list of IdPs (e.g. most relevant based on Principal IP@...). 3. Principal chooses IdP A. 4. SP requests IdP A to authenticate Principal. 5. IdP A authenticates Principal and returns an assertion to SP.
Post condition 1	Principal is authenticated with IdP A and can access his personalized zone.
Alternate course of action 2	This Alternate course of action begins at step 2 of the main Use Case. 2. SP shows an additional text field/search box where Principal can type the name of IdP.

	3. Principal enters "idpA.com". 4. SP uses a standardized mechanism to identify the IdP based on the text entry (e.g. IdP A). 5. SP requests IdP A to authenticate Principal. 6. IdP A authenticates Principal and returns an assertion to SP.
Post condition 2	Principal is authenticated with IdP A and can access his personalized zone.

3.3 Usage of Network-Authentication (Principal and SP Negotiate Which IdP to Use)

3.3.1 Main Description

The goal of this UC is to allow a Principal to seamlessly access a personalized zone in one SP without any explicit additional authentication by using the authentication given by the network provider.

3.3.2 Business Justification

Ability for Principal to request the use of a network authentication to access a personalized zone at an SP.

Ability for a network provider to extend its exposure toward more SPs.

3.3.3 Details

Title/ID	Usage of Network Authentication (e.g., GBA, reverse DNS resolution)
Pre conditions	1. Principal has an identity at IdP A, IdP B. 2. IdP A does network authentication. 3. SP has a relationship with IdP A and IdP B. 4. Principal has indicated to SP beforehand to use his network authentication for accessing the personal zone at SP. 5. Principal uses the network (IdP A) to access SP.
Constituents	Principal, IdP A (network provider), IdP B, SP
Use case	1. Principal is browsing SP and want to access a personalized zone. 2. SP detects that the Principal has indicated network AuthN as the preferred method to access the personal zone at SP. 3. SP detects that IdP A is doing network authentication. 4. SP requests IdP A to authenticate Principal. 5. IdP A detects that Principal uses its network, or that active authentication session (e.g., GBA) is available. 6. IdP A authenticates Principal and returns an assertion to SP.
Post conditions	Principal is authenticated at IdP A (network provider) and enters his personalized zone at SP.

3.4 Usage of Authentication Context to Discover the IdP (Principal and SP Negotiate Which IdP to Use)

3.4.1 Main Description

The goal of this UC is to allow an SP to specify a given Authentication Context (AC) for the IdP selection.

3.4.2 Business Justification

Ability for SPs to adapt the level of trustability/security to enter a specific zone for Principal by extending the scope of potential IdPs.

Ability for IdP with several ACs to raise its probability to be selected by an SP for the authentication phase.

3.4.3 Details

Title/ID	Usage of Authentication Context (AC) to Discover the IdP
Pre conditions	1. SP can delegate the authentication to many IdPs, among them IdP A and IdP B. 2. Principal has an identity at IdP A and IdP B. 3. IdP A is able to authenticate Principal with AC 1 and AC 2. 4. IdP B is able to authenticate Principal with AC 1.
Constituents	Principal, IdP A, IdP B, SP
Use case	1. Principal is browsing SP and want to access a personalized zone. 2. SP detects that to access this zone, Principal must be authenticated with AC 2. 3. SP detects that IdP A and IdP B can authenticate Principal. 4. SP detects that only IdP A can authenticate Principal with AC 2. 5. SP requests IdP A to authenticate Principal. 6. IdP A authenticates Principal and returns an assertion to SP.
Post conditions	Principal is authenticated at IdP A and enters his personalized zone at SP.

3.5 Usage of Assurance Level to Discover the IdP (Principal and SP Negotiate Which IdP to Use)

3.5.1 Main Description

The goal of this UC is to allow an SP to specify a given Assurance Level (AL) for the IdP selection.

3.5.2 Business Justification

Ability for SPs to adapt the level of trustability/security to enter a specific zone for Principal by extending the scope of potential IdPs.

Ability for IdP with several ALs to raise its probability to be selected by an SP for the authentication phase.

3.5.3 Details

Title/ID	Usage of Assurance Level (AL) to Discover the IdP
Pre conditions	1. SP can delegate the authentication to many IdPs, among them IdP A and IdP B. 2. Principal has an identity at IdP A and IdP B. 3. IdP A is able to authenticate principal with AL 1 and AL 2. 4. IdP B is able to authenticate principal with AL 1.
Constituents	Principal, IdP A, IdP B, SP
Use case	1. Principal is browsing SP and want to access a personalized zone. 2. SP detects that to access this zone, Principal must be authenticated with AL 2. 3. SP detects that IdP A and IdP B can authenticate Principal. 4. SP detects that only IdP A can authenticate Principal with AL 2. 5. SP requests IdP A to authenticate Principal. 6. IdP A authenticates Principal and returns an assertion to SP.
Post conditions	Principal is authenticated at IdP A and enters his personalized zone at SP.

3.6 Usage of Attributes or Claims Validation to Discover the IdP (Principal and SP Negotiate Which IdP to Use)

3.6.1 Main Description

The goal of this UC is to allow an SP to request the selection of the IdP from its ability to deliver an attribute or validate a claim.

3.6.2 Business Justification

Ability for SPs to define more precisely what IdP will be chosen to authenticate a Principal entering a specific zone at an SP in which some information will be necessary.

Ability for an IdP with several attributes or the ability to validate claims to raise its probability to be selected by an SP for the authentication phase.

268 _

269 3.6.3 Details

Title/ID	Usage of Attributes or Claims Validation to Discover the IdP
Pre conditions	1. SP can delegate the authentication to many IdPs, and among them IdP A and IdP B. 2. Principal has an identity at IdP A and IdP B. 3. IdP B can validate attributes or claims for Principals.
Constituents	Principal, IdP A, IdP B, SP
Use case	1. Principal is browsing SP and want to access a personalized zone. 2. SP detects that to access this zone, one or more attributes or claims will be necessary. 3. SP detects that IdP B is able to validate these particular attributes or claims of the user. 4. SP requests IdP B to authenticate Principal. 5. IdP B authenticates Principal. 6. SP requests that IdP B validate the attributes or claims. 7. IdP B returns an assertion to SP according to the validation of the attributes or claims.
Post conditions	Principal is authenticated at IdP B and enters his personalized zone at SP.

270 3.7 Usage of an IdP Selector Agent (Principal and SP 271 Negotiate Which IdP to Use)

272 3.7.1 Main Description

273 The goal of this UC is to describe the necessary behavior of an IdP Selector Agent (ISA),
274 running on an SP's site, in the network or on a Principal's device.

275 3.7.2 Business Justification

276 Ability for SP to determine the applicable IdPs to a Principal for selection through ISA.

277 Ability to allow IdPs with few customers to be chosen directly by Principal through ISA.

278 Details

Title/ID	Usage of an IdP Selector Agent (ISA)
Pre conditions	1. SP can delegate the authentication to many IdPs, and among them IdP A and IdP B. 2. Principal has an identity at IdP A and IdP B. 3. SP trusts ISA to display the recommended IdP list as is.
Constituents	Principal, IdP A, IdP B, SP, ISA

Use case	1. Principal is browsing SP and want to access a personalized zone. 2. SP detects that IdP A and IdP B can authenticate Principal. 3. SP triggers ISA with IdP A and IdP B as inputs. 4. ISA prints the list of IdP A and IdP B 5. ISA asks Principal to choose an IdP between IdP A and IdP B. 6. Principal chooses IdP B. 7. ISA redirects Principal to IdP B for authentication. 8. IdP B authenticates Principal. 9. SP is asserted with the fact that Principal is authenticated at IdP B.
Alternate course of action 1	This action begins at step 3 of the main Use Case. 3. SP requests ISA for the Principal authentication, without mentioning any IdP. 4. ISA shows Principal the whole list of known IdPs. 5. Principal chooses IdP B. 6. ISA redirects Principal to IdP B for authentication. 7. IdP B authenticates Principal. 8. SP is certified with the fact that Principal is authenticated at IdP B.
Post condition 1	Principal is authenticated at IdP B and enters his personalized zone at SP.
Alternate course of action 2	This action begins at step 4 of main Use Case 4. ISA displays an entry field/search box where Principal can enter directly the name of his IdP. 5. Principal types "idpB.com" in the text field. 6. ISA detects that "idpB.com" corresponds to IdP B. 7. ISA redirects Principal to IdP B for authentication. 8. IdP B authenticates Principal. 9. SP is certified with the fact that Principal is authenticated at IdP B.
Post condition 2	Principal is authenticated at IdP B and enters his personalized zone at SP.

3.8 The IdP Takes Control of the ISA User Interface (Principal Authenticates with IdP)

3.8.1 Main Description

The goal of this UC is to allow the IdP to interact with the user during the authentication phase initiated by an ISA.

3.8.2 Business Justification

Ability for IdPs to interact directly with the Principal while maintaining each IdP's specific marketing approach.

3.8.3 Details

Title/ID	The IdP Takes Control of the ISA User Interface
Pre conditions	1. SP can delegate the authentication to IdP A, B, C, D. 2. Principal has an identity at IdP A, B, C. 3. ISA has a reference or pointer to IdP A, B, C, D. 4. ISA controls the UI during the IdP selection phase and relinquishes the authentication phase to IdP through its UI. 5. ISA trusts IdP A, B, C, D. 6. IdP A, B, C, D trusts ISA.
Constituents	Principal, IdP A, B, C, D, SP, ISA
Use case	1. Principal want to access a personalized zone at SP. 2. SP detects that the Principal can be authenticated by IdP A, B, C. 3. SP requests ISA to display IdP A, B, C to Principal. 4. Principal chooses IdP A on ISA user interface. 5. IdP A's authentication interface is displayed. 6. IdP A interacts with (and authenticates) Principal. 7. An authentication assertion is returned to SP.
Post conditions	Principal is authenticated at IdP A and enters his personalized zone at SP.

3.9 The User is Authenticated with an IdP at an SP and Needs to Authenticate with Another IdP Temporarily (Principal Authenticates with IdP)

3.9.1 Main Description

The goal of this UC is to allow the user to authenticate temporarily with another IdP B during an existing session with IdP A, and recover the previous session with IdP A when resuming the session with IdP B.

3.9.2 Business Justification

Ability for an SP to choose specific IdP(s) for subsequent authentication for access to specified content.

Ability for some IdPs to extend their exposure by providing specific authentication means based on the context that transaction requested

3.9.3 Details

Title/ID	The User is Authenticated with an IdP at an SP and Needs to Authenticate with Another IdP Temporarily for a Specific Service
Pre conditions	1. Principal has an identity at IdP A, IdP B and IdP C. 2. Principal is authenticated with IdP A at SP.

	3. SP has commercial agreement with IdP B and IdP C. 4. IdP B and IdP C are accessible from the ISA.
Constituents	Principal, IdP A, IdP B, IdP C, SP, IdP Selector Agent (ISA)
Use case	1. User enters a specific area at SP that needs a subsequent authentication. 2. SP redirects the user to ISA, and requests ISA to display IdP B and IdP C. 3. User chooses IdP B. 4. IdP B's sign-in page is displayed (in its own page or embedded in the ISA page). 5. IdP B authenticates the user. 6. SP receives proof of authentication at IdP B. 7. IdP B session expires.
Post conditions	User continues his previous session with SP, IdP A.

4 Requirements

Req#	UC #	Requirements
1	3.1	Mechanism for an SP to detect what IdPs are able to authenticate Principal
2	3.1	Mechanism for an SP to order the list of IdPs according to the priority set by the Principal for authentication
3	3.1	Mechanism for an SP to have a Principal authenticated by following the IdP in the priority list in case of failure with the current IdP in the priority list
4	3.1	Mechanism for a Principal to define preferred IdPs based on priorities for an SP
5	3.1	Mechanism for a Principal to define preferred IdPs based on priorities for an ISA
6	3.2	Mechanism or capability for an SP to show all (or part of) IdPs available to a Principal
7	3.2	Mechanism or capability for an ISA to show all (or part of) IdPs available to a Principal
8	3.2	Mechanism for SPs to discover how each IDP needs to be displayed to the Principals and/or to be used to facilitate the selection (display of the logos, search text, etc.)
9	3.2	Mechanism for ISAs to discover how each IDP needs to be displayed to the principals and/or to be used to facilitate the selection (display of the logos, search text, etc.)
10	3.3	Mechanism for Principal to specify the IdP and Network Authentication to access an SP
11	3.3	Mechanism for SP to detect that the Principal has indicated a particular IdP and Network Authentication as the preferred method to access to that SP
12	3.4	Mechanism for SPs to discover the AuthN contexts/classes supported by IDPs
13	3.4	Mechanism for ISAs to discover the AuthN contexts/classes supported by IDPs
14	3.4	Mechanism for SP to request an IdP for a particular AuthN context/class to authenticate a Principal
15	3.5	Mechanism for SPs to discover the ALs supported by IdPs
16	3.5	Mechanism for ISAs to discover the ALs supported by IdPs
17	3.5	Mechanism for SPs to request an IdP for a particular AL to authenticate a principal

Req#	UC #	Requirements
18	3.6	Mechanism for SPs to select IdPs based on the profile attributes or claims they can deliver for a Principal
19	3.6	Mechanism for ISAs to select IdPs based on the profile attributes or claims they can deliver for a Principal
20	3.7	Mechanism for the SP to delegate the selection (display, choice, etc.) of the IdP by Principal to an ISA (other entity/actor)
21	3.7	Mechanism for the SP to express some criteria (list of accepted IdPs, AuthN contexts/classes, ALs, profile attributes or claims to validate) to be considered for the selection of the IdP by the IdP Selector Agent
22	3.7	Mechanism for the SP to be asserted in the end which IdP authenticated the principal (after IdP selection inside ISA)
23	3.8	Mechanism for ISA to display the authentication interface produced by the selected IdP
24	3.9	Mechanism for an SP to hold an existing authentication session with IdP X and begin another session temporarily with IdP Y, then resume to previous session
25	3.9	Mechanism for an SP to detect the relevant IdPs to a specific service

303

5 Glossary Terms

5.1 IdP Selector Agent

The IdP Selector Agent is a mechanism helping to manage the authentication phase with a user, many SPs and many IdPs. It filters IdPs to be shown to Principal based upon the criteria given by SP.

5.2 GBA

See 3GPP standards:
http://en.wikipedia.org/wiki/Generic_Bootstrapping_Architecture

6 References

[LibertyGlossary] Hodges, Jeff, eds. "Liberty Technical Glossary," Version v2.0, Liberty Alliance Project (30 July, 2006), *http://www.projectliberty.org/specs*

Open ID Authentication 2.0 Final, (December 5, 2007), *http://openid.net/specs/openid-authentication-2_0.html*

John Hughes, Scott Cantor, Jeff Hodges, Frederick Hirsch, Prateek Mishra, Rob Philpott, and Eve Maler, eds "Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard (15 March 2005), *http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf*