
# Phase 1 - Authentication Sharing Marketing Requirements Document

**Version:1.0**

**NOTE: This document is published for historical interest. Market Requirements Documents were originally not designed for publication outside of the Liberty Alliance membership, and so may not be readily understandable without prior knowledge of the technical terms used by the groups that wrote them. This MRD was developed by the Business Marketing Expert Group (BMEG) and passed on to the Technology Expert Group (TEG) as guiding input to the technical specification development process. As with any development process, changes were made to the list of requirements that the specifications were developed to meet during the course of their development. These changes were agreed to by both BMEG and TEG but were not folded back into this MRD, so there are some discrepancies between the contents of this document and the related technical specifications. Changes to the requirements were made for a number of reasons, both technical and market-related.**

## Notice

This document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby granted to use the document solely for the purpose of implementing the Specification. No rights are granted to prepare derivative works of this Specification. Entities seeking permission to reproduce portions of this document for other uses must contact the Liberty Alliance to determine whether an appropriate license for such use is available.

Implementation of certain elements of this document may require licenses under third party intellectual property rights, including without limitation, patent rights. The Sponsors of and any other contributors to the Specification are not, and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. **This Specification is provided "AS IS", and no participant in the Liberty Alliance makes any warranty of any kind, express or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose.** Implementors of this Specification are advised to review the Liberty Alliance Project's website (http://www.projectliberty.org/) for information concerning any Necessary Claims Disclosure Notices that have been received by the Liberty Alliance Management Board.



Liberty Alliance Project

**Abstract:**

The initial phase of Liberty Alliance deployments will focus on enabling businesses to form partnerships that link identity across service offerings and thus simplify the end-user's experience. By enhancing “affinity” relationships, end-users will be allowed to login at a Service Provider’s (SP's) site and then go to a partnership site without having to reestablish their identity. Similarly, during this phase, a business will be able to deploy a Liberty Alliance-based solution to consolidate identities within their own extended enterprise so that a customer or employee can move seamlessly from one portal to another without having to re-authenticate at every site.

**Filename:** liberty-phase-1-mrd-v1.0.pdf

**Contents**

# 1 Introduction

## 1.1 Purpose of the Liberty Alliance

The Liberty Alliance Project represents a broad spectrum of industries united to drive a new level of trust, commerce, and communications on the Internet.

### 1.1.1 Vision Statement

The members of the Liberty Alliance envision a networked world across which individuals and businesses can engage in virtually any transaction without compromising the privacy and security of vital identity information.

### 1.1.2 Mission Statement

To accomplish its vision, the Liberty Alliance will establish open technical specifications that:

- Support a broad range of identity-based products and services
- Provide businesses with new revenue opportunities that economically leverage their relationships with consumers, employees, and business partners
- Provide consumers with choice, convenience, and control when using the vast majority of devices connected to the Internet

### 1.1.3 Objectives

The Liberty Alliance recognizes that the widespread adoption of open identity standards will occur incrementally. For this reason, the Liberty Alliance will stage the introduction of its specifications in a manner than supports rapid acceptance and deployment.

The key objectives of the Liberty Alliance are:

- Enable businesses to maintain and enhance their customer relationships without undesirable third-party intervention
- Enable consumers to protect the privacy and security of their identity information
- Provide an open single sign-on standard that includes decentralized authentication and authorization from multiple providers
- Create a network identity framework that supports the vast majority of current and emerging network access devices

## 1.2 Why Adopt the Liberty 1.0 Specification?

This section highlights the value proposition and benefits of adopting the Liberty Alliance 1.0 Specifications.

### 1.2.1 Scope of This MRD 1.0 Document

#### 1.2.1.1 In Scope

This document introduces the first phase of developments underway in the Liberty Alliance. It highlights the benefits and opportunities of adopting the first phase specifications to address near-term realizable goals and builds a foundation for future development.

#### 1.2.1.2 Out of Scope

This document does not seek to describe the long-term requirements of the Liberty Alliance specifications. This will be accomplished in a pursuant series of Market Requirement Documents.

### 1.2.2 Objectives of Phase 1

#### 1.2.2.1 Authentication Sharing

The initial phase of Liberty Alliance deployments will focus on enabling businesses to form partnerships that link identity across service offerings, thus simplifying the end-user's experience. By enhancing “affinity” relationships end-users will be allowed to log in at a Service Provider’s site and then go to a partnership site without having to reestablish their identity. Similarly, during this phase a business will be able to deploy a Liberty Alliance-based solution to consolidate identities within their own extended enterprise so that a customer or employee can move seamlessly from one portal to another without having to re-authenticate at every site.

The Liberty Phase 1.0 Specifications will:

- Create an authentication sharing mechanism that is easy to use and will be interoperability with existing identification systems
- Pragmatically extends best-of-breed security to identity
- Use a decentralized approach that will build into a fully federated architecture
- Provides businesses with guidance about how to provide consumers with permission controls for identity sharing
- Be an open specification with:
  - Published technical specifications
  - Incorporation of relevant implementation guidelines
  - Support for multiple platforms and multiple access devices
- Accelerate time to market for identity based services
- Issue a compliance specification

### 1.2.3 Benefits of Phase 1

#### 1.2.3.1 Business: Enable New Business Solutions

| The Business Problem | The Liberty Solution |
|---|---|
| Lack of standards for linking and associating consumers across multiple Service Providers limits the ability of businesses to create integrated and seamless service with their business partners. | Liberty specifications enable Service Providers to link the identity of common customers and offer a rich set of innovative, combined products and services. |
| Corporations today have many incompatible ways to maintain their employees' and customers' identities resulting in data duplication and inconsistencies. | Liberty specifications will enable Service Providers to offer their employees and partners/customers seamless integration of services across today's multiple identities. |
| Product and Service Providers lack identity/authentication standards, which results in expensive and proprietary B2B integration. The cost of delivering the one-off solutions required to deliver cross-name space products and services is prohibitive. | Liberty specifications enable linking of existing name spaces in an open and extensible way. This reduces the high cost of proprietary identity integration solutions and lays the foundation for easy extensibility. |
| There are limited guidelines for presenting notice and gathering consent from consumers using Web-based services, leading to a fragmented and confusing user experience | Liberty will provide guidelines for businesses to create and communicate notice and gather choice from consumers. This will significantly reduce the burden for Service Providers, reassuring and enhancing their customers' experience. |

#### 1.2.3.2 Consumer: Enable Ease of Use

| The Consumer Problem | The Liberty Solution |
|---|---|
| Consumers deal with a fragmented user experience, transitioning from site to site as they communicate and transact on the Internet. Relevant products and services are not conveniently offered, resulting in a poor experience or abandonment. | Liberty enables users to harmonize their fragmented experience by allowing them to express consent for separate product and Service Providers to identify them as shared customers. This enables relevant product and services to be delivered more conveniently and allows consumers to demand and receive a whole new breed of products and services. |
| Consumers today have to remember and maintain tens to hundreds of different IDs, | Liberty will drastically cut down on the number of identities a consumer must |

| | |
|---|---|
| log-in names, passwords, and pin codes on their Web sites of choice. | handle in order to be recognized by sites compliant with Liberty specifications. |
| There are no consistent guidelines for providing consumers with privacy notice and consent, leading to confusion and the potential for abuse. | Liberty will provide Service Providers with guidelines for creating and communicating privacy notice and gathering consent from consumers leading to a more consistent experience for the consumer. |

#### 1.2.3.3 Technology Providers: Increase Adoption

| The Technology Provider Problem | The Liberty Solution |
|---|---|
| There are no standards for Web identity, leading to fragmented and proprietary installations which consequently limits the total demand for identity-based products and services. | Liberty specifications allow technology providers to create value-added products and services, safe in the knowledge that they are interoperable and extensible. |

# 2 Requirements for Phase 1

It should be noted that all requirements included below reflect functionality essential to Phase 1, only. Future phases may elaborate on some of the requirements in this document as needed to support enhanced functionality.

Template for each requirement includes the following detail:

- Main Business Requirement - definition of the requirement
- Requirement ID - reference number in the List of Requirements table
- Use Case Reference - reference number of the applicable use case(s) identified in Section 3
- Definition - detailed definition of the requirement
- As Is - if current technology exists or if there is an existing scenario to be improved upon
- To Be - Change from As Is and description of change (further clarifies definition)
- Benefits - Why and/or how the requirement supports the project objective
- Constraints - Factors that impact the type of solution suitable to meet the requirement
- Business Processes Impacted - What areas of the business will the requirement affect a change
- Constituents - All parties interested in or impacted by the requirement
- Stakeholders - Parties most at risk if requirement is not completed
- Responsibility - Party or parties responsible for implementing requirement

## 2.1 List of Requirements:

| Req# | UC # | Requirement |
|---|---|---|
| 2.2.1 | 3.1.1 | Mechanism for Principal to Link Identity at Identity Provider to Identity at Service Provider |
| 2.2.2 | 3.4.1 | Mechanism for Principal to Disable an Existing Link Between Their Identity at Identity Provider and Their Identity at Service Provider |
| 2.2.2b | 3.4.1 | Mechanism for Identity Providers and Service Providers to Permanently Delete Link When Principal Requests to Unlink Accounts |
| 2.2.3 | 3.2.1 | Mechanism for Identity Providers and Service Provider to Provide Principal with a Link History |
| 2.2.4 | 3.4.1 | Mechanism to Allow Identity Providers and Service Providers to Provide Notice of Principal's Action to Terminate Link to all Affected Identity Providers and Service Providers and Receive Confirmation of Link Termination |
| 2.2.5 | 3.4.2 | Guideline for Identity Providers and Service Providers to Notify Principals of Any Links Disabled or Deleted by Identity Providers and Service Providers |
| 2.2.5b | 3.4.2 | Mechanism for Identity Provider and Service Provider to Disable All the Links Between Identity Providers and Service Providers |
| 2.2.6 | 3.4.2 | Guidelines for Identity Providers and Service Providers to Track Principals That Have Existing Linked Identities for Purposes of Notification of Termination |
| 2.2.7 | 3.1.1 | Guideline for Identity Providers and Service Provider to Require a Minimum Data Confidentiality Requirement at the Principal Level |
| 2.2.8 | 3.1.1 | Mechanism for a Identity Provider and Service Provider to Maintain Data Confidentiality with Other Identity Providers and Service Providers Acceptable to Industry Security Standards |
| 2.2.9 | 3.1.1 | Guideline to Maintain Session Integrity |
| 2.2.10 | All | Mechanism to Support Variety of Maximum Possible Internet Access Methods (at minimum including desktop PCs, mobile phones, and PDAs with browsers) |
| 2.2.10b | All | Mechanism to Support Different Authentication Methods for Credentials |
| 2.2.10c | All | Mechanism to Support Different Authentication Strengths for Credentials |
| 2.2.11 | All | Mechanism to Provide Identity-Linking Solution without Mandating Client-Side Changes |

| Req# | UC # | Requirement |
|---|---|---|
| 2.2.12 | All | Mechanism to Ensure Identity-Linking Is Easily Deployable on Existing Network Infrastructures (IP and non-IP based) |
| 2.2.13 | All | Mechanism to Support Internationalization Standards for All Identity-Linking Requirements (thus operational across language and cultural domains) |
| 2.2.14 | 3.3.1 | Mechanism to Allow Identity Providers to Prove Authentication Method to Service Providers |
| 2.2.15 | 3.3.1 | Mechanism to Allow Identity Providers and Service Providers to Communicate Details About the Method(s) That Were Used to Validate the Principal |
| 2.2.16 | 3.3.2 | Mechanism to Allow Service Providers to Recognize Principal's Identity Provider Authentication Status and Send Principal to Identity Provider to Login when Appropriate |
| 2.2.17 | 3.1.1 | Mechanism for Identity Providers and Service Providers to Identify and Authenticate Other Identity Providers and Service Providers |
| 2.2.18 | 3.1.1 | Guidelines for Identity Providers and Service Providers to Provide Notice to Principals About Linking Opportunities and Allowing Identity Providers and Service Providers to Capture Consent for Each Linking Activity |
| 2.2.19 | 3.5.1 | Mechanism to Allow Principals to Explicitly Log Out of Services (including all linked services) |
| 2.2.20 | 3.5.2 | Mechanism to Ensure Inactive Principal's Session Is Not Misappropriated |
| 2.2.21 | All | Mechanism for Ensuring Integrity of Data Amongst Identity Providers and Service Providers |
| 2.2.22 | 3.3.1 | Mechanism for Service Provider to Request Re-Authentication of a Principal Specifying the Current or an Alternative Method of Re-Authentication that Is Required |

## 2.2 Requirement Details

| | |
|---|---|
| **Main Business Requirements:** | Mechanism for Principal to link identity at Identity Provider to identity at Service Provider |
| Requirement ID: | 2.2.1 |
| Use Case Reference: | 3.1.1 |
| Definition: | Principal to be able to link an existing identity at an Identity Provider to an identity at a Service Provider |
| As Is: | Principal authenticates at Identity Provider and Service Provider separately. |
| To Be: | Principal authenticates at Identity Provider and upon navigation to Service Provider, a linking relationship is recognized resulting in the Principal being authenticated at the Service Provider without additional login. |
| Benefits: | Saves Principal an additional login. Makes navigation and access to services easier and faster for customers. Allows the Identity Provider and the Service Provider to enhance their respective service offerings to the Principal. |
| Constraints: | • Principal must have existing relationship with Identity Providers and Service Providers to be linked before linking can occur<br>• Principal must initiate link (rather than linking being assumed for Principal)<br>• Identity Provider and Service Provider must provider notice of the linking opportunity and capture explicit consent before initiating link<br>• Identity Provider and Service Provider must not transfer identity information about Principal to another Service Provider without providing adequate notice and gaining Principal's explicit consent to do so<br>• There needs to be a business agreement between Identity Provider and Service Provider that Identity Provider has responsibility to provide delegated authentication for Service Provider |
| Business Processes Impacted: | Identity Provider's login, Service Provider's login |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Identity Providers, Service Providers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | **Mechanism for Principal to disable an existing link between their identity at Identity Provider and their identity at Service Provider** |
|---|---|
| Requirement ID: | 2.2.2 |
| Use Case Reference: | 3.4.1 |
| Definition: | Principal with an existing link between an identity at Identity Provider and an identity at Service Provider needs to have the option at both Identity Provider's and Service Provider's sites to disable that link |
| As Is: | Does not exist |
| To Be: | Principal logs on with existing linked identity at Identity Provider or Service Provider. Principal decides they no longer desire their identity to be linked. Identity Provider and Service Provider give the Principal a mechanism to unlink identities. Identity Provider and Service Provider disables link whilst maintaining its history. |
| Benefits: | Increases Principal's identity management control |
| Constraints: | • Identity Providers and Service Providers need to be aware of the discontinued link for subsequent logins and must change its status in the history of Principal's links<br>• Principal needs to have unlink option available at Identity Providers and Service Providers<br>• Identity Providers and Service Providers must comply with all applicable privacy regulations<br>• Deletion versus disablement of links is an option to be used at discretion of Service Provider; Service Provider must utilize at least one of the two options |
| Business Processes Impacted: | Identity Provider's Login, Service Provider Login<br>Identity Provider's Web pages, Service Provider Web pages (content) |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Customers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Mechanism for Identity Providers and Service Providers to permanently delete link when Principal requests to unlink accounts |
|---|---|
| Requirement ID: | 2.2.2b |
| Use Case Reference: | 3.4.1 |
| Definition: | Principal that has an existing link between an identity at Identity Provider and an identity at Service Provider needs to have the option at both Identity Provider's and Service Provider's site to permanently delete that link |
| As Is: | Does not exist |
| To Be: | Principal logs on with existing linked identity at Identity Provider or Service Provider. Principal decides they no longer desire their identity to be linked with the account at the other. Identity Provider and Service Provider give the Principal a mechanism to unlink identities. Identity Provider and Service Provider completes deletion of link. |
| Benefits: | Increases Principal identity management control |
| Constraints: | • Identity Providers and Service Providers on both sides of the linking need to be aware of the deleted link for subsequent logins and they must change its status in the list of Principal's link history<br>• Principal needs to have unlink option readily available at all Identity Providers and Service Providers<br>• Identity Providers and Service Providers must comply with all applicable privacy regulations<br>• Deletion versus disablement of links is an option to be used at discretion of Service Provider; Service Provider must utilize at least one of the two options |
| Business Processes Impacted: | Identity Provider login, Service Provider login<br>Identity Provider Web pages, Service Provider Web pages (content) |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Customers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Guidelines for Identity Provider and Service Provider to provide list of link history associated with that Identity Provider or Service Provider |
|---|---|
| Requirement ID: | 2.2.3 |
| Use Case Reference: | 3.2.1 |
| Definition: | Provide guideline so that Principal can view a history of links associated with the Identity Provider or Service Provider relationship |
| As Is: | Does not exist |
| To Be: | Each Identity Provider and Service Provider provides for review by the Principal a history of links between themselves and other Identity Providers and Service Providers. Principal can use this capability to manage links<br>View capability data to include:<br>• Status of Link<br>• Date Status of Link was last changed<br>• All Service Providers related to that Link |
| Benefits: | Supports Privacy laws; supports unlinking functionality |
| Constraints: | • Identity Providers and Service Providers must have explicit consent from each Principal<br>• Identity Providers and Service Providers only shows links created between themselves and others (Identity Providers and Service Providers are not responsible for showing all links a Principal creates only the ones related to themselves); Principal must have at least one existing link with a relevant Identity Provider and Service Provider<br>• Mechanism must be in compliance with applicable privacy regulations<br>• Details of history to be presented are part of pre-arrangement between Principal, Identity Provider, or Service Provider |
| Business Processes Impacted: | Identity Provider Information Management, Service Provider Information Management, Identity Provider Web page content, Service Provider Web page content, Identity Provider Information Transfer, Service Provider Information Transfer |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Customers |

| Responsibility: | Service Providers |
|---|---|

| | |
|---|---|
| **Main Business Requirements:** | Mechanism to allow Identity Providers and Service Providers to provide notice of Principal's action to terminate link to all affected Identity Providers and Service Providers and receive confirmation of link termination |
| Requirement ID: | 2.2.4 |
| Use Case Reference: | 3.4.1 |
| Definition: | Principal discontinues an existing link by informing Identity Provider or Service Provider. Identity Provider or Service Provider needs to communicate this to others so that Principal can no longer use the link at either Identity Provider or Service Provider. Identity Provider or Service Provider returns an acknowledgement to the other that the linking has been disabled or deleted. Requesting Identity Provider or Service Provider confirms this to the Principal |
| As Is: | Does not exist |
| To Be: | If a Principal discontinues an existing link between an Identity Provider and a Service Provider, the Principal ID, Service Provider ID (who provided the ability to terminate), link ID, and timestamp of disassociation need to be sent to the other associated with that link. The receiving Identity Provider or Service Provider must respond with an acknowledgement. The Identify Provider or Service Provider who was responsible for initiating the unlinking informs the Principal of successful unlinking. |
| Benefits: | • Principal will not be able to go directly to Service Provider and ask for Identity Provider login after the link has been cancelled<br>• Provides consistency across system<br>• Enhances Principal's experience (will not be told link does not exist each time login attempt occurs) |
| Constraints: | Principal must have at least one existing relevant link |
| Business Processes Impacted: | Identity Provider Information Transfer, Service Provider Information Transfer, Service Provider login |
| Constituents: | Identity Providers, Service Providers, Customer, Security |
| Stakeholders: | Identity Providers, Service Providers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Guideline for Identity Providers and Service Providers to notify Principals of any links disabled or deleted by Identity Providers and Service Providers |
|---|---|
| Requirement ID: | 2.2.5 |
| Use Case Reference: | 3.4.2 |
| Definition: | Identity Provider and Service Provider decide to terminate their business agreement and disassociate any appropriate existing links |
| As Is: | Does not exist |
| To Be: | Identity Provider and Service Provider agree to terminate the Principal's identity linking. Identity Provider and/or Service Provider send the Principal a communication informing them of the link termination. |
| Benefits: | Increases customer identity management control |
| Constraints: | • Identity Provider and Service Provider on both sides of the linking need to be aware of the discontinued link for subsequent logins<br>• Identity Provider and Service Provider have to decide who and how they should communicate the link termination to the Principal |
| Business Processes Impacted: | Identity Provider login, Service Provider login<br>Identity Provider Web pages (content), Service Provider Web pages (content) |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Customers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Mechanism for Identity Provider and Service Provider to disable all the links between Identity Providers and Service Providers |
|---|---|
| Requirement ID: | 2.2.5b |
| Use Case Reference: | 3.4.2 |
| Definition: | Identity Provider and Service Providers decide to terminate the business agreement between them and are able to disassociate any appropriate existing links |
| As Is: | Does not exist |
| To Be: | Identity Provider and Service Provider agree to terminate the Principal's identity linking. Identity Provider and Service Provider use mechanism to identify all Principal identities that have a link between Identity Provider and Service Provider. Appropriate links are disabled or deleted for the appropriate Principal's identities. |
| Benefits: | Increases customer identity management control |
| Constraints: | • Identity Providers and Service Providers on both sides of the linking need to be aware of the discontinued link for subsequent logins<br>• Identity Providers and Service Providers have to decide who and how they should communicate the link termination to the Principal |
| Business Processes Impacted: | Identity Provider login, Service Provider Login<br>Identity Provider Web pages (content), Service Provider Web pages (content) |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Customers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Guidelines for Identity Providers and Service Providers to track Principals that have existing linked identities for purposes of notification of termination |
|---|---|
| Requirement ID: | 2.2.6 |
| Use Case Reference: | 3.4.2 |
| Definition: | Identity Providers and Service Providers must maintain enough information about the Principal that has created a link so that the Principal can be contacted if a business agreement has been cancelled that results in the termination of a link |
| As Is: | Does not exist |
| To Be: | Identity Provider and Service Provider tracks all Principal links by a shared identifier. If a Principal has more than one link between Identity Provider and Service Provider, Identity Provider is required to be able to uniquely differentiate all of Principal's linked accounts. |
| Benefits: | Flexibility for business-initiated link termination |
| Constraints: | • Identity Provider and Service Provider must gather provable consent that Principal has granted permission to keep this information<br>• Identity Provider and Service Provider do not track Principal information outside of its linked relationships |
| Business Processes Impacted: | Identity Provider Information Management, Service Provider Information Management |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Identity Providers, Service Providers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Guideline for Identity Providers and Service Provider to require a minimum data confidentiality requirement at the Principal level |
|---|---|
| Requirement ID: | 2.2.7 |
| Use Case Reference: | 3.1.1 |
| Definition: | Identity Providers and Service Providers to require an industry-appropriate data confidentiality mechanism in Principal's client in order to proceed with using Identity Provider's and Service Provider's services as associated with Identity Management |
| As Is: | For example, on the Internet a Principal navigates to a logon Web page that enforces 128-bit encryption with a 40-bit encryption capability in their browser. Web page does not allow Principal to continue with logon until Principal has upgraded encryption. |
| To Be: | Same, based on industry acceptable standards. Identity Provider and Service Provider can reject connections based upon data confidentiality mechanism of the terminating connection. |
| Benefits: | Increases security |
| Constraints: | International data confidentiality mechanisms laws |
| Business Processes Impacted: | Identity Provider login, Service Provider login |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Identity Providers, Service Providers, Customers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Mechanism for an Identity Provider and Service Provider to maintain data confidentiality with other Identity Provider or Service Provider acceptable to industry security standards |
|---|---|
| Requirement ID: | 2.2.8 |
| Use Case Reference: | 3.1.1 |
| Definition: | Identity Providers and Service Providers ensures safe data transfer to other Identity Providers and Service Providers |
| As Is: | Exists but variation between technologies |
| To Be: | Same |
| Benefits: | Increases security |
| Constraints: | International encryption laws |
| Business Processes Impacted: | Identity Providers Information Transfer, Service Provider Information Transfer |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Identity Providers, Service Providers, Customers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Guideline to maintain session integrity |
|---|---|
| Requirement ID: | 2.2.9 |
| Use Case Reference: | 3.1.1 |
| Definition: | Once an end-user has been authenticated, session integrity should be maintained for that user until they log-out or are timed out. |
| As Is: | Principals, Identity Providers, and Service Providers today use multiple session integrity tools such as certificates, signatures, encryption keys, etc., in order to increase confidence that either party is properly being represented. |
| To Be: | Same. |
| Benefits: | Decreases risk of fraudulent activity |
| Constraints: | Identity Providers and Service Provider's communication mechanism may not allow for some session integrity tools to be used |
| Business Processes Impacted: | Identity Provider information transfer, Service Provider information transfer |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Identity Providers, Service Providers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Mechanism to support maximum possible Internet access methods (at minimum including desktop PCs, mobile phones, and PDAs with browser) |
|---|---|
| Requirement ID: | 2.2.10 |
| Use Case Reference: | All |
| Definition: | Identity Providers and Service Providers need to be able to authenticate, login, and link accounts when receiving user requests from various Internet access methods |
| As Is: | Same |
| To Be: | Regardless of cookie support, IP support, and device display limitations, the functionality of linking, de-linking, etc., needs to work on various Internet access methods |
| Benefits: | • Increases access mechanisms<br>• Increases audience<br>• Provides convenience to users |
| Constraints: | Device limitations exist |
| Business Processes Impacted: | Identity Provider Login and Authentication, Service Provider Login and Authentication |
| Constituents: | Identity Providers, Service Providers, Device Manufacturers, Customers |
| Stakeholders: | Identity Providers, Service Providers, Device Manufacturers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Mechanism to support different authentication methods for credentials |
|---|---|
| Requirement ID: | 2.2.10b |
| Use Case Reference: | All |
| Definition: | Liberty Alliance specs must provide for the use of various authentication methods such as IP address and MSISDN |
| As Is: | Some Identity Providers authenticate users on credentials such as password, IP address, MSISDN, smart cards and digital certificates |
| To Be: | Service Providers must be able to link accounts and accept users' credentials regardless of the technology used by Identity Provider |
| Benefits: | • Increased access mechanisms<br>• Increases security<br>• Provides convenience to users |
| Constraints: | |
| Business Processes Impacted: | Identity Provider login and authentication, Service Provider Login and Authentication |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Identity Providers, Service Providers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Mechanism to support additional authentication information |
|---|---|
| Requirement ID: | 2.2.10c |
| Use Case Reference: | All |
| Definition: | Liberty Alliance specs must provide a mechanism for Identity Providers to assert additional authentication information, such as strengths or any other information that Identity Providers and Service Providers may require to exchange as part of authentication |
| As Is: | Some Identity Providers authenticate users on credentials such as password, IP address, MSISDN, smart cards, and digital certificates |
| To Be: | Service Provider must be able to request additional authentication information from the Identity Provider. Identity Provider must choose an appropriate method, which is at least as strong as what has been requested by the Service Provider. |
| Benefits: | Increased access mechanisms provides convenience to Service Providers |
| Constraints: | Identity Providers and Service Providers are expected to agree the semantics and interpretation of the additional authentication information exchanged if this functionality is used |
| Business Processes Impacted: | Service Provider Login and Authentication |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Service Providers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Mechanism to provide identity linking solution without mandating client-side changes |
|---|---|
| Requirement ID: | 2.2.11 |
| Use Case Reference: | All |
| Definition: | Identity Providers and Service Providers need to be able to link and de-link accounts, etc., without any changes to the devices on the client side. This include no downloads, no client side certificates, and no client browser modifications from standard configuration |
| As Is: | Users of Web services today have the general expectation that they will not be required to install software or perform installation in order to use Web based services |
| To Be: | Same |
| Benefits: | • No requirements of customer,<br>• No product support requirements<br>• Increases accessibility to solution |
| Constraints: | Client side changes should not be made where possible and in all other cases kept to a minimum |
| Business Processes Impacted: | Identity Provider Authentication, Service Provider Authentication |
| Constituents: | Customers, Identity Providers, Service Providers |
| Stakeholders: | Customers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Mechanism to ensure identity linking is easily deployable on existing network infrastructures (IP- and non-IP-based) |
|---|---|
| Requirement ID: | 2.2.12 |
| Use Case Reference: | All |
| Definition: | Mechanism to support login, linking, and authentication from both IP- and non-IP-based network infrastructures |
| As Is: | Does not exist |
| To Be: | Principal comes from existing network and is able to perform all functions in solution regardless of network type |
| Benefits: | Increases customer accessibility and ease of use |
| Constraints: | None |
| Business Processes Impacted: | Identity Provider authentication, Service Provider authentication |
| Constituents: | Identity Providers, Service Providers, Customers, Technology Infrastructure Providers, Device Manufacturers |
| Stakeholders: | Device Manufacturers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Mechanism to support internationalization standards for all identity linking requirements (thus operational across language and cultural domains) |
|---|---|
| Requirement ID: | 2.2.13 |
| Use Case Reference: | All |
| Definition: | Solution must be architected to support multiple languages for use internationally according to internationalization standards |
| As Is: | Does not exist |
| To Be: | Support internationalization standards |
| Benefits: | • International acceptance<br>• Increases customer base |
| Constraints: | None |
| Business Processes Impacted: | Identity Provider login and authentication, Service Provider login and authentication |
| Constituents: | Customers, Identity Providers, Service Providers |
| Stakeholders: | Identity Providers, Service Providers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Mechanism to allow Identity Providers to prove authentication method to Service Providers |
|---|---|
| Requirement ID: | 2.2.14 |
| Use Case Reference: | 3.3.1 |
| Definition: | Provide mechanism for Service Providers to securely request of other linked Identity Providers if the User requesting access to their service has logged in and been authenticated |
| As Is: | Does not exist |
| To Be: | Identity Provider provides assertion specifying a Principal's current logged in status including authentication method to Service Provider |
| Benefits: | • Maintains session integrity<br>• Necessary for Service Provider login |
| Constraints: | Identity Providers and Service Providers must have explicit provable consent to share information |
| Business Processes Impacted: | Identity Provider Information Transfer, Service Provider Information Transfer, Identity Provider Login, Service Provider Login |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Identity Providers, Service Providers |
| Responsibility: | Service Providers |

| **Main Business Requirements:** | Mechanism to allow Identity Providers and Service Providers to communicate details about the method(s) that were used to validate the Principal |
|---|---|
| Requirement ID: | 2.2.15 |
| Use Case Reference: | 3.3.1 |
| Definition: | Identity Providers must be able to provide information to Service Providers about the method(s) and credentials used to authenticate a Principal (to be extensible for future requirements as they occur) |
| As Is: | Does not exist |
| To Be: | • All Identity Providers must be able to send the information about the method(s) used to authenticate a Principal with examples of some of the information such as:<br>• Registration-time method of Principal's Identity verification (on-line, physical identification, etc.)<br>• Quality of Credential's Protection (stored on PC, Smartcard, Personal Trusted Device, etc)<br>• Method of Credentials generation (Client-side, on-the Smartcard, Server-side, etc)<br>• Run-time authentication method (Password, X.509, Token, Biometrics, MSISDN/SIM, IP address, etc.)<br>• Credentials Policy (how often SP require Principal's to renew passwords, required password entropy, etc)<br>• If the Service Provider’s decision to allow or disallow access to certain services is be based on the "method of authentication assertion" notice sent by Identity Provider, this is a business decision made by Service Provider as part of the business arrangement with Identity Provider." |
| Benefits: | Allows Service Providers to assess what level of access to provide to an authenticated Principal |
| Constraints: | There needs to be an understood and consistent schema for the assertions if confusion is to be avoided. |
| Business Processes Impacted: | Principal authentication |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Identity Providers, Service Providers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Mechanism to allow Service Providers to recognize Principal's Identity Provider authentication status and send Principal to Identity Provider to login when appropriate |
|---|---|
| Requirement ID: | 2.2.16 |
| Use Case Reference: | 3.3.2 |
| Definition: | Provide ability for Service Provider to understand Principal authentication status and send to appropriate Identity Provider's login when necessary |
| As Is: | Does not exist |
| To Be: | Provide mechanism so that if Principal goes directly to Service Provider in a linked relationship for that Principal with Identity Provider, Service Provider will recognize that user has not logged into Identity Provider and send to appropriate login. |
| Benefits: | • Prevents Principal logging in twice on linked accounts<br>• Improvement to user experience |
| Constraints: | Service Provider needs to know of linked relationship and with which Identity Provider that linked relationship is |
| Business Processes Impacted: | Service Provider login |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Identity Providers, Service Providers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Mechanism for Identity Providers and Service Providers to identify and authenticate other Identity Providers and Service Providers |
|---|---|
| Requirement ID: | 2.2.17 |
| Use Case Reference: | 3.1.1 |
| Definition: | Provide ability for Identity Providers and Service Providers to authenticate other Identity Provider and Service Providers as part of authentication process |
| As Is: | Does not exist |
| To Be: | Identity Providers and Service Providers must be able to securely identify each other prior to exchanging any data |
| Benefits: | Supports provable consent function, prevents spoofing of Principal identity |
| Constraints: | None |
| Business Processes Impacted: | Identity Provider Login, Service Provider Login |
| Constituents: | Identity Providers, Service Providers |
| Stakeholders: | Identity Providers, Service Providers |
| Responsibility: | Identity Providers, Service Providers |

| | |
|---|---|
| **Main Business Requirements:** | Guidelines for Identity Providers and Service Providers to provide notice to Principals about linking opportunities and allowing Identity Providers and Service Providers to capture consent for each linking activity |
| Requirement ID: | 2.2.18 |
| Use Case Reference: | 3.1.1 |
| Definition: | Identity Providers and Service Provider to display textual notice to Principal of information requested and how it will be used. Principal is then to be given the option to agree with the terms. Principal must then be given access to review and or correct the data once collected. |
| As Is: | Many and varied |
| To Be: | Identity Providers and Service Providers will provide the Principal with a consistent experience for how notice is presented, how consent is gathered, how the notice and consent are bound, and how access will be provided to this information. Notice and consent must be securely bound together, allowing Identity Provider and Service Provider to store this bound data in such a way that Principal can later access this bound data. |
| Benefits: | • Provides a consistent and easy to understand audit trail of permission<br>• Supports Privacy laws<br>• Supports non-repudiation |
| Constraints: | • Each separate linking activity with the same Principal must include this consent<br>• Identify Provider and Service Provider is not to exchange information of any kind on that Principal without this consent |
| Business Processes Impacted: | Identity Provider linking, Service Provider linking, Identity Provider Information Transfer, Service Provider Information Transfer, Identity Provider Information Management, Service Provider Information Management |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Identity Providers, Service Providers, Customers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Mechanism to allow Principals to explicitly log out of services (including all linked services) |
|---|---|
| Requirement ID: | 2.2.19 |
| Use Case Reference: | 3.5.1 |
| Definition: | Principal is logged into identity at Identity Provider that is linked to Service Provider. Principal logs out of identity at Identity Provider without ever navigating to Service Provider. Principal, after logging out, now navigates to Service Provider B and is presented with login.<br>Principal is logged into account at Identify Provider that is linked to Service Provider B. Principal navigates to Service Provider and does not have to login to access services because of link. Principal selects to log out of Service Provider. Principal should now be logged out of both Identity Provider and Service Provider. |
| As Is: | Does not exist |
| To Be: | Principal logs out of a linked account and is logged out of services provided by all Identity Providers and Service Providers associated with that link. |
| Benefits: | • Decreases risk of fraudulent use of logged in account<br>• Increases customer satisfaction to have logout feature<br>• Decreases security risks |
| Constraints: | None |
| Business Processes Impacted: | Identity Provider session management, Service Provider session management |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Identity Providers, Service Providers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Mechanism to ensure inactive Principal's session is not misappropriated |
|---|---|
| Requirement ID: | 2.2.20 |
| Use Case Reference: | 3.5.2 |
| Definition: | If an existing session is open for any account with linking abilities (whether they are linked or not) and that session has been inactive for a determined period the server should expire the session and request re-authentication. |
| As Is: | Same |
| To Be: | Principal logs into linked identity at Identity Provider and has not navigated to Service Provider. Principal is inactive for a determined period of time and server expires session. Principal begins activity but cannot proceed because they are asked to login again.<br>Principal logs into linked identity at Identity Provider A and then navigates to Service Provider. Principal is inactive for a determined period of time at Service Provider and server expires session. Principal begins activity again but cannot proceed at Service Provider because they are asked to log in again. Principal navigates back to Identity Provider and cannot proceed with activity until they login again (should show as not logged in). |
| Benefits: | Prevents fraudulent activity |
| Constraints: | • Automatic timeout should not cause unnecessary user burden<br>• Identity Provider and Service Provider timeouts that vary in length will need to be agreed upon as part of business agreement |
| Business Processes Impacted: | Identity Provider session management, Service Provider session management |
| Constituents: | Identity Providers, Service Providers, Customers |
| Stakeholders: | Identity Providers, Service Providers |
| Responsibility: | Identity Provider, Service Providers |

| **Main Business Requirements:** | Mechanism for ensuring integrity of data amongst Identity Providers and Service Providers |
|---|---|
| Requirement ID: | 2.2.21 |
| Use Case Reference: | All |
| Definition: | Mechanism in place that uses commonly accepted online security best practices to ensure integrity of communications of authentication information such that misappropriating or misuse of unauthorized access to information is prevented. |
| As Is: | Varies by country |
| To Be: | Communication between Identity Providers and Service Providers to be protected with commonly used integrity practices such that attempts to intervene and misuse information by outside parties are reasonably deterred |
| Benefits: | • Prevention of identity spoofing<br>• Protection of Principal information<br>• Supports value proposition of security and privacy |
| Constraints: | Must be in compliance with all applicable security and privacy regulations |
| Business Processes Impacted: | Identity Provider login, Service Provider Login, Identity Provider information exchange, Service Provider information exchange |
| Constituents: | Identity Providers, Service Providers |
| Stakeholders: | Identity Providers, Service Providers |
| Responsibility: | Identity Providers, Service Providers |

| **Main Business Requirements:** | Mechanism for Service Provider to request re-authentication of a Principal specifying the current or an alternative method of reauthentication that is required |
|---|---|
| Requirement ID: | 2.2.22 |
| Use Case Reference: | 3.3.1 |
| Definition: | Service Provider must be able to request re-authentication of a Principal from an Identity Provider and communicate the authentication method required |
| As Is: | Does not exist |
| To Be: | Service Provider requests that Identity Provider re-authenticate the Principal with a specified method |
| Benefits: | Allows Service Providers to tier access to services based on different authentication methods and to request re-authentication when an unacceptable method is presented. |
| Constraints: | Identity Providers and Service Providers must agree authentication methods as part of business agreements |
| Business Processes Impacted: | Identity Provider information exchange, Service Provider information exchange |
| Constituents: | Identity Providers, Service Providers |
| Stakeholders: | Identity Providers, Service Providers |
| Responsibility: | Identity Providers, Service Providers |

# 3 Use Cases for Phase 1

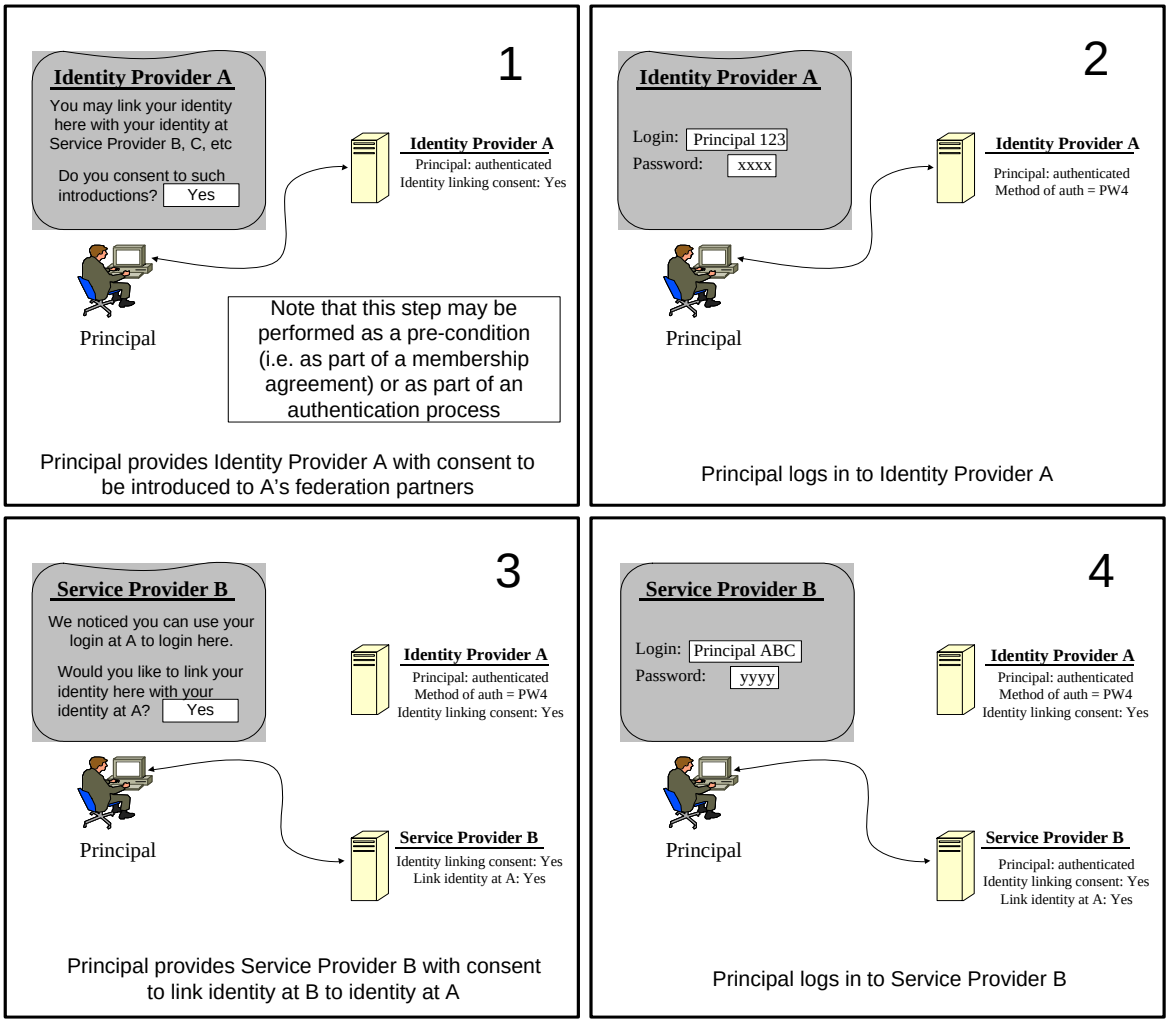
In order to realize the benefits outlined in section 1.2, the Liberty Alliance has created the following use cases to describe the various constituents' experiences.

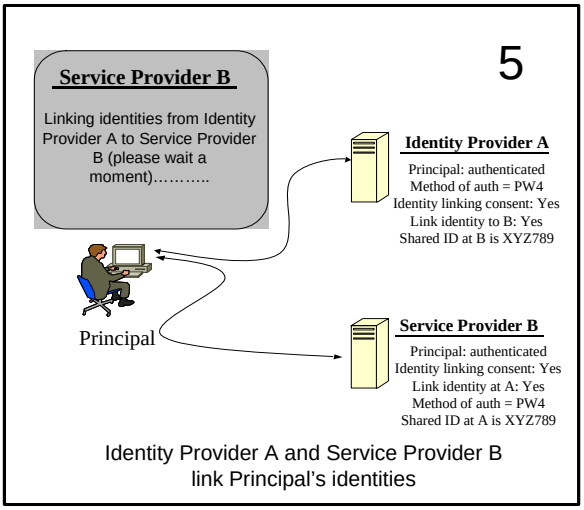
These use cases cover the constituent's experiences for Phase 1 only.

## 3.1 Creating Identity Links

### 3.1.1 Principal Links their Identity at Identity Provider to their Identity at Service Provider

This use case describes the initial linking of a Principal's identity at two Service Providers.






Identity Provider A and Service Provider B link Principal's identities

| | |
|---|---|
| **Title/ID** | Principal Links One Identity to Another Identity |
| **Pre-conditions** | Principal has an identity at Identity Provider A.<br>Principal has an identity at Service Provider B.<br>Identity Provider A has entered an agreement with Service Provider B through which Service Provider B accepts authentication of a Principal from Identity Provider A and has agreed what methods of authentication they will accept.<br>Identity Provider A has followed Liberty guidelines for provisioning identities and managing the linking of a Principal's identity at Identity Provider A to the Principal's identity at Service Provider B.<br>Identity Provider A provides Principal with notice of how their identity at Identity Provider A can be linked to their identity at Service Provider B (and any other Service Providers with whom Identity Provider A has a relationship) in accordance with Liberty Alliance guidelines.<br>Principal gives consent to link their identity at Identity Provider A with their identity at Service Providers with whom Identity Provider A has a relationship.<br>Identity Provider A binds the Principal's consent to the notice in accordance with Liberty Alliance guidelines.<br>Identity Provider A stores the bound notice and choice such that the Principal can gain later access to this information in accordance with Liberty Alliance guidelines.<br>Service Provider B has followed Liberty guidelines for provisioning identities and managing the linking of a Principal's identity at Identity Provider A to the Principal's identity at Service Provider B. |
| **Constituents** | Principal, Identity Provider A, Service Provider B |
| **Use Case** | Principal navigates to Identity Provider A and can securely verify the identity of Identity Provider A.<br>Identity Provider A authenticates Principal.<br>Principal navigates to Service Provider B and can securely verify the identity of Service Provider B.<br>Service Provider B securely recognizes that Principal was authenticated by Identity Provider A. |

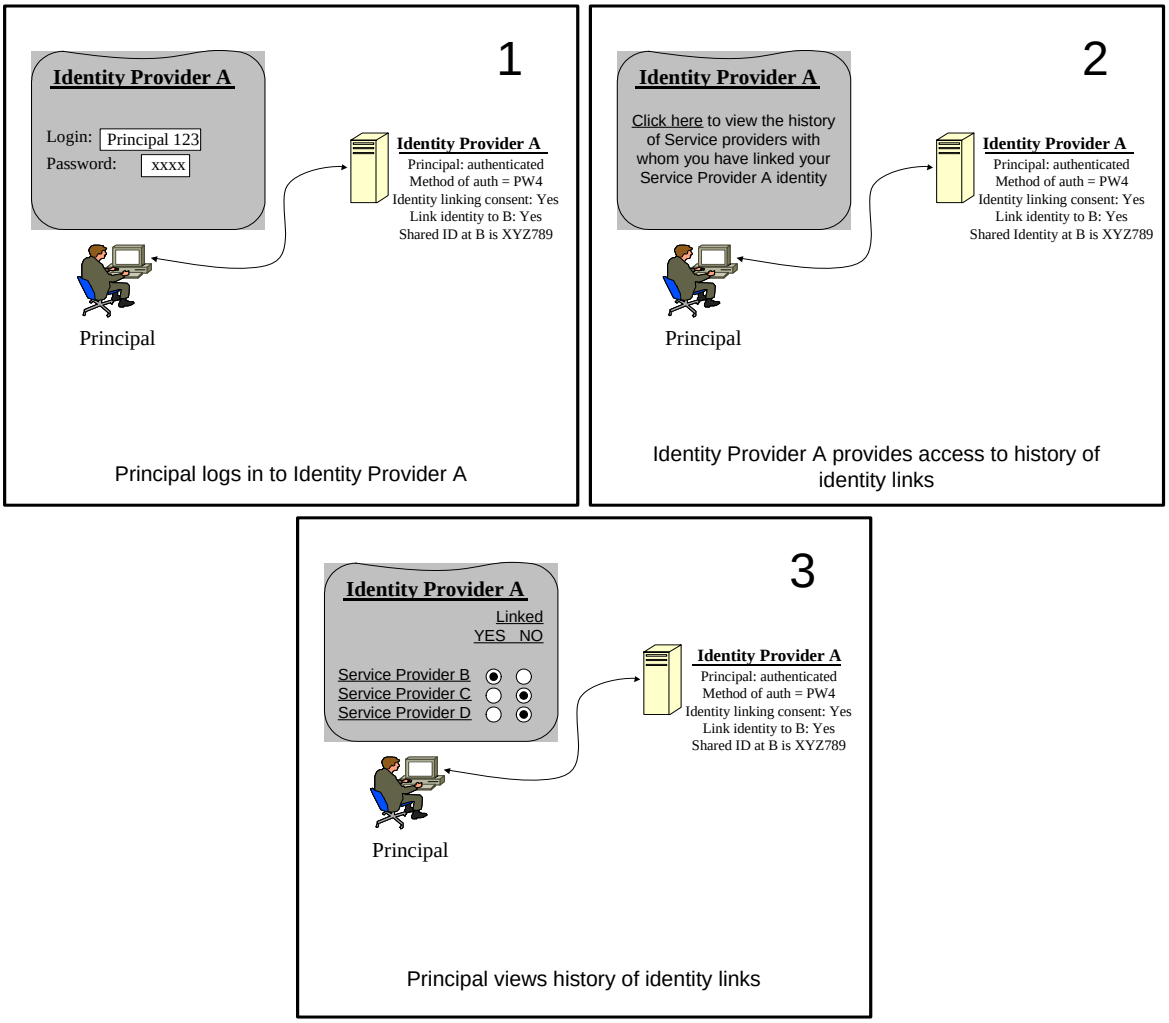
| | |
|---|---|
| | Service Provider B provides the Principal with notice that they have the opportunity to link their identity at Service Provider B to their identity at Identity Provider A in accordance with Liberty Alliance guidelines.<br>Principal chooses to link identities and gives Service Provider B their consent.<br>Service Provider B asks Principal to login with his Service Provider B credentials.<br>Service Provider B applies their consent, binding and storage policies in accordance with Liberty Alliance guidelines.<br>Identity Provider A and Service Provider B securely link identity of Principal. |
| **Notes** | Following this use case results in a unidirectional linking from A to B. It is not explicit in this use case that A could recognize and perform the same linking for the Principal, using B as an Identity Provider, without repeating the same process in reverse. |

## 3.2 Reviewing Identity Links

### 3.2.1 Principal Views Linkage History

This use case describes how Identity Providers and Service Providers provide a Principal with access to the history of links.

The Principal can view the identity link from both the Identity Provider's and Service Provider's sites. The presentation of the history is defined as part of the business relationships between the Identity Provider and the Service Provider. In certain circumstances an Identity Provider may be in a position to provide more relevant information about the linking than the Service Provider due to the limited amount of information shared between them.

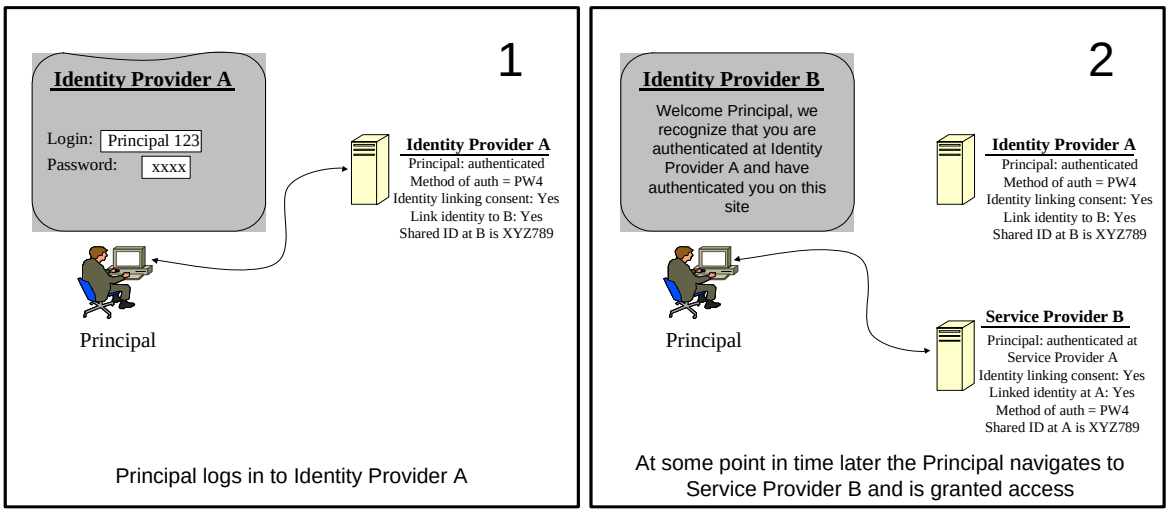


| | |
|---|---|
| **Title/ID** | Principal Views Linkage History |
| **Pre-conditions** | 1. Principal has an identity at Identity Provider A<br>2. Principal has an identity at Service Provider B.<br>3. Identity Provider A has entered an agreement with Service Provider B through which Service Provider B accepts authentication of a Principal by Identity Provider A and has agreed what method(s) of authentication they will accept.<br>4. Identity Provider A has followed Liberty guidelines for provisioning identities and has given notice and obtained consent from the Principal to link the login status and method of authentication of the Principal at Service Provider B.<br>5. Identity Provider A has provided the Principal with an ability to locate and access the linking history from Identity Provider A.<br>6. Service Provider B has followed Liberty guidelines for provisioning identities and has given notice and obtained consent from the Principal to use the login status and method of authentication of the Principal identity at Identity Provider A to link to the Principal's identity at Service Provider B.<br>7. Service Provider B has provided the Principal with an ability to allow them to locate and access the linking history. |
| **Constituents** | Principal, Identity Provider A, Service Provider B |
| **Use Case** | 8. Principal logs into Identity Provider A<br>9. Identity Provider A provides the Principal with an ability to locate and access the linking history from Identity Provider A<br>10. Principal views list of both current and previous identity links that have existed between Identity Provider A and other Service Providers including Service Provider B<br>11. Principal navigates to Service Provider B<br>12. Principal logs into Service Provider B<br>13. Service Provider B provides an ability to allow the Principal to locate and access the linking history from Service Provider B |

| | |
|---|---|
| | 14. Principal views list of both current and previous identity links that have existed between Service Provider and other Identity Providers |

## 3.3 Using Identity Links

### 3.3.1 Principal Is Granted Access at Service Provider B after Having Authenticated at Identity Provider A




**Notes on link transitivity and non-transitivity**

Definition of transitivity

Transitivity: Of or relating to a relationship between three elements such that if the relationship holds between the first and second elements and between the second and third elements, it necessarily holds between the first and third elements.

Rules for transitivity of authentication linking

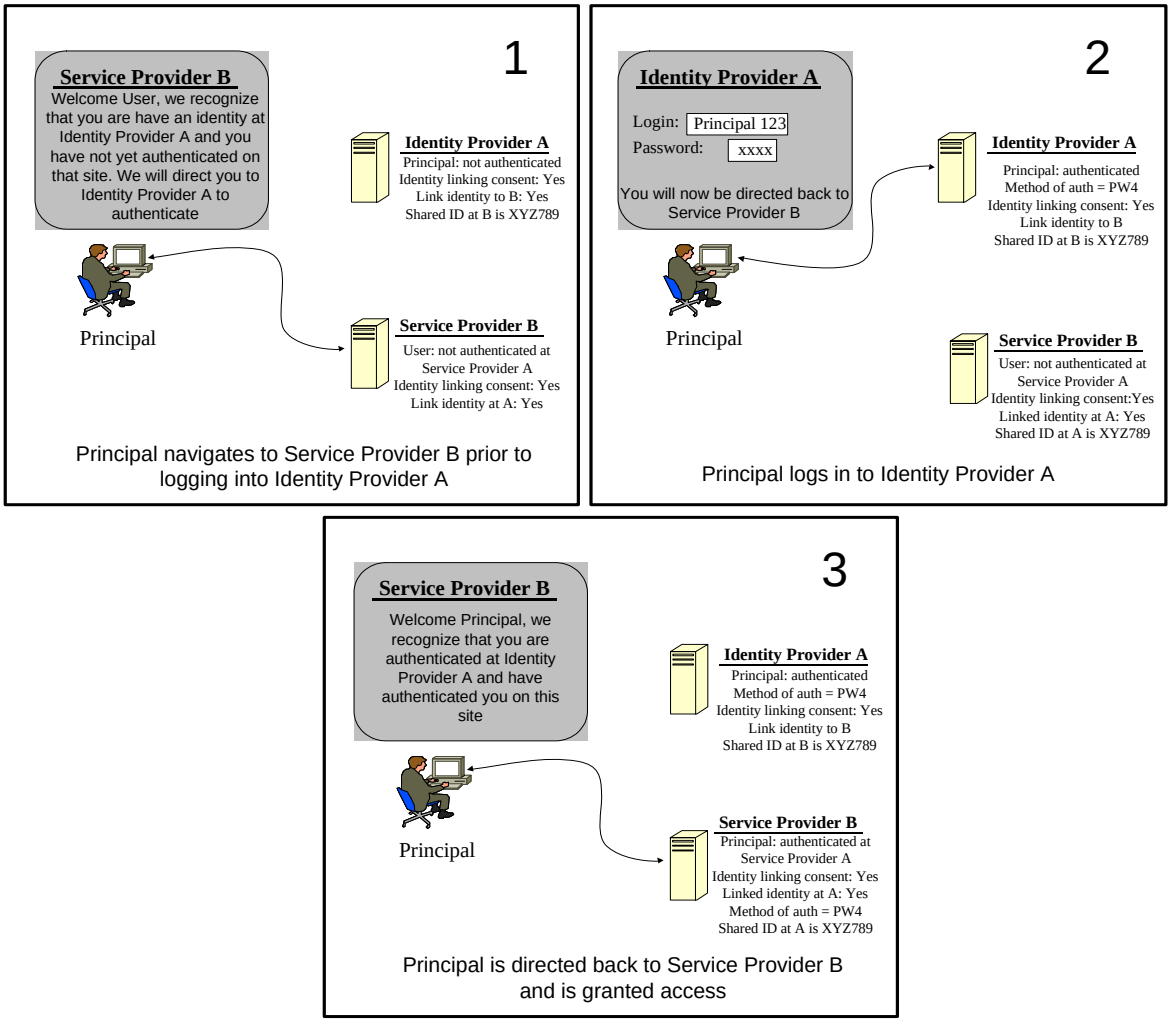
An Identity Provider A and Service Provider B have entered into a business agreement and created a “Circle of Trust” which allows B to trust the authentication assertion made by A.

If a third Service Provider is added to the scenario, Service Provider C, and Service Provider B has a business agreement with Service Provider C, but Service Provider A does not, there is no explicit transitivity of trust between A and C.

A Principal who consents to link their identity at A to their identity at B and who separately links their identity at B with their identity at C cannot explicitly link their identity at A with their identity at C. In order for this to be accomplished, Identity Provider A and Service Provider C would be required to enter into a business agreement to allow identity linking.

| | |
|---|---|
| **Title/ID** | Principal Who Is Authenticated at Identity Provider A Is Granted Access by Service Provider B |
| **Pre-conditions** | 1. Principal has an identity at Identity Provider A.<br>2. Principal has an identity at Service Provider B.<br>3. Identity Provider A has entered an agreement with Service Provider B by which Service Provider B accepts authentication of Principal by Identity Provider A and has agreed what method(s) of authentication they will accept. The agreement describes what method of authentication is required to access which services at B.<br>4. Identity Provider A has followed Liberty guidelines for provisioning identities and has given notice and obtained consent from the Principal to use the login status and method of authentication of the Principal at Identity Provider A to link the Principal's identity to other Service Providers.<br>5. Service Provider B has followed Liberty guidelines for provisioning identities and has given notice and obtained consent from the Principal to use the login status and method of authentication of the Principal at Identity Provider A to link the Principal's identity to their identity at Service Provider B.<br>6. Principal's identity is linked.<br>7. The Principal is currently authenticated at Service Provider A. |
| **Constituents** | Principal, Identity Provider A, Service Provider B |
| **Use Case** | 8. Principal navigates to Service Provider B and verifies the identity of Service Provider B.<br>9. Identity Provider A securely asserts Principal's authentication and method of authentication to Service Provider B.<br>10. Service Provider B recognizes that Principal is currently authenticated by Service Provider A and recognizes that the method of authentication is acceptable to access requested service.<br>11. Service Provider B delivers service to Principal. |

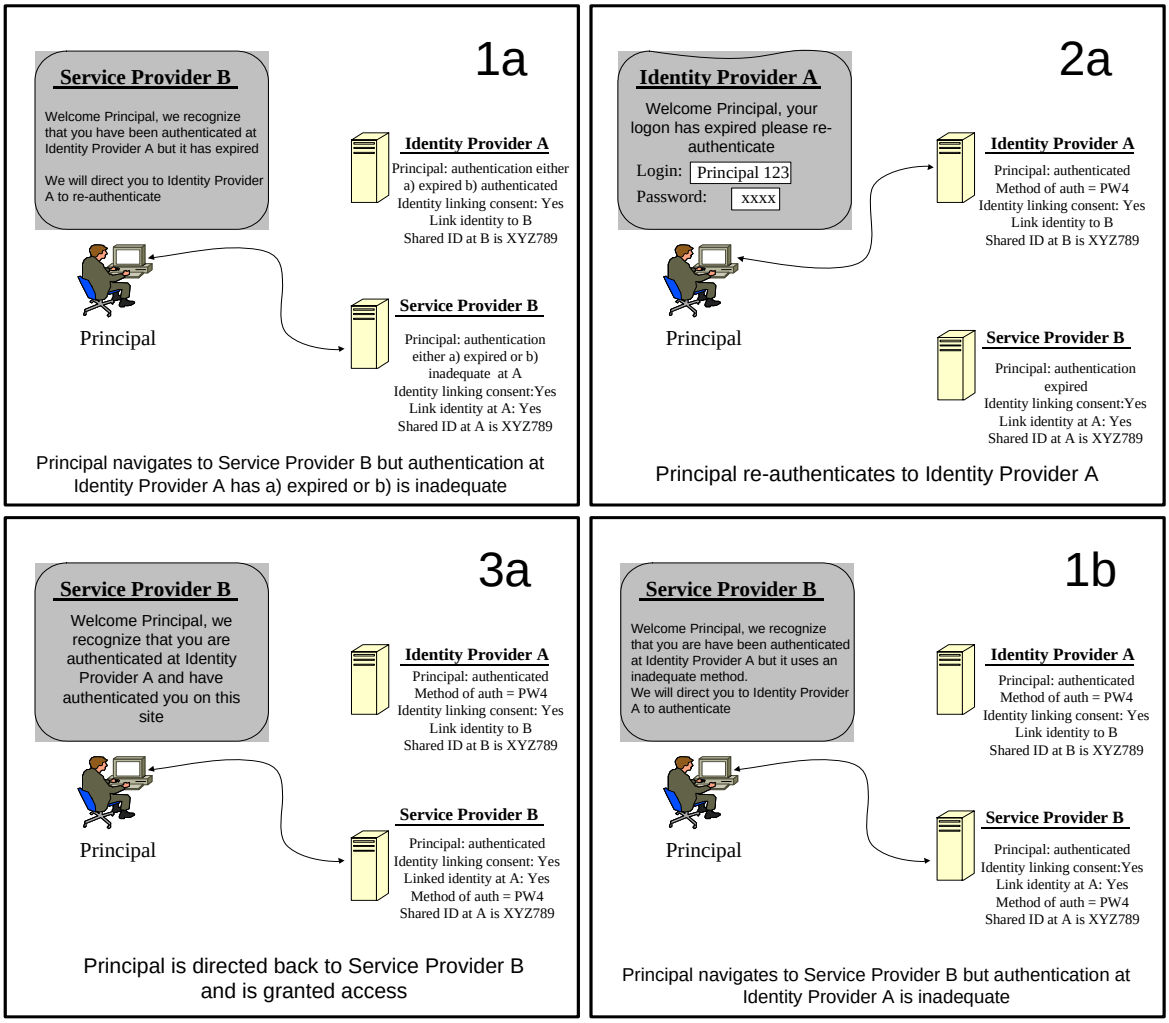
### 3.3.2 Principal Attempts to Authenticate at Service Provider B Prior to Authenticating at Identity Provider A

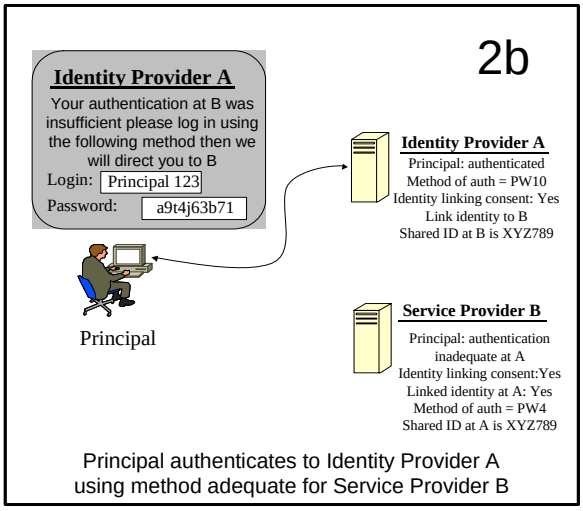


| | |
|---|---|
| **Title/ID** | Principal Attempts to Authenticate at Service Provider B Prior to Authenticating at Identity Provider A |
| **Pre-conditions** | 1. Principal has an identity at Identity Provider A.<br>2. Principal has an identity at Service Provider B.<br>3. Identity Provider A has entered an agreement with Service Provider B by which Service Provider B accepts authentication of Principal by Service Provider A and has agreed what method(s) of authentication they will accept.<br>4. Identity Provider A has followed Liberty guidelines for provisioning identities and has given notice and obtained consent from the Principal to use the login status and method of authentication of the Principal at Identity Provider A to link the Principal's identity.<br>5. Service Provider B has followed Liberty guidelines for provisioning identities and has given notice and obtained consent from the Principal to use the login status and method of authentication of the Principal at Identity Provider A to link the Principal's identity to their identity at Service Provider B.<br>6. Principal's identity is linked.<br>7. The Principal is not currently authenticated at Identity Provider A. |
| **Constituents** | Principal, Identity Provider A, Service Provider B |

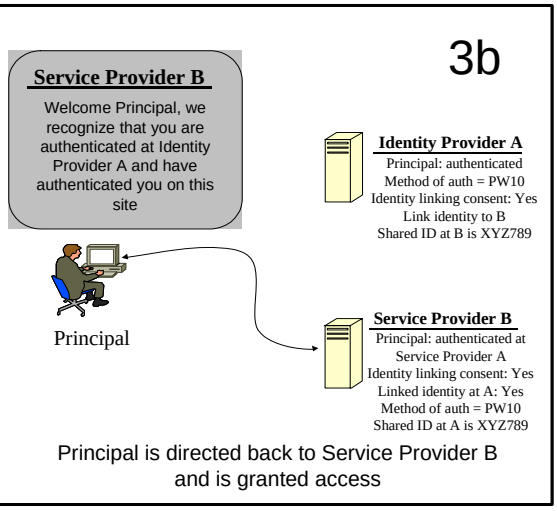
| | |
|---|---|
| **Use Case** | 8. Principal navigates to Service Provider B and securely verifies the identity of Service Provider B.<br>9. Service Provider B recognizes that Principal uses Service Provider A as an Identity Provider and is not currently authenticated with them.<br>10. Principal is directed to Service Provider A.<br>11. Principal presents their credentials at Identity Provider A for authentication.<br>12. Identity Provider A verifies Principal's credentials.<br>13. Principal is directed to Service Provider B.<br>14. Identity Provider A securely asserts Principal's authentication and method of authentication to Service Provider B.<br>15. Service Provider B recognizes that Principal is currently authenticated by Identity Provider A and recognizes that the method of authentication is acceptable to access requested service.<br>16. Service Provider B delivers service to Principal. |

### 3.3.3 Service Provider B Requires Re-Authentication of Principal by Identity Provider A






Principal authenticates to Identity Provider A using method adequate for Service Provider B



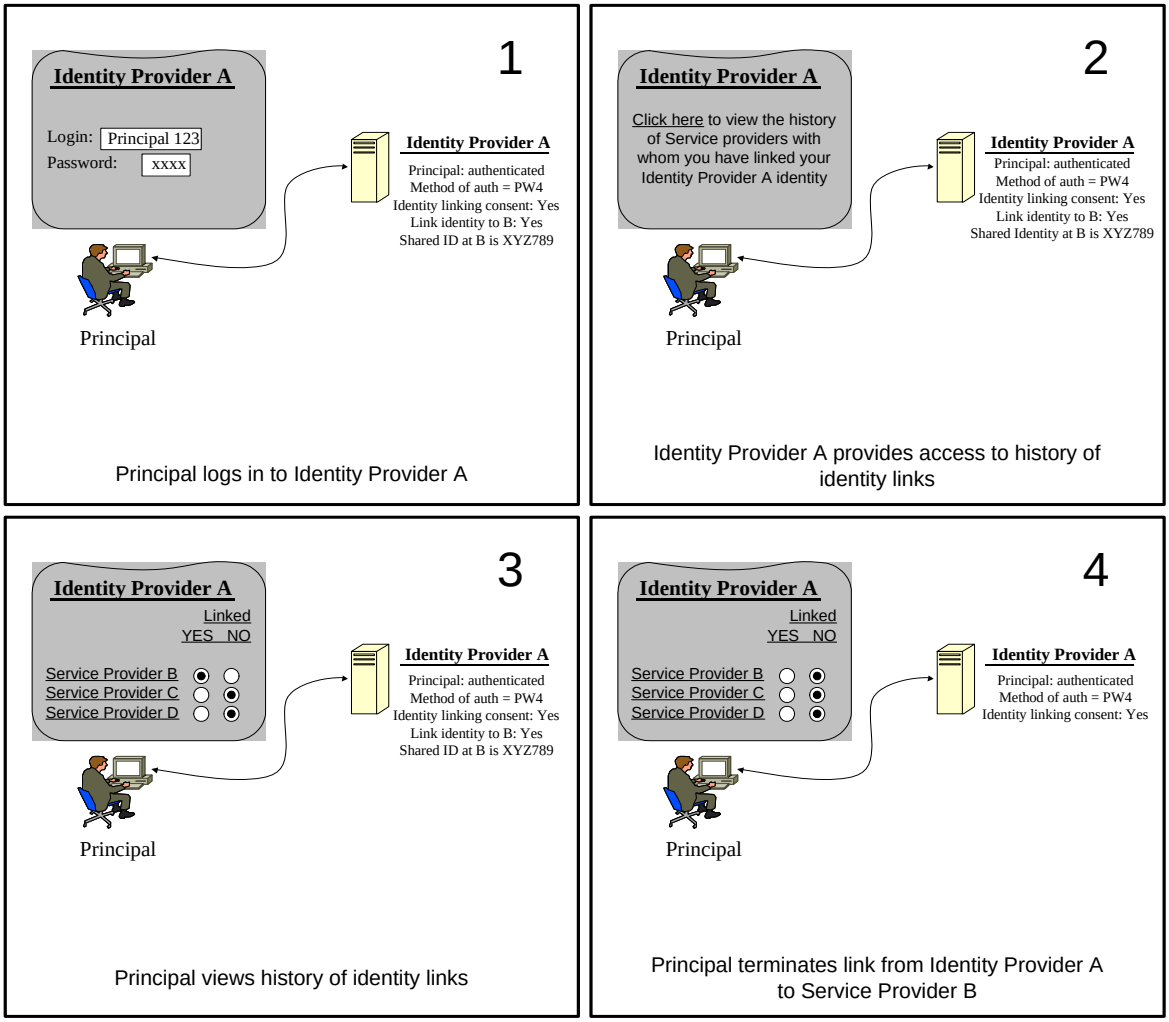

Principal is directed back to Service Provider B and is granted access

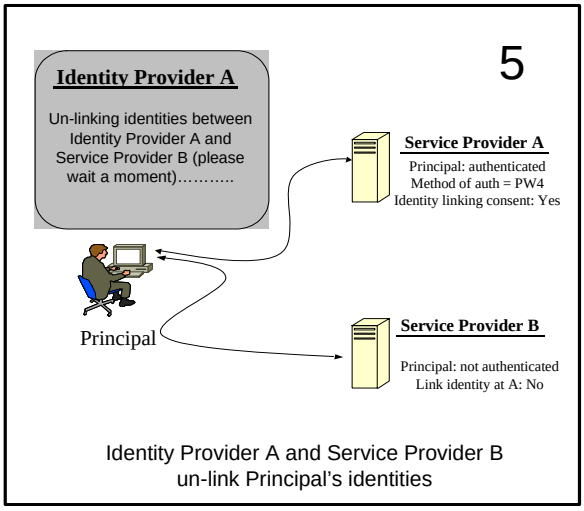
| | |
|---|---|
| **Title/ID** | Service Provider B Requires Re-Authentication of Principal by Identity Provider A |
| **Pre-conditions** | 1. Principal has an identity at Identity Provider A.<br>2. Principal has an identity at Service Provider B.<br>3. Identity Provider A has entered an agreement with Service Provider B by which Service Provider B accepts authentication of Principal by Identity Provider A and has agreed what method(s) of authentication they will accept.<br>4. Identity Provider A has followed Liberty guidelines for provisioning identities and has given notice and obtained consent from the Principal to use the login status and method of authentication of the Principal at Identity Provider A to link the Principal's identity.<br>5. Service Provider B has followed Liberty guidelines for provisioning identities and has given notice and obtained consent from the Principal to use the login status and level of authentication of the Principal at Identity Provider A to link the Principal's identity to their identity at Service Provider B.<br>6. Principal's identity is linked.<br>7. The Principal's authentication at Identity Provider A is either a) expired or b) currently authenticated with a specified method at Identity Provider A. |
| **Constituents** | Principal, Identity Provider A, Service Provider B |
| **Use Case** | 8. Principal navigates to Service Provider B and securely verifies the identity of Service Provider B.<br>9. Identity Provider A securely asserts Principal's authentication and method of authentication to Service Provider B.<br>10. Service Provider B recognizes that Principal has been authenticated by Identity Provider A and recognizes that the authentication method used has a) expired or b) was not acceptable to access the requested service, as specified in their business agreement.<br>11. Service Provider B denies access to service to Principal.<br>12. Service Provider B directs Principal to Identity Provider A to a) re-authenticate or b) authenticate using an acceptable method. |

| | |
|---|---|
| | 13. Service Provider B communicates to Identity Provider A that a) re-authentication is required or b) that another authentication method is required for the Principal as previously defined in their business agreement.<br>14. Identity Provider A re-authenticates the Principal in accordance with the information received from Service Provider B.<br>15. Identity Provider A directs the Principal to Service Provider B.<br>16. Identity Provider A securely asserts Principal's authentication and method of authentication to Service Provider B.<br>17. Service Provider B recognizes that Principal is currently authenticated by Identity Provider A and recognizes that the authentication method used was acceptable to access the requested service, as specified in their business agreement.<br>18. Service Provider B delivers service to Principal. |
| **Alternative Actions** | 19. Service Provider B asks Principal to sign-in with its Service Provider B authentication. |

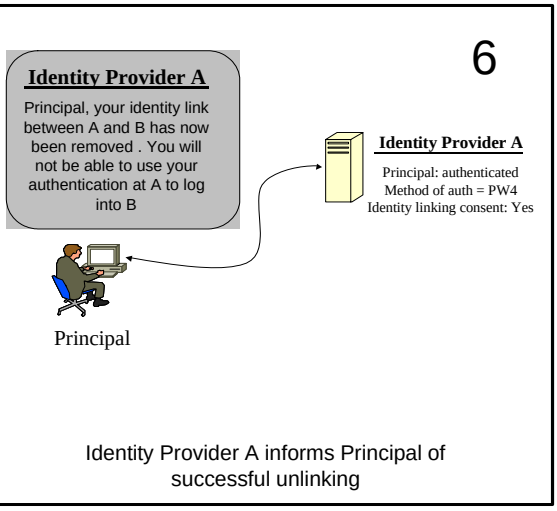
## 3.4 Termination of Linking

### 3.4.1 Principal Terminates the Link Between Their Identity at an Identity Provider and Their Identity at a Service Provider






Identity Provider A and Service Provider B un-link Principal's identities




Identity Provider A informs Principal of successful unlinking

| | |
|---|---|
| **Title/ID** | Principal-Initiated Termination of Linkage |
| **Pre-conditions** | 1. Principal has an identity at Identity Provider A.<br>2. Principal has an identity at Service Provider B.<br>3. Identity Provider A has entered an agreement with Service Provider B through which Service Provider B accepts authentication of a Principal by Service Provider A and has agreed what method(s) of authentication they will accept.<br>4. Identity Provider A has followed Liberty guidelines for provisioning identities and has given notice and obtained consent from the Principal to use the login status and method of authentication of the Principal at Service Provider B to link the Principal's identity.<br>5. Identity Provider A has provided the Principal with an ability to locate, access, and modify the linking history from Identity Provider A.<br>6. Service Provider B has followed Liberty guidelines for provisioning identities and has given notice and obtained consent from the Principal to use the login status and method of authentication of the Principal identity at Identity Provider A to link the Principal's identity at Service Provider B.<br>7. Service Provider B has provided the Principal with an ability to allow them to locate, access, and modify the linking history. |
| **Constituents** | Principal, Identity Provider A, Service Provider B |
| **Use Case** | 8. Principal navigates to Identity Provider A and authenticates.<br>9. Principal views list of both current and previous identity links that have existed between Identity Provider A and other Service Providers including Service Provider B.<br>10. Principal selects "Service Provider B" and requests termination of link between their identity at Identity Provider A and their identity at Service Provider B.<br>11. Identity Provider A removes linking arrangement.<br>12. Identity Provider A securely informs Service Provider B that Principal requests that Principal's identity be un-linked. |

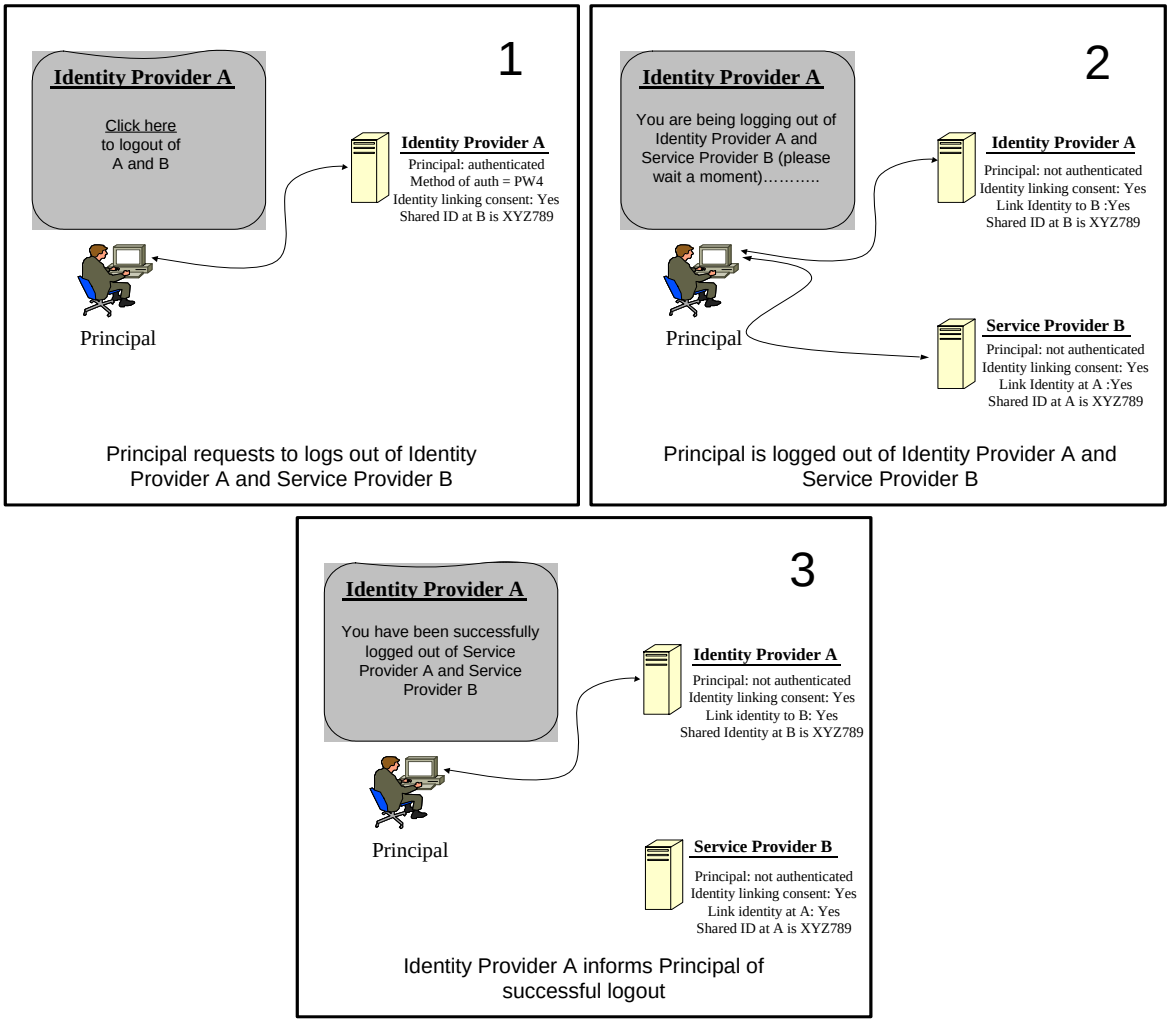
| | |
|---|---|
| | 13. Service Provider B removes linking arrangement.<br>14. Service Provider B securely acknowledges that link had been removed.<br>15. Identity Provider A confirms this change of status to the Principal.<br>16. Principal can no longer benefit from Identity Provider A authentication at Service Provider B. |

### 3.4.2 Identity Provider A and Service Provider B Terminate Business Relationship and Unlink the Principal's Identities Links

| | |
|---|---|
| **Title/ID** | Business-Initiated Termination of Linkage |
| **Pre-conditions** | 1. Principal has an identity at Identity Provider A.<br>2. Principal has an identity at Service Provider B.<br>3. Identity Provider A has entered an agreement with Service Provider B through which Service Provider B accepts authentication of a Principal by Identity Provider A and has agreed what method(s) of authentication they will accept.<br>4. Identity Provider A has followed Liberty guidelines for provisioning identities and has given notice and obtained consent from the Principal to use the login status and method of authentication of the Principal at Identity Provider A to link the Principal's identity.<br>5. Identity Provider A has provided the Principal with a secure mechanism to allow them to locate and access the linking history.<br>6. Service Provider B has followed Liberty guidelines for provisioning identities and has given notice and obtained consent from the Principal to use the login status and method of authentication of the Principal identity at Identity Provider A to authenticate the Principal at Service Provider B. |
| **Constituents** | Principal, Identity Provider A, Service Provider B |
| **Use Case** | 7. Identity Provider A and Service Provider B decide to terminate business agreement.<br>8. Identity Provider A and Service Provider B both provide notice to Principal who has consented to link their identities between A and B.<br>9. Identity Provider A removes Principal's identity link(s) with Service Provider B.<br>10. Service Provider B removes Principal's identity link(s) with Identity Provider A.<br>11. Principal can no longer benefit from Identity Provider A authentication at Service Provider B. |

## 3.5 Logging Out

### 3.5.1 Principal Logging Out



| | |
|---|---|
| **Title/ID** | Principal Logging Out (Explicitly) |
| **Pre-conditions** | 1. Principal has an identity at Identity Provider A.<br>2. Principal has an identity at Service Provider B.<br>3. Principal's identities are linked at Identity Provider A and Service Provider B.<br>4. Principal is authenticated at Identity Provider A.<br>5. Principal may or may not be authenticated at Service Provider B. |
| **Constituents** | Principal, Identity Provider A, Service Provider B |
| **Use Case** | 6. Principal ends session by logging out at Identity Provider A.<br>7. The Principal's session with Identity Provider A is terminated.<br>8. Identity Provider A securely informs Service Provider B that Principal has logged out.<br>9. If the Principal is authenticated at Service Provider B then Service Provider B logs the Principal out.<br>10. Service Provider B confirms that Principal is logged out to Identity Provider A.<br>11. Identity Provider A informs the Principal. |