Deployment Guidelines for Policy Decision Makers

Version 2.9

September 21, 2005

Editor:

Christine Varney, Hogan & Hartson
Victoria Sheckler, Hogan & Hartson

Contributors:

Piper Cole, Sun Microsystems
Peter Lord, Oracle
Yvonne Wilson, Sun Microsystems
Darrell Shull, BIPAC

Abstract:

Privacy and security are key concerns in the implementation of Liberty Alliance specifications and deployment of Liberty-enabled technologies and business models. As such, the Liberty Alliance has and will continue to provide tools and guidance to implementing companies that enable them to build more secure, privacy-friendly identity-based services that can comply with local regulations and create a more trusted relationship with customers and partners.

The following document addresses certain privacy and security related considerations businesses should take into account when deploying Liberty-enabled technology in business to consumer contexts. This document is intended to supplement the following Liberty guidance documents: "Liberty Alliance Privacy and Security Best Practices v. 2.0", "Establishing a Legal Framework for Circles of Trust-Implications of EU data protection and privacy law", and "Liberty Alliance Business Guidelines".

Table of Contents

1. Executive Summary

The Liberty Alliance Project ("Liberty Alliance" or "Liberty") has created open, technical specifications for federated network identity that provide for (i) interoperability; (ii) simplified sign-on capabilities using a federated network identity architecture; (iii) permissions-based attribute sharing to enable organizations to provide users with choice and control over the use and disclosure of their personal information; and (iv) a commonly accepted platform and mechanism for building and managing identity-based web services based on open industry standards. Liberty recognizes that privacy and security are key concerns in implementing and deploying a federated network identity solution. Liberty offers the non-normative guidance set forth in this paper to assist businesses deploying Liberty-enabled solutions with identifying and addressing certain privacy and security issues that arise in business to consumer business applications.

Liberty considers privacy and security of a principal's personal information to be extremely important, and recommends that entities implementing the Liberty specifications and deploying Liberty-enabled solutions do so in a responsible manner consistent with all applicable laws and in a manner that addresses certain baseline fair information practices. This document highlights the key decision areas that must be addressed when deploying a Liberty-enabled solution and, where appropriate, the particular Liberty specifications that may be invoked. These decision areas include: identifying the underlying business purposes for the deployment; the purposes for which data will be collected; when data will be shared; how notice is delivered and consent obtained; how data may be accessed and maintained accurately; and appropriate security concerns. This document should be read in conjunction with other Liberty publications, including the "Liberty Alliance Privacy and Security Best Practices", which offers certain non-normative best practices for addressing those issues.

Companies implementing and deploying any identity-related services or applications should consult with local counsel to ensure that the solutions they provide comply with applicable privacy and security laws and regulations.

2. Introduction

The Liberty Alliance Project ("Liberty Alliance" or "Liberty") is an unincorporated, contract-based group of more than 150 companies and other organizations from around the world. Liberty has created open, technical specifications ("Liberty specifications") that (i) enable simplified sign-on through federated network identification on all current and emerging network access devices, and (ii) support and promote permissions-based attribute sharing to enable a user's ("Principal's") choice and control over the use and disclosure of such Principal's personal information.

Liberty envisions that entities will implement the Liberty Specifications in connection with their web-based offerings. Because privacy is important in these contexts, the Liberty Specifications include the necessary features and functionality to enable an implementing entity to comply with its national privacy laws and regulations, or, in the absence of laws or regulations, best practices.

Liberty has previously offered guidance on privacy and security best practices with respect to Liberty-enabled solutions. In this paper, Liberty offers more detailed guidance to assist entities in deploying Liberty-enabled technologies in a consumer-facing context in an appropriately secure and privacy-friendly manner.

These guidelines are non-normative – they are not the rules defining the Liberty Specifications, but rather identify the privacy and security concerns that should be addressed when deploying Liberty-enabled technology. Due to the global nature of e-commerce and the myriad of laws that apply to privacy, Liberty cannot and does not (i) advise as to what laws, regulations, or fair information practices are applicable to any given entity, (ii) condition use of the Liberty specifications on adoption of a particular set of fair information practices, (iii) monitor, audit or enforce compliance with applicable laws and regulations, nor (iv) have any liability with respect to an implementing entity's use of the Liberty specifications. The

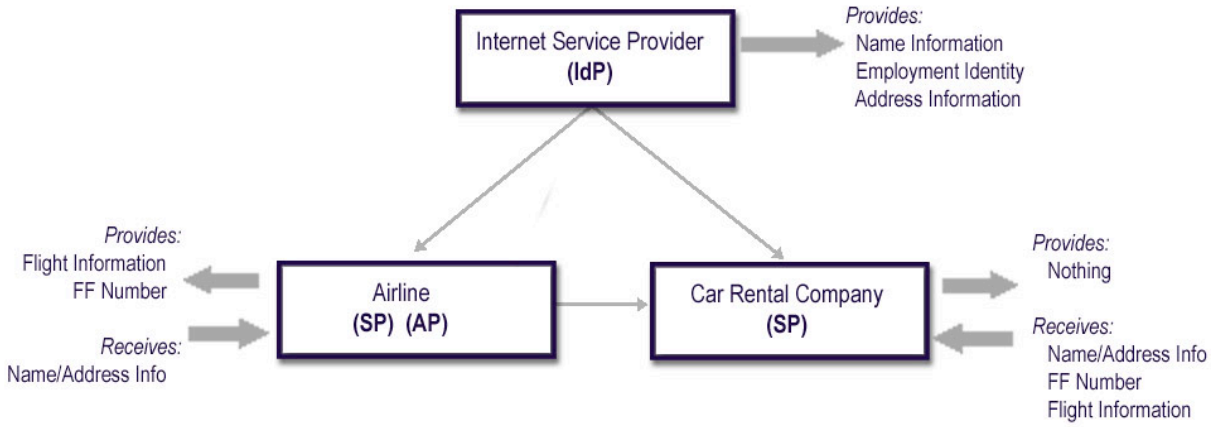
implementing entities remain responsible for monitoring implementation and, as is the case today, remain answerable to local enforcement authorities for non-compliance with applicable laws. Therefore, entities that implement the Liberty specifications are advised to consult with local counsel to ensure that the solutions they provide, based upon the Liberty Specifications, comply with applicable law.

3. Liberty's Perspective on Privacy

Liberty has offered the following baseline set of fair information practices as guidelines that companies should consider adopting when implementing Liberty specifications: notice, choice and control, access, security, quality, relevance, timeliness and accountability. Entities deploying a Liberty-enabled solution should address a variety of privacy and security related issues and concerns in order to comply with these fair information practices noted above and applicable law. In addition, data theft and identity theft are an increasing problem in society as a whole. Liberty believes that measures to combat data theft and identity theft must be taken at every point in the data chain. Improved data collection, retention, exchange and security practices and technologies must be deployed by all entities in a data chain. Technology alone, while helpful, cannot cure what are inherently bad practices. See the "Liberty Alliance Privacy and Security Best Practices" for further information.

3.1. Example Business Model

For purposes of this paper, the discussion is framed around the following business model. Three entities operating in the United States, an internet service provider, an airline, and a car rental company desire to set up and administer a single sign-on, federated experience for their adult customers, so that such customers can easily interact with each of these entities, and the entities can interoperate among themselves on the customer's behalf. In this business model, the companies would have the following roles within the Liberty framework:



3.2. Definitions

The following defined terms are used throughout this paper:

Circle of Trust ("CoT"): The "Circle of Trust" refers to the contractual relationship (or "federation") formed between the internet service provider, airline and car rental company that addresses, among other things, (i) what type of information will be shared among the companies, (ii) how and when it will be shared, (iii) how will it be treated, (iv) what security procedures will be used to maintain the confidentiality of such information, (v) how participants may join or leave the circle of trust and (vi) how the circle of trust will be administered. Liberty envisions that these companies will have business relationships based on Liberty architecture and operational agreements that address these and other concerns in a manner that permits customers to transact business in a secure and apparently seamless environment.

Principal: The Principal is the customer. As a "Principal", the customer should be able to (i) acquire a federated identity from the Circle of Trust, and (ii) make decisions about how his or her personally identifiable information ("PII") is transferred and used.

Identity Provider ("IdP"): The Identity Provider is an entity that creates, maintains and manages identity information for Principals, and authenticates and vouches for the Principal to other Service Providers. In our business model example, the internet service provider would have such identity information for the customer, and could serve as the IdP. However, it is also possible that the airline or car rental company could also serve as the IdP, for example, if the customer has a local account with the company.

Service Provider ("SP"): The Service Provider is the entity that provides the services to the customer. In our example, each of the internet service provider, airline and car rental company would be Service Providers. Liberty envisions that the Service Providers would either themselves authenticate (if they are also acting as an Identity Provider), or request that the Identity Provider authenticate, the Principal, prior to providing services to the Principal. It is also possible that the Service Provider would request attribute data concerning the Principal from an "Attribute Provider" in order to provide the requested services to the Principal. For example, the car rental company, as a Service Provider, may request that the internet service provider authenticate the Principal, and then, in order to comply with the Principal's request to credit his purchase to his frequent flyer account, the car rental company may ask the airline to provide the Principal's frequent flyer number.

Attribute Provider ("AP"): The Attribute Provider is a provider that provides attribute data regarding the Principal to Service Providers based on its own policies and the Principal's usage directives. In our example, the airline could be the Attribute Provider in connection with the car rental company's request to receive the customer's frequent flyer number.

Discovery Service ("DS"): The Discovery Service is an entity, usually an IdP, that has the ability to direct Service Providers to the relevant Attribute Provider who provides the requested classes of attributes for the specified Principal. The Discovery Service should provide such information only in accordance with the usage directives of the Principal. In our example, the internet service provider could also be a discovery service, and, for example, retain such information as: the airline has the Principal's frequent flyer number information, and the car rental company has the Principal's driver's license information.

Member: Member of a Liberty-enabled Circle of Trust.

Personally Identifiable Information ("PII"): Any data that identifies or locates a particular person, consisting primarily of name, address, telephone number, e-mail address, bank accounts, or other unique identifiers such as Social Security numbers.

4. Decision Areas

The following deployment guidelines highlight key considerations that the CoT (in this case the internet service provider, airline and car rental company) should address in federating a Principal's account for single sign-on among the entities, using the Principal's PII and sharing the Principal's PII within CoT. This paper also address certain privacy and security related risks and issues an entity should consider in (a) designing the Liberty-enabled solution, (b) federating identities within the CoT, and (c) operating and providing the online services within the CoT (including not only run-time operations, but also customer support and disaster recovery operations), along with pointers to where the Liberty Specification will help mitigate such risks.

4.1. Forming and Managing the Circle of Trust

4.1.1. Guidelines

When forming and managing a Circle of Trust, best practices for protecting a Principal's privacy and security can be designed into the CoT. What follows is a non-exclusive review of the initial issues that founding Members of a CoT may wish to consider.

4.1.2. Decision Points

- What are the goals of the CoT?
- What are each of the Members' data practices, including collection, use, transfer, and retention?
- What are each of the Members' security practices, including system security, trustedness/validity of the data collected, personnel policies, and organizational practice?
- How will the Members handle differences in their privacy and security practices? Will there be a baseline requirement to which all Members must adhere?
- How are data policies and practices communicated between the CoT Members?
- What are the CoT's guiding principles for data collection decentralization or data aggregation?
- What geographic regions and industry sectors do the Members operate in? Are there conflicts among the applicable regional or sectoral data protection laws? How will Members and the CoT comply with applicable regional or sectoral laws?
- Have Members checked with legal counsel to determine compliance with regional and industry-specific applicable laws?
- Do any of the Members have legacy identity schemes? Can the CoT identity scheme be mapped to the legacy scheme? How will conflicts between the identity schemes be handled?
- Have the Members executed all necessary and appropriate contracts and agreements?
- How is liability handled? Who handles notification to the consumer and/or service provider?

4.2. Business Purpose(s) of Data Collection

4.2.1. Guidelines

It is important to understand and clearly articulate the business purpose and goals of the CoT. Data may then be collected, used, and secured in accordance with these business purposes. Identifying the business purpose will also help to inform the notice and consent language displayed to the Principal.

4.2.2. Decision Points

- What are the Members' goals in forming or joining the CoT?

- What data consent, collection, use, retention, and storage activities are necessary to meet the CoT's goals?
- Have the Members or the CoT identified an "owner" for each activity (there may be multiple owners across entities)?
- Have Members involved their privacy officers, technology department, legal, and HR or other responsible internal parties when forming or joining the CoT?
- Does the CoT documentation reflect the articulated business purposes?

4.3. Relevance of Data Collected and Shared

4.3.1. Guidelines

Some of the most important and preliminary questions facing a CoT when designing a Liberty-enabled deployment revolve around the CoT's and its Members' data practices. The CoT needs to consider what data is needed for the identified purpose, how will it be collected, by whom, where will it reside, how will it be controlled, how will it be shared, what controls will there be in sharing, when will consent be required, and what each Member's role will be in connection therewith. A key privacy principle to keep in mind in considering these questions is data relevance.

To put into practice the principle of relevance in a Liberty-enabled solution, Members should embrace data minimalization and data decentralization practices. Members should limit the PII collected to that reasonably necessary for the primary purpose for which such information is given. For example, a Principal's meal preferences should not be available to the car rental company when a Principal reserves a car. Members should also use PII only for the purpose for which it was collected, or purposes for which the Principal has consented. Members should share PII only to the extent that the Principal has provided consent and then only to the extent necessary to fulfill the primary purpose for which the consent has been given. Generally, if the PII is not relevant for the primary purpose for which the information will be used, such PII should not be collected or shared.

Limiting data collection to relevant information may help minimize the opportunities for successful identity theft. In addition, keeping data in a disaggregated manner further limits opportunities for identity theft. In order to implement a decentralized approach, the Members will need to determine, considering relevance as a primary factor, which Members will be the custodians of which type of data (i.e., who will be the attribute provider for such data) and for how long, and under what general guidelines (subject to receipt of permission from the Principal) each Member may request such information from another. The Members will also need to consider how, whether and when a Member may ask the Principal for information directly.

Liberty Specifications Can Help

Detailed data models for employee and personal profiles, as well as specialized models for other integrations, have been published by the Liberty Alliance and are listed below.

The following table summarizes some attributes available in the Personal Profile data models. This and other models can be used as CoT Members work on the business agreements by focusing the conversation on the information that is most relevant to the business purpose. Please note that not all of the data elements noted below may be used in every business case, and specific implementations may choose to develop additional extensions to this data model that should be considered in a deployment roadmap.

Many of these attributes are of particular interest and concern to privacy and should be handled with care. Decision makers may wish to include other departments, including technical resources and privacy officers, when mapping data to activity requirements.

Liberty Attribute Container	Brief Description
Informal Name	Screen name of the Principal
Common Name	Principal's nickname – name used in everyday situations May include attributes such as *title* and *full name*
Legal Identity	Official Legal identification of Principal May include attributes such as *title* and *full name*, as well as *date of birth* and *unique identifying numbers*
Employment Identity	Minimal Employer and employment details
Address Card	Address card for Principal May include attributes such as *postal address* and *postal code*
Message Contact	Generic phone, email or instant messaging contact May include attributes such as *phone numbers, email addresses,* and *IM addresses*
Façade	Principal's look and sound façade May include attributes such as the principal's photo, web site, how the name is pronounced, and greeting sounds
Emergency Contact	Next of kin or other person to contact if Principal has medical emergency May include attributes such as *full name, postal address, phone numbers, email addresses*, and *IM address*
Extensions	An element that can contain arbitrary content from miscellaneous attributes

Due to the complexities of various privacy laws and guidelines, custodians of data must look at the impact of inadvertent or improper disclosure of combinations of multiple data elements, rather than just individual data elements. For example, any one of the below data combinations may be an improper disclosure:

- Individual elements of a Principal's name when used in conjunction with other information that would point at a specific person; or
- DOB, in conjunction with individual's name; or
- Postal address, in conjunction with name that would identify/point at a specific individual.

Others elements of concern in a consumer driven example include financial information (credit cards, checking account numbers, pin numbers, etc); Social Security Number or National Identification Number; Passport Number; Driver License Number; medical information; E-Mail address (sensitive in a spam context); and phone numbers (sensitive in a telemarketer context).

4.3.2. Decision Points

- Is PII necessary for the business purpose?
- Is the data collected and stored essential to the activity?
- Which data model(s) are appropriate for the activities of the CoT?
- Can the stored data be used to recreate history for an individual without consent?
- Can any single data attribute convey unintended PII?
- Can a photo provide a biometric?

- Can individual data attributes be aggregated?
- Have the CoT Members taken all reasonable steps to avoid wholesale data theft or individual identity theft?

4.4. Notice to the Principal

4.4.1. Guidelines

Consumer-facing Members should provide clear notice to the Principal of who is collecting the information, what information they collect, how they collect it (e.g., directly or through nonobvious means, such as cookies), how they provide choice, access, security, quality, relevance and timeliness to Principals, whether they disclose the information collected to other entities, and whether other entities are collecting information through them. Providing notice is particularly important for Service Providers who may seek additional information beyond what is provided through other Members.

Liberty believes that any notice should at minimum satisfy the following requirements:

Accessibility: The notice must be clear, easy to read and understand, easy to locate, and continuously be available to the Principal.

Timeliness: The notice should be presented to the Principal prior to any collection, receipt or transfer of any PII.

Include Necessary Information: The notice should address (i) who is collecting the PII, (ii) for what purpose, (iii) how it will be collected, (iv) how it will be used, (iv) if, when, and how it will be transferred, (v) what choices the Principal has with respect to the collection, use, and transfer of PII (and what are the consequences of the possible choices), (vi) how the Principal may access and verify the accuracy of the PII, (vii) how the PII is stored, and what security measures are taken to protect it, and (viii) what the Member's policies are with respect to ensuring the quality, relevance and timeliness of the information, and when the information is removed from the Member's databases. (*See* Privacy Best Practices document for additional guidance.)

4.4.2. Decision Points

- How will notice be provided?
- How detailed is the notice or what is legally required in the notice?
- Are there legal or regulatory exceptions to notice and disclosure?
- What are the various current or potential future uses of the data?
- Have potential future uses of the data been disclosed and consent obtained?
- Are there regulatory requirements regarding future data uses?
- Is third-party sharing of data necessary, permitted, or required?
- What is the process for changing the terms of notice or consent?
- What is the process to notify Principals if data is compromised?

4.5. Choices and Consent of the Principal

4.5.1. Guidelines

Consumer-facing Members that maintain PII should obtain the Principal's consent for the data collection and use. Liberty recommends consent be both verifiable and auditable.

Consumer-facing Members should offer Principals choices, to the extent appropriate given the circumstances, regarding what personally identifiable information is collected and how the PII is used beyond the use for which the information was provided. In addition, when appropriate (such as in the case of a consumer-facing enterprise), Members should allow Principals to review, verify, or update consents previously given or denied. The Liberty Specifications provide for both access permissions to allow a Principal to specify whether and under what circumstances a Service Provider can obtain given attributes, as well as an "envelope" for usage directives that contain the permissions for attribute use and sharing. Both aspects of the privacy capabilities (e.g., access and usage) established by the Liberty Specifications should be fully implemented in a manner that is easy for the Principal to configure. Members should consider supporting usage directives through either contractual arrangements, or through the use of Rights Expression Languages.

4.5.2. Decision Points

- Is consent necessary? Is there a legal basis for lack of consent?
- Is consent explicit or implied?
- Is consent revocable?
- Is consent auditable?
- How much control over the data use resides with the Principal? Can services be partly or wholly turned on or off? How often can changes be made?
- Has the Principal consented to all anticipated data uses?
- Is the consent reasonable and informed?
- Is there consistency between online and offline consent, and if not, how are conflicts resolved?
- How are conflicts between consent provided or not provided to Members resolved?

4.6. Access and Accuracy of the Data

4.6.1. Guidelines

Consumer-facing Members that maintain PII should offer a Principal reasonable access to view the non-proprietary PII that it collects from the Principal or maintains about the Principal. While access should not be construed to require access to proprietary data, public record data, or aggregate data, access should be available to all PII that is collected by the Member. As noted above, a Principal should also have quick and easy access to the choices he or she has made with respect to the uses and sharing of his or her PII.

Members that collect and maintain PII should permit Principals a reasonable opportunity to provide corrections to that PII. "Reasonable opportunity" means that a Principal should be able to review and

correct the PII quickly and easily. As noted above, a Principal should also be able to quickly and easily review and modify or revoke his or her choices with respect to the uses and sharing of his or her PII.

If a Principal corrects or modifies any PII or any of his choices or usage directives, the Principal should be given the option of having the corrected or modified information shared with the relevant Members of the CoT.

4.6.2. Decision Points

- How is the Principal's identity authenticated for the purposes of updating data?
- How do you verify data provided by the Principal?
- How does the CoT provide Principals or Members access to review data? How may data be modified, updated, or deleted?
- How does the CoT provide updated data between Members? How are conflicts reconciled?

4.7. Security

4.7.1. Guidelines

Members should take reasonable steps to protect and provide an adequate level of security for PII. The security measures used should include technological, procedural, organizational and contractual standards. In addition, Members should guard against fraud, misuse and accidental loss or "data leakage." Each Member should understand the other Member's security practices and the associated risks. The Members should negotiate security practices, and then consider what data will be transferred in light of each Member's security practices. The Members should consider setting standards for the following: session management/time out requirements, levels of encryption, strength of authentication mechanisms used, invalid password attempts lockout, lockout intervals, conditions such as hours of allowed access or source IP addresses/firewall rules, practices around authorized personnel, auditing frequency and areas, forced password change frequency, password minimum standards, practices for validating user before password resets, procedures for validating data, especially that used for entitlement, and software change management practices.

The security measures should comply with applicable law and be consistent with industry standards. The appropriate level of security will depend upon the nature and sensitivity of the PII at issue and the manner in which it will be used and/or shared. In general the more sensitive the data, the greater the security measures that should be implemented. For particularly sensitive information, such as health or financial data, there should be specific access controls implemented. The security measures to be used should be considered and implemented both at the time of system design as well as at the time of data collection, use and/or transfer. The security measures used should be continually assessed as new technologies become available and security risks become known. The parties should consider adoption of international security standards as a baseline, such as ISO 17799.

In addition to informing the Principal of the security measures taken, Members should also warn Principal of any significant security risks before the Principal is requested to provide PII.

4.7.2. Decision Points

- Is the Chief Security Officer and Chief Privacy Officer early in the decision making process?

- What are the security policies of all Members of the CoT and do they conform with the CoT standards?
- How are modifications to a Member's security policy implemented?
- How often is a security audit performed, is the audit independent, and how are deficiencies remedied?
- Is the data secured according to best practices? Is personnel access to sensitive systems restricted? Are offsite backup facilities also secured?
- Does the cross-entity communication system meet the chosen specifications for security?
- Are security systems redundant and in a high-availability environment?

4.8. Complaint Resolution

4.8.1. Guidelines

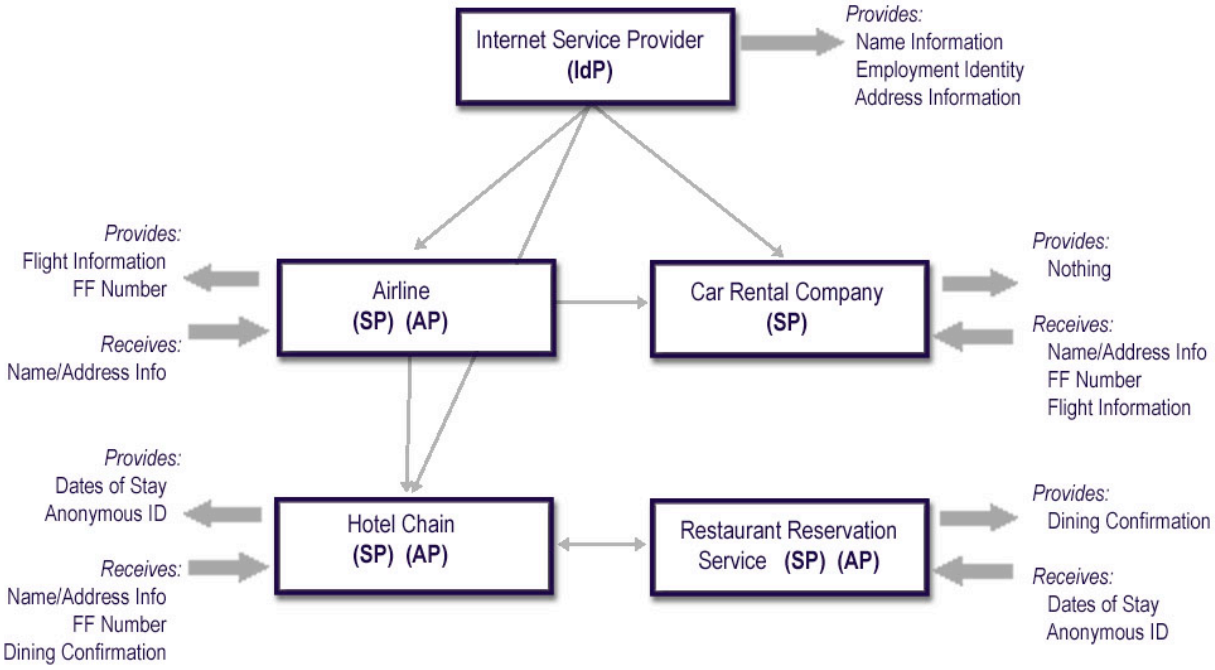
Members should offer a complaint resolution mechanism that is clear, easy to access and without cost for Principals who believe their PII has been mishandled.

4.8.2. Decision Points

- Do you have a complaint resolution process?
- Is the complaint resolution process easily accessible and timely?
- What are the regulatory requirements for complaint resolution?
- Is there harmonization across jurisdictions?
- How transparent is your complaint resolution process?

5. Alternate Business Model

A Circle of Trust need not be limited to two or three Members. The following alternate business model diagrams a Circle of Trust consisting of five Members providing expanded services to a Principal. In deciding the relevance of collected and shared data, decision makers should carefully determine the overall data needs, and then decide the minimum set of attributes needed by each company. Note that the added restaurant reservation service receives no personally identifiable information from the Principal.



All decision points identified in section 4, supra, would now be addressed by the two new Members.

6. The Application of Liberty Specifications

The Liberty architecture provides many specifications that influence the way data is shared across multiple Members. These include encryption, usage, audience, and consent capacities to enable both the asserting and relying parties to comply with the privacy requirements of their respective roles in a federation.

Interaction Service: The interaction service provides a means for an Attribute Provider (AP) to request that a Service Provider obtain consent from a Principal, for the AP to release the requested attribute. This is important in the event that the consents held by the AP do not cover the requested attribute release.

Consent Header: The consent header in an attribute request carries an indication of whether consent has been obtained from the Principal, in order to authorize the release of, or enable the recordation of, the release of PII.

Usage Directives: Attributes may be coupled with usage directives, which provide permissions to the AP for the use and sharing of that attribute. Members are strongly urged to:

- Identify and reference a rights expression language (REL) to have a common language for the retention and use of the PII being exchanged; and
- Provide audit and log capability to document compliance with privacy requirements

Message Transport Protection: Liberty specifications strongly suggest transport protection for attribute requests and responses, even those on otherwise 'trusted' networks.

Principal Identifier Uniqueness: In order to ensure the prevention of third party Principal correlation (collusion), the Principal (subject) identifier 'nameIdentifier' in SAML 2.0 should always be unique for every pair-wise federation. This is precisely laid forth in Liberty ID-FF v1.2, and is preserved in SAML v2.0.

NameIdenitifier Mapping Encryption: ID-ff v1.2 and SAML v2.0 provide mechanisms for the protection of nameIdentifiers (EncryptedNameIdentifier), when service providers request interaction with other service providers in the federation. Specifically, implementations MUST implement support for this capability in order to prevent potential collusion between service providers.

Decentralized Attribute and Discovery Authorities: Liberty ID-WSF allows the PII of a Principal to be distributed across many Service Providers. The capacity allows Service Providers in the federation to retain (and make available) only the necessary PII attributes that are appropriate for them to retain. For example, banks retain credit card information, shipping entities maintain 'ship to' address information, and airlines retain affinity membership identifiers.

This distribution of authority allows Services Providers who need PII for a specific transaction to request, then discard, this information, rather than forcing them to retain (other than for audit/tracking purposes) this PII.

The Liberty ID-WSF Discovery Service (DS) can also operate as a separate entity (e.g., not operated by the IdP), and thus can act as an intermediary between the Service Providers and the IdPs in a federation. This intermediation minimizes the number of transactions the IdP is a party to, and enhances the privacy properties of the federation as a result.

7. Other Data Services

Liberty has published implementation guidelines for other services that may provide guidance for your specific application. Broadly speaking, these services are built on specifications within the "Liberty Identity Web Services Framework" (ID-WSF). ID-WSF provides the framework for building interoperable identity services, permission-based attribute sharing, identity services description and discovery, and the associated security profiles. A brief discussion of these services and the issues associated therewith is described below.

7.1. Geolocation

Location-Based Services are applications that provide content or services to a person based on a combination of their registered personal profile and their location – often relative to some other location. Location-Based Services will likely bring many advantages to end-users. Notwithstanding this potential value to users, such services introduce new privacy risks that must be addressed. The portability and increasing ubiquity of mobile devices, coupled with the ability to determine their location (and consequently the owning user) pose new risks for abuse. While these applications promise significant benefit to end users, the potentially sensitive nature of location information requires that the privacy issues be addressed.

7.1.1. Decision Points

- Since a device must be "on" to give consent, and location can be transmitted as soon as the device is turned on, how may a user exercise control over choices?

- If geolocation is added to our example business model, should the rental car company have access to the Principal's location, direction, and speed?

- Have you informed users about the possibility of coincidental geolocation service?
- If external requirements regarding data retention are available or required, can the user be given notice about what controls are offered?

7.2. Contact Book

The Liberty Contact Book Service Specification defines a Liberty identity service that supports information regarding the Principal and his or her contacts. The information regarding the Principal is stored in a unique card called “My Card” or “Self Card.” This card is not intended to substitute for the Liberty ID-SIS Personal Profile Service, as the Contact Book service also allows the Principal to manage contacts for private and business acquaintances, friends, family members, and even for him or herself. The Principal can also create a Distribution List in order to simplify the management of his or her contacts.

7.2.1. Decision Points

- Should a Contact Book service have access to geolocation data, and under what circumstances?
- What provisions are available in a CoT to determine the necessary permissions on the use of names in Contact Book?
- In multiple CoTs, what rules might you apply to sharing between circles?
- Can you select specific Contact Book data for sharing, such as email vs. regular mail, or business phone vs. home phone?
- Have you determined how to maintain the wishes of the data owner regarding how their data is redistributed?
- How do you reconcile differences in Contact Book among other people in your CoT?

7.3. Presence Service

Presence information, by its very nature, is fairly sensitive. Even a simple on/off presence indication allows a watcher to have an idea of where a user may be and his or her typical schedule. When detailed status information – for example geolocation data – is added to the presence information, control of the data becomes even more of a concern.

7.3.1 Decision Points

- How does your Presence Service interact with geolocation or other services?
- How much data do you want to communicate and what might be unintended uses of that data?