



Liberty Alliance Contractual Framework Outline for Circles of Trust

Editor:

Victoria Sheckler, Hogan & Hartson

Contributors:

Piper Cole, Sun Microsystems
Peter Lord, Oracle
Joseph Alhadef, Oracle
Robin Wilton, Sun Microsystems
Jane Winn, University of Washington School of Law
Colin Wallis, SSC, New Zealand Government

Abstract

This document provides guidance on suggested business structures and terminology for a Liberty enabled technology deployment necessary to create a legally binding Circle of Trust (CoT). Its purpose is to facilitate a Liberty enabled deployment of identity management specifications and technology by assisting stakeholders and their legal and executive management teams in the identification of the legal structure best suited for their deployment. Such structures and contractual agreements among participating parties serve to create a trusted and legally binding relationship among the participants.

This document describes the rationale for using a contractual framework for the Circle of Trust, offers practical guidance for developing those contractual frameworks, discusses considerations that should be taken into account in selecting and structuring the contractual framework, and describes other Liberty guidance documents that may be useful as references or starting points for terminology and certain other aspects of the contractual framework. This document is intended to supplement other Liberty guidance documents.

1. Introduction

Liberty Alliance (or “Liberty”) has developed and continues to develop specifications, guidelines and educational materials to help businesses, governments, and individuals establish and operate solutions for federated identity and identity-based Web services and applications. Liberty specifications offer substantial benefits, including choice, convenience, and control over what types of identify information are shared, and how such identity information is shared and used.

In connection with a Liberty specification enabled deployment, Liberty recommends that the parties implementing the specifications establish a legally binding Circle of Trust (“CoT”) by committing to abide by certain agreed upon obligations, rules, and remedies that will govern their relationship. Liberty envisions that the CoT will take some contractual form that is legally enforceable.

The purpose of this document is to facilitate a Liberty enabled deployment of identity management specifications and technology by assisting stakeholders and their legal and executive management teams in the identification and development of the legal structure best suited for the deployment. This document describes the need for a contractual framework, suggestions as to what should be addressed in the contractual framework, offers practical guidelines for developing those contractual frameworks, discusses considerations that should be taken into account in selecting and structuring the contractual framework, and describes other Liberty guidance documents that may be useful as references or starting points for terminology and certain other aspects of the contractual framework.

This document is not intended to provide legal advice. Given the global nature of e-commerce and digital information sharing, the myriad of laws that apply, and the fact that the Liberty Alliance itself does not provide any services, the Liberty Alliance cannot and does not (i) advise as to what laws, regulations or fair information practices are applicable to any given entity or relationship among entities, (ii) condition use of the Liberty specifications on adoption of a particular set of laws or 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 or any Liberty guidance documents. 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 and establish contractual frameworks for their CoTs are advised to consult with counsel to ensure that the solutions they provide, based upon the Liberty specifications, comply with applicable law.

2. Why use a Contractual Framework and What Should it Address

As noted above, Liberty recommends that the parties implementing the specifications establish a contractual framework for a legally binding CoT that obligates the parties to abide by certain agreed upon obligations, rules, and remedies that will govern their relationship.

The purpose of these contractual agreements is to:

- set forth the agreed upon rules, policies, obligations, procedures, risk allocation, and remedies that will govern the (a) relationship among the participants, (b) relationship between the users of a participant’s services within the federated structure and the

- participants, (c) use, storage, protection and sharing of identify information, (d) the administration of the CoT, and (d) technical implementation of the Liberty specifications,
- act as a legal buttress to the operational rules and technical standards implemented using the Liberty specifications, and
- provide participants with legally enforceable remedies in the event a participant does not abide by the agreed upon rules, policies, obligations and procedures.

To ensure for a robust relationship among the participants, Liberty recommends that the parties address the following issues in their contractual agreement(s) (in addition to implementing the agreed upon operational rules and technical standards, to the extent applicable, through the Liberty specifications):

- **Terminology:** What terminology will be used by the parties to describe the CoT, their relationship, and the rights and obligations of the parties? Will the parties reference Liberty published terminology? Please see Section 5 to this document for a discussion of such terminology.
- **Roles, Rights and Obligations:** What are each party's roles and attendant operational rights and obligations within the CoT? Do these arise out of a mutually recognized source, such as legislation, an industry code of conduct, accepted best practice, Liberty guidance documents, or other sources?
- **Privacy & Security:** What are the privacy and security standards that apply?
- **Confidentiality:** What level of confidentiality obligations should be imposed on the participants?
- **Technical Interface:** How will the technical interface and other standards be established, communicated, and implemented?
- **Service:** What are the minimum service levels that will apply? Will they be targets or minimum obligations?
- **Other Rules and Policies:** What other rules and policies will apply to the CoT? Please see Section 4 of this document for suggested categories of rules and policies that should be addressed.
- **Governance, Version Control and Change Management:** Who will be responsible for day-to-day governance of the CoT? How will the parties communicate regarding operational issues that arise? How will changes to the rules, policies, and/or main contractual agreements be approved and implemented? What audit/verification/certification rights should each participant have?
- **Enforcement; Remedies:** How will the rules and policies be enforced? What dispute resolution mechanism should be used? What remedies will be available to the participants in the event the rules and policies are not followed?
- **Intellectual Property:** Who will own any intellectual property that might be created as a result of the deployment?
- **Liability and Risk Allocation:** What should the risk allocation be among the parties and what liability should each participant reasonably bear? How does each participant's role, scope of activities, and level of control in the CoT affect the risk allocation?
- **Indemnification:** Under what circumstances, if any, participants have indemnification rights for the acts or omissions of the other participants?
- **Insurance:** Should there be any minimum insurance requirements?
- **Entrance and Exit of Members:** Under what circumstances may (i) a new participant be added to a CoT, (ii) an existing participant terminate its involvement in a CoT, and (iii) may the other participant(s) have a participant removed from the CoT?

Liberty believes that having such a legally enforceable framework as a buttress to the Liberty enabled deployment will help ensure compliance with such rules and obligations among the participants. Ultimately this combination of technical implementation of the rules using Liberty specifications and a legally enforceable contractual framework will lead to a more robust and trustworthy CoT.

3. Organizational Models

3.1 Introduction to Models

Below are three approaches to the contractual framework for establishing a CoT among parties implementing Liberty specifications. Each of these organizational models contemplates that various rules, regulations, policies, and guidelines will be developed, implemented, and enforced by the initial organizers of the CoT (the “Founders”) to govern their ongoing relationship with and among CoT participants (the “Members”).

Collaborative Model. As depicted in the diagram below, a group of Founders forms an entity that establishes the rules for the operation and governance of the CoT, and then also undertakes the day-to-day governance of the CoT. This approach is perhaps the most complex, but arguably provides the most flexibility for a large CoT with many Founders and fluctuating membership – and once the initial work has been done to establish the Governing Entity, this model provides a single consistent entity with which to contract.

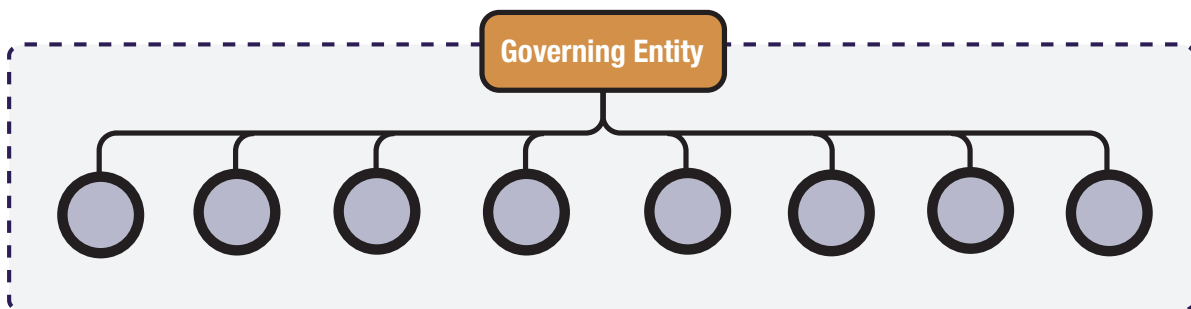


Figure 1: Collaborative Model

Consortium Model. A small number of Founders forms a consortium via a multi-party contract that sets the rules and governance for the CoT. This approach offers more direct control by each of the Founders. However, this model is not recommend where the membership is in flux, as the ongoing entrance or exit of members of the CoT is likely to be cumbersome and require amendment to the consortium agreement. Following is a diagram of this approach.

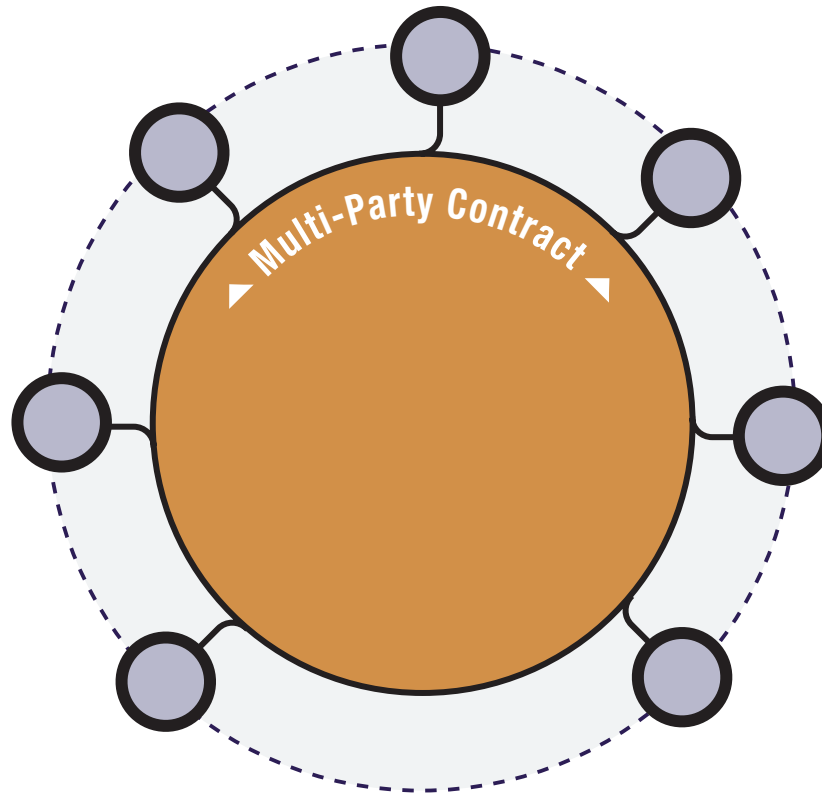


Figure 2: Consortium Model

Centralized Model. A single Founder sets the rules and governance for the CoT, and contracts individually with each other Member. This approach provides the Founder with a significant amount of control, and significantly less control to the other Members. As the diagram below implies, the Founder may use this model to establish two-party relationships, n-party relationships, and relationships in which it (the Founder) acts as an intermediary between other entities (partners, suppliers, customers and so on).

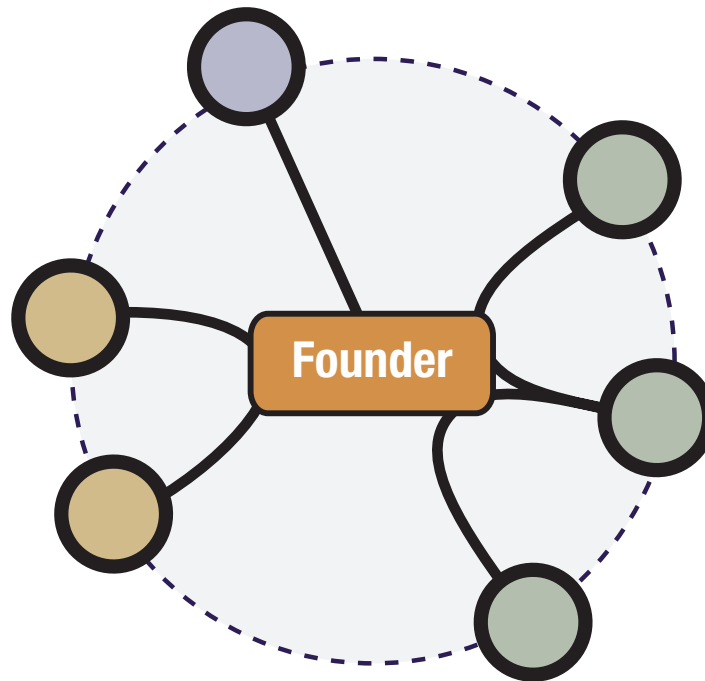


Figure 3: Centralized Model

Below please find a more detailed description of each model, followed by a list of considerations Founder(s) should consider in selecting the business model for their CoT.

3.2 Collaborative Model

The Collaborative Model is appropriate for (a) a large CoT in which the parties anticipate that Members will be entering and exiting the CoT over a period of time; (b) no one participant wants to bear the burden for establishing, governing, and enforcing the CoT, and (c) the parties are willing to take on the expense in forming and funding a separate entity to establish, govern, and enforce the CoT. The Collaborative Model also has the advantage of shifting some risk and liability from the Founders to the newly established entity and permitting the Founders to use (to some extent) the newly established entity as a liability shield.

The Collaborative Model is less appropriate for a smaller and more stable CoT where the membership is not in flux, where the parties do not want to expend the funds necessary to set up and operate a separate entity, where only one party will be establishing the rules and will govern the CoT, or where the parties desire a simple contractual mechanism for establishing direct contractual privity and enforceability vis a vis each participant.

Under the Collaborative Model, the Founders will agree via some form of formation agreement to organize a separate entity (“NewCo”) to establish the rules and policies of the CoT, and to govern and manage the CoT. The rules, policies, and governance model for the CoT will be established and set forth in separate documents developed by NewCo or by adoption and reference to relevant Liberty guidance documents (modified as applicable for the CoT).

Liberty anticipates that such a formation agreement would address, among other things:

- the establishment of a committee(s) responsible for the adoption of such rules and polices (including participation eligibility criteria, operational and technical rules, interface requirements, minimum standards, etc. further described below) and the day to day governance of the CoT,
- what matters would be left to the committee versus what matters would require Founder approval, and
- the procedures and criteria for permitting new Members and removing existing Members.

In addition, there will be a participation component that will require each Member in the CoT to adhere to the rules, policies and procedures of the CoT adopted by NewCo. The participation component could either be included in the formation agreement or, more likely, be implemented via separate participation agreements between NewCo and each Member of the CoT.

Liberty anticipates the participation agreement would address, among other things:

- the right of the Member to participate in the CoT (including the scope of such participation),
- the obligations on the Member to adhere to the agreed upon rules and procedures,
- how audits and verification will be handled,
- any payment or other covenants or considerations unique to the relationship between such participant and NewCo, and
- other operational and risk allocation matters.

Under this model, new Members to the CoT could be added either by making the new participant a member of NewCo or by having the new participant enter into a participation agreement with NewCo.

If appropriate, NewCo could also establish forms of affiliate agreements to be entered into solely among the Members (based on the Member’s role) governing the exchange of information among the Members and providing for the direct liability of each Member to the other Members. The primary purpose of such affiliate agreements would be to establish direct contractual privity between the Members (outside of the formation agreement) so that such Members have a direct contractual mechanism to enforce key obligations (such as data security and data sharing) among themselves. Alternatively, these issues could be addressed in the other documents noted above, with dispute resolution handled pursuant to the dispute resolution mechanism established by NewCo.

3.3 Consortium Model

The Consortium Model may be appropriate for (a) a small CoT in which the parties do not anticipate that Members will be entering and exiting the CoT over a period of time; and (b) no one participant or entity is to have primary control over the CoT. It has the advantage of offering each of the participants more direct control over the CoT and providing direct contractual privity among all of the participants through one consortium agreement.

The Consortium Model is not recommended for situations in which the participants may be entering or exiting the CoT because each entrance/removal likely will require an amendment to the consortium agreement. It is also less appropriate in situations where the parties desire to take advantage of the liability shield offered by forming a separate entity to establish the rules for, and govern, the CoT or where one party desires to have primary control of the CoT.

Under this model, the CoT participants enter into a multi-party consortium agreement that will form a steering committee to establish the rules, regulations, policies, and guidelines of the CoT, and to manage the governance of the CoT. The consortium agreement will include some of the elements of the “formation agreement” and the “participation agreement” described above. For example, Liberty anticipates such a consortium agreement would address, among other things, the roles of each participant, each participant’s rights and obligations, establishment of the steering committee(s) and the scope of the authority and responsibility of the steering committee(s), governance issues (including day to day management as well as version control and change management), audit and verification rights, and other operational and risk allocation matters.

3.4 Centralized Model

The Centralized model may be adopted in situations where (a) the CoT is being established primarily for the benefit of one party or business entity; and (b) that sole Founder desires to have increased control over the CoT.

This model is less appropriate in situations where other Members desire to have a stronger voice in the establishment of the rules and policies governing the CoT, where the Founder(s) desire to take advantage of the liability shield offered by setting up a separate entity to establish the rules and policies for and to govern the CoT, or where the parties desire to share the burdens (and cost) associated with establishing and governing the CoT.

Under this model, the Founder takes the role of NewCo under the Collaborative Model, and independently establishes the rules, regulations, policies, and guidelines for the operation of the CoT. The Founder is also responsible for the operation and management of the CoT. As the sole operator, the Founder will contract individually with each participant to the CoT under a participation agreement substantially similar to the participation agreement contemplated in the Collaborative Model above, requiring each CoT Member to comply with the rules, regulations, policies, and guidelines established by the Founder. For the reasons noted above, if appropriate, the Founder may also wish to establish forms of affiliate agreements to be entered into by the other participants to govern the security and sharing of information among the participants, and the allocation of risk and liability directly among such participants.

3.5 Considerations for Selection of Model

Each of these models should be evaluated in light of considerations including:

- **Founders.** How many Founders plan to establish the CoT?
- **Control.** How much control do the Founders wish to maintain over the CoT?
- **Administration.** How many Founders will administer the CoT and what are their interests?
- **Resources.** How much time and resources do the Founders plan to dedicate to the ongoing maintenance and administration of the CoT?
- **Membership.** Will the number of Members in the CoT change over time?

- **Jurisdiction.** What are the applicable legal jurisdictions in which the Founders and Members are located and/or doing business?
- **Business.** What type or class of business is to be conducted within the CoT?
- **Economic and tax Considerations.** What are the economic and tax considerations applicable to the venture?
- **Privacy, Security & Other Applicable Laws.** What is the impact of applicable privacy and data security, labor, antitrust/competition, intellectual property and other laws and regulations?

For example, if the Founders wish to enter into a legal business relationship for the operation and control of an ongoing CoT with fluctuating membership, a Collaborative Model may be appropriate. If there is a small group of Founders who wish to maintain control over the CoT, the group may choose a Consortium model rather than organizing a separate company under the Collaborative Model. If a single party intends to organize and maintain the governance and operations of the CoT, the Centralized approach may be selected.

Additionally, the jurisdiction(s) in which the CoT operates and the class of business (whether business to consumer, business to business, government to business/customer, etc., and whether involving industries with sensitive personal data) will dictate what applicable laws and customs apply, and whether and to what extent the parties can contractually agree to operate under an agreed upon choice of law. The agreed upon economics for the Founders and Members, and associated tax consequences, may also drive the selection of the contractual framework. Finally, regional variations in applicable law may dictate that one approach should be favored over another for use in the jurisdiction.

4. Terminology, Rules and Policies Applicable to any CoT

In each of the models described above, a party (or parties or a subset thereof) will need to define the terminology, rules and policies needed to establish and operate the CoT. These may include the following:

- i. *Terminology*
 - a. Definitions of roles/types of participants and end users with the CoT
 - b. Definitions/classifications of the types of processes that can be performed
- ii. *Business Rules*
 - a. Responsibilities/Obligations/Rights of each role/type of participant
 - b. Transparency standards
 - c. Audit/verification rights
 - d. Enforcement procedures
 - e. Liability for non-conformance
- iii. *Privacy and Security Requirements*
 - a. Establishment of privacy floor (restrictions on use/sharing of personal information, minimum guidelines on rights to be afforded to end user regarding data integrity, verification, options regarding use)
 - b. Rules for sharing of personal information; implementation of usage directives, etc.
 - c. Rules for transborder data flows (if applicable)
 - d. Technical, operational and administrative security and authentication standards
 - e. Incident notification/response

- iv. *Technical Standards*
 - a. Interface standards
 - b. Implementation requirements
 - c. Communication standards
- v. *Operational Rules*
 - a. Performance standards / service levels
 - b. Service levels
 - c. Project management / day to day governance
 - d. Version Control and Change management, including standards and mechanism for acceptance of changes (i.e. is electronic acceptance sufficient/enforceable, what type of electronic signature, etc.), and procedures and standards for implementation of accepted changes.
- vi. *New Participant Eligibility Requirements (if applicable)*
- vii. *End User Interface Requirements*
 - a. Minimum flow-down provisions for end user / subscriber agreements
 - b. Consistency regarding look/feel/style/branding of end user experience (to the extent appropriate)

5. Liberty Resources to Assist with Development of Terminology, Rules and Policies for the Contractual Framework

Liberty has, and intends to continue to develop and publish guidance documents that either offer sample approaches based on certain use cases, provide additional guidance, or describe decision points that should be considered, in addressing the terminology, rules, policies and guidelines noted above. This guidance includes the following:

- i. *Liberty Glossary*. The Liberty Glossary provides a common set of Liberty specific terminology that can be used as a basis for defined terms used in, or incorporated by reference within, the contractual agreement(s) to ensure that the participants using a common and Liberty compliant set of terms when describing the roles, classifications and other terms used within the Liberty architecture.
- ii. *Liberty Specifications and Related Service Implementation Guidelines*.
- iii. *Deployment Guidelines for Policy Decision Makers* (September 21, 2005). This document addresses certain privacy and security related considerations participants should take into account when deploying Liberty-enabled technology in business to consumer contexts. It provides a list of decision points participants should consider in establishing some of the rules and policies identified in Section 4 of this document.

Liberty recommends that participants review the guidance noted above, and if appropriate, incorporate by reference the applicable Liberty documents addressing terminology, specifications, and other guidance. Please note that if the documents are incorporated by reference, the participants will also need to address how to approve, adopt, and implement updates and modifications to such documents (such as updates to the Liberty specifications, etc.). Liberty anticipates that the procedures for handling this will be set forth within the governance, version control, and change management procedures to be included within the contractual agreements.

For additional background information and guidance on Liberty specifications and Liberty enabled identity federated and identity-based web services deployments please see the other resources available at <http://www.projectliberty.org/resources>.

6. Summary

Liberty has developed and continues to develop identity federation based specifications, guidelines and educational materials to help businesses, governments, and individuals establish and operate solutions for identity federated and identity-based web services applications. Liberty anticipates that participants to a Liberty enabled deployment will enter into contractual relationship(s) that delineate their rights, obligations, remedies, and allocation of risk with respect to the deployment. This document provides guidance on addressing contractual relationship structures that will likely be part of every Liberty enabled deployment, and provides practical outlines and checklists for developing those contractual relationships.