

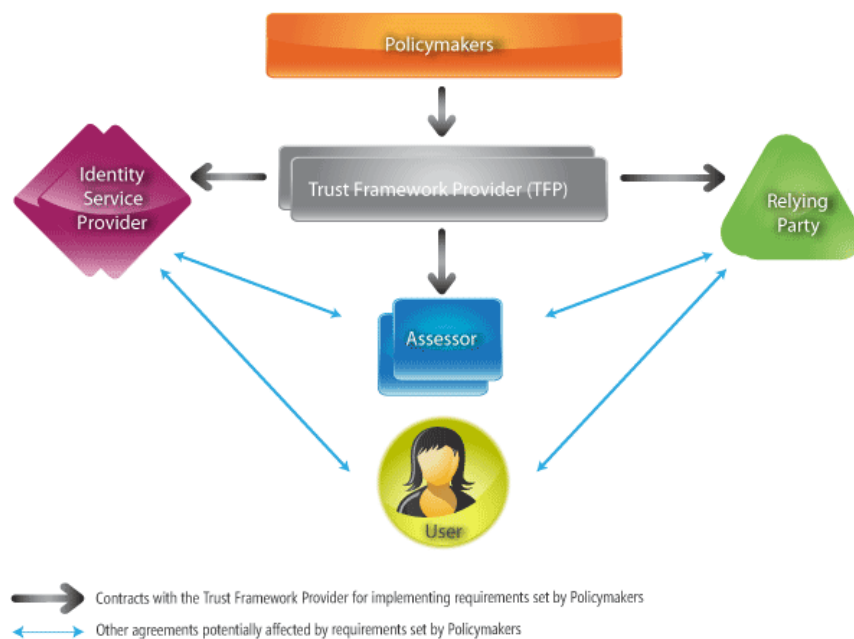
## Trust Framework Requirements and Guidelines V1 (DRAFT 01)

---

### Introduction

In the context of digital identity systems, a *trust framework* is a certification program that enables a party who accepts a digital identity credential (called the *relying party*) to trust the identity, security, and privacy policies of the party who issues the credential (called the *identity service provider*) and vice versa.

The following illustration of the basic architecture of trust frameworks is from [The Open Identity Trust Framework \(OITF\) Model](#), a white paper published jointly by the [OpenID Foundation](#), the [Information Card Foundation](#), and [OIX](#).



**Fig. 1: The basic architecture of trust frameworks in the OITF Model**

In the OITF model, an open identity trust framework provider can administer any trust framework that meets: 1) the Principles of Openness, and 2) any additional requirements imposed by the TFP.

This document sets forth the requirements for any trust framework specification that will be administered by OIX. It is organized into the following sections:

- Authority
- Name
- Version
- Purpose
- Scope
- Roles
- Levels of Assurance
- Levels of Protection
- Technical Profiles
- Special Legal Terms and Requirements
- Other Special Requirements
- Principles of Openness
- Working Group

## Formatting Conventions

To express requirements and guidelines with clarity, this document uses the keywords specified by [RFC 2119, Keywords for Use in RFCs to Indicate Requirements Levels](#).

Normative requirements for OIX trust framework specifications appear with yellow shading, e.g.:

*This is an example of how a requirement **MUST** appear in this document.*

## Authority

Every trust framework is defined by a set of policymakers that represent a *trust community*—a set of parties who need to maintain trust in online interactions. Technically these policymakers are the authors of the trust framework specification and the authority for its content. In OIX this legal entity is referred to as the Trust Framework Authority.

*Note: OIX has a specific membership classification called Trust Framework Authorities for organizations that serve primarily in this role. However any OIX member in any member classification may list a trust framework in the OIX Listing Service.*

Since OIX requires every member organization to maintain a copy of its current legal contact information in the OIX member directory, which appears on the OIX website, the following requirement applies:

*An OIX trust framework specification MUST be listed by an OIX member organization (the Trust Framework Authority), who is the sole legal authority for its content.*

## Name

Although OIX will assign a unique URI to each trust framework when it is accepted for listing in the OIX Listing Service, for all other purposes OIX will use the human-friendly name assigned by the Trust Framework Authority.

*The Trust Framework Authority MUST assign a human-friendly name to the trust framework capable of unambiguous encoding in UTF-8.*

## Version

A key goal of the [Open Identity Trust Framework Model](#) is to support the evolution of trust frameworks as technologies, policies, and marketplace conditions change. To support this goal, queries to the OIX Listing Service need to be able to identify the most recent version of any OIX trust framework. OIX will assign a unique URI to each version of trust framework when it is accepted for listing in the OIX Listing Service; this URI will incorporate the version number assigned in the trust framework specification.

*The Trust Framework Authority MUST assign a version number to each version of the trust framework listed with the OIX Listing Service. For simplicity it is RECOMMENDED to use sequential integers beginning with the number "1". The use of major/minor version numbers or other forms of version numbering is NOT RECOMMENDED.*

## Purpose

A trust framework is created to achieve an overall purpose for achieving trust in online (and possibly offline) interactions shared by the members of a trust community.

*An OIX trust framework specification MUST include a clear human-readable statement of its purpose. This statement SHOULD NOT be more than one paragraph in length.*

## Scope

Although the purpose and scope of every trust framework are closely interrelated, a separate scope statement helps explicitly delineate the online actors and scenarios for which the trust framework is or is not intended.

*An OIX trust framework specification MUST include a clear human-readable statement of its scope. This statement SHOULD include scope restrictions (in or out) for the following: legal jurisdictions, audiences, technologies, interaction or transaction types, and assurance or protection types. It MAY include other forms of scope restrictions.*

## Roles

The rules of every trust framework are defined for a particular set of participants in online (and possibly offline) interactions. [The Open Identity Trust Framework Model](#) defines six standard trust framework roles (in addition to the trust framework provider role played by OIX):

1. Users
2. Identity service providers
3. Relying parties
4. Assessors
5. Auditors
6. Dispute resolution service providers

In addition, OIX has defined a seventh role, Special Assessor, which is an assessor responsible for assessing the qualifications of other assessors.

*An OIX trust framework specification MUST include a clear definition of its participant roles. This definition MUST include a statement of which of the six standard OITF roles are included. If the trust framework specifies an Assessor role, the Special Assessor role MUST be included.*

This section must also state any requirements that are unique to a particular role.

*For each role, the specification MUST specify any qualifications for serving in this role that are not specified for a particular LOA, LOP, or Technical Profile. These qualifications MUST be specified in enough detail that an Assessor (or a Participant, if self-assessment is supported) may reasonably make an assessment of compliance. If a trust framework includes an Assessor role, it MUST specify how the Special Assessor will be selected.*

## Levels of Assurance (LOA)

As defined in the [Open Identity Trust Framework Model](#), a level of assurance (LOA) is a unit of measure for the degree of confidence a relying party can have in the assertions in an identity credential from an identity provider.

*If assurance is in scope for an OIX trust framework specification, it MUST specify at least one LOA. It MAY specify multiple LOA. If it specifies multiple LOA, the LOA MUST be sequential, and a participant certified to be compliant at one LOA MUST be compliant with all lower LOA. Each LOA MUST have a unique identifier within the trust framework that SHOULD be a sequential integer. A specification MAY reference LOA defined in any other OIX Listed Trust Framework, or in another publicly available specification.*

From an assurance standpoint, the heart of the specification is the policies that apply to each LOA.

*For each LOA, the specification MUST specify the policies to which a participant must conform in order to be certified as compliant. Each policy SHOULD have a unique name and MUST have a unique number that can be used to reference it within the scope of the specification. Each policy SHOULD be stated using the keywords specified in [RFC 2119, Keywords for Use in RFCs to Indicate Requirements Levels](#). Whenever interpretation of a policy may be ambiguous, the specification SHOULD provide examples and/or guidance to Assessors in order to make it as objectives as possible to certify compliance. LOA policies with cross-dependencies on LOP policies or Technical Profile requirements SHOULD include cross-references to their unique numbers.*

## Levels of Protection (LOP)

As defined in the [Open Identity Trust Framework Model](#), a level of protection (LOP) is a unit of measure for the degree of confidence: a) an identity provider can have in the protection provided by a relying party for the identity information disclosed in an identity credential, or b) a user can have in the protection provided by an identity provider and/or a relying party for the identity information disclosed in an identity credential.

*If protection is in scope for an OIX trust framework specification, it MUST specify at least one LOP. It MAY specify multiple LOP. If it specifies multiple LOP, the LOP MUST be sequential, and a participant certified to be compliant at one LOP MUST be compliant with all lower LOP. Each LOP MUST have a unique identifier within the trust framework that SHOULD be a sequential integer. A specification MAY reference LOP defined in any other OIX Listed Trust Framework, or in another publicly available specification.*

As with LOA, if protection is in scope for a trust framework, the crux of the specification is the privacy, security, and data protection policies that apply at each LOP.

*For each LOP, the specification MUST specify the policies to which a participant must conform in order to be certified as compliant. Each policy SHOULD have a unique name and MUST have a unique number that can be used to reference it within the scope of the specification. Each policy SHOULD be stated using the keywords specified in [RFC 2119, Keywords for Use in RFCs to Indicate Requirements Levels](#). Whenever interpretation of a policy may be ambiguous, examples and/or guidance to Assessors SHOULD be given in order to make it as objectives as possible to certify compliance. LOP policies with cross-dependencies on LOA policies or Technical Profile requirements SHOULD include cross-references to their unique numbers.*

## Technical Profiles

As defined in the [Open Identity Trust Framework Model](#), a Technical Profile is a specification of the requirements for the use of a specific technology or technologies

in order to achieve technical interoperability in the exchange of digital identity credentials that is consistent with the associated LOA or LOP.

*If an OIX trust framework relies on one or more specific technologies, it MUST specify at least one Technical Profile. It MAY specify multiple Technical Profiles. Each Technical Profile MUST have a unique identifier within the trust framework. A specification MAY reference all or part of Technical Profiles defined in any other OIX Listed Trust Framework, or in another publicly available specification.*

As with LOA and LOP, each Technical Profile is a collection of policies. Each policy states the requirements for usage, implementation, or operation of a specific technology, typically a subset of the requirements in a separate specification from a standards body (e.g., OpenID 2.0, IMI 1.0, SAML 2.0).

*A Technical Profile MUST specify the policies to which a participant must conform in order to be certified as compliant. Each policy SHOULD have a unique name and MUST have a unique number that can be used to reference it within the scope of the specification. Each policy SHOULD be stated using the keywords specified in [RFC 2119, Keywords for Use in RFCs to Indicate Requirements Levels](#). Whenever interpretation of a policy may be ambiguous, examples and/or guidance to Assessors SHOULD be given in order to make it as objectives as possible to certify compliance. Technical Profiles with cross-dependencies on LOA and/or LOP policies requirements SHOULD include cross-references to their unique numbers.*

## Special Legal Terms and Requirements

Once an OIX trust framework is accepted for listing in the OIX Listing Service, participants may apply for certification. To be listed as a certified participant, participants enter into the standard OIX Participant Listing Agreement [*reference to this document to be added once it is posted to the OIX website*]. However if any additional legal terms or requirements apply, they must be stated.

*If an OIX trust framework has any special additional legal or contractual requirements that apply to all participants, or just to participants in a particular role, these terms and requirements MUST be clearly stated in the Special Legal Terms and Requirements section of the specification.*

## Other Special Requirements

The preceding sections cover all the typical elements of a trust framework specification. However if there are other special requirements that are unique to a particular trust framework, they may be included in a section for this purpose.

*If an OIX trust framework has any additional special requirements that apply to all participants, or just to participants in a particular role, these requirements MUST be clearly stated in the Other Special Requirements section of the specification.*

## Principles of Openness

The final requirement of an OIX trust framework is a statement from the Trust Framework Authority that enables potential participants (direct or indirect) to evaluate the trust framework from the standpoint of how well it supports transparency, accountability, and open competition.

*An OIX trust framework specification MUST include a self-assessment by the Trust Framework Authority as to how the specification conforms to the Principles of Openness as defined in [The Open Identity Trust Framework Model](#). If there is a limitation to conformance on any Principle, this limitation MUST be explicitly stated and explained by the Trust Framework Authority.*

## Working Group

OIX offers the ability for any set of OIX members and non-members to form an OIX Working Group for the purpose of developing and/or maintaining a trust framework. This is not required—an OIX trust framework may be developed anywhere by any group. However if such a Working Group is established, under OIX or any other auspices, it must be clearly referenced in the specification.

*If an OIX Trust Framework Working Group is established for development or maintenance of an OIX Trust Framework, or a referencable Working Group exists under any other auspices, the trust framework specification MUST include a reference to this Working Group and its charter.*