Trust Framework

The ultimate goal of any identity system is to provide identity assertions that are sufficiently reliable for the intended purpose,[1] and to do so in a manner such that all of the relevant parties are willing to participate and to rely on the results. Achieving that goal requires building a "Trust Framework" for each identity system that addresses both the operational requirements and the legal rules necessary to define a trustworthy identity system. This is sometimes referred to as the "tool and rules" of an identity system.

The concept of a Trust Framework is often referred to in discussions of identity management systems,[2] but usually without a detailed analysis and often in an inconsistent manner. For the purposes of this [ABA Report], the following definition will be used:

> A Trust Framework is a set of documents developed or tailored for a specific identity system, which sets forth:
>
> - the ***Operational Requirements*** for the identity system (such as technical and functional specifications, processes, standards, policies and rules) that have been developed to ensure the proper operation of the system and to provide adequate assurance regarding the accuracy, integrity, privacy and security of its processes; and
> - the ***Legal Rules*** that govern the identity system and that make the Operational Requirements legally binding on and enforceable against the participants, regulate the content of the Operational Requirements, and define and govern the legal rights, responsibilities, and liabilities of the participants of the identity system.

The **Operational Requirements** of a Trust Framework will likely consist of several different components addressing a variety of key operational and policy issues. While the content and structure of these components will vary from one identity system to another, the Operational Requirements of each Trust Framework will likely include common core components, such as an identity proofing component,[3] an authentication component,[4] a credential management component, a privacy component,[5] a security component, an assessment/audit component.[6]

Each component of the Operational Requirements establishes the technical specifications, processes, standards, policies, rules and performance requirements necessary to address one or more issues of importance to the operation of the identity system. Taken together they form the

---

[1] Recognizing that the intended use will vary, and thus so will the requirements necessary to make it sufficiently trustworthy *for that purpose*.

[2] See examples attached at end of document.

[3] NASPO is currently developing an ANSI standard for such an identity proofing framework.

[4] See, e.g., Entity Authentication Assurance Framework, ISO/IEC 29115:2010 (Draft)

[5] Kantara is currently developing a Privacy Framework component for a Trust Framework.

[6] See, e.g., _____.

Operational Requirements necessary to ensure that the identity system operates properly and in a manner that all parties trust will be appropriate for the task.

The **Legal Rules** complete the Trust Framework by rendering the various components of the Operational Requirements binding and enforceable.

The Legal Rules consist of both existing statutes and regulations (i.e., publicly-created law), and agreements between or among the participants (i.e., privately-created law). They affect the Trust Framework in three ways:

- They make the specifications, standards, and rules comprising the various components of Operational Requirements legally binding on and enforceable against each of the participants.
- They define the legal rights and responsibilities of the parties, clarify the legal risks parties assume by participating in the Trust Framework (e.g., warranties, liability for losses, risks to their personal data); and provide remedies in the event of disputes among the parties, including methods of dispute resolution, enforcement mechanisms, termination rights, and measures of damages, penalties and other forms of liability.
- In some cases, they also regulate the content of the Operational Requirements.

The Legal Rules may be set out in numerous contracts at varying management and execution layers, depending on the governance structure used. In many cases they operate as gap-fillers with respect to issues not addressed by the existing law. Where existing laws address issues in a permissive rather than mandatory manner, the Legal Rules may also express the choices of the parties among legally permissible alternatives. And in both cases they can have the effect of providing the legal certainty and predictability necessary to encourage participation

The relationship between the Operational Requirements and Legal Rules of a Trust Framework is similar to the relationship between a contract and several sets of technical specifications attached to the contract as exhibits. Execution of the contract is what creates a legally binding relationship between the parties; the technical specifications in the exhibits detail the parties' expectations of how the contract will be performed. While it might be possible for the parties to work together with reference only to the technical specifications, by incorporating them into a contract, the technical specifications give rise to legally enforceable rights and responsibilities.

In some cases, Trust Frameworks may be developed by a single entity, often referred to as a Trust Framework Provider, which is established to provide both the Trust Framework and the governance infrastructure needed to support it. Such an entity may be established by a group of companies or an industry sector that require a legally binding Trust Framework in order to work together efficiently.

Examples of such Trust Framework Providers include IdenTrust, Inc.[7] which has established an identity Trust Framework for the financial sector, the SAFE-BioPharma Association,[8] which has established an identity Trust Framework for the pharmaceutical sector, and CertiPath,[9] which has established an identity Trust Framework for the aerospace sector. Trust Frameworks may also be established by a single entity for its own purposes. Examples of this approach include the e-Authentication Trust Framework established by the General Services Administration

[7] http://www.identrust.com

[8] http://www.safe-biopharma.org

[9] http://www.certipath.com

Examples of Trust Framework Definitions

CDT: "A Trust Framework often connects the user, the identity provider, and the service provider (often called the relying party), laying out a set of conditions that each party should adhere to in order to maintain a trusted system." See "CDT Discusses Key Policies Issues Surrounding User-Centric Identity Management" at http://www.cdt.org/policy/cdt-discusses-key-policies-issues-surrounding-user-centric-identity-management;

GSA-ICAM: Definition of Trust Framework: "Trust Framework Provider processes and controls for determining an identity provider's compliance to OMB M-04-04 Levels of Assurance." See ICAM Trust Framework Provider Adoption Process (TFPAP) For Levels of Assurance 1, 2, and Non-PKI 3, at p. 42, available at http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf;

Kantara: "In electronic communication, a *Trust Framework* (TF) is a complete set of contracts, regulations or commitments that enable participating actors to rely on certain assertions by other actors to fulfill their information security requirements." See Trust Framework Architecture webpage at http://kantarainitiative.org/confluence/display/idassurance/Trust+Framework+Architecture#TrustFrameworkArchitecture-WhatisaTrustFramework%3F;

NSTIC – June 25 Public Release: Definition of Trust Framework: "The underlying structure of standards and policies that defines the rights and responsibilities of the various participants in the Identity System, specifies the rules that govern their participation, outlines the processes and procedures to provide assurance, and provides the enforcement mechanisms to ensure compliance." NSTIC, at p. 34; available at http://www.dhs.gov/xlibrary/assets/ns_tic.pdf;

OIX: "In 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." http://openidentityexchange.org/what-is-a-trust-framework; http://openidentityexchange.org/how-it-works/what-is-a-trust-framework; and

OpenID: A Trust Framework is "a set of technical, operational, and legal requirements and enforcement mechanisms for parties exchanging identity information" The Open Identity Trust Framework (OITF) Model, p. 2; available at http://openidentityexchange.org/sites/default/files/the-open-identity-trust-framework-model-2010-03.pdf