Building the Legal Framework for Browser-Enabled Identity

Thomas J. Smedinghoff[1]

As the Web becomes a focal point for economic and social activity, there is an urgent need for trustworthy, widely-applicable, and interoperable digital identity management. The use of browser technology can help to realize this vision. But at the end of the day technology is only part of the solution.

The ultimate goal of any identity system is to provide identity assertions that are sufficiently reliable for the intended purpose, and to do so in a manner such that all relevant parties are willing to participate and to rely on the results. Enabling a system for identification, authentication, and authorization that works across multiple websites, enterprises, devices, and browsers in a uniform and easy-to-use manner requires both the tools to ensure that it operates properly and in a trustworthy manner, and the rules to ensure that it fairly allocates rights and responsibilities among the parties, and that is enforceable.

Achieving that goal requires building what is frequently referred to as a "Trust Framework."[2] An identity system Trust Framework addresses both the operational specifications and the legal rules necessary to define a functional and trustworthy identity system.

The concept of a Trust Framework is often referred to in discussions of identity management systems, but usually without a detailed analysis and often in an inconsistent manner. Basically, a Trust Framework is the legally regulated structure for a specific identity system consisting of:

- the ***Operational Specifications*** (such as technical and functional specifications, processes, standards, policies and rules for identification, authentication, credential management, assessment, etc.) that have been developed:
  - ➢ to define the requirements for the proper operation of the system (i.e., so that it works), and
  - ➢ to provide adequate assurance regarding the accuracy, integrity, privacy and security of its processes and data (i.e., so that it is trustworthy); and
- the ***Legal Rules,*** composed of a combination of existing law and contractual agreements, that govern the identity system and that:
  - ➢ regulate the content of the operational specifications,
  - ➢ make the operational specifications legally binding on and enforceable against the participants, and
  - ➢ define and govern the legal rights, responsibilities, and liabilities of the participants of the identity system.

[1] Partner, Wildman Harrold, Allen & Dixon LLP, Chicago; Co-Chair, ABA Identity Management Legal Task Force. Portions of this paper will form part of the input to the Report being developed by the ABA Identity Management Legal Task Force,

[2] The U.S. National Strategy for Trusted Identities in Cyberspace refers to this as the "Identity Ecosystem Framework" (at p. 24). See http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

The **Operational Specifications** 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 specifications 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, and an assessment/audit component.[6]

Each component of the operational specifications establishes the normative and informative 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 operational specifications 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 specifications binding and enforceable, and addressing related legal issues.

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 regulate the content of the operational specifications;
- They make the specifications, standards, and rules comprising the various components of operational specifications legally binding on and enforceable against each of the participants; and
- They define the other 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.

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

[3] For example, the NASPO National Identity Proofing and Verification Standards Development Committee is currently developing an ANSI standard for such an identity proofing framework. See http://www.naspo.info/pages/idpvprojects.html

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

[5] For example, Kantara is currently developing a Privacy Framework component for a Trust Framework. See http://kantarainitiative.org/confluence/display/p3wg/Privacy+Framework+SubGroup

[6] See, e.g., Kantara Identity Assurance Framework: Assurance Assessment Scheme, at http://kantarainitiative.org/confluence/download/attachments/41025670/Kantara+IAF-1300-Assurance+Assessment+Scheme.pdf.

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 specifications and legal rules of a Trust Framework is similar to the relationship between a construction contract and the blueprints and other 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.

Perhaps the best example of a browser-based Trust Framework is the EV SSL Guidelines developed by the CA Browser Forum,[7] which bind CAs by self assertion, and are enforced by audit requirements. Among other things, the EV SSL Guidelines impose minimum requirements for identity proofing, require that CAs commit to minimum warranties, and restrict the ability of CAs to limit their liability.

Building a Trust Framework for an identity system presents numerous challenges, not the least of which is reaching agreement on the appropriate rights, responsibilities, obligations, and liabilities of the various participants. But even assuming such agreement can be reached, numerous challenges remain. These challenges include:

> **Deciding What Rules Are Necessary.** The operational specifications of the Trust Framework must define the rules and obligations to be imposed on each of the participants in any identity management system. For example, an Identification component must specify the rules for identity proofing of Subjects and the issuance of credentials, an Authentication component must specify the technology and rules for authenticating identity assertions, verifying that credentials are not revoked, and the like, a Privacy Framework must set the rules for collection, use, processing, storage, and transfer of personal information, and a Data Security component must set out the rules for data security (such as the PCI standard does for the credit card systems).
>
> **Figuring Out How Existing Law Impacts the Required Rules.** The task of developing a Trust framework is further complicated by the fact that existing law in the relevant jurisdictions may limit or restrict the implementation of the standards, policies, procedures,

[7] www.cabforum.org.

rules, and requirements deemed desirable. For example, it may be deemed desirable (or even an absolute necessity) to encrypt certain identity-related communications. Yet applicable law in some jurisdictions may restrict or limit (or even prohibit) the use of such encryption. Likewise, the need to ensure a highly reliable identity proofing process may require the collection of extensive personal data about the subject from a variety of sources, yet local data privacy laws may prohibit such activity, or at least subject it to extensive regulations that must be complied with. In addition, data security laws in some jurisdictions may impose requirements not otherwise contemplated, or consumer protection laws in other jurisdictions may limit or restrict the imposition of certain obligations on consumer subjects.

Binding all Relevant Parties. Both the operational specifications and the legal rules that make up the Trust Framework (identification, authentication, privacy, security, etc.) must somehow be made binding on, and enforceable against, each of the participants to whom they apply. To the extent that the standards, policies, procedures, rules, and requirements are embodied in existing law, this may not be a problem. Otherwise, however, there must be a mechanism (such as a contract) by which they become binding on each relevant participant and non-participant.

Dealing with Inadequacies of Publicly-Created Law – Modifying it Where Necessary. At its essence, existing law poses four basic problems for an identity management Trust Framework –

- There are some key identity management issues that existing law simply does not address;
- There are some issues that it may address, but the fact of its application to such issues, or the manner of its application, is unclear, uncertain, or ambiguous, leaving the participants with a great deal of legal uncertainty;
- There are some key issues that it may address in a manner that is contrary to the intentions of the participants or in a manner that constitutes a barrier to the operation of the identity system;
- There are some key issues on which the application of existing law varies considerably across jurisdictions, often in an inconsistent manner.

The Trust Framework must contractually address these problems and barriers created by existing law, as well as fill gaps and uncertainties in the way existing law applies to identity systems. For example, existing law might apply a standard of performance to Identity provider conduct, or a warranty to the issuance of a credential, that is inappropriate under the circumstances.

Dealing with Publicly-Created Law that Cannot be Modified by Contract. Where portions of existing law in one or more jurisdictions cannot be modified by contract (e.g., certain consumer protection laws), compliance may be the only option. Thus, identifying such laws will be critical for the development of the Trust Framework. In such cases, the Trust Framework must either adopt an approach that complies with all such laws in all applicable jurisdictions, or alternatively alter the Trust Framework so as to avoid the need for compliance

<u>Dealing with Cross-Border Inconsistencies in Publicly-Created Law</u>. A Trust Framework must comply with applicable existing law. This is, of course, made problematic where applicable law comes from different jurisdictions, and such laws differ, are inconsistent, and/or are in conflict. How does the IdM contractual framework address those differences?