Trust Frameworks: Their Critical Role in Governing Identity Systems and Allocating Liability

Don Thibeau & Tom Smedinghoff
Technology Tools + Governing Rules = Trust
Governance Rules: Options

Bi-lateral Contracts
Loosely Coupled SLA’s
Terms of Service Agreements
Trust Frameworks
Why Trust Frameworks?

Functionality/Interoperability

Internet/Scalability

Openness/Transparency

Opportunity Cost /Time-to-Market
Evolving Definitions of Trust Frameworks

**US FICAM:** processes and controls for determining an identity provider’s compliance to OMB M-04-04 Levels of Assurance

**ISO 29115 Draft:** a set of requirements and enforcement mechanisms

**OITF Model:** a set of technical, operational, and legal requirements and enforcement mechanisms

**US NSTIC 4/15/2011 Final:** It defines the rights and responsibilities; specifies the policies and standards; and defines the community-specific processes and procedures
A Trust Framework Is:

a legally enforceable
set of specifications, rules, and agreements
that governs an identity system.
Identity System: Tools + Trust Framework: Rules
An Identity System is Governed by a Trust Framework
Characteristics of a Trust Framework

1. Scope
2. Purpose
3. Form
4. Role Definition
5. Content / Issues Addressed
6. Authorship and Control
7. Enforceable
Trust Framework Scope

- Governs a single identity system
  - i.e., each identity system will have its own trust framework
  - Many identity systems interoperate

- Thus, many trust frameworks will exist
  - Many trust frameworks will interoperate
Trust Framework Purpose

- Defines and governs the operation of a specific identity system
- Defines the rights, responsibilities, and obligations of the participants

For three basic purposes:

1. To ensure that the identity system is operational
   - i.e., that it functions properly
2. To ensure that the identity system is trustworthy
   - i.e., that the participants are willing to participate, trust the results, and act in reliance on them
3. To address the legal issues
   - And ensure that it is enforceable
Identity Systems **Need Trust Frameworks** to:

Make the system “operationally functional”
- So it “works”
- So everyone knows what to do
- So everyone knows who’s responsible for what

Make the system “trustworthy”
- Goes beyond merely functional
- Address and minimize risks
- So participants trust the results and are willing to rely on them

Address the **legal issues**
- Define participant legal rights, duties, and obligations
- Define and allocate liability risks
- Make duties and obligations binding and “enforceable”
Trust Framework Form

- Words on paper
- Can take a variety of forms
- Can be one or several documents
- Can be long or short
- Can be self-contained or incorporate pre-existing standards or requirements
- Can be comprehensive or defer to existing standards and/or laws for many issues
Typically defines specific roles

Operational Roles
- To develop and maintain the trust framework itself
- To govern aspects of the operation of the identity system

Participating Roles
- Identity issuing roles
- Identity verification roles
- Identity consuming roles (relying parties)
Trust Framework Roles

Trust Framework (Operational Roles)
- Policy Development
- Policy Enforcement
- Network Evolution
- On-boarding/Assessment
- Central Services

Identity System (Participating Roles)
- Identity Issuing
- Authentication Management
- Authorization Management
- Identity Verification
- Attribute/Assertion Management

Participating entities
- Services
- Participating entities
- Services
- Services

End Users
Specifications, rules, and agreements that address the

- business,
- technical,
- operational, and
- legal issues

of importance to the functioning and trustworthiness of the identity system
Trust Frameworks Might Include . . .

Business, Technical, and Operational Rules

- Technical Specifications
- Credential Issuance
- Authentication Requirements
- Reliance Rules
- Credential Management
- Identity Proofing
- Privacy Standards
- Security Standards
- Audit & Assessment Oversight
- Enrolment Rules

Existing Law

Legal Rules (Contractual)

- Liability for Losses
- Warranties
- Termination Rights
- Dispute Resolution
- Measure of Damages
- Enforcement Mechanisms

Enforcement Element

Contract(s): “I Agree” to . . .
Who writes and updates the trust framework?

Many options, including –

- A separate entity established for the express purpose of writing and updating the trust framework (think, e.g., Visa in the credit card world)
- A participating entity that established or controls the identity system (e.g., GSA, UK Cabinet Office, Google, Facebook, etc.)
- A committee of all or some of the participants in the identity system
- Other
Trust Framework Enforceability

- How is trust framework made enforceable on the parties?
- Private sector identity systems – usually rely on contracts
- Public sector identity systems – can rely on either contract or regulations
Sources of Law Governing an Identity System

1. **General Commercial Law - Public law applicable to everybody**
   - Existing statutes, regulation, and case law
   - Not written to address identity issues
   - E.g., contract law, tort law, data protection law, commercial law, personal injury law, family law, competition law, etc.

2. **General Identity Management Law - Public law applicable to all identity systems**
   - New statutes and/or regulations
   - Written to address online identity management generally – i.e., all identity systems
   - E.g., Virginia Electronic Identity Management Act

3. **Identity System-Specific Rules (Contracts or Laws) – Trust Frameworks**
   - Also called scheme rules, system rules, or operating rules
   - Written to govern a specific identity system
Identity System Law: Three Levels of Rules Can Govern

1. **General Commercial Law**
   - Contract law, Tort law, Competition law, Privacy law, Family law, Law of Trespass, etc.

2. **General Identity Management Law (NEW)**
   - Virginia legislation,
   - Other?

   Contract-based Trust Frameworks must comply with 1 and 2 above

3. **Trust Frameworks for Identity System**
   - Trust Framework for Identity System 1
   - Trust Framework for Identity System 2
   - Trust Framework for Identity System N

General Public Law (Rules)

ID System-Specific Law (Rules)
1. General Commercial Law

2. General Identity Management Law

   - Trust Framework 1
     - Identity System 1
   - Trust Framework 2
     - Identity System 2
   - Trust Framework N
     - Identity System N

3. Identity System-Specific Rules
Addressing Liability Concerns of All Participants

Identity Provider
- What is my liability if I make an incorrect identification?
- What is my liability if I misuse personal data?

Relying Party
- What is my liability if I rely on a false credential?
- What is my liability if I misuse personal data?

User / Data subject
- What is my liability if someone else uses my credential?
- What happens if someone misuses my personal data?
Where is Liability Addressed?

**Default** is that liability rules come from existing General Commercial Law

Three **problems** with that approach –

- Existing law is not written to address identity systems, so the answers may be vague and uncertain – no predictable rules
- Many of the potential liability situations that could occur in an identity context may simply not be anticipated or addressed by existing law
- If liability is addressed, we may not like the answers we get from existing law

**Solution** is to use the trust framework

- Tailored for a specific identity system
- Can set liability rules appropriate for the identity system, its goals, and its participants
- Parties agree to liability rules by contract
- Can alter rules under existing law (except where expressly prohibited)
AN OPEN MARKET SOLUTION FOR ONLINE IDENTITY ASSURANCE

A New Solution for Internet-Scale Identity Assurance: the Open Identity Exchange

AUTHORS:
Don Thibeau - OpenID Foundation
Tony Nadalin - Microsoft
Mary Rundle - Microsoft
Drummond Reed - Information Cards
Eve Maler - PayPal

MARCH 2010

March 2010

THE VOCABULARY OF IDENTITY SYSTEMS LIABILITY

What is Liability? When Does it Arise?

Identity System Liability White Paper, Phase 1

THE OPEN IDENTITY EXCHANGE | EDWARDS WILDMAN PALMER LLP

By Thomas J. Smedinghoff, Mark Deem, and Sam Eckland

June 2014

Trustmarks in the Identity Ecosystem

Definitions, Use, and Governance

White Paper

IDENTITY STEERING GROUP

By Dr. Gilad L. Rosner

September 2015
Trust Frameworks for Identity Systems

Esther Makaay - SIDN
Tom Smedinghoff - Locke Lord LLP
Don Thibeau - Open Identity Exchange

May 2017


Tom Smedinghoff - Locke Lord LLP

August 2017

A Global Inventory of Trust Frameworks and Trust Schemes

Sue Dawes - Open Identity Exchange
Mike Leszcz - Open Identity Exchange
Don Thibeau - Open Identity Exchange

May 2017

Soon to be Published OIX Trust Framework White Papers
OIX Curates a Global Conversation

Trust Frameworks and Attribute Exchanges

Self-Certification and Identity Systems

A Case Study: Cross Border Banking Services

The Connect Europe Facility (CEF) Project

December 2017

Ocotber 2017

December 2017

OIX Trust Framework White Papers Being Developed
International Identity Management Law & Policy Workshops

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

AMERICAN BAR ASSOCIATION
Identity Management Legal Task Force
A Trusted Place for Trust Frameworks

tScheme Trust Body for UK’s Trust-Service Status List (TSL)

Creates, hosts and maintains the UK’s Trust Service-status List (TSL) on behalf of the Department for Business, Innovation and Skills (BIS)
Technology Tools + Governing Rules = Trust
Join and help shape the markets you intend to lead.

Don Thibeau
Chairman | Open Identity Exchange
Executive Director | OpenID Foundation

don@openidentityexchange.org
Skype: donthibeau
Twitter: @4thibeau