

# Interagency Advisory Board

*Meeting Agenda, February 23, 2011*

---

1. **Open Remarks** (*Mr. Tim Baldrige, IAB Chair*)
2. **The Business Reinvention that CAC Has Enabled in the DoD**  
(*Mary Dixon, DMDC--Director*)
3. **Update of Identity Proofing and Verification Standard Development Efforts** (*Mr. Tom Lockwood, Mr. Dan Combs, and Mr. Graham Whitehead*)
4. **Juniper Approach in Supporting the Implementation of SHA-256** (*Jay Dineshkumar, Juniper*)
5. **Draft Trust Framework** (*Tom Smedinghoff, ABA IDM Taskforce*)
6. **Closing Remarks** (*Mr. Tony Cieri*)

# Defining the Concept of a Trust Framework

**Thomas J. Smedinghoff**

**Wildman, Harrold, Allen & Dixon LLP  
Chicago**

**Co-Chair, ABA Identity Management Legal Task Force**

Wildman Harrold | 225 West Wacker Drive | Chicago, IL 60606 | (312) 201-2000 | [wildman.com](http://wildman.com)

Wildman, Harrold, Allen & Dixon LLP

# Key ABA Topics



Wildman Harrold  
*Attorneys and Counselors*

- Primary Risks for IdM participants
- The concept of a Trust Framework to address those risks
- The Legal Barriers to identity management
- Understanding Liability and Possible Liability Models

# Key Risks to the Participants



Wildman Harrold  
*Attorneys and Counselors*

- Technology risk
- Process risk
- Performance risk
- Privacy / Data Protection risk
- Data security risk
- Liability risk
- Enforceability risk
- Regulatory compliance risk



# Addressing Those Risks

- Everyone seems to agree that addressing those risks requires a Trust Framework
- But no one seems to agree on what a Trust Framework is
- We need a common understanding of what we're building

# Much Disagreement Re What a Trust Framework Is



Wildman Harrold  
Attorneys and Counselors

- CDT: lays out a **set of conditions that each party should adhere to** in order to maintain a trusted system
- GSA-ICAM: processes and **controls for determining an identity provider's compliance to OMB M-04-04** Levels of Assurance
- Kantara: 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
- NSTIC Draft: 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.
- OIX: 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.
- OpenID: a **set of technical, operational, and legal requirements and enforcement mechanisms for parties exchanging identity information**

# Making It Work Requires A “Trust Framework” Composed of:



Wildman Harrold  
*Attorneys and Counselors*

- **Operational Requirements**

- Goals

- Ensure proper operation of the identity system
- Ensure that operation will protect accuracy, integrity, privacy and security of processes and data

- Content

- Technical specifications, process standards, policies, procedures, performance requirements of the participants, etc.

- **Legal Rules**

- Goals

- Make Operational Requirements legally binding on the participants
- Define and govern the legal rights and responsibilities of the participants

- Content

- Existing legislative/regulatory rules
- Contractual obligations



# “Trust Frameworks” . . .

- Will often/usually be created by the private sector
- Will vary with the purpose of the identity system
- Will be primarily based on private contracts
- Will seek to support participant trust in the identity system by:
  - Imposing enforceable specifications, standards, and rules on all parties
  - Adequately defining the rights and responsibilities of the parties
  - Fairly allocating risk and responsibilities among the parties
  - Providing legal certainty and predictability to the participants
  - Complying with existing law
  - Working cross-border

# Proposed Definition of Trust Framework



Wildman Harrold  
Attorneys and Counselors

A **Trust Framework** is a set of documents developed or tailored for a specific identity system which sets forth:

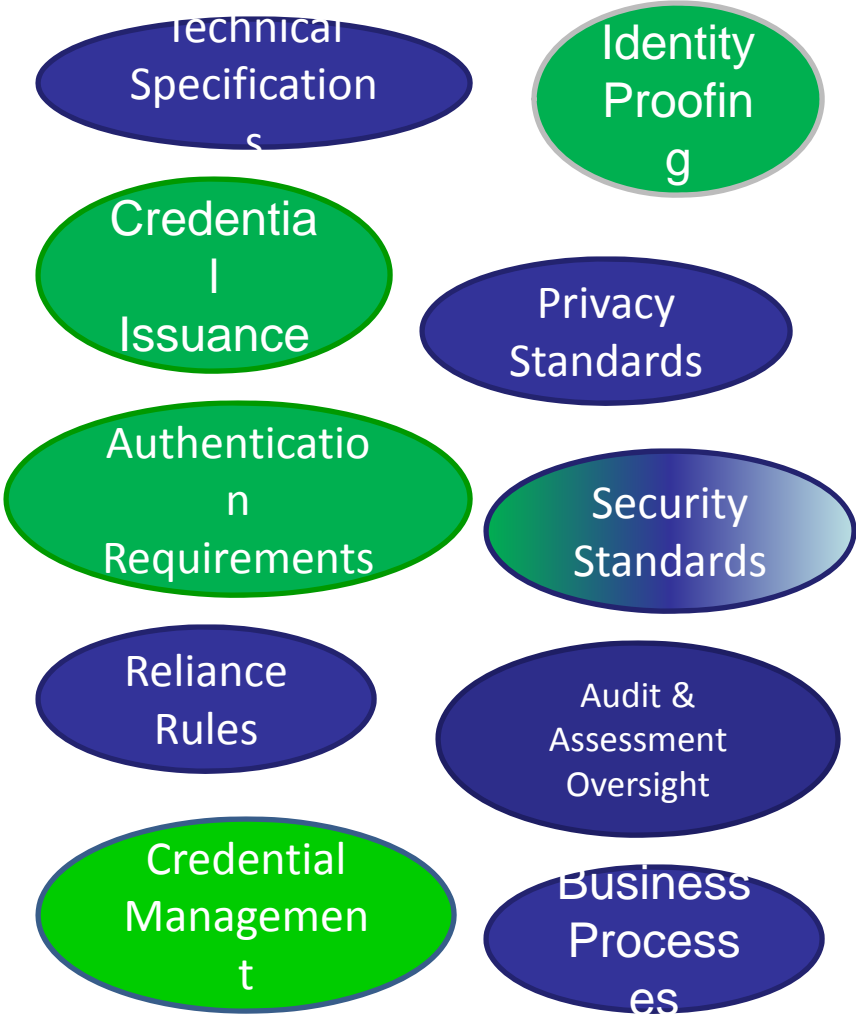
- the **Operational Requirements** for the identity system (such as technical and functional specifications, processes, standards, policies and rules) that have been developed –
  - to ensure the proper operation of the system and
  - to provide adequate assurance regarding the accuracy, integrity, privacy and security of its processes and data; 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.

# Operational Requirements

## Things Necessary to “Make it Work”



Wildman Harrold  
Attorneys and Counselors



Partial listing of Operational Requirements

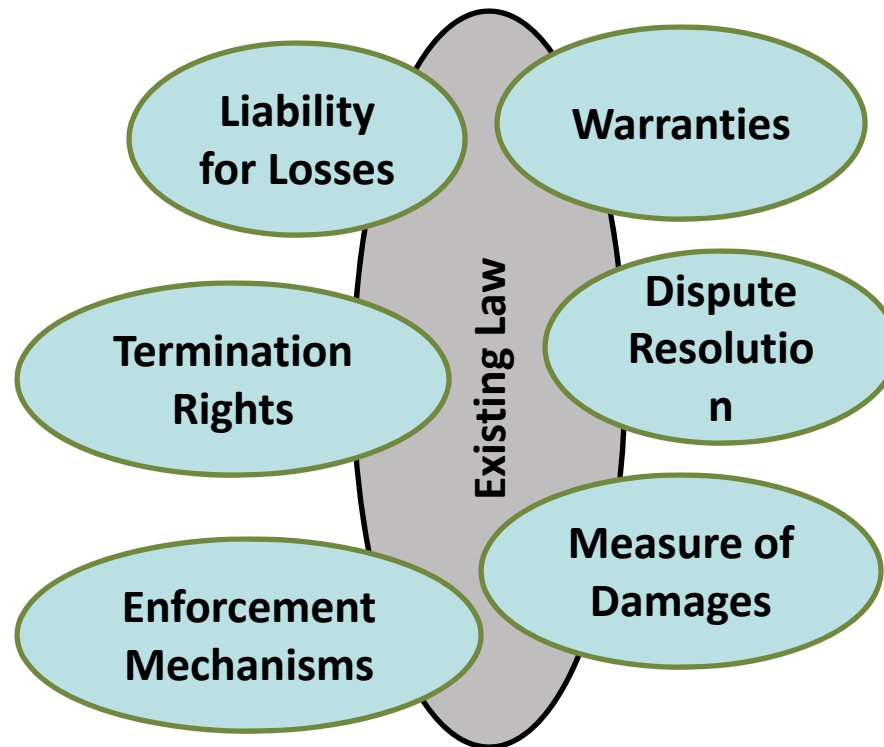


# Legal Rules To Govern Legal Rights of the Parties



Wildman Harrold  
*Attorneys and Counselors*

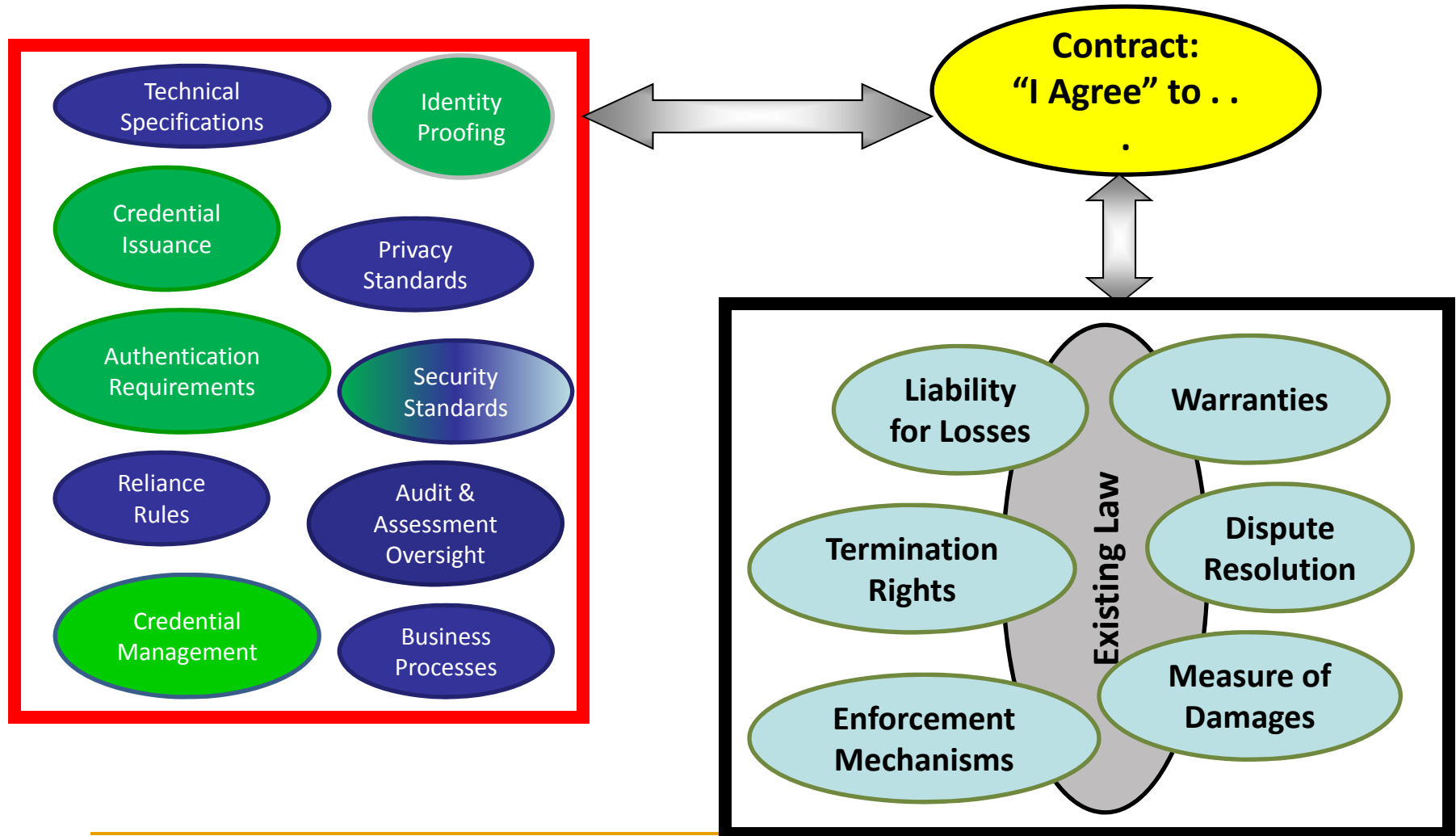
## Existing Law as Supplemented and/or Modified by Contract



# Trust Framework: Putting It All Together



Wildman Harrold  
Attorneys and Counselors



# Common Legal Problems to Be Addressed By a Trust Framework



Wildman Harrold  
Attorneys and Counselors

- Legal Uncertainty
  - (i) Lack of legal rules and (ii) lack of clarity re applicable legal rules
- Liability Risk / Liability Allocation
  - Uncertainty over potential liability is key issue!
- Legal Compliance
  - E.g., privacy law requirements; security law requirements, etc.
- Legal Barriers
  - Some laws may adversely impact Identity systems;
  - Can they be altered by agreement?
- Contract Enforceability
  - How can we bind all participants (and affected non-parties) in an enforceable Trust Framework?
- Cross-Border Issues
  - Regulatory law in one jurisdiction may differ from another

# Status of Industry Work to Date (1): Limited to Operational Requirements



Wildman Harrold  
Attorneys and Counselors

- Operational Requirements
  - Much work being done by many groups and governments
  - Groups: Kantara Initiative, Open Identity Foundation, ITU, EURIM, STORK, OIX, WS-Federation, etc.
  - Governmental: Australia, Belgium, Finland, EU, Germany, India, OECD, Scotland, Sweden, U.S., etc.
- Legal Rules
  - ***Largely unaddressed!***
  - Some private (closed) identity systems such as IdenTrust, SAFE-BioPharma, CertiPath, etc.
  - American Bar Association Identity Management Legal Task Force

# Status of Industry Work to Date (2): Most Existing TFs Are Just Components



Wildman Harrold  
Attorneys and Counselors

- Most existing work focuses only on a subset of the total set of operational requirements and legal rules, and thus are only components of a Trust Framework, such as:
  - NIST SP 800-63, Electronic Authentication Guideline
  - Kantara Privacy Framework (being developed)
  - FICAM Security Assertion Markup Language (SAML) 2.0 Profile
  - NASPO National Identity Proofing and Verification Standards (being developed)
  - Entity Authentication Assurance Framework, ISO/IEC 29115:2010 (draft)
  - Kantara Identity Assurance Framework: Assurance Assessment Scheme
- Examples of complete Trust Frameworks might include SAFE-BioPharma, CertiPath, and IdenTrust



# We Need Consistent Understanding

- Developing any TF requires understanding of what is required
- Differences in language, scope and approach limit understandability and ability to leverage prior work
- Need for interoperability requires consistent understanding of TF
- Mapping between different TFs is difficult. Terminology is inconsistent. Participants cannot identify all risks
- The process starts with agreement on a high level description of a Trust Framework
- Next steps – identifying the topics to be addressed for the Operational Requirements and Legal Rules

# Further Information



Wildman Harrold  
Attorneys and Counselors

## **Thomas J. Smedinghoff**

Wildman, Harrold, Allen & Dixon LLP

225 West Wacker Drive

Chicago, Illinois 60606

312-201-2021

*smedinghoff@wildman.com*