Gaps and Challenges for Advancing the Global Identity Ecosystem

Thomas J. Smedinghoff
ABA IdM Legal Task Force
Edwards Wildman Palmer LLP
March 12, 2012
All Identity Systems Require Rules

♦ **Business and Technical Rules**
  ♦ **Content**
    ♦ Business and Technical specifications, process standards, policies, operational procedures, performance rules and requirements, assessment criteria, etc.
  ♦ **Goals**
    ♦ Make it work – from a functional perspective
    ♦ Make it trustworthy – willingness to participate

♦ **Legal Rules** *(Contractual)*
  ♦ **Content**
    ♦ Contractual obligations, including agreement to follow Business & Technical Rules
  ♦ **Goals**
    ♦ Define and govern the legal rights and responsibilities of the participants
    ♦ Address liability and risk allocation
    ♦ Provide mechanism for enforcement of rights / Address dispute resolution
    ♦ Make it trustworthy – willingness to participate
Those Rules Go By Various Names

- Trust Framework – NSTIC / Kantara / OIX
- Operating Policies - SAFE-BioPharma / InCommon
- Operating Rules – FIXs / CAHQ (health info exchange)
- Operating Rules and System Documentation - IdenTrust
- Common Operating Rules - CertiPath
- Guidelines - CAB Forum
- System Rules - ABA (draft)

- Operating Regulations - Visa (credit)
- Operating Rules - ACH (electronic payments)
- Operating Procedures - Bolero
Each Identity System Builds its Own System Rules / (Trust Framework)

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

**Enforcement Element**
- Contract(s): “I Agree” to . . .
- Legal Rules (Contractual)
  - Liability for Losses
  - Warranties
  - Termination Rights
  - Dispute Resolution
  - Measure of Damages
  - Enforcement Mechanisms
System Rules Operate Within Existing Laws

**Laws & Regulations***
(in all relevant jurisdictions)

- Authentication law
- Data retention law
- Privacy law
- IdM laws
- Tort law
- EU Data Protection Directive
- Crypto regulations
- PKI laws
- EU E-Signatures Directive

**System Rules**

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

**Legal Rules (contractual)**

- Contract: “I Agree” to . . .”
- Liability for Losses
- Warranties
- Termination Rights
- Dispute Resolution
- Enforcement Mechanisms
- Measure of Damages

---

* Written by governments; applies to all identity systems
** Written by private parties; a/k/a “trust framework;” applies to a specific identity system
All Identity Systems Use Private System Rules that Operate Within a Public Legal System

* Written by governments; applies to all identity systems
** Written by private parties; a/k/a “trust framework;” applies to a specific identity system
# Building It Internationally From the Top Down
Start with Layer 1 – Existing Laws and Regulations

## Laws & Regulations*
*(in all relevant jurisdictions)*

- Data security law
- E-transaction law
- Authentication law
- Data retention law
- Privacy law
- IdM law
- Tort law
- EU Data Protection Directive
- Crypto regulations
- PKI laws
- EU E-Signatures Directive
- Contract law
- Consumer protection law
- Warranty law
- Rules of evidence
- Law of negligent misrepresentation

* Written by governments; applies to all identity systems
Add Layer 2 -- the Concept of a Voluntary Identity Ecosystem Framework

**Laws & Regulations***
(in all relevant jurisdictions)

- Data security law
- E-transaction law
- Authentication law
- Data retention law
- Privacy law
- IdM law
- Tort law
- EU Data Protection Directive
- Crypto regulations
- PKI laws
- EU E-Signatures Directive
- Contract law
- Rules of evidence
- Law of negligent misrepresentation
- Consumer protection law
- Warranty law

**Identity Ecosystem Framework – NSTIC**
(The overarching set of interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms that structure the Identity Ecosystem)

- To be written by NSTIC Steering Group
- Not Law (but must comply with law)
- Voluntarily adopted by identity systems
- Adherence accredited - Trustmark

* Written by governments; applies to all identity systems
Add Layer 2 -- the Concept of a Voluntary Identity Ecosystem Framework

**Laws & Regulations**
* (in all relevant jurisdictions)

- Data security law
- E-transaction law
- Authentication law
- Data retention law
- Privacy law
- IdM law
- Tort law
- EU Data Protection Directive
- Crypto regulations
- PKI laws
- EU E-Signatures Directive
- Contract law
- Consumer protection law
- Warranty law
- Rules of evidence
- Law of negligent misrepresentation

**Identity Ecosystem Framework – NSTIC**
(The overarching set of interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms that structure the Identity Ecosystem)
- To be written by NSTIC Steering Group
- Not Law (but must comply with law)
- Voluntarily adopted by identity systems
- Adherence accredited - Trustmark

* Written by governments; applies to all identity systems
Add Layer 3 – Individual System Rules / Trust Frameworks (May or May Not Conform to Ecosystem Framework)

**Laws & Regulations**
*(in all relevant jurisdictions)*

- Authentication law
- Data security law
- E-transaction law
- System Rules / Trust Framework K**
- System Rules / Trust Framework D**
- System Rules / Trust Framework Z**
- System Rules / Trust Framework 4**
- System Rules / Trust Framework X**

Alternate Identity Ecosystem Frameworks – e.g., EU

- EU Data Protection Directive
- Crypto regulations
- PKI laws
- EU E-Signatures Directive

IdM law

- Data retention law
- Privacy law
- Tort law

*Written by governments; applies to all identity systems*

**Written by private parties; a/k/a “trust framework;” applies to a specific identity system
Gaps and Challenges

♦ Public Laws and Regulations
  ♦ Incomplete/ambiguous
  ♦ Don’t meet NSTIC goals/requirements
  ♦ Vary by jurisdiction – may be incompatible

♦ Ecosystem Framework
  ♦ Risk of creating competing/incompatible identity ecosystem frameworks
  ♦ Will identity systems adopt it?
  ♦ Do we need internationally agreed-upon ecosystem framework?
    ♦ At the standards level?? (Voluntary)
    ♦ At the treaty level? (Law)

♦ System rules
  ♦ Vary by identity system – may be incompatible