Building the Legal Framework for Using Digital Identity in Electronic Commerce

Seminario Internacional de Identidad Digital
Lima, Perú
5, 6 y 7 de Agosto de 2015

Thomas J. Smedinghoff
UNCITRAL

Locke Lord LLP

Locke Lord

Looking at the Complete Picture

- Digital identity raises numerous issues, including:
  - Technical
  - Processes
  - Standards
  - Social
  - Legal

- Legal issues are new and global
  - No one has figured them out yet
  - The process is starting locally
  - But no agreement on what law should do!
  - Like e-commerce law 20 years ago

New Digital Identity Laws Are Coming Online

- July 2014 – European Union **eIDAS Regulation**
  - (Electronic identification and signature)
- March 2015 – Virginia **Electronic Identity Management Act**
- July 2015 – UNCITRAL approves project to develop an international digital identity legal framework
  - Offers potential for a uniform global solution

Agenda

- The role of UNCITRAL
- The legal challenges of digital identity systems
- Building a legal framework for digital identity

The Role of UNCITRAL

United Nations
UNCITRAL

UNCITRAL

- **United Nations Commission on International Trade Law**
- **CNUDMI -- Comisión de las Naciones Unidas para el Derecho Mercantil Internacional**
- Established by the UN General Assembly in 1966
- Membership –
  - 60 member states elected by the UN General Assembly
  - All other member states invited to participate
- Core legal body of the United Nations system in the field of international trade law.
- Focus is on the modernization and harmonization of rules on international business

UNCITRAL

- Six Working Groups
  - I -- Micro, Small and Medium-sized Enterprises
  - II -- Arbitration and Conciliation
  - III -- Online Dispute Resolution
  - **IV -- Electronic Commerce**
  - V -- Insolvency Law
  - VI -- Security Interests
- State delegations to Working Groups are typically composed of subject matter experts

UNCITRAL

- Work Methods
  - Trade law texts are developed by the Working Groups
  - Non-member states and international and regional organizations are invited to actively participate
  - Decisions taken by consensus, not by vote
- Trade law texts developed by UNCITRAL include –
  - Conventions
  - Model laws
  - Legislative guides
  - Contractual rules
  - Legal Guides

Example -- Consider UNCITRAL Role in Development of E-Commerce Law

- Problems with individual early efforts
  - Utah, Germany, Colombia, and Malaysia
  - Most U.S. states, and several other countries
  - All inconsistent

- UNCITRAL entered process
  - All parties participated
  - Very synergistic process
  - Developed an agreed-upon approach – model law
  - Had major influence on development of e-commerce law globally

Highlights – WG IV: Electronic Commerce

- Model Law on Electronic Commerce (1996)
  - Legislation based on or influenced by the Model Law has been adopted in 64 States and a total of 139 jurisdictions
- Model Law on Electronic Signatures (2001)
  - Legislation based on or influenced by the Model Law has been adopted in 31 States
- UN Convention on the Use of Electronic Communications in International Contracts (2005)
  - Ratified by 7 States so far
- Major impact on development of e-commerce law and on international harmonization of such law
  - New paradigm for development of law

UNCITRAL - Identity Management Proposal

- July 2015 meeting –
  - Proposal that WG IV undertake a project to address digital identity management
  - Submitted by --
    - Austria, Belgium, France, Italy, and Poland
    - American Bar Association Identity Management Legal Task Force
  - Goal – Develop a "basic legal framework covering identity management transactions"

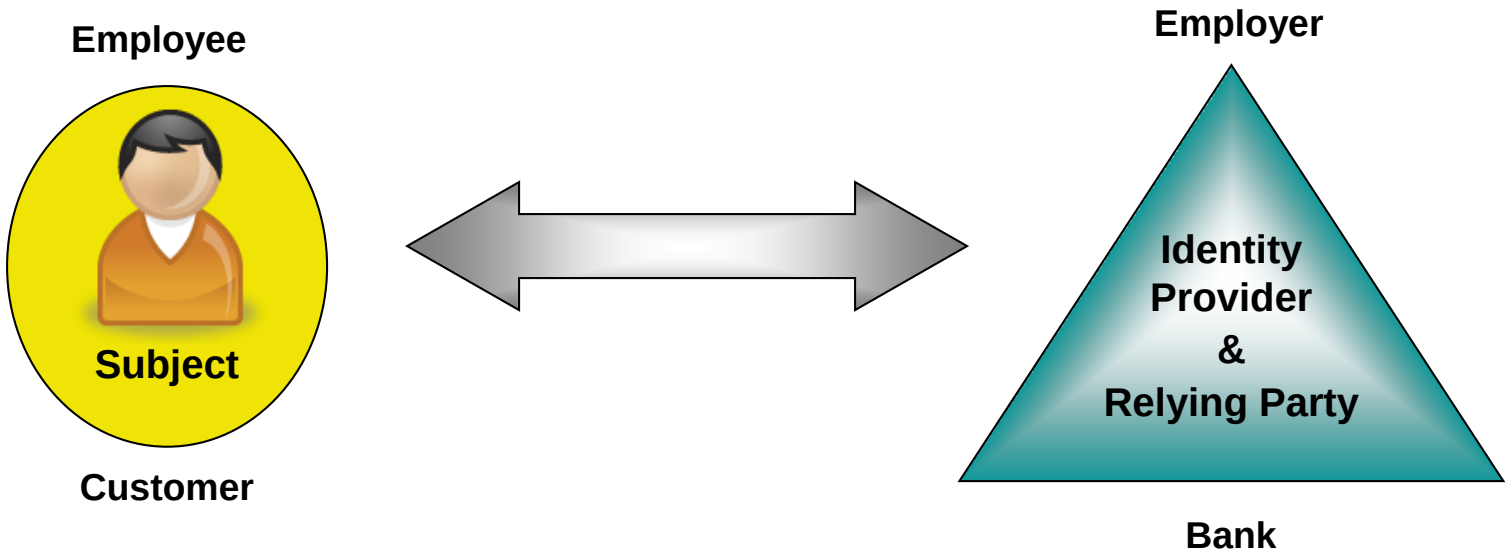
- UNCITRAL agreed that Working Group IV should begin the process of undertaking work on a legal framework for digital identity management

THE LEGAL CHALLENGES OF DIGITAL IDENTITY SYSTEMS

1. Digital Identity Involves Multi-Party Systems

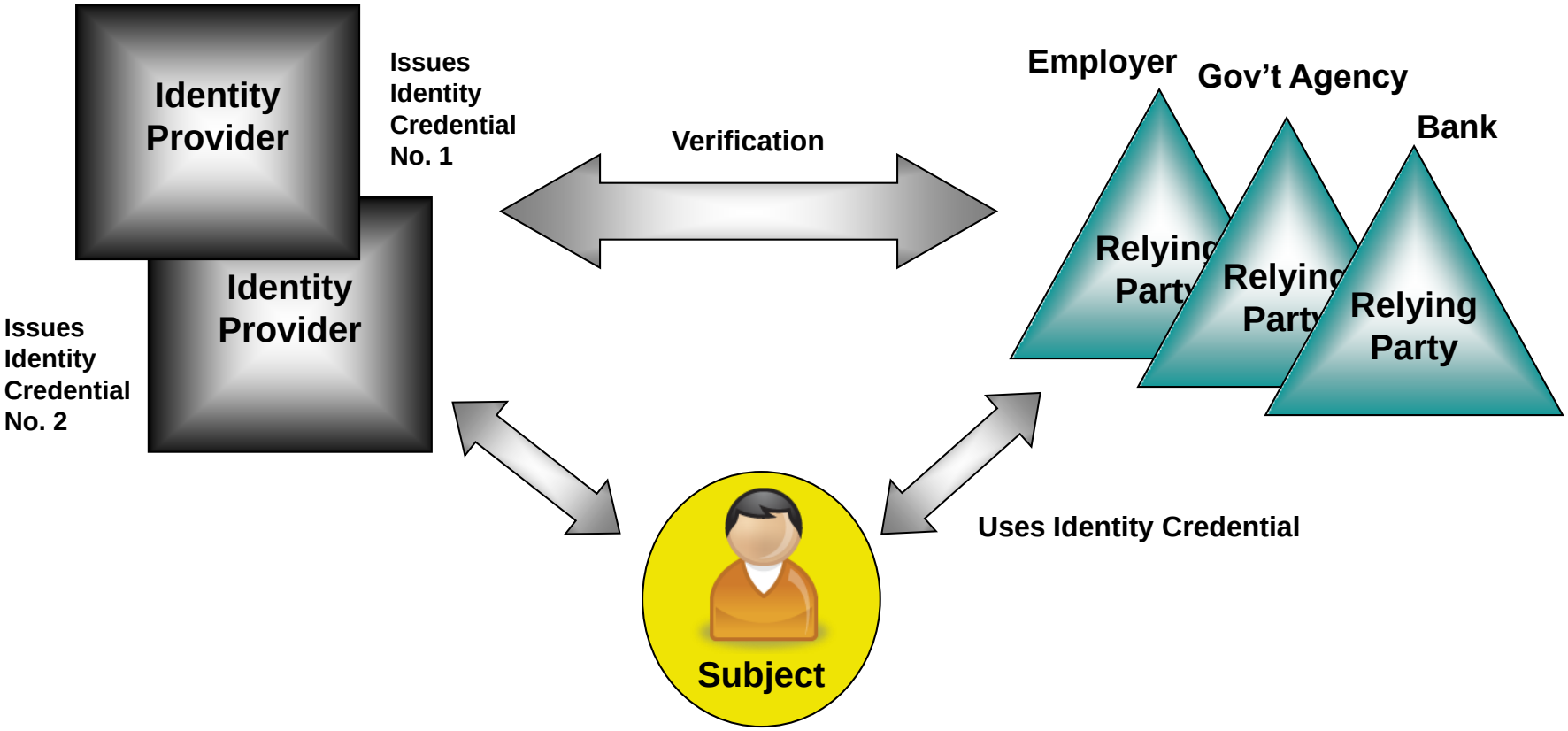
Traditional Two-Party Approach to Identity

Relying party and identity provider are the same entity



Emerging Multi-Party Approach: Federated Identity Management

Relying Parties rely on identity credential from multiple third party Identity Providers



Key Goals

- Allow users to -
  - Obtain identity credentials -
    - From one or more identity providers
  - Use credentials -
    - At multiple relying parties
    - Located in multiple jurisdictions
- Allow relying parties to accept and verify credentials -
  - From multiple identity providers
  - From multiple jurisdictions
- And all parties trust the processes and results

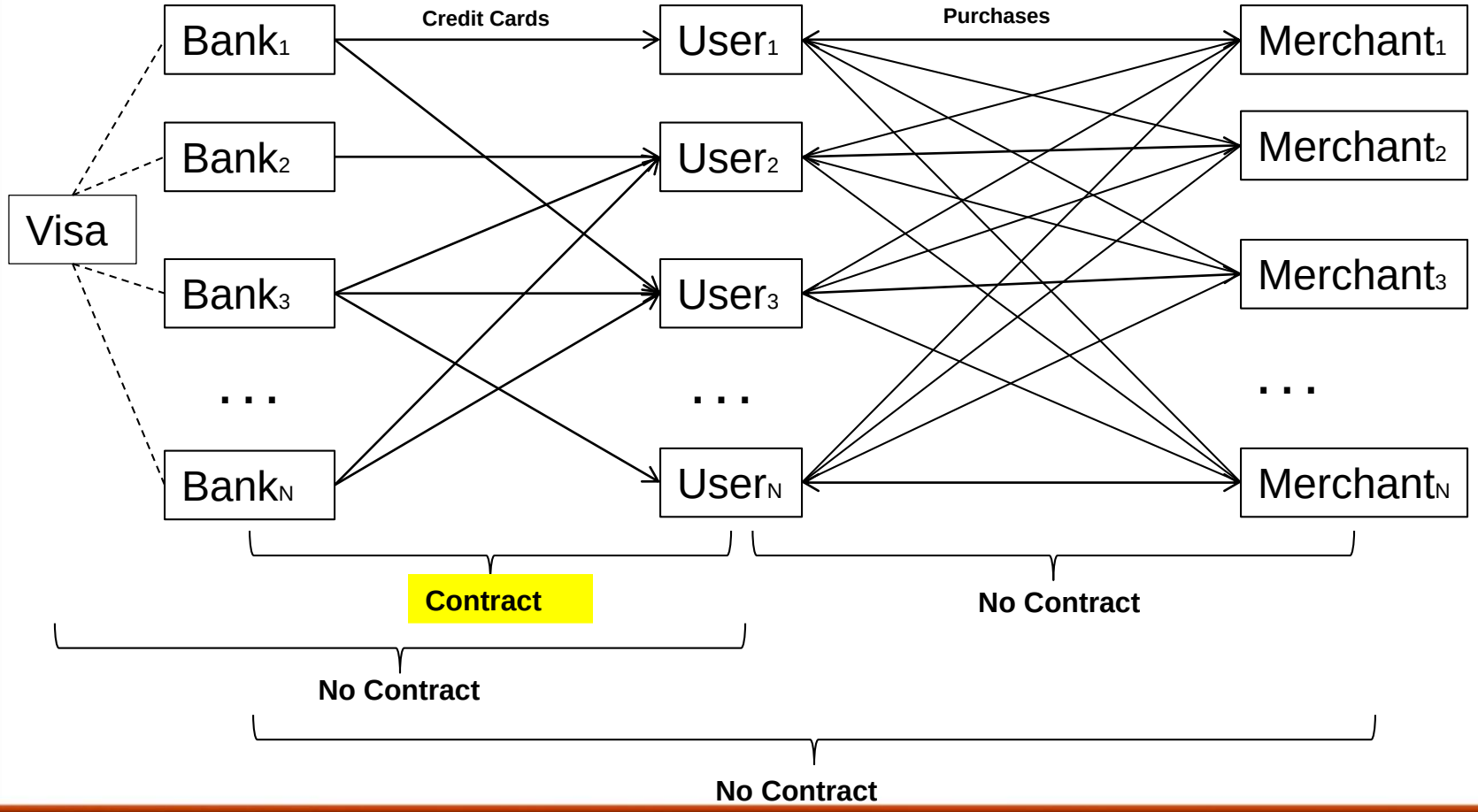
Issues with a Multi-Party System

- Large pool of participants interact with each other on a random basis
- Connections between participants are often indirect
- Need to be sure everyone acts properly so the system works for all participants
- Need to ensure that all participants trust both –
  - The operation of the system, and
  - The performance of each participant
- Not practical to have bi-lateral contractual relationships between all of the parties – need alternate approach

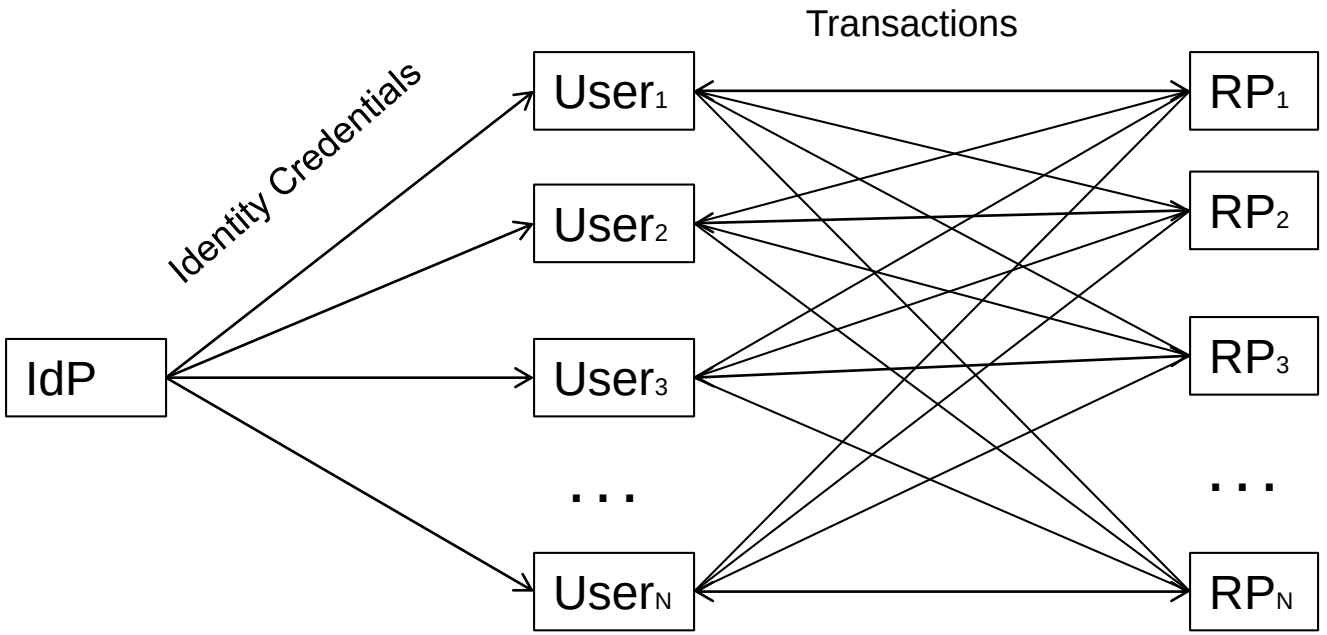
- **Note:** Identity systems are **analogous to credit card systems**

Interactions of a Multi-Party Credit System

Data Flow: Multiple Banks issue credit cards to multiple cardholders (Users) who use those cards to make purchases from multiple Merchants

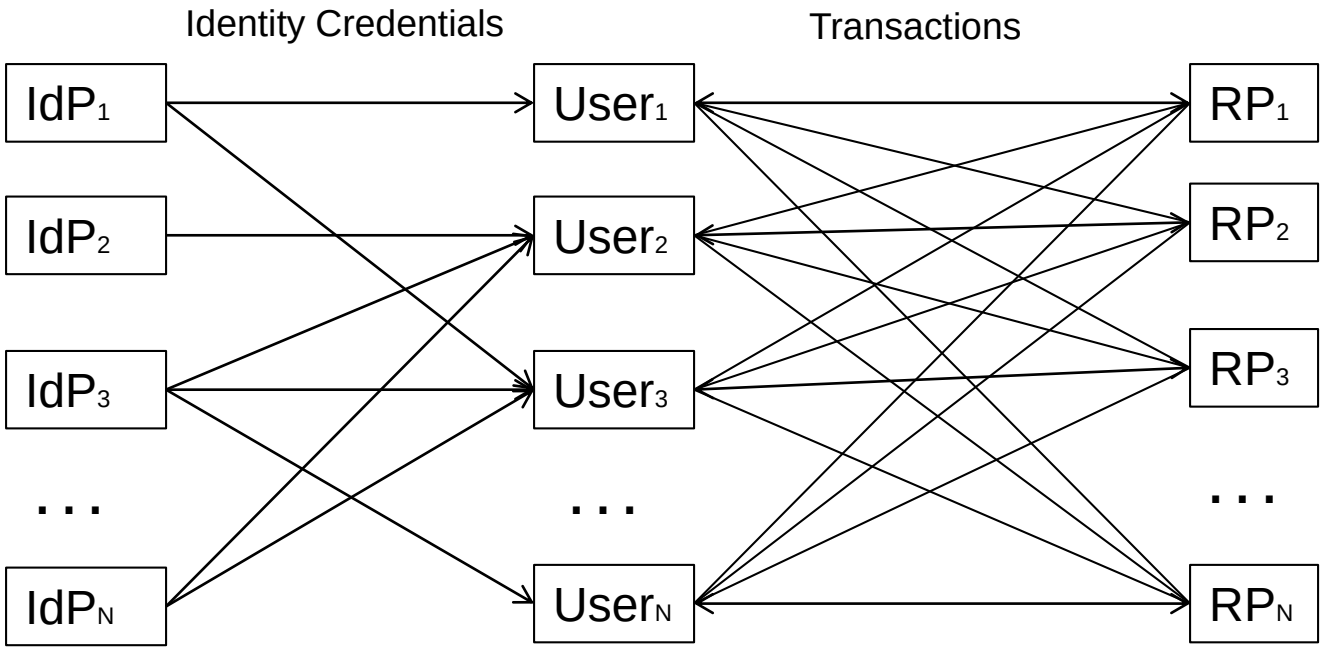


Interactions of a Multi-Party Identity System



Data Flow: Multiple IdPs issue identity credentials to multiple users who use those credentials to make enter into online transactions with multiple RPs

Interactions of a Multi-Party Identity System



Data Flow: Multiple IdPs issue identity credentials to multiple users who use those credentials to make enter into online transactions with multiple RPs

Problems Can Arise;
Key Multi-Party Identity System Risks

- Operational Risk
- Data Accuracy Risk
- Authentication Risk
- Privacy Risk
- Data Security Risk
- Legal Risk (e.g., liability, violation of law)
- Enforceability Risk

Mechanisms to Reduce Risks

- Technology
- Processes
- Performance of the participants
- Defined duties and obligations

2. Multi-Party Identity Systems Need Rules and a Legal Framework

Multi-Party Identity Systems Need Rules to -

- Make the system "operationally functional"
  - To specify technology and processes so that it "works"
  - So that everyone knows what to do
- Make the system "legally functional"
  - Define participant legal rights, duties, and obligations
  - Clearly define and fairly allocate liability risks
- Make the system "trustworthy"
  - Address and minimize the risks (beyond mere functionality)
  - Make duties and obligations binding and "enforceable"
  - Ensure that participants have confidence in the results and are willing to rely on them

Rules Require a Legal Framework to . . .

- Define and clarify which rules apply
- Specify which rules apply to which participants
- Allocate risk and liability among participants
- Make the rules enforceable
- Provide remedies for violations

Some Basic Questions . . .

- What is a legal framework?
- How is it structured?
- Who builds it?
- How is it enforced?
- How does it work cross-border?

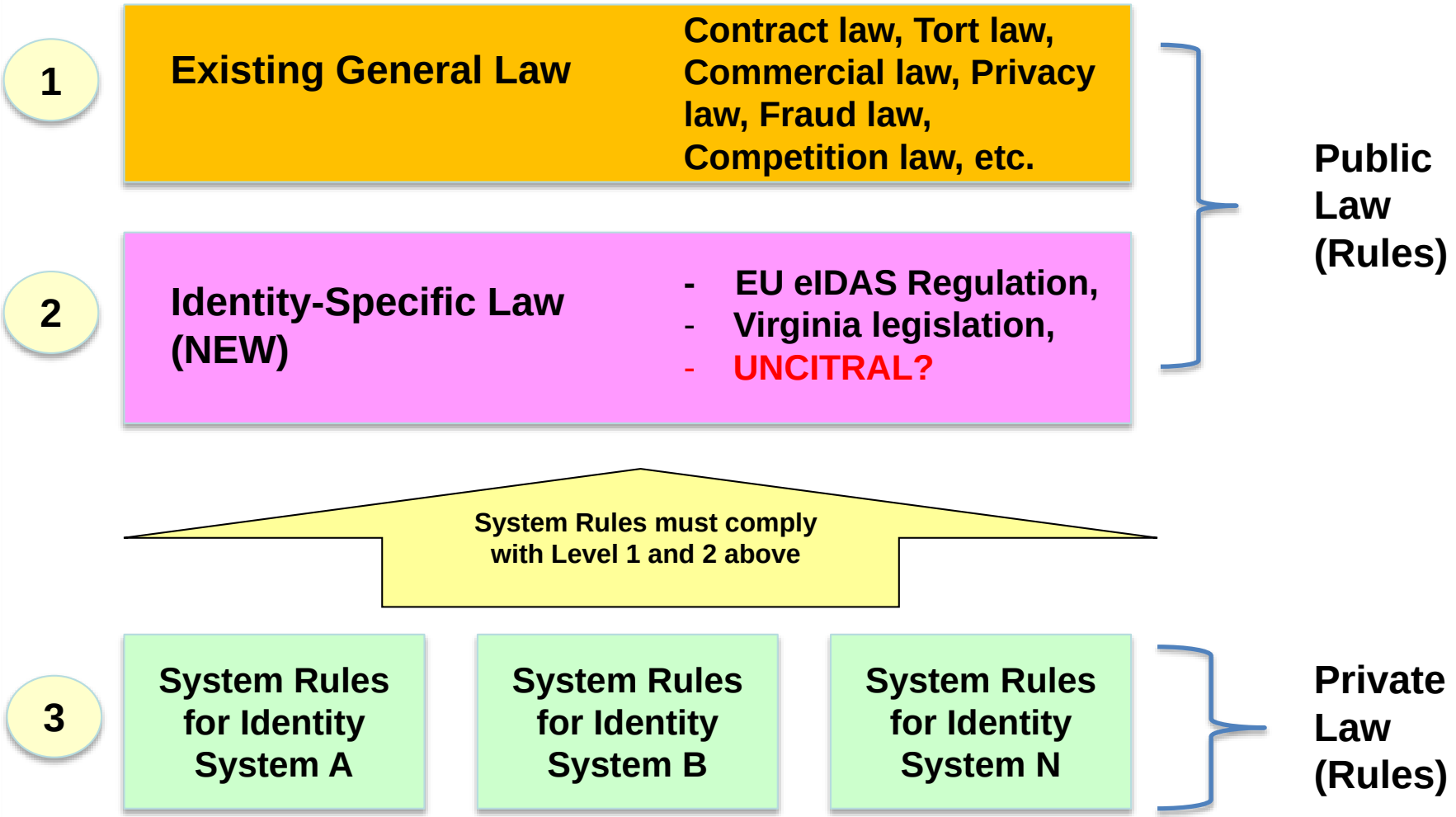
- How does UNCITRAL fit in?

Developing a Legal Framework for Digital Identity

What Is a Legal Framework?

- A broad system of **rules**
- consisting of the **laws, regulations**, and binding **contractual commitments**
  - that apply to a specific system, or in a specific context, and
  - that establish the rights and obligations of the relevant parties

Identity Systems are Governed by a Three-Level Legal Framework



Legal Framework – Level 1
Existing General Law

- Characteristics
  - Public law (enacted by government)
  - Currently exists – consists of existing statutes, regulation, and case law
  - Not written to address identity issues
  - Not always clear how it applies to identity
- Examples
  - Existing contract law, tort law, data protection law, commercial law, personal injury law, fraud law, competition law, etc.
- Problems
  - Not easily applied to digital identity
  - Not interoperable
  - Not easily changed
  - May raise legal barriers

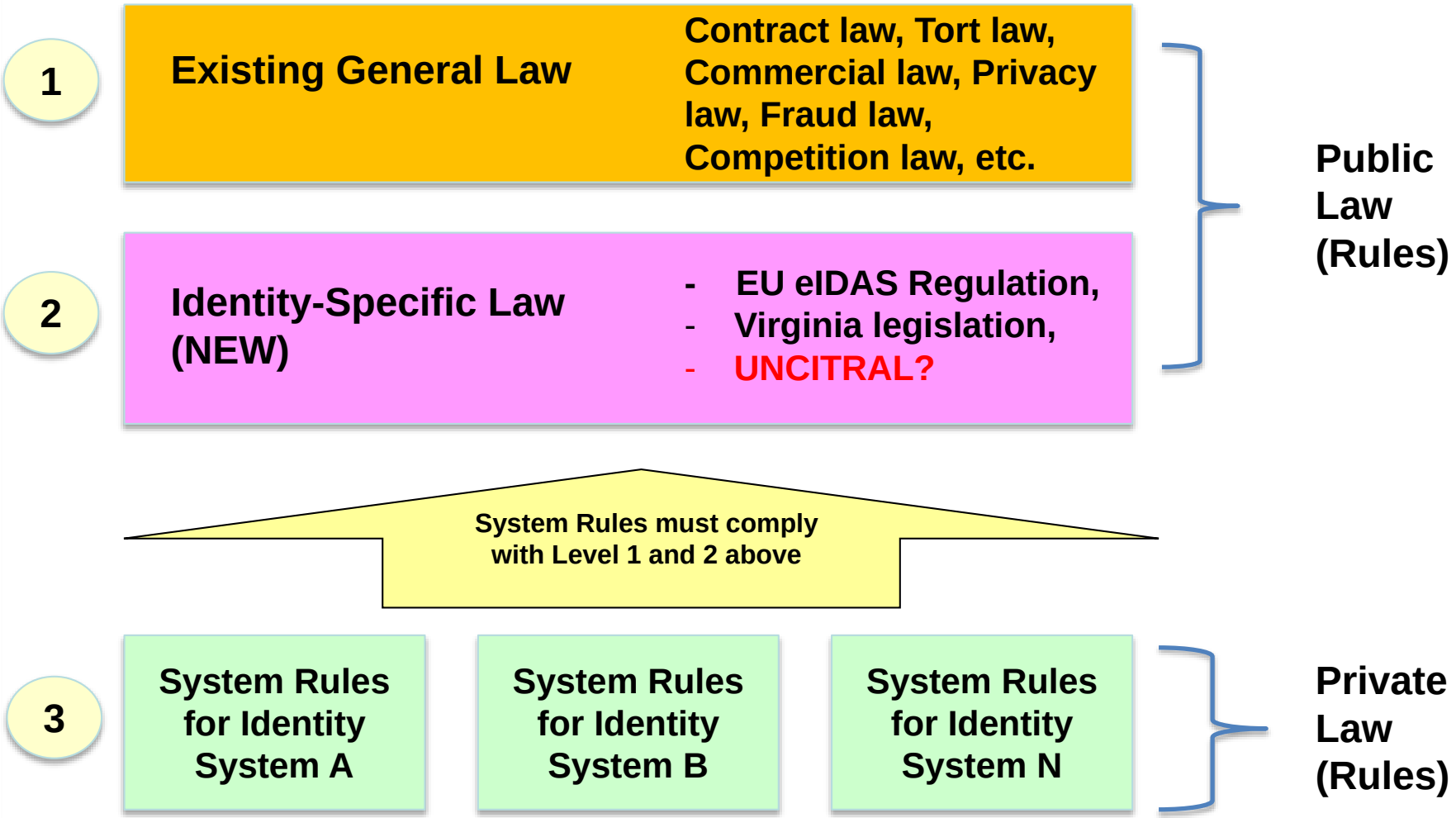
Legal Framework – Level 2
(New) Identity-Specific Law

- Characteristics
  - Public law (enacted by government)
  - Consists of new statutes and/or regulations
  - Written to specifically address online identity management
  - Apply to all identity systems
  - Can be used to encourage the marketplace or regulate it
- Examples
  - EU eIDAS Regulation,
  - Virginia Electronic Identity Management Act
  - UNCITRAL?
- Possible Problems
  - No one is sure what issues it should address
  - May become outdated as technology or business models change
  - May stifle marketplace development
  - May not be interoperable; Hard to change

Legal Framework – Level 3 Contracts (Private Law)

- Characteristics
  - Private law – (contract-based; agreed to by the participants)
  - Developed specifically for a particular identity system
  - Applies only to a specific identity system
  - Applies only to those participants that contractually agree
- Examples
  - System rules for Gov.UK.Verify, US FICAM, IdenTrust, SAFE-BioPharma, Certipath, CA/Browser Forum, etc.
- Problems
  - May conflict with existing law
  - Need to get agreement on terms
  - Need to get all participants to sign

Identity System Legal Framework: Three Levels of Rules Can Govern



Level 3 Law
Private System Rules

Level 3 Private Law - System Rules Are . . .

- A contract-based set of
  - Business and technical rules
  - Contractual legal rules
- That include
  - Standards, processes
  - Rules, requirements, and obligations
  - Enforcement mechanisms

  applicable to the parties exchanging identity information

- They function like the rules that govern other multi-party systems such as the –
  - Credit card system operating rules, or
  - Payment system operating rules

Those Contract-Based System Rules Go By Various Names, such as . . .

- **Trust Framework** – NSTIC / Kantara / U.S. FICAM
- **Scheme Rules –** UK IDAP / GOV.UK.Verify
- **Operating Policies** - SAFE-BioPharma
- **Federation Operating Policies & Practices** - InCommon
- **Operating Rules** – FIXs / CAHQ (health info exchange)
- **Operating Rules and System Documentation** - IdenTrust
- **Common Operating Rules** - CertiPath
- **Guidelines** – CA/Browser Forum

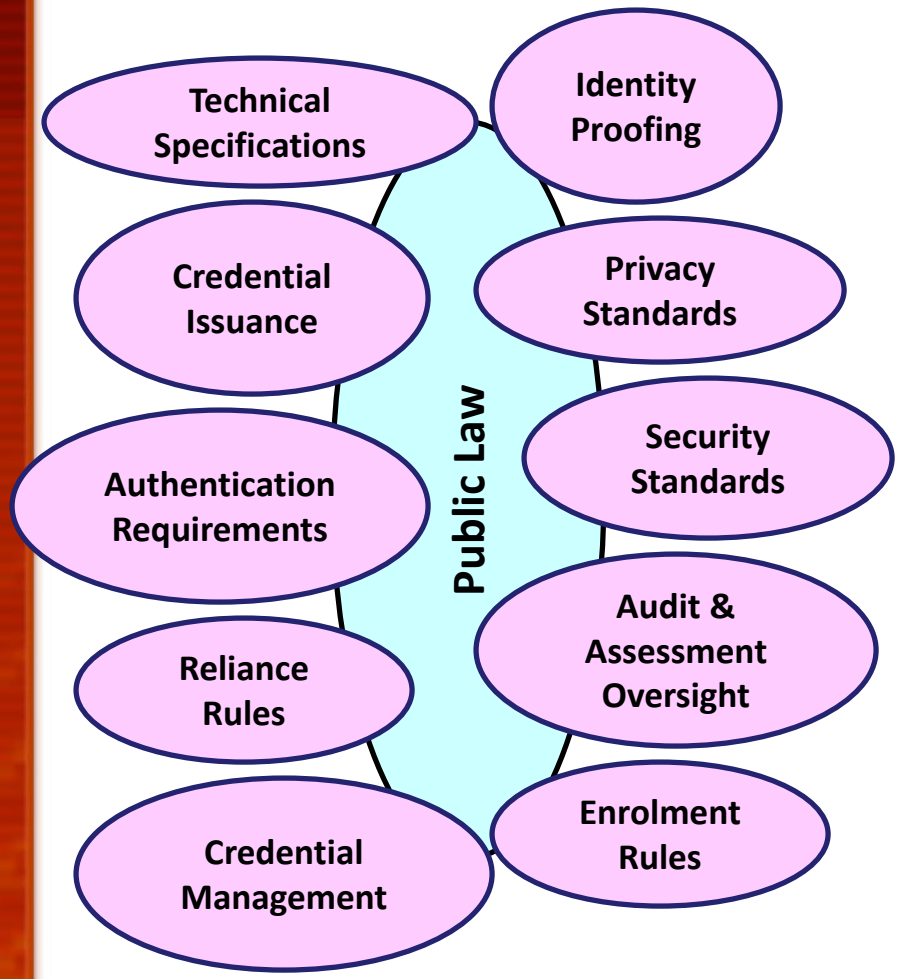
- **Operating Regulations** - Visa (credit)
- **Operating Rules** – NACHA (electronic payments)
- **Operating Procedures** – Bolero (e-bills of lading)

Level 3 Contract-Based System Rules Cover Two Categories of Issues

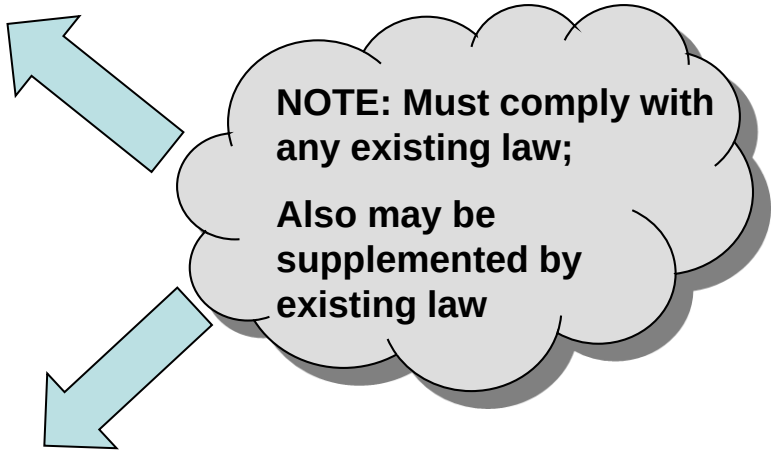
- 1. Business and technical rules and standards
  - To make identity system work
  - To minimize risks

- 2. Legal rules (defined by contract)
  - To govern the legal rights of the parties
  - To allocate risks

Business & Technical Rules: (Components Necessary to "Make it Work")



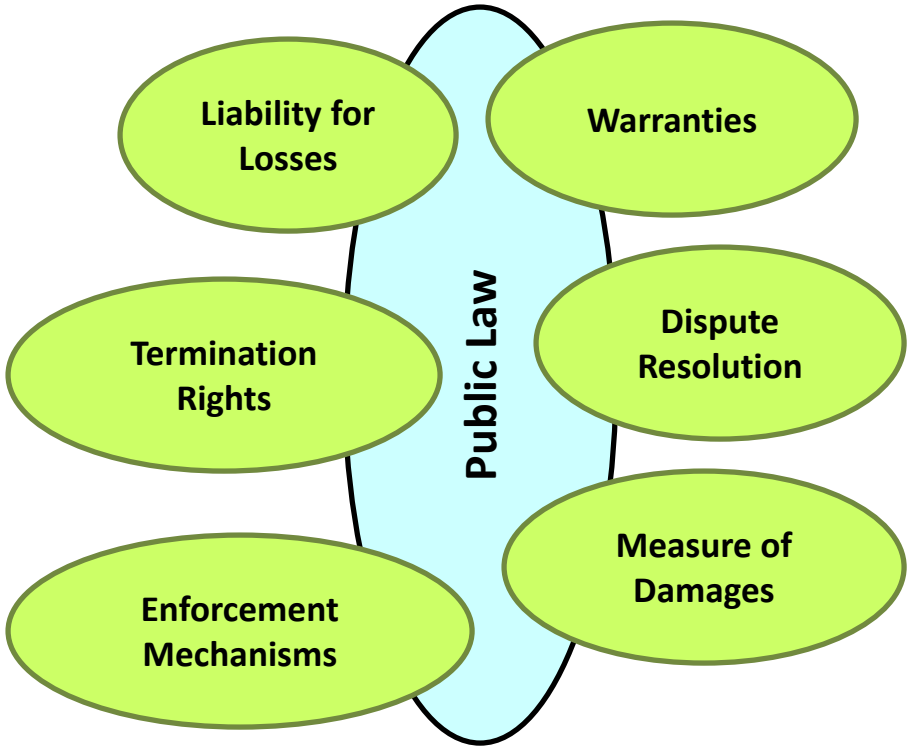
Partial listing of Business & Technical Rules



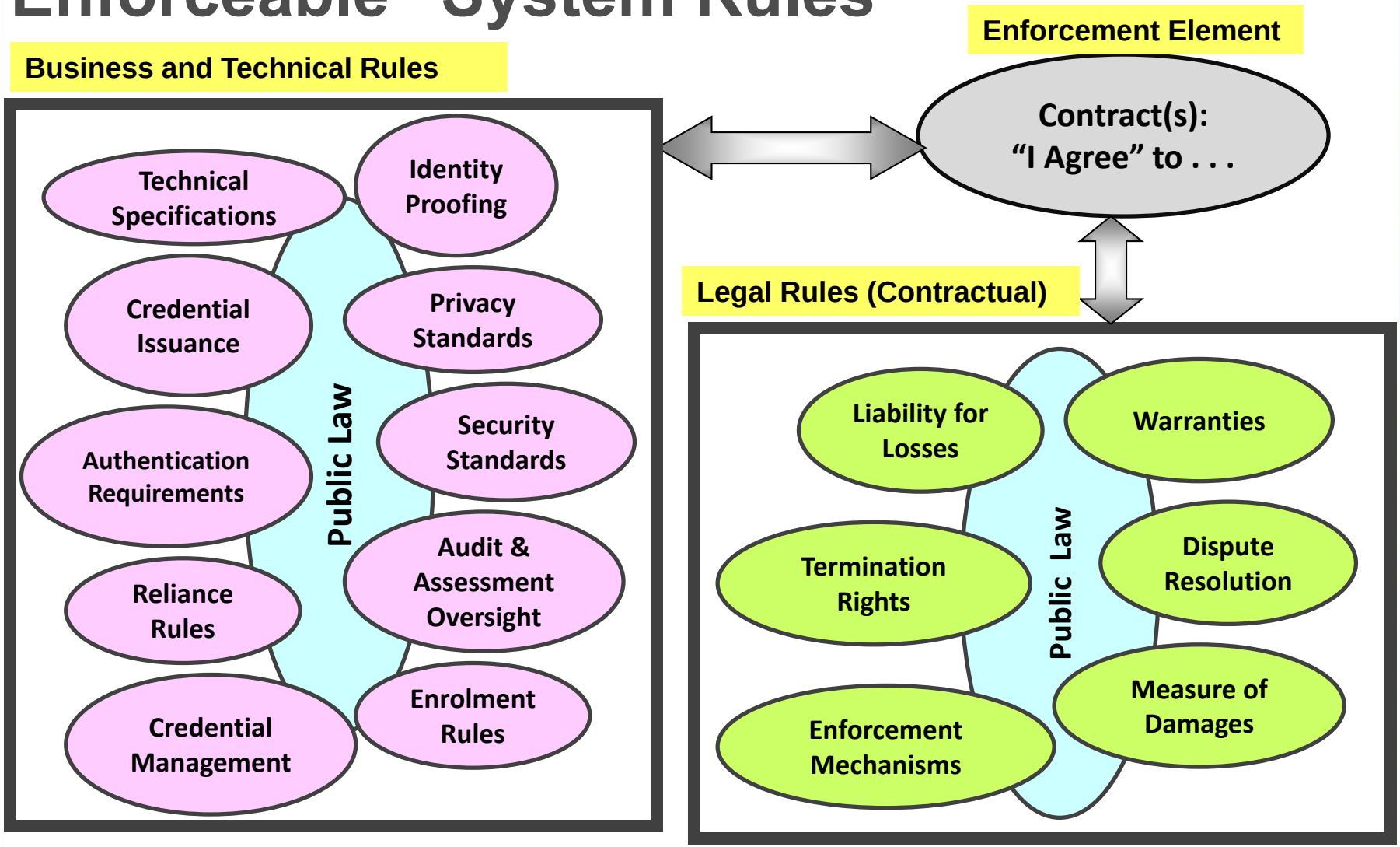
Legal Rules (contract-based) (To Govern Legal Rights of the Parties)

Existing Law as Supplemented and/or Modified by Private Legal Rules

Partial listing of Legal Rules



Putting It All Together to Form Enforceable "System Rules"



So What Is the Role of Level 2 Identity-Specific Law?

And How Does UNCITRAL Fit In?

Key Question for Level 2 Law

- What issues should Level 2 identity-specific law address?
- Which issues should be left to the parties to contractually define in Level 3?

UNCITRAL Role

- UNCITRAL provides an international process by which States can jointly figure out how to address the legal issues of digital identity management

- Determine appropriate goals
- Design identity-specific law to meet those goals
- Assist States in developing domestic identity-specific law
- Assist in facilitating international interoperability of identity systems

Potential UNCITRAL Goals Include . . .

- Encourage the development of identity systems
- Facilitate use of digital identity for both commercial use and access to government services
- Facilitate use of digital identity across borders – i.e., internationally
- Facilitate interoperability across different identity systems
- Harmonize international legal approaches to facilitate commercial transactions that require identity

Possible Approach of Identity-Specific Law

- Remove barriers created by existing Level 1 law
- Fix problems with existing Level 1 law
  - E.g., issues that Level 3 private system rules cannot resolve
- Provide gap-fillers (for issues not addressed at Level 3)
- Promote trust in identity systems
- Facilitate legal recognition of identity and authentication
- Facilitate identity system interoperability
  - Both cross-system and cross-border
- Encourage and incentivize development of identity systems
- Regulate Level 3 private system rules

Possible Principles for Identity-Specific Law

- Technology neutrality
- Identity system neutrality
  - Accommodate many different identity systems models
  - Recognize that there is no one-size-fits-all approach
- Adaptability
  - Accommodate future changes in technology, standards, and business models
- Party autonomy
  - Allow variation by contract
  - e.g., via system rules

Possible Issues That Identity-Specific Law Might Address

- Remove legal barriers, ambiguities, and uncertainties in existing Level 1 public law
  - Liability
  - Reliance
  - Third party rights
  - Legal effect of authenticated identity
- Interoperability of identity credentials
  - Cross-system
  - Cross-border (legal interoperability)
- Facilitate trustworthiness
  - Levels of assurance
  - Data security
  - Certification, audits, etc.
  - Presumptions

Consider Liability for Example; Concerns for all Roles

- Identity Provider
  - Incorrectly identifying or authenticating a user
  - Failing to protect or misusing a user's personal data
  - Delay or failing to verify or revoke credential
- Relying Party
  - Relying on a false credential
  - Failing to protect or misusing a user's personal data
- User / Data subject
  - Providing false identity data
  - If someone else uses the credential
  - If someone misuses personal data?

Some Basic Liability Questions

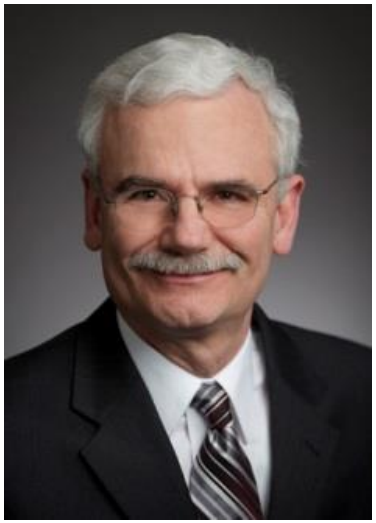
- Liability of each role
- Liability for what?
- Liability to whom? Third parties?
- What legal theories are applicable?
- Impact of system rules?
- Any safe harbors?
- Rights to limit liability?

Can We Legislate Trust?

Next Step for UNCITRAL

- Convene experts group in Fall 2015
- Hold a colloquium
- Decide on a direction, and begin work in 2016

Questions?



Thomas J. Smedinghoff
Locke Lord LLP
111 S. Wacker Drive
Chicago, IL 60606
Tom.Smedinghoff@lockelord.com