Facilitating Identity Management in the Digital Economy:

UNCITRAL's Post-COVID Challenge for eCommerce

Thomas J. Smedinghoff
Locke Lord LLP
Chicago

UNCITRAL Texts
and COVID-19 Response and Recovery
Identification and Authentication in the Digital Economy
July 8, 2020

© 2016 Locke Lord LLP
www.lockelord.com

What Are We Talking About?

- **Identity Management (IdM)** -- A set of processes, policies, and procedures to address two basic questions –
  - Who are you? (**Identification**)
  - How can you prove it? (**Authentication**)
- **Identity Management System (IdM system)** –
  - a group of participating entities,
  - acting in accordance with a set of rules, and
  - utilizing a set of IdM processes, policies, and procedures, specified in those rules,
  - to provide, or use, identity management services
  - that allow an individual to identify himself with multiple unaffiliated entities in the system
    - Like the global passport system
    - Analogous to a credit card system

Why Is IdM Important?

- It facilitates online commerce and other digital transactions
  - Online access; e-signatures; e-contracting; digital communications, etc.
- It helps to manage data security
  - Restrict access, communications, etc. to "*authorized* persons"
- It's the answer to the challenge we face in remote transactions – Trust!
  - How to obtain sufficiently reliable identity information about a remote party in an online transaction to proceed

COVID Has Accelerated the Need for Remote Identity Management

- COVID has emphasized the need for remote transactions
  - "Work from home" is the new norm
  - eCommerce is the way most purchases are made
  - Financial transactions rapidly becoming remote, enhancing the need for eKYC
- eCommerce, remote transactions, and remote electronic access is becoming the way of commerce in the post-COVID

- It is often critical to know "who"?
  - Who wants access?
  - Who signed?
  - Who is being certified as COVID-free?
  - Who am I dealing with?

COVID Is Also Introducing New Identity Requirements

- A need for new data attributes, such as test status
  - E.g., Tested negative as of [date]
  - E.g., Has COVID antibodies
- A need for new identity credentials
  - E.g., Certified COVID-free
- A need for adaptability, flexibility, and speed to respond to new COVID challenges, such as contact tracing

Private Sector Is Uniquely Positioned to Provide Needed Identity Systems

- The private sector is leading the way in:
  - developing IdM systems to support a variety of economic activities
  - experimenting with new types of identity systems
  - developing identity standards and protocols
  - writing the software

- Identity for eCommerce will likely be provided primarily by private sector identity systems

Private Sector also in a Unique Position to Address New COVID Issues

- The private sector is often **best able to react quickly** to new challenges like COVID,
- It has the **adaptability, flexibility, and speed** needed to –
  - Respond to new COVID challenges
  - Develop new IdM system models, as needed
  - Partner with and support government efforts to respond
- An example is the **COVID-19 Credentials Initiative** currently working to develop a COVID-related identity system (see https://www.covidcreds.com/)
- Government IdM systems are often not set up to address unique COVID requirements – e.g., COVID status, etc.

The Challenge: IdM Systems are Complex Multi-Party Systems

- **Multiple participants and participant roles**
  - IdPs, Identity verifiers, identity authenticators, RPs, attribute providers, hubs, brokers, certifiers, auditors, etc.
- **Numerous critical IdM processes**
  - Enrolment, identity verification, credential issuance, authentication, credential revocation, data encryption, etc.
- Each IdM system **needs to coordinate** the conduct of the participants and the IdM processes, policies, and procedures so that the –
  - System works properly
  - Participant rights and responsibilities are defined
  - System is trustworthy
- Solution is a **Governance Framework**

What Is a Governance Framework?

- A Governance Framework is –
  - A written **set of rules,**
  - **Uniquely designed** to govern a specific IdM system,
  - Addresses the **business, technical, and legal issues** necessary to the operation of that IdM system,
  - **Legally binding** on all of the participants

- It is sometimes referred by other names such as –
  - Trust Framework
  - Scheme Rules
  - Operating Rules
  - System Rules

- Analogous to –
  - Credit card system rules (e.g., Visa or Mastercard)
  - Payment system rules (e.g., ACH or Swift)

Purpose of a Governance Framework

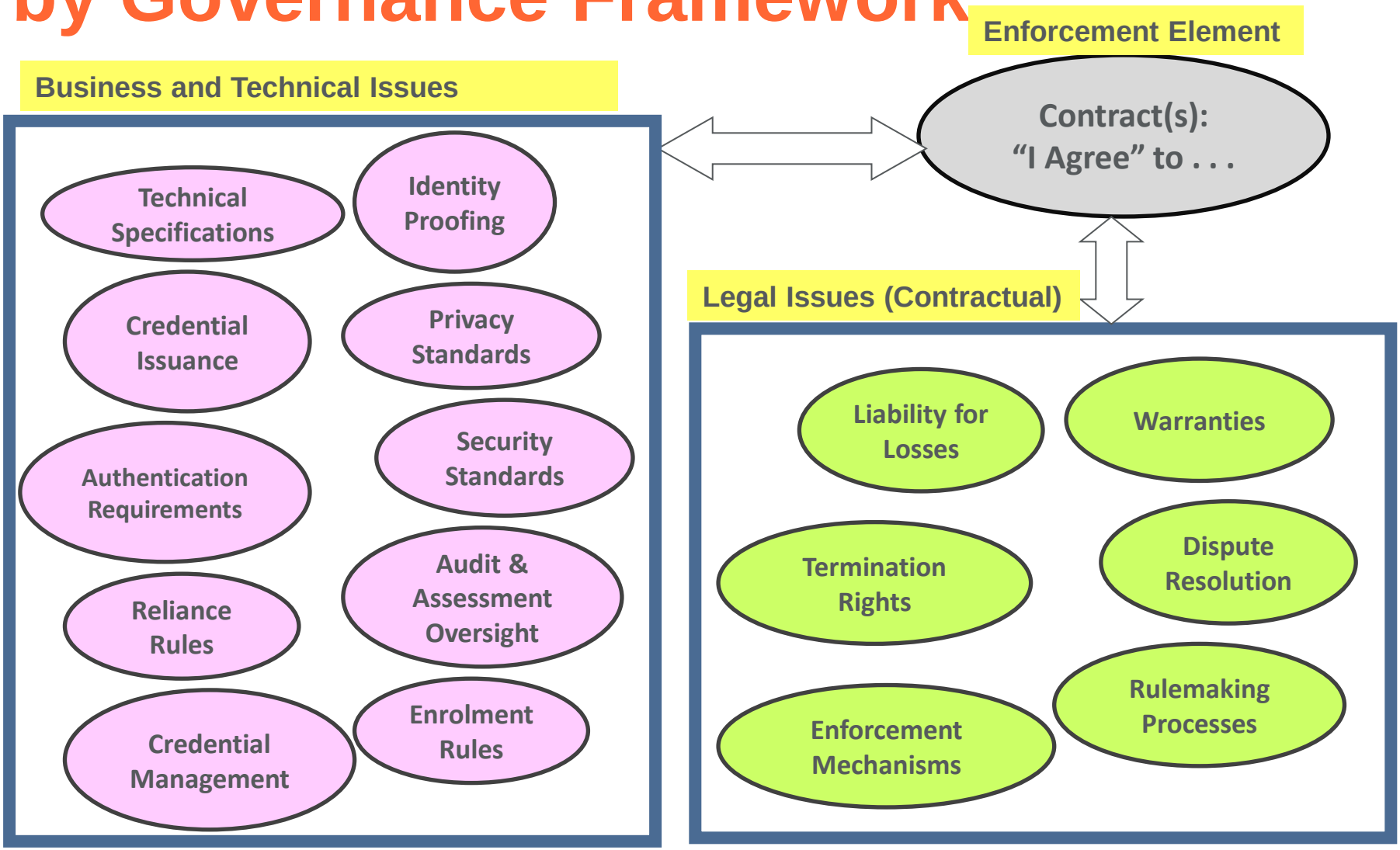
- Make the specific IdM system "operationally functional"
  - Specify all of the procedures and processes, so that it "works"
  - Specify duties of each role, so that everyone knows what to do
- Define the "rights & responsibilities" of the participant roles
  - Define procedural and legal rights, duties, and obligations
  - Define and fairly allocate liability risks
  - Make duties and obligations binding and "enforceable"
- Make the specific IdM system "trustworthy"
  - Goes beyond merely functional
  - Address and minimize the risks
  - Implement steps to ensure that participants have confidence in the results and are willing to rely on them

Source of Governance Framework

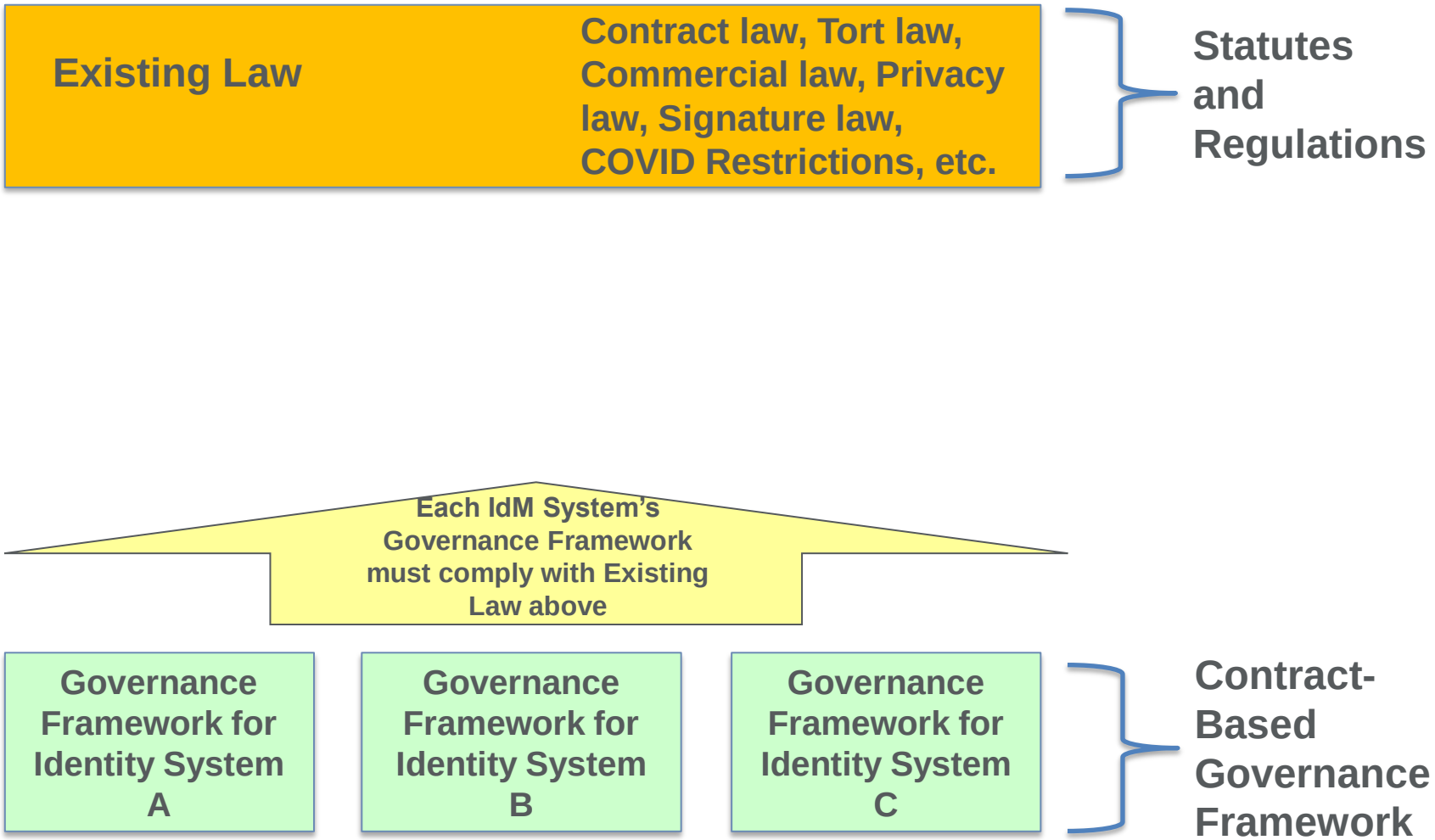
- **Public Sector ID systems** typically use **statutes** and/or regulations to provide the Governance Framework – e.g.,:
  - India - Aadhaar Act
  - Estonia - Identity Documents Act
  - EU – eIDAS Regulation

- **Private Sector ID system**s typically use **contracts** to provide the Governance Framework – e.g.,:
  - SAFE BioPharma Trust Framework
    https://www.safe-biopharma.org/SAFE_Trust_Framework.html
  - Sovrin Governance Framework
    https://sovrin.org/library/sovrin-governance-framework/
  - Pan-Canadian Trust Framework
    https://drive.google.com/file/d/1Xmjh8QJZKWmRkaTtE2f43ISntD7jE6D5/view

Types of Issues Potentially Addressed by Governance Framework



Contract-Based Governance Framework Must Comply With Existing Law



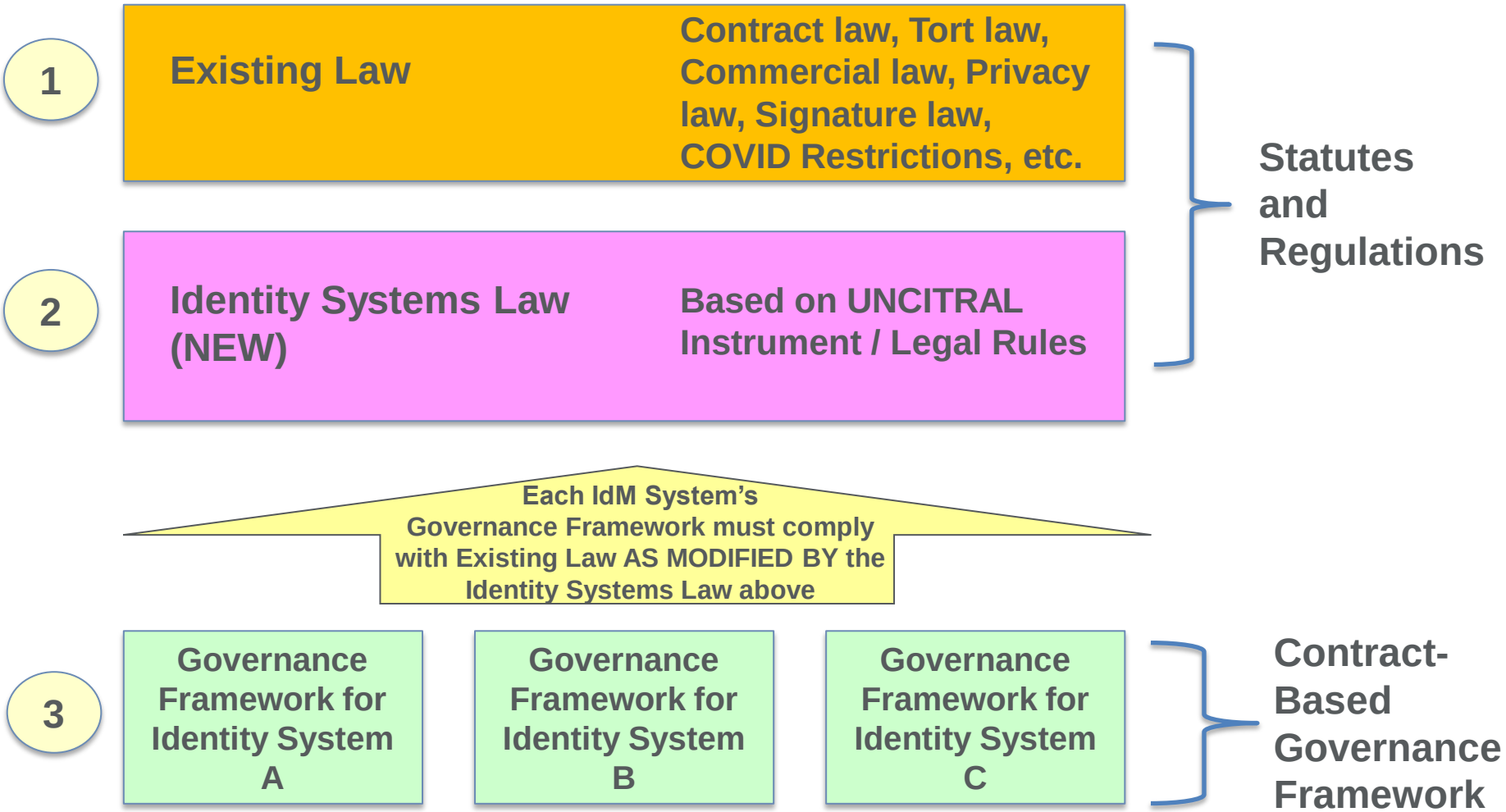
But Existing Law Raises Problems for Private Sector IdM Systems

- **Barriers** to ID systems, such as requirements to use specific documents to satisfy identification requirements
- **Ambiguities** in existing law, such as whether tort liability can be limited or disclaimed; how data security law applies
- **Inappropriate rules** for IdM systems, such as form requirements for certain identity documents
- **Prohibitions** on private IdM system –
  - Interaction with government IdM systems, or
  - Use of government identification numbers, such as SSN

UNCITRAL's Challenge: Develop an Instrument that --

- Recognizes that the structure and design of each IdM system is unique, and should be governed by a Governance Framework specific to that IdM system,
- Addresses the problems existing law creates for IdM systems that cannot be addressed via a Governance Framework
- Facilitates flexible and adaptable Governance Frameworks for a variety of IdM system solutions to assist the private sector in --
  - Meeting the increasing need for remote identification and authentication in a variety of commercial situations
  - Responding to COVID and other unique challenges that arise from time-to-time

Solving the Problem with an Identity Systems Law Based on UNCITRAL Instrument:



Moving Forward, UNCITRAL's Instrument Might Address --

- Equivalence of digital IDs to paper IDs
- When IdM system credentials satisfy various legal identification requirements
- The right of IdM systems to:
  - use / rely on information from government identity systems
  - use government issued identifiers (e.g., SSN, national ID number, etc.)
- Applicability of existing tort law to IdM system participants
- Right of participants to limit or disclaim existing tort law liability
- Requirements for the enforceability of a Governance Framework
- Rules for domestic and cross-border recognition of identity credentials
  - In private sector transactions
  - When used to satisfy legal identification requirements
- Applicability of Governance Framework to non-contracting relying parties