United Nations A/CN.9/WG.IV/WP.165

General Assembly

Distr.: Limited
30 September 2020

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Sixtieth session
Vienna (online), 19–23 October 2020

Reconsideration of approach to identity management and trust services

Submission by the United States of America

Note by the Secretariat

The United States of America submitted a paper for consideration at the sixtieth session of the Working Group. The paper is reproduced as an annex to this note in the form in which it was received by the Secretariat.

V.20-05628 (E)

Annex

Reconsideration of approach to identity management and trust services

1. The United States is pleased to submit this paper on the current project in Working Group IV on identity management (IdM) systems and trust services. This paper is divided into three sections. The first section of this paper provides a general overview and executive summary of the subsequent sections. The second section provides background on IdM systems and their operating rules. Finally, the third section provide an overview of the legal framework on which all IdM systems generally operate and a conceptual framework for how the Working Group could adapt WP.162 to effectively address private sector IdM systems.

2. For purposes of this paper, the United States focuses only on IdM systems and how the Working Group can address IdM systems effectively. That said, the United States would welcome a similar discussion in the Working Group on the trust services portion of WP.162, as we believe it raises many of the same conceptual issues as outlined below regarding the IdM provisions.

I. Overview and executive summary

3. As an overarching matter, the United States has fundamental concerns with the current approach of the Working Group regarding IdM systems reflected in WP.162 (see appendix), and is of the view that a discussion in the Working Group at a conceptual level is necessary to address these concerns.

4. The task for UNCITRAL should be to provide a framework that can help States navigate the legal issues that may arise with private sector IdM systems, in particular in areas that the individual contract-based operating rules governing each IdM system cannot cover. This could include revising existing national law to remove barriers and uncertainties in existing law, filling gaps in existing law relevant to IdM systems that cannot be addressed by contract, or addressing new issues that can promote the development of private sector identity systems. However, WP.162 takes a significantly different, and, in the U.S. view, unworkable, approach.

A. What are IdM systems?

5. **Identity management** involves a set of policies, processes, and procedures to allow for identification of an individual or entity (i.e., who are you?) and authentication of that identity (i.e., how can you prove it?). As more fully described in Section II below, an **identity transaction** is a communication that provides some of that identity information about a subject to a relying party in a manner that authenticates the relationship between that identity information and the subject. Such **identity transactions** are facilitated by IdM systems. **IdM systems** are complex arrangements that involve a coherent combination of participating entities, processes, and technology, where each participant performs the responsibilities of one or more predefined roles, in accordance with a predefined set of legally binding processes, policies, and procedures, for the purpose of facilitating identity transactions that will allow an individual to identify him or herself with multiple unaffiliated entities.

6. To make this work, each IdM system needs an enforceable set of Operating Rules. As more fully described in Section II below, Operating Rules govern the operation of the individual IdM system, specifying how its identity management processes and the corresponding identity transactions are to be conducted, and the rights and responsibilities of the various parties to the arrangement. As each IdM system is different, each one requires a unique set of Operating Rules tailored to its purpose, structure, participant base, and risk profile.

7. In the case of public sector IdM systems, the Operating Rules are usually set out in a statute or regulation, and thus, made binding on the participants by force of law. In the case of private sector IdM systems, the Operating Rules are set out in a document written by the system operator (or some other person or entity), and made binding on the participants by contract.

B. What should an UNCITRAL instrument address?

8. Any instrument developed by UNCITRAL for private sector IdM systems should consider both existing national law and the varying contract-based Operating Rules used by each individual IdM system. Specifically, an UNCITRAL instrument should address issues regarding the applicability of existing national law to private sector IdM systems that (i) cannot be addressed by the individual contract-based Operating Rules adopted by each IdM system, or (ii) otherwise create problems for all private sector IdM systems. Examples of areas to address in an UNCITRAL instrument would therefore include: the legal recognition of identity transactions from private sector IdM systems, the requirements for determining whether a private sector identity transaction satisfies applicable legal requirements to identify someone, and applicability of laws that cannot be modified by IdM system Operating Rules, such as laws regarding use of government identifiers, consumer protection law, and tort law.

9. This approach is based on the recognition that private sector IdM systems are governed by a three-tier legal framework, with existing national law at the top (Tier 1), and individual contract-based IdM system Operating Rules at the bottom (Tier 3). The middle layer of that legal framework (Tier 2) would provide a bridge between Tier 1 and Tier 3. UNCITRAL's objective should be to develop an instrument that provides guidance to States about what a Tier 2 law would contain. This legal framework is more fully described in Section III, below (including Figure 1, which provides a pictorial representation of these three tiers of law, and their relationship). Section III also provides a detailed roadmap of how UNCITRAL might think about the contents of such an instrument.

10. WP.162 fails to recognize this legal framework, and instead takes a fundamentally different and, in our view, unworkable approach. While it addresses some issues that would properly be covered by a Tier 2 instrument, it combines and confuses them with numerous issues that should more properly be addressed by the contract-based Operating Rules of an individual IdM system (Tier 3). As a result, it frequently adopts a one-size-fits-all approach to issues that will vary widely between and among the various contract-based Operating Rules governing individual IDM systems. As the negotiations on the draft text have progressed, it has become increasingly clear that this is not a workable approach.

11. WP.162 uses the Operating Rules for a public sector IdM system (i.e., eIDAS), as a conceptual model and seeks to expand that globally to all IdM systems. e-IDAS is, indeed, a highly innovative approach to regulating IDM systems, and it has made a significant contribution to worldwide understanding of how IdM systems could work and how they might be regulated for public sector use. The problem, however, is that eIDAS is a unique set of Operating Rules for a single public sector IdM system (consisting of the various EU country identity providers). Thus, it is the public sector equivalent of the contract-based Operating Rules that would govern a specific private sector IdM system. Attempting to impose those operating rules on all other IdM systems is not appropriate.

12. In other words, whereas eIDAS is a set of Operating Rules to govern *one IdM system* (Tier 3), UNCITRAL should develop an instrument that would apply to *all IdM systems* (Tier 2). Whereas eIDAS is a set of operating rules for a *public sector* IdM system (i.e., regulating identity transactions for public sector use), UNCITRAL should develop an instrument that applies to *private sector* IdM systems. Specifically, an UNCITRAL instrument should provide a bridge between the contract-based

Operating Rules governing each individual private sector IdM system (Tier 3), and those aspects of existing national law (Tier 1) that adversely affect all IdM systems but cannot be resolved by the individual IdM system Operating Rules (such as legal recognition of identity transactions or tort liability).[1]

13. Instead, WP.162 sets forth rules with respect to a number of issues that would typically be addressed by the contract-based Operating Rules of each individual IdM system. This includes topics such as obligations of IdM service providers (in Article 6), obligations in case of a breach (in Article 7), obligations of subscribers (in Article 8), or liability of IdM service providers (in Article 12). At the same time, it fails to clearly delineate where parties to a contract may deviate from existing law in relation to these topics and where they must conform to existing law.

14. Moreover, whereas the eIDAS framework, upon which WP.162 is based, relies on a centralized mechanism for regulating, setting standards, and certifying IdM systems, no such centralized mechanism exists globally to underpin an UNCITRAL instrument such as WP.162. WP.162 simply presupposes the existence of such a global mechanism. Without such a global mechanism, the provisions in WP.162 relating to cross-border recognition and reliability standards raise a number of unanswered questions that require further discussion in the Working Group. Indeed, eIDAS provides for recognition of trust services by providers outside the EU only where a specified type of agreement concluded between the EU and the third country is in place (Article 14.1 of eIDAS).

15. In addition to the incongruity with the eIDAS model, WP.162's reliance on the UNCITRAL Model Law on E-Signatures as a template is misplaced. E-signatures are relatively simple and standardized, whereas IdM systems are more complex and multi-layered. For example, while e-signatures typically involve two parties, IdM systems typically involve many parties. The rules in the Model Law on E-Signatures simply do not work for IdM systems.

16. These fundamental issues raise very basic but critical questions: how would the approach reflected in WP.162 be useful to States once it is adopted? In the absence of a centralized mechanism for regulating or certifying IdM systems or trust services, how will this text accomplish what it sets out to accomplish e.g., with respect to cross-border recognition or reliability standards? If, as the United States understands it, the intention is for WP.162 to apply to private sector IdM systems, then how do the rules set forth in WP.162 relate to the Operating Rules set forth by the parties to a contract that governs an IdM system?

17. The United States previously responded to the Secretariat's template and provided written reactions to the latest text, and the appendix here contains an article-by-article analysis of WP.162. However, the U.S. view is that before moving forward with WP.162, the Working Group should first undertake a conceptual discussion to clarify how WP.162 will fit into the overall legal framework governing IdM systems. While the United States appreciates that considerable work has gone into the development of WP.162 and that efforts have been made to reach consensus on the document, it would be regrettable for the Working Group to continue down a path toward an instrument that is of little use to Member States or to private sector IdM systems.

18. As reflected in this paper, there are a number of areas where WP.162 is addressing topics that are appropriate and germane to the issue of IdM systems but where the approach is unworkable, and in those areas, the Working Group may be

[1] While eIDAS arguably includes both Tier 2 and Tier 3 elements for the various EU country identity providers that agree to participate in the single EU framework, we believe that UNCITRAL's focus should be solely on the development of a Tier 2 instrument that would apply to all private sector IdM service providers. Moreover, eIDAS operates as an IdM system for public sector use, whereas the task for UNCITRAL is to develop an instrument that applies to private sector IdM systems.

able to build on WP.162 and incorporate conceptual changes into existing provisions. In other areas, more significant changes or deletions may be warranted.

19. The United States offers the framework in Section III below as a roadmap to guide a conceptual discussion that will help to chart a path forward.

II. Background on IdM systems

20. We believe that the goal of this project should be to establish a legal framework that will enable and encourage the development of a robust identity ecosystem, where multiple private sector IdM systems of all types can flourish and support national and global commerce. This requires a focus on identifying any barriers or gaps in existing national law that need to be addressed. Moreover, to encourage the development of new and different IdM systems, it is important that the Working Group avoid one-size-fits-all solutions with respect to issues and problems that should be addressed through the unique contract-based Operating Rules established by individual IdM systems.

21. To identify the barriers and gaps in the legal framework for identity management that need to be addressed, we first need to do the following:

- Examine the concepts of identity transactions and IdM systems;
- Examine the need for, and the role of, the Operating Rules that govern the operation of each private sector IdM system; and
- Understand the overall legal framework that governs IdM systems, and where and how an UNCITRAL instrument might help/fit in.

22. With that background, the Working Group can then identify the legal issues that cannot be addressed by the unique contract-based Operating Rules that are part of each IdM system, and thus need to be addressed by additions and changes to national law using a legal instrument developed by UNCITRAL.

A. Identity Transactions

23. An identity transaction is a communication whereby a relying party receives some identity information about an individual [2] (identification), along with verification that the person purporting to be that individual is, in fact, that individual (authentication). It is usually done for the purpose of either: (1) engaging in some sort of transaction with the subject (e.g., entering into a contract, providing benefits, communicating information, etc.), or (2) granting the subject access to some sort of a digital or physical facility (e.g., website, database, building, etc.).

24. Identity transactions generally require (1) the collection and verification of information (attributes) about an individual data subject (an identification process), (2) the issuance of a credential containing one or more of those attributes (a credential issuance process), and (3) the association of the identity attributes in that credential with a specific individual, who is often remote (i.e., an authentication process). Through those processes, identity transactions are designed to verify the identity of an individual, and authenticate the relationship of that identity to a specific person.

25. Thus, for example, presenting one's passport at the border to obtain admission to a country is an identity transaction. In that case, the relying party (border control agent) is provided with previously verified identity attributes about an individual (as stated in the passport), along with a method for verifying that the person presenting the passport is the individual named in the passport (i.e., via the photo or fingerprint data embedded in the passport). Likewise, the process of signing into an online

[2] The subject of an identity transaction could be an individual, an entity, a device, or a digital object. This paper will focus on individuals, as that has been the focus of the Working Group's discussion to date.

network with a username and password to obtain access to a database is an identity transaction. It involves the association (via the secret password) of previously verified identity attributes about an individual (as referenced via the username) with a person purporting to be that individual (i.e., the person entering the username).

B. IdM systems are multi-party systems designed to facilitate identity transactions

26. An **identity management (IdM) system** is a coherent combination of participating entities, processes, and technology, where each participant performs the responsibilities of one or more predefined roles,[3] in accordance with a predefined set of legally binding processes, policies, and procedures, for the purpose of facilitating identity transactions.

27. IdM systems are complex multi-party systems. They involve multiple participants who fill a variety of roles, such as registration authorities, identity proofers, attribute providers, trust providers, identity providers, credential providers, verification providers, hubs, etc. They coordinate the work needed to collect and verify the identity (attributes) about an individual data subject, issue a credential containing one or more of those attributes, and authenticate those identity attributes with a specific individual in the context of an identity transaction. Those participants work together to facilitate identity transactions for multiple relying parties.

28. In terms of complexity of structure, an IdM system is analogous to a credit card system set up for the purpose of facilitating credit transactions (such as MasterCard or Visa), or an electronic payment system set up for the purpose of facilitating payment transactions (such as SWIFT or ACH). While each of these types of systems is designed using a different structure and for a different purpose, they are all multi-party systems designed to facilitate a particular type of economic transaction (e.g., credit card, payment, or identity transactions).

29. The structure of an IdM system can vary widely. For example, IdM systems may be centralized (with a single identity provider that facilitates identity transactions for multiple relying parties), federated (with a limited set of identity providers that centrally store and provide user identity information to facilitate identity transactions with one or multiple relying parties), or distributed (with multiple identity providers that authenticate identity information stored locally by users to facilitate identity transactions with multiple relying parties). This variety in IdM system structure is one of the key reasons that the instrument being developed by the Working Group cannot take a one-size-fits-all approach with respect to numerous issues.

C. IdM Systems need legally binding operating rules

30. Because IdM systems are complex multi-party systems, the coordination and cooperation of the participating entities is essential to accomplish the desired objective. Thus, IdM systems require an organized, purposeful structure that consists of interrelated and interdependent participating entities filling a variety of roles, performing a set of detailed processes, and following a set of policies and procedures, all designed to achieve a specific objective – i.e., to facilitate identity transactions.

31. Moreover, because IdM systems involve multiple independent participating entities potentially interacting with each other to carry out a series of complex transactions, IdM systems do not automatically operate on their own. Each of the participants must be guided by a set of rules or instructions regarding the way in which it should act for its particular role. And such rules must typically be legally enforceable to ensure that all of the participants comply with the requirements

[3] Such roles might include, for example, registration authority, identity proofer, identity provider, broker, hub, attribute provider, relying party, etc.

applicable to them, and can rely on all of the other participants to adhere to the rules and produce a trustworthy result.

32. Accordingly, each IdM system requires a legally enforceable set of **Operating Rules**[4] to govern its operation. Those Operating Rules serve three important functions:

- They ensure that the IdM system **operates properly** – i.e., they specify the policies, procedures, and processes required for operation of the system, so that the IdM system "works" as it is supposed to;
- They define the **duties and obligations** of each of the participant roles (e.g., so that each participant knows what to do), as well as its legal responsibilities, and (if appropriate) define and fairly allocate liability risks; and
- They specify additional requirements to help make the IdM system "**trustworthy**" for its intended purpose – i.e., they impose requirements that go beyond ensuring that the IdM system is merely functional, and implement additional steps to ensure that participants have confidence in the resulting identity transactions and are willing to rely on them.

33. To achieve those goals, the Operating Rules are typically designed to address the specific business, technical, and legal issues that arise in the operation of a particular IdM system. This may include, for example, issues such as participation requirements, role definitions and responsibilities, processes and procedures for data subject enrolment, identity proofing, credential issuance, and identity authentication, technical specifications and standards, data security requirements, warranties, liability allocations, dispute resolution procedures, and termination rights. Operating Rules also address governance of the IdM system, such as qualifications to participate, enforcement of rules, and revisions of the rules. They form the governance framework for the IdM system. Moreover, because the structure, technology, and purpose of each IdM system may be different, the Operating Rules for each individual IdM system will likely vary widely.

34. To ensure that IdM system Operating Rules are legally binding and enforceable, they can take the form of a statute or regulation, or contract.

35. In the case of **public sector** IdM systems, the Operating Rules typically take the form of a detailed **statute** or regulation. Examples include the Aadhaar Act in India,[5] the Identity Documents Act in Estonia,[6] and the eIDAS Regulation in the EU.[7] However, some public sector IdM systems, such as the GOV.UK.Verify IdM system, have made use of contracts.[8]

36. In the case of **private sector** IdM systems, the Operating Rules take the form of a **contract** that binds the participants in the system (just as the participants in a credit card system or payment system agree via contract to the terms of the Operating Rules applicable to their role). Examples of private sector IdM system Operating Rules

[4] Operating Rules are also frequently referred to by a variety of other names, such as a Governance Framework, Trust Framework, Scheme Rules, and System Rules.

[5] Aadhaar (Targeted Delivery of Financial and other Subsidies, benefits and services) Act, 2016, https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.

[6] Identity Documents Act, Passed 15.02.1999, RT I 1999, 25, 365, Entry into force 01.01.2000 www.riigiteataja.ee/en/eli/ee/504112013003/consolide.

[7] The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted on 23 July 2014 provides a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities; at https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014.

[8] www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.

include the SAFE Identity Trust Framework,[9] the Sovrin Governance Framework,[10] and the Pan-Canadian Trust Framework.[11] See also "A Guide to Trust Frameworks and Interoperability."[12]

D. Operating Rules are unique to each IdM system

37. Each IdM system is different, and thus requires a unique set of Operating Rules tailored to its structure, technology, purpose, market, and risk profile.

38. Private sector IdM systems employ a wide variety of **structures and technologies**, each of which will require different approaches to Operating Rules. Development of such private sector IdM systems will be inhibited by attempts to impose a uniform one-size-fits-all set of such rules on all systems.

- Examples of differing IdM **system structures** identified by the World Economic Forum in 2016[13] include internal IdM systems, external authentication IdM systems, centralized identity IdM systems, federated IdM systems, and distributed identity IdM systems. Other IdM system structures deployed more recently include hub-based IdM systems and self-sovereign IdM systems, as well as IdM systems being developed with mobile phones. Each will require a different approach to Operating Rules, and will suffer from attempts to impose a uniform set of such rules on all systems.
- Examples of differing IdM **system technologies** include PKI-based IdM systems, blockchain IdM systems, and systems using the OAuth and OpenID Connect standards, each of which will require different approaches to Operating Rules, and will suffer from attempts to impose a uniform set of such rules on all systems.

39. Private sector IdM systems are also typically designed for a variety of different **purposes and/or markets**, which will require a variety of different approaches, trust requirements, and risk allocations in its Operating Rules. Development of such IdM systems will be inhibited by attempts to impose a uniform one-size-fits-all set of such rules on all such IdM systems.

- Examples of IdM systems designed for a variety of different **purposes and markets** include: the InCommon IdM system designed for the educational use (e.g., universities and students); the SAFE BioPharma IdM system designed for the pharmaceutical industry; the CertiPath IdM system designed for the international aerospace industry; the CA Browser Forum IdM system designed to identify website operators; the ZenKey designed for mobile identity; and the lightweight Google, LinkedIn, and Facebook IdM systems designed for low risk website access.

40. Because they are designed to address the unique requirements of a particular IdM system, the matters addressed by such Operating Rules should be outside the scope of the instrument being developed by the Working Group.

41. Because private sector IdM system Operating Rules are based in contract and tied to the unique requirements of a particular IdM system, it is important that any instrument developed by UNCITRAL not attempt to duplicate those Operating Rules with a one-size fits-all approach applicable to all IdM systems. Thus, a challenge for the Working Group will be develop an instrument that does not infringe on, or inhibit,

[9] www.globenewswire.com/news-release/2020/05/19/2035512/0/en/SAFE-Identity-Announces-Revamped-SAFE-Biopharma-Trust-Framework-and-New-Services-to-Expand-and-Evolve-Digital-Trust-in-Healthcare-Sector.html.

[10] https://sovrin.org/library/sovrin-governance-framework.

[11] https://drive.google.com/file/d/1Xmjh8QJZKWmRkaTtE2f43ISntD7jE6D5/view.

[12] Open Identity Exchange, "A Guide to Trust Frameworks and Interoperability," at https://openidentityexchange.org/guide-trust-frameworks-interoperability.

[13] See World Economic Forum, "A Blueprint for Digital Identity," August 2016, at http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

the need for or ability of a private sector IdM system to develop its own Operating Rules while at the same time making clear those legal requirements to which contract-based Operating Rules must conform.

III. The legal framework governing private sector IdM systems and a potential UNCITRAL instrument

A. The overall legal framework

42. As a prerequisite to developing an instrument of the type envisioned by WP.162, we believe the Working Group needs to consider the structure of the overall legal framework that governs private sector IdM systems. Specifically, the Working Group should consider how (i) the individual Operating Rules of the various private sector IdM systems, and (ii) the proposed UNCITRAL instrument, would fit into that framework. This will be important for determining what issues should be addressed in the UNCITRAL instrument.

43. Private sector IdM systems, like most commercial multi-party transaction systems, are typically governed by a legal framework consisting of a combination of (i) government-made law, and (ii) contractual agreements of the participating entities. **Government-made law** consists of the rules enacted as statutes by legislatures, adopted as regulations by government agencies, or determined by judicial decision. **Contract-based law** consist of the rules drafted by one or more participants or IdM system governing bodies – i.e., the Operating Rules of the IdM system – which are made binding on the participants in an IdM system by contract.

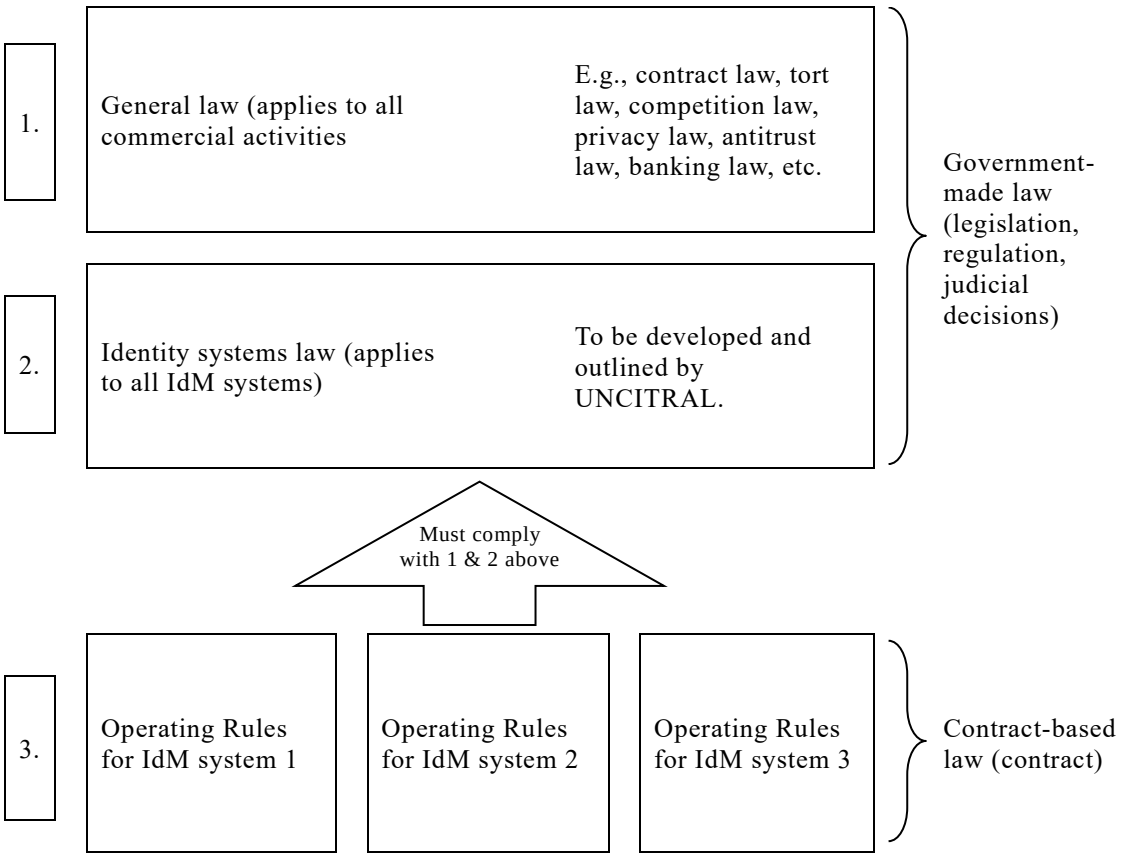
44. The legal framework in which any private sector IdM system operates typically consists of up to three tiers (or levels) of law, with each successive tier governing IdM systems at an increasing level of specificity. The three tiers of the legal framework are described as follows (and are depicted in the diagram on the following page):

- **(Tier 1) Existing Law:** The top tier, and the most general, is simply **existing national law**. That is government-made law, including statutory laws, regulations, and judicial decisions. Such law governs all types of commercial activities, was not written specifically for IdM systems, and may in some cases be hundreds of years old. Nonetheless, it is frequently applicable to private sector IdM system activities. This includes general contract law, tort law, privacy law, export control law, warranty law, consumer protection law, competition law, banking law, and the like.
- **(Tier 2) Identity Systems Law:** The second tier of law governing private sector IdM systems can be referred to as **Identity Systems Law**. It is written expressly to govern ***all*** private sector IdM systems, regardless of type, structure, technology, or purpose. Tier 2 Identity Systems Law is also government-made law, is designed to address problems that Tier 1 existing law causes for all IdM systems, and may fill some of the gaps that Tier 1 law simply does not address. It should fit between the Tier 1 existing law and the Tier 3 individual IdM system contract-based Operating Rules.
- **(Tier 3) Individual IdM System Operating Rules:** The third tier of law governing private sector IdM systems consists of the contract-based Operating Rules written specifically by each private sector IdM system to govern its own environment. Unlike Tier 2 Identity Systems Law, which applies to all IdM systems, the Tier 3 Operating Rules are designed to address the unique requirements of a particular IdM system.[14] These Operating Rules can be quite detailed, but must comply with the law in Tier 1 and in Tier 2.

[14] Note that, in the case of public sector IdM systems, such as a national ID system, the system-specific Operating Rules are embodied in a statute or regulation. Thus, Tier 2 and Tier 3 law are combined.

45. The task for the Working Group is to develop an instrument that outlines the elements of a Tier 2 law.

Figure 1
Legal framework for private sector IdM systems: three tiers of law



B. What should an UNCITRAL instrument do?

46. To avoid adopting a one-size-fits-all approach that inhibits the development of private sector IdM systems and associated commercial activities, the Working Group should develop an instrument that addresses only issues that cannot be addressed in individual IdM system Operating Rules. Further, it should be limited to modifying and/or supplementing Tier 1 existing national law only to the extent necessary to encourage and promote the development of private sector IdM systems to support online commercial activity. That involves designing a Tier 2 instrument that:

- Removes barriers and eliminates the uncertainties in Tier 1 existing law that inhibit the development of private sector IdM systems;
- Fills gaps in Tier 1 existing law of importance to the success of private sector IdM systems, but that cannot be addressed by contract; and
- Addresses new universally applicable issues to promote the development of all private sector IdM systems.

47. Moreover, given the varied nature of IDM systems and the unique needs of each one, any Tier 2 instrument developed by the Working Group should adhere to the principles of technology neutrality and identity system neutrality. In particular, identity system neutrality is critical in light of the wide variety of structures, technologies, purposes, and markets used by private sector IdM systems as outlined above.

48. By contrast, WP.162 is written in a manner that imposes rules regarding *Obligations of IdM service providers* (Article 6), *Obligations of IdM service providers*

in case of data breach (Article 7), *Obligations of subscribers* (Article 8), or *Liability of IdM service provider* (Article 12). Private sector IdM systems need to address these issues in their individual IdM system Operating Rules. Each of those issues will require a unique approach tailored to the particular IdM system structure, technology, purpose, and market involved. Any attempts to address issues such as the foregoing will be problematic because they will likely vary significantly from one IdM system to another, and imposing a one-size-fits-all approach on IdM systems will only result in inhibiting the development of private sector IdM systems.

C. Outline for an UNCITRAL Instrument

49. Instead, the issues that might be addressed by the Working Group fall into the following categories[15]:

- Explicit recognition of the role of Operating Rules for IdM system governance
- Issues not addressed in Tier 1 existing law that by their nature cannot be addressed by contract-based Operating Rules. Examples include:
    - The legal recognition of IdM[16]
    - The requirements for determining when an identity transaction satisfies applicable legal requirements to identify someone[17]
    - Whether (and if so, how) the reliability of private sector IdM systems should be evaluated[18]
- Issues addressed to some extent in Tier 1 existing law, but with uncertain applicability to IdM systems, thereby creating an ambiguity that may constitute a problem for IdM systems because of the difficulty in addressing them in the contract-based Operating Rules. Examples include:
    - The applicability of existing tort law to IdM system participants;
    - The applicability of the law of negligent misrepresentation;
    - The applicability of existing law regarding implied warranties
- Issues that may need to be added to existing law, such as addressing:
    - The right of IdM systems to use information from government IdM systems;
    - The right of IdM systems to use government issued identifiers (e.g., SSN, national ID number, etc.).
- Issues that, regardless of whether they could be addressed by contract-based Operating Rules, should be addressed in the same way by all IdM systems due to public policy considerations, such as:
    - Whether, and if so how, to provide for cross-border recognition[19]
    - Whether, and if so how, to address reliability from a legal perspective[20]

---

[15] This is intended as a preliminary list of potential issues to be taken up in a Tier 2 instrument, subject to development and refinement by the Working Group, and based on the needs of various existing national level regimes among other factors.

[16] WP.162, Article 5 seeks to address this issue. See our comments regarding the problems with the current draft Article 5 in the appendix.

[17] WP.162, Article 9 seeks to address this issue. See our comments regarding the problems with the current draft Article 9 in the appendix.

[18] WP.162, Article 11 seeks to address this issue. See our comments regarding the problems with the current draft Article 11 in the appendix.

[19] WP.162, Articles 10 and 11 seeks to address this issue. See our comments regarding the problems with the current draft Articles 10 and 11 in the appendix.

[20] WP.162, Articles 10 and 11 seeks to address this issue. See our comments regarding the problems with the current draft Articles 10 and 11 in the appendix.

50. An UNCITRAL instrument containing these elements will help States to develop a Tier 2 Identity Systems Law designed to (1) encourage the development of private sector IdM systems, (2) remove barriers to such development, and (3) respect and support the need of each private sector IdM system to develop its own Operating Rules to the extent possible.

Appendix[21]

Article-by Article Analysis of WP.162

In this appendix to our comments, we provide a detailed article-by-article commentary on WP 162. We reiterate, though, that we do not believe that a simple set of revisions to the text of WP 162 will result in a viable instrument. To achieve this, we believe the Working Group must make the conceptual and structural changes required to address the current reality of IdM systems that we set forth in Sections II and III of our comments.

Before turning to the article-by-article analysis, here is a summary of the U.S. concerns with WP.162:

(a) The definitions in WP 162 are both incomplete and based on a static model for IdM that is not reflective of the wide variety of actual IdM systems;

(b) WP.162 does not provide a basis for determining how and when the instrument would accede to or supersede existing laws that require identification in a specific form. The failure to provide guidance on this issue is compounded by the fact that articles 2, 5 and 9 contradict one another;

(c) The articles on obligations (art. 6–8) and liability (art 12) do not reflect the wide variations among types of IdM systems nor the multiple types of roles that may make up any specific IdM system. These one-size-fits all provisions do not accurately reflect the rights and obligations that different IdM system roles may have or expect in various IdM systems;

(d) We do not believe the provisions on cross-border recognition are workable without an enacting jurisdiction having some basis for assuming the reliability of a system in another jurisdiction. We do not believe this obligation is realistic.

Draft Article 1: Definitions

We believe the Working Group should revisit the definitions after the articles in the rest of the draft are concluded. Base on the current draft,[22] we make the following observations for consideration by the Working Group.

The term “electronic identification” may describe or be easily confused with the entire process of identity proofing, credential issuance, and authenticating the relationship between the credential data and an individual. Thus, we recommended that the Working Group consider whether there is an alternative term to “electronic identification” that could be used for the authentication process.

All the stages of the IdM process might collectively be defined as “identity verification.” The modifier “electronic” should not be used in this definition, however, since all or part of the stages of the IdM process might not be done electronically.

“Authentication” is used only in terms of trust services; it has the same meaning as “electronic identification”. We believe it could be misleading to have two terms for the same concept and would recommend using the same term for this concept throughout the draft. As noted above, however, we believe the term “electronic identification” itself may be misleading.

As to the secretariat’s inquiry whether there should be a definition of levels of assurance, we believe such a definition is unnecessary. We note the secretariat’s

[21] The Appendix has been provided to Member States in English only. However, significant portions of the substance of the Appendix are a reproduction of the U.S. response to the Secretariat’s questionnaire for A/CN.9/WG.IV/WP.162, which has been circulated in all official languages as A/CN.9/WG.IV/WP.164 and Add.1.

[22] A/CN.9/WG.IV/WP.162.

proposed language provides that “identification factors are those factors that are necessary to make an electronic identification” In other words, the proposed definition does not provide any guidance; it simply restates the obvious. Moreover, we believe this proposed language could cause confusion, as it implies that there are specific factors that an IdM service provider must manage. Depending on the nature of the identity system involved, there could be numerous such factors. The relevant factors, however, will vary from IdM system to IdM system, and the responsibility for managing these factors will vary from system role to system role.[23] We note also that the proposed definition appears to combine two very different concepts: identity attributes (that vary depending on purpose for which identity is used), and identity processes that are used for identity proofing, credential issuance, or authentication processes.

Draft Article 2: Scope of application

The draft instrument provides that it “applies to the use and cross border recognition of IdM systems and trust services in the context of commercial activities and trade related services.” As we discuss below, we believe the Working Group needs to closely examine how the draft instrument will apply to cross-border transactions, and how the rules in this instrument relate to existing legal requirements regarding identification and authentication.

Draft article 2(3) provides that “[n]othing in this [instrument] affects a legal requirement that a [subject][person] be identified in accordance with a procedure defined or prescribed by law.” We understand this exclusion as being necessary as most if not all jurisdictions have some mandatory requirements for the form in which identification is to be made.

The question then is whether this section can be reconciled with articles 5(a), which provides that “The electronic identification of a [subject][person] shall not be denied legal effect, validity, enforceability or admissibility as evidence on the sole ground that …[t]he identity proofing and electronic identification are in electronic form” and article 9(1) option A, which provides that ” Where a rule of law requires or permits the identification of a [subject][person], that rule is satisfied with respect to IdM if a reliable method is used for the electronic identification of the [subject][person].”

We believe article 2(3) and article 5(a) might be reconciled by expressly clarifying these two sections to indicate that article 5(a) is not intended to overrule any other law, but is only intended to provide that, as between the parties, the law will not block the choice of the parties to use an electronic means of identification if the law would otherwise allow this under freedom of contract. This reading would appear to narrow the scope of article 5, and if the Working Group intended article 5 to have this limited meaning, this needs to be clarified in the text and comments.

We do find a more serious problem reconciling draft article 2(3) with draft article 9(1) Option A. These two sections, we believe, cannot be reconciled. Were the instrument intended to supersede all laws that may require a specific mode of identification, the instrument would risk being non-enactable. In addition, this interpretation would expressly contradict the language of draft article 2(3). In our view, the draft instrument provides contradictory rules: electronic identification meets the requirements of other legal identification requirements, and the instrument does not displace any other legal identification requirements. These conflicting rules cannot co-exist if the draft instrument. We view Option B of draft article 9 as essentially restating the rule of Option A. We believe the Working Group must re-examine these

[23] This potential confusion raises the issue of whether draft article 6 may itself create minimum obligations that should not necessarily apply to all IDM service providers. In other words, article 6 may assume a one size fits all IDM service provider that does not reflect the multitude of existing and developing models.

draft articles and reformulate them to express a non-contradictory policy that respects the existing legal requirements that are recognized in draft article 2(3).

Draft Article 3: Voluntary use of IdM and trust services

We believe both the current text of the draft[24] as well as the proposed new language by the secretariat[25] shows confusion on the role of consent. We suggest the Working Group examine the rule on consent to determine which parties are required to consent and the relationship between article 3 on consent and how it works with both article 2 and 5 on freedom or lack of freedom to choose the mode of identity management.

Draft Article 4: Interpretation

Although we appreciate that this language has appeared in prior model laws,[26] we note this language was drawn from the United Nations Convention on Contracts for the International Sale of Goods,[27] and it is language specifically tailored for an international convention. As such, we are not sure that it is appropriate for a model law that is drafted for domestic legislation.

Thus, for example, we are not clear on what the "international character" of the draft model law refers to. As the draft instrument is neither derived from international instrument nor intended to be used primarily in international transactions, we do not know what constitutes the instrument's "international character".

Moreover, although uniformity of interpretation is a useful admonition for an international convention,[28] the utility of this interpretive rule is not clear in an instrument designed for domestic legislation. When, as with an international convention, an autonomous interpretation is useful to create a universal understanding that parties can rely upon in international commercial transactions, the application of this rule is unclear and probably redundant for a domestic law.

As for the rule that the instrument should be interpreted on the general principles on which it is based,[29] we suggest that either the draft provide the guidance of what these principles are[30] or this rule should be removed. To do otherwise creates the risk of vagueness and uncertainty in the text.[31]

---

[24] A/CN.9/WG.IV/WP.162, draft article 3.

[25] "There have been questions about the relationship between articles 2 and 3. Would their relationship be clearer by recasting article 3 to state that "Nothing in this [instrument] requires a [person][relying party] to accept the electronic identification of a subject or to rely on a trust service without the [person's][relying party's] consent. "?".

[26] UNCITRAL Model Law on Electronic Commerce (1996), article 3; UNCITRAL Model Law on Electronic Signatures (2001), article 4.

[27] United Nations Convention on Contracts for the International Sale of Goods (1980), article 7.

[28] We note this language is also derived from the CISG.

[29] A/CN.9/WG.IV/WP.162, footnote 23.

[30] We note that a statement of underlying principles was removed from the last draft.

[31] The Working Group may want to consider the comments of the World Bank in WP.163 to ensure that the Draft Provisions do not discriminate among IdM system models by including the concept of IdM system neutrality (or identity transaction neutrality). Because there are many different ways of conducting online identity transactions (e.g., single identity provider (IdP) systems, federated (multiple IdP) systems, user controlled/user centric systems, hub systems, DLT systems, systems without credentials, self-sovereign identity systems, etc.), it is important that these Draft Provisions do not require or assume a particular approach to the identification and/or authentication processes, or the system that delivers them. Thus, the Working Group should consider ways to ensure that these Draft Provisions do not imply and/or require a certain system model.

Draft Article 5: Legal recognition of IdM

As we discussed above in our analysis of draft Article 2, we believe the Working Group needs to clarify how this rule is intended to work with identifications that are required to be in a specific form such as a driver's license or passport.

Draft Article 6: Obligations of IdM service providers

As noted in Sections II and III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems.

As noted in the World Bank's comments,[32] the obligations set out in draft article 6 for IdM service providers assume a model where the IdM service provider provides all the services. This may not always be the case. There could be several parties that contribute to or provide part of an IdM service (e.g., trust providers, registrars, enrolment agents, credential service providers, stewards, authentication providers, hubs, etc.). Given the increasing diversity of IdM system models, the Working Group should consider whether it is still appropriate to restrict the definition of the roles or to impose a one-size-fits-all set of IdM service provider obligations. We believe the Working Group needs to address article 6 to consider the potential multiple parties that may contribute to the IdM service, and to consider whether it is still appropriate to impose a one-size-fits-all set of IdM service provider obligations.

Draft Article 7: Obligation of IdM service providers where there is a breach

As noted in Sections II and III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems. We agree that there should be some obligations by an IdM service provider where there has been a breach of security. As we noted note our comments to draft article 6, however, there may be multiple parties involved in the IdM service provider process.[33] For this reason, we believe the Working Group should reconsider the language of draft article 7 to reflect the various parties that may be involved in IdM process and accordingly fix the obligations based on the respective nature and status of these parties consistent with which party is best placed to respond to the breach.

Draft article 7 is limited to breaches that have "a significant impact". We do not understand what "significant impact "means in this context. In addition to being a vague standard, we are not sure why a "breach" is not enough in and of itself to justify some remedial action by the entity that bore the risk the breach.

We are not sure what "remedies" are or should be available where there has been a breach of security.[34] We believe the Working Group should clarify this issue.

---

[32] A/CN.9/WG.IV/WP.163.

[33] We agree with the comments by the World Bank in WP.163 that the current draft compresses and confuses the distinction between and the respective roles of IdM systems and IDM service providers.

[34] See Draft article 7(1)(b).

We do not know what "applicable law" refers to in 7(1)(c). If it refers to a notification obligation from the draft instrument, this obligation should be referred to. If this refers to law outside of the instrument, it is not clear what law would impose an obligation of notification.

Draft Article 8: Obligation of subscribers

As noted in Sections II and III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems.

We agree with the comments by the World Bank that the duties imposed on subscribers (particularly individuals, such as data subjects) in Article 8 may not be reasonable in all circumstances.[35] For example, there may be situations where an individual subscriber may be aware of circumstances indicating there may have been a compromise, but simply does not understand their significance.

We believe Article 8 should be clarified that it is not intended to impose these duties on relying third parties that have no contractual relationship with the issuing IdM service provider but who may nonetheless rely on a credential because:

(a) it would be difficult to enforce as it will likely be hard to identify such relying third parties;

(b) it imposes an undue burden on relying third parties to police identity system credentials for an IdM service provider with whom they have no relationship; especially when their use of and reliance on such credentials may be sporadic at best; and

(c) it is not currently required by law applicable to paper-based credentials (e.g., the bartender who refuses entry to a person because he determines that the person has presented a false driver's license or someone else's driver's license is not required to report that to the issuing authority).[36]

The requirement to notify in cases of a "substantial" risk seems problematic, as subscribers will likely have no way of knowing (and in most cases will not even be qualified to determine) what constitutes a substantial risk as opposed to some lesser risk.

Draft Article 9: Identification of a person using IdM

We address our concerns on draft article 9 in our discussion of draft article 2 above.

Draft Article 10: Factors relevant in determining reliability

As noted in Sections II and III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if

[35] A/CN.9/WG.IV/WP.163.

[36] We also agree with the comments by the World Bank in WP.163 that if the draft is going to raise issues about third parties, more clarification would be useful as to which third parties are envisaged. We also note that if there is going to be a notification requirement on non-contracting parties, there needs to be some sanction for failure to notify, as otherwise the requirement is meaningless.

it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems.

Draft article 10 provides an illustrative list of factors to determine the reliability of an IdM service. If article 10 only applies to systems governed by contractual rules, it is not clear what the purpose of the list of possible considerations serve. This list is not useful to explain and interpret an otherwise applicable contractual agreement. If draft article 10 is intended to provide a minimal standard of reliability for IdM systems, then it is not clear how an illustrative and not a mandatory list would operate.

Moreover, it is not clear how this would override, if at all, otherwise agreed to contractual standards.

Moreover, in any given situation, there are numerous factors that may affect reliability. We question whether attempting to list them in these rules is appropriate in any event.

Draft Article 11: Designation of reliable IdM systems

Although this provision is made optional, as we note in our analysis of draft article 24, this section may impose quite a financial and administrative burden to implement by a jurisdiction that adopts this instrument. We recommend to the Working Group that this provision be bracketed with extensive commentary to explain how similar provisions have been implemented elsewhere and what an implementation would entail.

In addition, we believe this provision, as presently drafted, rests on the flawed assumptions that there are “recognized international standards and procedures” for determining the reliability of a IdM service, and that there is a centralized body that can make these determinations.

Draft Article 12: Liability of IdM service providers

As noted in Section III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems.

We do not believe any of the three options in the current draft are sufficient. Both Options A and B state, albeit unartfully, that an IdM service provider will be legally responsible under otherwise applicable law outside of this instrument. If liability rules are to be included in this instrument, some guidance would be necessary. The term “applicable law” is vague. Does this refer to contract law, tort law, privacy law, data security law, etc. or all of them? If the answer is it could apply to any law otherwise deemed to be appropriate, then no function is served by this provision. Likewise, we have no idea what type of guidance is intended by the phrase “legal consequences”.

The word “damage” in option 3 we assume means “harm”, but as with all the options in the current draft, we fear no real guidance or standards are provided.

We suggest that the rules governing liability should likely vary depending upon the nature of the identity system, and will most likely to be determined by the applicable trust framework (subject, of course, to any existing law that cannot be varied by agreement).

At a minimum, we believe a further discussion is warranted on what type of liability the rules of the draft would invoke. We think a discussion of liability should go beyond service providers and consider liability for all parties that may come within the scope of the draft. We also believe that a discussion on contractual waivers to liability should be included in any discussion on liability. Further, as noted above, we

do not believe that a universal one-size-fits-all approach to liability is appropriate in any event, as identity systems, their purposes, and their participants will vary widely.

Draft Article 13: Legal recognition of trust services

As we have noted, we believe trust services should be addressed in a separate instrument.

This provision states that a trust service may be provided in electronic form. As the purpose of a trust service is, in fact, to verify electronic data, this provision would appear to be tautological and unnecessary. If the intent of draft article 13 is to make clear that a third party may provide a trust service, that should be clarified.

Draft Article 14: Obligations of trust service providers

As a conceptual matter, this draft provision raises two questions. First, how does this provision interact with contractual obligations that a trust service provider may have to remedy a breach of loss of integrity? If the intent of Article 14(2) is to impose obligations for breaches or losses of integrity that are not covered by contract (i.e., because it refers to impact on the trust service itself), this should be made clear.

If the intent is to impose some minimal obligation on trust service providers below which the parties cannot contract, this should be expressly stated. If that is the intent, we believe the Working Group should address the question of mandatory rules and their relationship to freedom of contract.

A second question unexamined in this draft provision is the question of the consequence for failing to meet the obligations set out in Article 14? If a trust service provider fails to fulfil a contractual obligation owed to a customer, then customer/other party to the contract could pursue a contract claim. Article 14 does not appear to impose any consequences or sanction for failure to fulfil the obligations set out therein, assuming they are distinct from contractual obligations.

Draft Article 15: Obligations of trust service providers

This draft article, as with draft article 14, purports to impose obligations without any corresponding sanctions. As we mentioned in our comments to draft article 12, we believe the Working Group needs to examine fully the question of liability throughout the draft instrument.

Draft Articles 16–20: Various trust services

Articles 16–20 address the issue of the validity of a data message (such as an e-signature) and not the use of a trust service to validate the data message. In some cases, such as with e-signature, there is already existing law that governs the validity of the data message itself (this was the subject of the United Nations Convention on the Use of Electronic Communications in International Contracts and the UNCITRAL Model Law on Electronic Signatures). But in any event, because these provisions are not concerned with trust services, they do not belong in this instrument.

Draft Article 21: Website authentication

As drafted, article 21 appears to confuse the authenticity of the website, which is the true concern, with the owner of the domain, which does not prove the authenticity of website itself. We believe the Working Group should reconsider this draft article to provide a rule that achieves its intended purpose.

Draft Article 22: Identification of objects

We do not believe the identification of objects should be covered in the draft. We also note that given the limited scope of trust services in the draft, that being to verify information (data messages), the identification of objects is more appropriately covered in the provisions on identity management and not trust services.

Draft Article 23: Reliability standards for trust service providers

While Art. 23(1) lists the contractual agreement involving a trust service provider as one of the factors among others to weigh in determining reliability, it is unclear how that should be weighed relative to the other factors listed or how these standards interact with contractual agreements. As contract underlies trust service relationships, we believe this is an essential clarification that the Working Group should explore.

Draft Article 24: Designation of reliable trust services

Although this provision is made optional, as we have noted in our analysis of draft article 11, this section may impose quite a financial and administrative burden to implement by a jurisdiction that adopts this instrument. We recommend to the Working Group that this provision be bracketed with extensive commentary to explain how similar provisions have been implemented elsewhere and what an implementation would entail.

As we noted with our analysis of draft article 11, this provision ought to be reconsidered as it rests on flawed assumptions. These assumptions include, for example, that there are “recognized international standards and procedures” for determining the reliability of a trust service, and that there is a centralized body that can make these determinations. Moreover, while Art. 23(1) lists the contractual agreement involving a trust service provider as one of the factors among others to weigh in determining reliability, it is unclear how that should be weighed relative to the other factors listed or how these standards interact altogether with contractual agreements.

Draft Article 25: Liability for trust service providers

We think this section needs to be reconsidered. Option A, which leaves liability to otherwise applicable law, should be clarified to state whether it includes both contact and torts, and if it includes contractual liability, the extent to which, if at all, the liability may be excluded. As with our concerns with Option A, we believe Option B is too vague because we are not sure what the scope of “legal consequences” entails. Option C provides tort liability but leaves open the question of contract responsibility. This should be clarified. We note we expressed similar concerns with the current drat of Article 12.

Draft Article 26(1): International aspects of the draft law

Given that modern commercial transactions often transcend national borders, we believe cross- border recognition is an admirable and hopefully achievable goal in this and any commercial law instrument. We are concerned, however, that the current draft does not provide adequate standards and guidance to achieve this goal.

Draft article 26(1) provides that: “An IdM system operated or a trust service provided outside [the enacting State] shall have the same legal effect in [the enacting State] as an IdM system operated or a trust service provided in [the enacting State] if it offers a substantially equivalent level of reliability.” We believe this raises two issues that we believe deserve consideration by the Working Group.

First, the language of draft article 26(1) is derived from article 12 of the UNCITRAL Model Law on Electronic Signatures.[37] However these two articles serve significantly different functions. Article 12 of the MLES provides for non-discrimination of a certification service provider that verifies the public key of a PKI transaction. This quite limited function allows parties to choose a third-party certification provider to verify the authenticity of a signature between two parties who have chosen the third-party certifying provider. This is a simple application of freedom of contract.

Unlike article 12 of the MLES, draft Model Law article 26 would impose an obligation on all parties who rely on IDM systems and trust service providers that reside in other jurisdictions without these relying parties necessarily having the ability to choose the providers and therefore evaluate the risks attendant to the choice of a specific provider. These third parties in reliance on the IDM and trust services systems would not normally have any power to choose the providers and therefore would have to rely on assurances of providers outside the jurisdiction of the enacting state.

It is this broader scope of application of draft article 26 that suggests that article 12 of the MLES may not be the appropriate rule for IDM and trust services.

The second concern we have is whether the standard of "substantial equivalent level of reliability" (also taken from article 12 of the MLES) is either meaningful or realistic. The language itself is vague, but more importantly this standard raises a fact question that would be burdensome and expensive to prove or disprove. To meet the standard, a party would have to show both the level of reliability of the domestic system as well as the level of reliability the non-domestic system and then make some qualitative judgment on substantial equivalence. This, we believe would be unduly burdensome for parties.

We note that, for example, the recognition of foreign IDM and trust service providers under eIDAS requires an extensive and complex verification process in which each respective country in the European Union participates. This provides a level of reliability and certainty that minimizes the risks for parties relying on a non-domestic system. Thus, under the eIDAS, the "substantial equivalence" has already been established for parties relying on any respective system within the European Union. Outside such a closed system such as eIDAS, the burden on parties to prove or disprove "substantial equivalence" would itself be substantial. We think it is important to note that this is not primarily a legal but is a factual and technological question that is not easily resolved by a vague legal mandate.

This issue of "substantial equivalence" is further complicated, we believe, because what parties that use IDM and trust service systems understand about the systems is often quite different from the underlying technological structure of those systems. Most parties who must rely on IDM and trust services are not in a position to evaluate the reliability of the systems, and therefore the parties must assume reliability with the knowledge that if the systems are certified and responsible under the domestic law, the parties will have recourse under the domestic law in the case of failure. But where the domestic law, as in draft article 26 only provides protection to parties if the parties can show "substantial equivalence" of a foreign system.

Draft Article 26(2): International aspects of the draft law

Draft article 26(2) provides that "recognized international standards' shall be used to determine "substantial equivalence". We appreciate the aspirational nature of this provision. We believe, however, before adopting this provision, which was borrowed from article 12(4) of the MLES, this provision should be further discussed by the working group to determine its applicability to the draft law. We see two points which should be discussed. First, we are not certain at this time that there are generally recognized international standards in this evolving area of the law and technology. At best, we believe that the rule should also provide for evolving standards as a basis for

[37] UNCITRAL Model Law on Electronic Signatures (2001), article 12.

determining equivalence. Guidance would be most useful in how these standards should be determined. Moreover, irrespective of the standard, we note that this involves a factual issue of technological reliability that creates a substantial burden on parties to prove what "international standards" are.

Draft article 27: International Aspects of the Draft Law

We find article 27 an admirable but possibly impractical rule as may place a burden on the enacting states of significant obligations to coordinate and cooperate with foreign entities. We would not want to discourage this cooperation, but merely to ensure that it is optional and not mandatory. Legislation that creates a significant financial burden on the state often creates an impediment to adoption. This section risks posing a financial burden on the governments of jurisdictions that adopt this law that go shifts the risks of using foreign IDM and trust services providers on the respective governments instead of the private parties that choose to use these systems.

Although this may be a useful and possibly mandatory provision in a law that is designed to provide government created or recognized IDM or trust services that may be used in cross-border transactions, we are not convinced that this burden on governments is not excessive for the draft law that is designed for privates users and private providers.

We suggest that if this provision is retained, it be placed in brackets with commentary that explains fully the obligations this article would impose on the enacting jurisdiction. We suggest this article be optional for those states that have or would be willing to develop the cooperative framework necessary to implement this article.