United Nations A/CN.9/WG.IV/WP.163

General Assembly

Distr.: Limited
20 February 2020

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Sixtieth session
New York, 6–9 April 2020

Draft Provisions on the Use and Cross border Recognition of Identity Management and Trust Services

Submission by the World Bank

Note by the Secretariat

The World Bank 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.20-01482 (E)

Annex

Comments of the World Bank Regarding WP.162

The World Bank is pleased to submit the following comments on document A/CN.9/AG.IV/WP.162, "*Draft Provisions on the Use and Cross-border Recognition of Identity Management and Trust Services*" ("Draft Provisions"), on the occasion of the meeting of the Working Group in New York on 6–9 April 2020.

I. General Background Comments and Observations

1. Focus on IdM: Generally, the World Bank supports the work of Working Group IV, particularly with regard to identity management ("IdM"). Because the primary interest of the World Bank is identity management, the following comments focus on the identity management sections of the Draft Provisions.

2. IdM Systems vs Identity Transactions: The Draft Provisions are focused primarily on IdM systems and IdM service providers, rather than identity transactions. Because of the importance of identity transactions, particularly from the perspective of legal compliance and legal recognition, and because of the fact that electronic identity transactions can be, and typically are, conducted without the use of an IdM system or an IdM service provider, the Working Group should consider further addressing issues regarding identity transactions.

3. Roles: The Draft Provisions focus primarily on regulating IdM systems and IdM service providers, and (except for Arts. 5 and 8) do not really address the needs of relying parties, subjects, or other potential participants in an IdM system or transaction. For example, the Draft Provisions do not address the right of the relying party to use a third-party to verify identity wherever a law requires the relying party to verify identity. As with the issue of identity transactions, the Working Group should consider more focus on issues affecting IdM system roles other than the IdM service provider.

4. Relationship between Public Sector and Private Sector IdM Systems: The Draft Provisions are focused on private-sector IdM systems and private-sector IdM service providers. Facially, the Draft Provisions do not apply to IdM systems or IdM service providers operated by the public sector, such as national IdM systems. Accordingly, because many of the national IdM systems are government-run IdM systems (e.g., India, Estonia, etc.), they are outside the scope of the work product envisioned by the Draft Provisions.

However, it is important to recognize that there will likely be significant interaction between public sector and private sector IdM systems. For example, the Draft Provisions will presumably apply where a government agency is a customer (e.g., relying party or data subject) of a private-sector IdM service provider, or relies on a private sector federated identity system in lieu of a government operated IdM system. In addition, the identity proofing and authentication processes used by private-sector IdM service providers frequently rely on foundational identity credentials issued by government systems, which are often considered as authoritative and highly reliable.

Accordingly, the Working Group should examine and clarify the nature of the relationship between public and private sector IdM systems, including, but not limited to, addressing when and/or how it might be appropriate for private-sector IdM systems to leverage foundational identity information and authentication processes provided by governments. This might include, for example, considering rules relating to private sector IdM system:

- Use of government issued identity numbers or other identifying information
- Use of government issued identity credentials

- Access to government databases for identity proofing and authentication processes or
- Reliance on government-supplied information or processes generally

5. Trust Frameworks: The Draft Provisions do not address the role of contract-based rules for individual IdM systems, often referred to as trust frameworks, system rules, or scheme rules (collectively referred to herein as "trust frameworks"), and how they interface with the Draft Provisions.[1] The Working Group should consider revising the Draft Provisions to clarify the interface between the Draft Provisions and IdM trust frameworks, as well as what issues, and what level of detail, should be addressed in the Draft Provisions as opposed to individual IdM system trust framework. For example, issues such as participant obligations, reliability, and levels of assurance are frequently addressed in the unique trust framework for an individual IdM system.

Likewise, the Working Group should consider addressing the extent to which the terms of a trust framework can modify or overrule the terms in the Draft Provisions. For example, notwithstanding the terms of the Draft Provisions regarding liability, it is unclear whether the parties can work out their own liability rules in their own IdM-specific trust framework.

6. Reliance on e-Signature Legal Models: The structure and approach taken in the Draft Provisions is based in large part on UNCITRAL's Model Law on Electronic Signatures, and thus, fails to consider the fact that that the issues involving signatures are very different from the issues required to address identity (although identity is sometimes a component of a signature). Thus, while defining a single electronic legal equivalent to signature requirements, the same cannot readily be done for requirements to verify identity.

Part of the problem stems from the fact that laws requiring a signature all require the same thing (i.e., a signature), whereas laws requiring identification of a person often impose a variety of different requirements the identification process must satisfy (depending, e.g., whether the identity is "foundational" versus "functional",[2] the purpose for which identification is required, the risk involved, etc.). Accordingly, while it is relatively easy to define a legal equivalence to the unitary concept of a signature, the same approach does not necessarily work with respect to the various legal approaches to identification. Thus, it is important that the Working Group not be locked into a predefined structure from the law of e-signatures, and instead, independently consider the legal issues that need to be addressed for identity.

7. Options for Identity Verification: There are two options for any relying party to verify the identity of the person it is dealing with – i.e., the relying party can:

- Do the identity verification by itself; or
- Use a third-party IdM service provider

Most relying parties use the first option. Yet the Draft Provisions focus only on the second option. The Working Group may want to consider whether the Draft Provisions should take a broader approach to the subject of identity, and address issues in both situations.

8. Relying Party Rights to Rely: Ideally, the Draft Provisions should address issues regarding a relying party's right to rely. This might include, for example, a relying party's right (i) to rely on an identity credential generally; (ii) to rely on a third-party credential to satisfy specific requirements of a particular law imposing a duty to

[1] While the term "rules governing the operation of the IdM system" appears in Articles 6(c), 6(f), 10(1)(b), and 23(1)(a) of the Draft Provisions, the term is never defined nor addressed in any detail.

[2] See, e.g., "Practitioners Guide" (World Bank, 2019) at pages 12 and 13 (inter alia), available at: https://id4d.worldbank.org/guide.

identify, and (iii) to use a third party IdM service provider to satisfy its legal obligations to identify someone.

9. Relying Party Rights to Use Third Party: Relatedly, while some laws that impose a duty to identify specifically authorize the use of third-party service providers (e.g. the California Consumer Privacy Act regulations),[3] many laws are silent on the point (or require that relying parties do the identification themselves). The Working Group should consider these identity issues as well.

II. Section-by-Section Comments

1. Article 1. Definitions

(a) **Missing Terms**: Several terms used throughout the Draft Provisions are not defined. Terms that are used but not defined include:

- "Electronic identification factors;" see Article 6(d)(i)
- "Electronic identification mechanisms;" see Articles 6(d)(ii), 8(a), 8(b)
- "Identity management;" used as a modifier throughout, but never defined
- "Identifier;" – see Articles 1(b)
- "Rules governing the IdM system;" – see Articles 6(c), 6(f), 10(b), and 23(a)
    - This term could be intended to refer to an individual IdM system trust framework, although as currently worded it could apply to any law or regulation governing the IdM system. Its use should be clarified.
- "Verification;" – see Article 6(a)(ii)
    - It may also be important to clarify the concept of "verification," as this term often leads to a great deal of confusion. For example, the term "verification of identity" is often used in some cases to mean identification of the data subject, and in other cases to mean authentication of that data subject. The extent this term is used, it needs to be carefully clarified and used properly throughout.

(b) **Authentication**: The terms "authentication" and "electronic identification" are used to mean essentially the same thing, although authentication is used in the context of trust services and electronic identification is used in the context of IdM services. Since the concepts are the same, the working group could consider using the same term in both cases.

(c) **Electronic Identification**: Replacing the single term "identification" with the terms "identity proofing" and "electronic identification" is an important step to clarifying and distinguishing two aspects of the identity process. However, there may be a concern that the term "electronic identification" describes or is easily confused with the entire process of identity proofing, credential issuance, and authenticating the relationship between the credential data and an individual. Thus, it is recommended that the Working Group consider whether there is an alternative term to "electronic identification" that could be used.

In addition, using the word "electronic" for this term, which is intended to describe "the process to achieve assurance and the binding between a subject and an identity" creates potential confusion regarding the nature of the processes, systems, and the services addressed by the Draft Provisions. The same issue arises in the definitions of "identity management (IdM) services" and "identity management (IdM) system", which both require that they be "an electronic form." Describing the binding process as "electronic", or IdM services or IdM systems as being "in electronic form" ignores the fact that, in

[3] See, California Consumer Privacy Act Regulations at Article 4, Section 999.323(b); available at www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf?.

some cases, all or part of the process may not be electronic. For example, some functions may be performed in a non-electronic form, or rely on paper documents, such as identity proofing. Accordingly, it is recommended that the Working Group consider recognizing the fact that the processes, systems, and services covered by the Draft Provisions may well include a variety of non-electronic elements.

(d) **Identity**: Defining identity as a set of attributes that allows a [subject][person] to be "uniquely distinguished" within a particular context seems overly restrictive. In many cases, identification is used for purposes of qualification rather than uniqueness. For example, identification may be used simply to determine whether a particular person is a member of a specified group – e.g. are you over 21?, are you a member of the club?, are you a citizen? Etc. Presumably many people would possess those attributes, and thus the identity would not need to be unique, but it would sufficiently distinguish the data subject in the context in which such limited identity is required.

(e) **Identity credentials**: The Working Group should consider new developments regarding means of communicating identity information. While identity credentials are the typical means by which identification is asserted and verified, it is noteworthy that many new IdM systems do not use identity credentials per se. Thus, although the definition is not necessarily inappropriate, care should be taken to avoid building into the Draft Provisions an assumption that an identity credential will always be used. In addition, note that the definition is limited to "electronic form." The Working Group may want to consider whether the Draft Provisions should also cover traditional paper or in person forms of identification.

(f) **Identity Proofing**: The process of identity proofing need not completely "define and confirm" the identity of a subject. That is, identity proofing could presumably include collecting, verifying, and/or validating one or more attributes which, although by themselves not sufficient to define and confirm an identity, could be used by others to confirm an identity. Thus, the working group may want to consider a broader definition of identity proofing.

(g) **Relying Party**: Deleting this definition and replacing it with the term "subscriber" may not be appropriate. The concept of a subscriber implies an active participant in the system who is bound by the rules. While that may include a relying party, other persons/entities may enter into an arrangement for the provision of IdM services, including, for example, subjects. As a result, failing to differentiate between relying parties and subjects (or other users of an IdM system) may cause confusion in the application of the rules in the Draft Provisions. It is suggested that the Working Group consider retaining a definition of "relying party" so that the issues addressed in subsequent sections will appropriately apply to either relying parties or subjects.

(h) **Subject**: In the context of IdM services, a subject is a person or object that is identified, or at least engaging in the identity proofing process. Removing the reference to identification renders the term generic, and probably not helpful.

(i) **Subscriber**: As noted above, the concept of a subscriber as a person "who enters into an arrangement for the provision of IdM services or trust services with an IdM service provider or a trust service provider," appears overly inclusive, as it could include numerous roles in an identity system, as well as subjects. For example, paragraph 3 of Option C of Article 12 is written on the assumption that subscribers are relying parties. Yet subscribers could also be subjects or one of many of the other roles in an IdM system in which case the provisions of that section would be inappropriate.

2. Article 2. Scope of Application

The Working Group should consider reassessing the scope of the Draft Provisions as they relate to identity management. As Article 2 is currently written, the scope is

limited to two topics: (1) the ***use*** of ***IdM systems***, and (2) the ***cross-border recognition*** of ***IdM system***s.

The working group may want to consider whether the scope should also address ***IdM transactions***, as well as, perhaps, a reference to the ***functioning of*** an IdM system and/or the ***provision of*** IdM services.

Further, given the Working Group's recognition that it does not have the authority to draft rules for government-operated IdM systems (e.g., national IdM systems), the Working Group should consider revising Section 2 to clarify that it "applies to… ***private sector*** IdM systems."

3. Article 3. Voluntary Use of IdM and Trust Services

Under Article 3(2) a person's consent to use an IdM system is inferred from his or her conduct. Yet the Working Group should take note of the fact that this is not an appropriate inference in a case where the person's identity has been usurped – e.g., where an identity thief is using a fake credential, or alternatively, is using a real credential issued to somebody else. In such cases, the person whose consent is inferred is not the person engaging in the referenced conduct.

4. Article 4. Interpretation

The Working Group may want to consider ensuring 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.

5. Article 5. Legal Recognition of IdM

Some further review and analysis may be required with respect to Article 5(a). That section states that an electronic identification shall not be denied legal effect on the sole ground that it is in electronic form. We assume (but have not verified) that some laws regarding the use of identity credentials require the presentation of a paper or other physical form rather than electronics. Thus, before pre-empting such laws, we recommend some further review and analysis to determine the impact of this provision.

6. Article 6. Obligations of IdM Service Providers

Appropriateness of One-Size-Fits-All Approach: Article 6 lays out a set of obligations for IdM service providers. The obligations listed are obligations that fit the traditional IdM system model, and they assume that the IdM service provider performs, or is responsible for, all of the functions of such a traditional IdM system. However, IdM system models are undergoing a variety of changes and experimentation, raising concerns that using this list of obligations is based on an old model, that may not fit newer IdM systems and/or may unduly inhibit further experimentation. In many newer IdM systems, for example, some of IdM service provider functions listed in Article 6 may be the responsibility of a variety of different entities (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 impose a one-size-fits-all set of IdM service provider obligations in these Draft Provisions.

Source of Obligations: The Working Group may also want to consider a key threshold question. That is, whether the obligations of private sector IdM service providers (or

any other IdM system roles) should be set out in the Draft Provisions and made applicable to all IdM systems, or whether each private sector IdM system should define such obligations in its own contract-based trust framework. If the obligations of each role are included in the applicable IdM system's trust framework, this will allow the system operator and the participants to tailor those obligations to fit the purpose and use of the specific IdM system, as well as to comply with applicable law.

Rules Governing the IdM System: Finally, it should be noted that this section references "the rules governing the IdM system," which is not defined. It is not clear, for example, whether such rules are intended to be the contract-based trust framework that applies to a particular IdM system, or something else.

7. Article 7. Obligations of IdM Service Providers in Case of Data Breach

Responsibility for Breach Response: As currently written, Article 7 seems to confuse IdM systems and IdM service providers, and seems to assume that an IdM system will be under the control of a single IdM service provider who performs all of the IdM system functions. Moreover, Article 7 imposes obligations on such IdM service provider whenever a breach of security or loss of integrity "occurs," regardless of the IdM service provider's knowledge of that breach or responsibility or control over it. But the reality is that multiple parties may be involved in an IdM system, many of whom may not have any responsibility for, or control over, the server/network/system, employees, or other person or device that is the subject matter of the breach.

In many newer approaches to IdM systems, some of these functions may be done by different entities (e.g., trust providers, registrars, enrolment agents, credential service providers, authentication providers, hubs, etc.). Such roles may independently be the source of a breach, and such breach may not even be known by the IdM service provider.

Thus, when addressing the issue of a data breach, the Working Group should consider the *distinction between IdM systems and IdM service providers*, and the fact that *multiple IdM service providers* (as well as multiple other roles) may be participating in a single IdM system. Accordingly, the first issue will likely be determining responsibility for the subject matter of the breach, and responsibility for the notification obligations.

Ideally, the breach response duties imposed in Article 7 (e.g., to remedy the breach, revoke credentials, notify authorities, or notify affected data subjects and relying parties) should be imposed only on the party that actually suffered, or is otherwise responsible for, the specific server/network/system that was breached or compromised. For example, in the case of an IdM system that includes multiple IdM service providers or multiple roles, it may be appropriate to (i) impose the duty to remedy the breach on the entity that actually suffered the breach and is in a position to contain and remedy the breach, and (ii) impose the duty to notify subjects on the entity that has the relationship with the subjects.

System-Level Breach: Relatedly, the Working Group should also consider revising Article 7 to address the possibility that a major system-level breach in a multi-IdM service provider IdM system (such as a compromise of a root private key) could compromise the entire IdM system and all its IdM service providers, depending on the type and structure of the IdM system. In that case, a breach could affect all IdM service providers, regardless of their responsibility for the actual breach. Accordingly, a different type of response will likely be required, and all IdM service providers will presumably need to undertake certain responsive obligations, even though they may have no responsibility for the breach.

Responsibility for the Loss: Finally, note that Article 7(1)(b) requires the IdM service provider to "remedy the breach or ***loss***." While it may be appropriate to require an IdM service provider to remedy a breach (at least a breach over which it has control), the Working Group should consider whether it is appropriate to require the IdM service provider to also remedy the "loss." The loss could be substantial, and whether,

or the extent to which, and IdM service provider is liable for the losses incurred should be subject to the applicable liability rules, however they may be determined.

8. Article 8. Obligations of Subscribers

Role Obligations to Address: As a general comment, if these Draft Provisions are going to address obligations of IdM system participants (e.g., Arts. 6, 7, and 8), the Working Group may want to consider addressing the obligations of ***all*** system participants – e.g., the obligations of enrolment agents, attribute providers, IdM service providers, identity verification providers, users, hubs, relying parties, trust providers, subscribers, etc. This would also seem to be important for the purposes of allocating liability per Article 12 below.

Where to Address Obligations: Further, the Working Group may want to consider where best to address the obligations of IdM service providers, subscribers, and other participants in IdM systems. Articles 6, 7, and 8 of these Draft Provisions provide a one-size-fits-all approach to addressing the obligations of IdM service providers and subscribers. But given the diversity of IdM systems, it may be more appropriate to allow or require each IdM system to address the obligations of all of its various roles in a trust framework tailored to its specific technology, methodology, and purpose, rather than using the Draft Provisions to impose a one-size-fits-all approach on all IdM systems. This is due, in part, to the fact that the categories and definitions of system roles, as well as the obligations of participants filling those roles, will likely vary greatly from one IdM system to another. One factor giving rise to such variations is the purpose for which a particular IdM system is established (e.g., to facilitate online communications within the pharmaceutical industry, such as the SAFE BioPharma IdM system, to facilitate sharing of academic information, such as the InCommon IdM system used by universities, or to facilitate communications with government agencies, such as the eIDAS system).

In addition, as noted above regarding Article 6, IdM system models are undergoing a variety of changes and experimentation, raising concerns that it may not be appropriate to include a standard list of obligations, due to the risk that it may impose an outdated model that does not fit well with many current IdM systems, and inhibit further experimentation.

Duty of Subject Subscribers: Article 8 relates to subscribers (i.e., persons who enter into an arrangement for IdM services). This presumably includes numerous participants in an IdM system, such as relying parties, individual data subjects, and perhaps various other roles in the IdM system. It imposes obligations on subscribers to notify the IdM service provider whenever any subscriber knows that any identity credentials or electronic identification mechanisms in the IdM system has been compromised, or knows of circumstances that give rise to a substantial risk that a compromise may have occurred.

In the case of subscribers who are individuals (e.g., data subjects), this may impose a burdensome and unreasonable requirement. For example, there are presumably numerous situations where an individual IdM system subscriber may be aware of circumstances indicating there may have been a compromise, but simply does not understand their significance. Moreover, because this obligation appears to apply to the entire IdM system (rather than, e.g., a single identity credential issued to a particular individual), this provision seems to impose a significant burden on individuals (and for that matter, other system subscribers), who may be aware of, but simply don't understand, the system-wide significance of certain information.

Even regarding the loss or compromise of an individual's personal identity credential, it may not always be appropriate to impose on the individual a duty to report the loss. As with stolen credit card numbers, requiring a subject to report these events may simply not be realistic, or even appropriate (especially in the case of unsophisticated users or breaches occurring on the Internet or in other ways of which they may have no ability to discern). And in the case of IdM systems that are not based on the use of

physical credentials, a subject may simply have no idea that his or her credential data (e.g., ID number) has been compromised.

9. Article 9. Identification of a [Subject][Person] using IdM

Appropriateness of Preempting Existing Law: Article 9 is largely adapted from the E-signature Model Law and the United Nations Convention on Use of Electronic Communications in International Contracts, and appears to have the effect of pre-empting existing laws that define unique requirements for identification in particular cases. In the e-signature laws, this general approach of pre-empting all other signature laws worked well. However, the Working Group may want to evaluate whether this is necessarily true in the case of identification of a subject. Specifically, because some laws require simple identification, but others get very specific as to the manner and method of identification (including privacy laws, KYC laws, notary laws, etc.), a general rule indicating compliance simply by meeting a reliability standard may not be appropriate.

Presumably, a general identification process – even a "reliable" one – is not likely to satisfy the varying identification requirements of all existing laws. Moreover, to the extent that the parties to a commercial transaction have their own requirements for identification, an electronic substitute that meets the general standard of "reliability" may also not be sufficient to meet the particular or unique requirements of the parties.

Potential Conflict among Articles: The Working Group should also consider what appears to be a potential conflict between Article 2(3) and Article 9. Article 2(3) recognizes that many existing laws impose on private sector parties a variety of requirements for identification, and to that end, states that "Nothing in this instrument affects a legal requirement that a [subject][person] be identified in accordance with a procedure defined or prescribed by law." However, the one-size-fits-all approach of Article 9 appear to contradict this provision.

Option A of Article 9 states that:

> "Where the law or a party requires the identification of a [subject][person] the rule is satisfied with respect to IdM if a reliable [method][IdM system] is used for the electronic identification of the [subject][person]."

Option B of Article 9 is similar, and states that:

> "A subject may be identified by using IdM services if a reliable method is used for the electronic identification of the [subject][person]."

Given the wide variety of requirements in various laws for identification processes, the one-size-fits-all approach of Article 9 does not appear to be workable approach. Part of the problem, it would appear, is that identification is being treated in the same manner as electronic signatures. In the case of an electronic signature, creating an electronic signature in the manner prescribed by the Model Law will satisfy the requirement of any law requiring a signature. But the same is not true of identification requirements.

Legal requirements to identify someone vary greatly depending upon the law involved, the purpose for which the identification is required (foundational vs. functional), and the significance of the matter. For example, the recently released regulations governing the California Consumer Privacy Protection Act impose extensive identification requirements that must be met before personal data may be released or deleted at the request of a person claiming to be the subject.[4] Likewise, financial sector KYC rules impose a variety of specific identification requirements. Thus the Working Group may also want to consider whether, or under what circumstances, it is appropriate to use a one-size-fits-all blanket statement to the effect that using a reliable system satisfies a legal identification requirement.

[4] See, California Consumer Privacy Act Regulations at Article 4, available at www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-clean-020720.pdf?.

The conflict of these provisions illustrates the problem of attempting to build a set of identity rules using the same approach as previously used for electronic signatures.

Reliability as Relative Concept: In addition, it is important to consider whether Article 9 adequately recognizes that reliability (like security) is a relative concept. A reliable method in one context may not be reliable in another. For example, using Facebook or Google to conduct an electronic identification of a person is often sufficiently reliable for simple website account access, but likely not sufficient for accessing a bank account and authorizing an online transfer of funds from that account. Thus, if the reliability approach to obtaining a legal effect is to be retained, the Working Group is encouraged to consider changing the text of Article 9 to recognize that "reliable method" is a relative concept. One possible approach would be to incorporate something like the "reliable as appropriate" concept that was used in the United Nations Convention – i.e., where the method used is either: (i) As reliable as appropriate for the purpose for which the identification was required, in the light of all the circumstances, including any relevant agreement; or (ii) Proven in fact to have been sufficiently reliable.

Multiple Processes Relevant to Reliability: By applying the reliability requirement only to the method used for electronic identification,[5] Article 9 also appears to ignore all of the other process requirements for identification that could also have an impact on reliability of the outcome, and the methods potentially used for those processes. Such processes include identity proofing processes, enrolment processes, credential security, authentication processes, electronic identification processes, software, data security, employees, etc. For example, even if an objectively reliable method is used for the electronic identification of a person, that will be of no value if the identity proofing process was not also sufficiently reliable.

10. Article 10. Factors Relevant to Determining Reliability

Article 10 specifies only the factors relevant to determining the reliability of a "method ... for electronic identification"[6] referenced in Article 9. It does not, however, specify the factors that should be evaluated for determining the reliability of any other key processes performed by an IdM system, such as identity proofing.

Article 10 focuses on four categories of factors as follows:

- Compliance with the obligations in Article 6
- Compliance of the "rules governing the operation of the IdM system," with any recognized international standards and procedures, including level of assurance framework
- Any supervision or certification provided for the IdM system and
- Any "agreement between the parties."

Yet while the four factors listed focus on compliance with rules or standards, certification, and agreement between the parties, they do not necessarily establish reliability. The fact that rules and standards, certification, or agreements exist, and are complied with, does not necessarily mean that an IdM system compliant with them is reliable for any particular use. Thus, if the Working Group determines to address factors for determining reliability of a "method ... for electronic identification," it may want to consider what specific processes are relevant to reliability (e.g., identity proofing processes, enrolment processes, credential security, authentication processes, electronic identification processes, software, data security, employees,

[5] See Draft Provisions Article 1(d), which defines electronic identification as "a process used to achieve sufficient assurance in the binding between a [subject][person] and an identity."

[6] As set out in Article 1(d), the definition of "electronic identification" is limited to the process used to achieve sufficient assurance in the binding between a subject/person and an identity. It does not cover the many other processes that are required for an IdM system.

etc.), and then look at what rules or standards establish reliability with respect to each of those processes.

Moreover, as the foregoing list suggests, there are many different processes used by IdM systems, each of which can be done using one or more of a variety of "methods" that may, or may not, be reliable. Moreover, establishing that a "method ... for electronic identification," is being done via a reliable method, for example, does not necessarily mean the identity proofing process on which it relies was accomplished using a reliable method.

11. Article 11. Designation of Reliable IdM Systems

Criteria and Competence: Article 11 gives a public or private sector person or authority specified by the State (a "**Reliability Authority**"), the right to designate IdM systems that are considered reliable. However, Article 11 does not specify any criteria regarding the competence of the Reliability Authority to make such a designation. Moreover, it does not specify the process that should be used, other than a requirement to take into account all relevant circumstances, including the factors listed in Article 10, and a general requirement to be consistent with unspecified "recognized international standards and procedures relevant for determining reliability." As a result, this raises a concern that unqualified Reliability Authorities may evaluate reliability using inappropriate criteria, and thus, that unreliable IdM systems may be designated as reliable. Moreover, designations of reliable IdM systems are likely to vary widely between States, even for the same IdM system. Given the importance of such a designation under Article 9 (i.e., Art. 9 presumes that such designated IdM systems use "reliable methods" with resulting legal effect), this could result in significant problems.

The Working Group may also want to consider how a State will designate such a Reliability Authority as competent, as well as how it will ensure that such a Reliability Authority has the expertise, processes, and resources necessary to designate "reliable" IdM systems. For example, should the Reliability Authority specified by the State undergo some certification before being given this authority?

Reliability of Systems vs. Reliability of Transactions: Because reliability is a relative concept, assessments of reliability will presumably need to ask "reliable for what purpose?" This raises the threshold question as to whether the Working Group should be focused on the reliability of IdM systems generally (regardless of the type of identity transaction for which they are used) or to the reliability of IdM transactions (which provide a specific context in which to judge reliability).

Reliability of IdM Systems vs. Reliability of a "Method … for Electronic Identification": Article 11 focuses on the reliability of "IdM systems," whereas Article 9 determines the legal effect of an identification based on the reliability of the "method ... for electronic identification." These two approaches appear to be inconsistent, particularly because the reliability for a method for electronic identification is merely a subset of the overall reliability of the functions of an IdM system.

Practical Issues: The focus on the role of the Reliability Authority in Article 11 (and its importance in obtaining the legal effect provided under Art. 9) suggests the need for a centralized institutional mechanism to assess IdM systems in each State, and the involvement of public authorities, at least to appoint the Reliability Authority. We encourage the Working Group to consider whether this is practical.

In addition, the working group may want to consider whether the need to obtain benefit of being a designated reliable IdM system will discriminate against those IdM systems that are unable to afford the expense of the reliability designation process. Other issues that the Working Group may want to consider include –

- Who is appropriate to designate as the Reliability Authority?
- How to determine whether a Reliability Authority is qualified and competent?

- How reliable is a designation of reliability by a Reliability Authority (since it is an evaluation at a point in time)? How often does it have to be repeated?
- Should the State be in the business of appointing Reliability Authorities for private sector IdM systems, or conditioning certain legal effects on obtaining such a reliability designation?
- Does this have the practical effect of requiring all IdM systems to meet the standards selected by the State and or the Reliability Authority (since everyone will want to be designated as reliable), thereby potentially stifling future development?
- What qualifies as a "recognized international standard"? Who does the recognizing? What if the standard changes?
- Is the imposition of, and compliance with, a selected standard, likely to require potentially expensive and complex certification procedures?
- How do the factors for determining reliable methods (in Art. 10) relate to the requirements for determining reliable IdM systems (in Art. 11)?

Finally, because Article 11 contemplates designating IdM systems regardless of geographic location, the Working Group should consider whether this will create a practical need for IdM systems to seek such designation in each State where its subscribers will do business, and whether this will inhibit cross-border transactions.

12. Article 12. Liability of IdM Service Providers

There are a number of concerns regarding the liability provisions in this draft that the Working Group may want to consider.

Underlying Assumption: Article 12 (at least Options B and C), like Article 6, appear to be based on the assumption that the same rules can be applied to all identity systems. But given the ever-widening variation in IdM system types, purposes, scope, functionality, operation, and participant roles and responsibilities, it seems highly unlikely that the rules specified in Article 6, or the liability rules specified in Options B or C of Article 12, will be appropriate in all cases. One need only compare the differences between traditional PKI-based identity systems, blockchain-based identity systems, user-centric identity systems, and self-sovereign identity systems to see that these rules will not fit in all cases. Because IdM systems may differ significantly, any standard allocation of liability may not be appropriate for all IdM systems. Thus, the Working Group may want to consider whether a one-size-fits-all approach to liability is appropriate.

Roles Covered: Article 12 addresses the liability of only the IdM service provider. If the Working Group concludes that the issue of liability should be addressed in these Draft Provisions, it may be appropriate to consider the allocation of liability among all of the participants. This might include, for example, the liability of IdM service providers, enrolment agents, attribute providers, identity providers, subjects, users, hubs, verification providers, trust providers, relying parties, etc. This is important because addressing the liability of one system role does not mitigate or eliminate damages that may flow from a problem. It merely shifts that loss to someone else. An appropriate liability allocation should consider who should properly bear that loss.

Right to Disclaim or Limit Liability: The Working Group may want to consider whether the IdM service provider (or other system participants) should have the right to disclaim or limit its liability, by contract, or other means. Option A may allow for limitations or disclaimers, at least to the extent allowable under applicable law. This presumably recognizes that there are many other scenarios and types of liability that the IdM service provider or others may legitimately seek to disclaim or limit, and at least defers to the flexibility of liability limitation and disclaimer options available under applicable law.

While Option C does provide a limited right to disclaim liability, it is very limited in scope and does not allow for flexibility. Moreover, there is a question as to whether the provisions of Options B or C generally, prohibit an ID service provider from disclaiming liability altogether (as a government entity would typically do).

Also, to the extent that Option B and C limit an IdM service provider's liability to a breach of their obligations as set out in Article 6, there is a question as to how this limit will work in the case of an identity thief. That is, if an IdM service provider issues a credential to, or electronically identifies, an identity thief without breaching the provisions in Article 6, who bears the loss? Should an identity theft victim who may have no interaction or contract with the IdM service provider suffer the loss?

Liability Limitations of Option C: Article 12(3) of Option C is based on the assumptions that (1) purpose or value limitations can be placed on specific identity transactions (although it doesn't specify where or how those limitations are imposed), and (2) that such limitations can be easily known by the relying party before it relies. This appears to be a holdover from the original approach used in some early PKI systems, whereby the certificate issued by the certification authority (CA) would contain a purpose or dollar limitation that the relying party was expected to review prior to any reliance. Given the wide-ranging variety of IdM systems in existence today, the Working Group may want to consider whether a transaction-based limitation on liability is workable. For example, this Article might be changed to recognize that such limitations may be specified in the IdM service provider's trust framework or contract with relying parties, rather than in individual transactions.

Government Interface: Finally, the Working Group may also want to consider the potential interplay with government IdM systems. In many cases, IdM service providers rely on attribute assertions from third parties, such as national IdM systems or other government databases (e.g., DMV). Since government IdM systems are often viewed as authoritative, although they will also typically not accept any liability for errors, determining who bears the loss in the case of errors in government supplied information should be considered. Thus to the extent public entities are involved, a different approach may be required.

We urge the Working Group to consider avoiding attempts to allocate liability, particularly in light of the wide-ranging variety of IdM systems, processes, and participants. If the Working Group determines to address liability, we encourage reference to the methods by which liability may be determined, but not to actual standards, specifications, or liability rules themselves. Such methods might include, for example, reference to existing law (as in Option A), or reference to contract-based trust frameworks adopted by an IdM system and contractually agreed to by the parties.

13. Article 26. Cross-border recognition of IdM and trust services

- Regarding the issue of cross-border "recognition," the Working Group may want to clarify answers to three fundamental questions: Recognition of what? Recognition by whom? Recognition for what purpose?
- Recognition of what? Article 26(1) appears to answer this question by focusing on "IdM systems" and the "legal effect" of "IdM systems." It is not clear, however, how an IdM system can have a legal effect, or what the legal effect of a system might be. Presumably, reliance on the identity proofing and/or the electronic identification processes performed by an IdM system could have a legal effect, but it is not clear how an IdM system itself could be deemed to have a legal effect.

By analogy, States recognize passports issued by other States based on ICAO standards. Each State presumably agrees on the validity of the ICAO standards, and may or may not evaluate whether the passport-issuing system of each other State complies with those standards, but it is the credential – i.e., the passport issued by each State's system – that is given "legal effect" at the border.

- Recognition by whom? Presumably the entity recognizing a foreign IdM system is either: (1) a public entity, such as a government or a court applying the associated the law/legal system (e.g., as in satisfying a legal requirement to verify identity, or constituting admissible evidence in a court), or (2) a relying party (public or private sector). Draft article 26 presumably focuses on the first option, as it refers to the "legal effect" of whatever it is that is being recognized. Moreover, the second option doesn't require a law or legal conclusion, as relying parties are certainly free to make their own decisions regarding whether they will recognize and/or rely upon IdM systems or identity for purposes of whatever transaction they are engaged in.
- Recognition for what purpose? If an "IdM system" is being recognized by the law of a foreign State, what does that mean? The concept of an IdM system having a legal effect seems somewhat confusing. For example, does that mean that the foreign State will automatically accept the results of an electronic identification done by the recognized IdM system, or does it simply mean that the recognized IdM system will be allowed to do business in the foreign jurisdiction, but it's processes may need to be modified to satisfy legal requirements that the foreign jurisdiction imposes on its own IdM systems?

The Working Group should consider clarifying what it means to say that an IdM system operated outside [the enacting State] shall have the same legal effect in [the enacting State] as an IdM system operated in [the enacting State].

14. Article 27. Cooperation

The intent of Article 27 is not clear. The focus appears to be on exchanging information, experience, and good practice – something certainly not objectionable and ideally, to be encouraged, especially if the exchange is voluntary and does not involve the negotiation of agreements binding on entities not party to the cooperation. In that case, however, it would not seem necessary to require that the entity exchanging the information be specified by the enacting State as competent. Moreover, it would not seem necessary to focus the cooperation to the three categories listed in Article 27.

If the cooperation and exchange is mandatory, or serves as a basis for legal recognition by a State or the negotiation of agreements binding on entities not party to the negotiation, this would seem to raise a variety of concerns that would seem to require further discussion and clarification by the Working Group.

Also, note that article 27 allows (or requires) an entity or agency specified by the enacting State as competent to cooperate "with foreign entities." It is not clear what the term "foreign entities" refers to – e.g., is it the foreign government, is it any IdM service provider that happens to operate in the foreign State, etc.? Presumably, such cooperation with "foreign entities" should be limited to foreign entities that are also specified as competent by the foreign State.