United Nations A/CN.9/WG.IV/WP.145

General Assembly

Distr.: Limited
20 February 2017

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Fifty-fifth session
New York, 24-28 April 2017

Legal issues related to identity management and trust services

Proposal by the United States of America

Note by the Secretariat

The United States of America submitted to the Secretariat a paper for consideration at the fifty-fifth 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.17-01089 (E)

Annex

I. Introduction

At its 54th session, Working Group IV (Electronic Commerce) began its discussions on the topic of identity management (IdM) and trust services. The tentative initial conclusions of the Working Group were as follows:

> 118. After discussion, the Working Group agreed that its future work on IdM and trust services should be limited to the use of IdM systems for commercial purposes and that it should not take into account the private or public nature of the IdM services provider.
>
> 119. The Working Group also agreed that work on IdM could take place on a priority basis. It further agreed that focus should be placed on multi-party identity systems and on natural and legal persons, without excluding consideration of two-party identity systems and of physical and digital objects when appropriate.
>
> 120. In addition, it was agreed that the Working Group should continue its work by further clarifying the goals of the project, specifying its scope, identifying applicable general principles and drafting necessary definitions.

(A/CN.9/897 at paras. 118-120).

To help focus the discussion for the 55th session of the Working Group and thereafter, the delegation of the United States of America has prepared this paper in an attempt to provide an outline of issues for the Working Group to consider. While there are undoubtedly many other issues that the Working Group will need to consider, the following initial list can hopefully be used as a starting point to guide initial discussions and to help focus the efforts of the Working Group. It is our hope the discussion of these issues, and other issues that may be identified by the Working Group, may provide direction to the Secretariat for the preparation of a Working Paper on IdM.

We understand that experts have engaged in an informal discussion of relevant terminology during the intersessional period. Although we believe that it will ultimately be necessary to carefully consider the wording of the definitions of the terminology to be used in this project, at this initial stage we recommend that the Working Group consider using initial definitions simply as the basis for facilitating its discussion. We recognize, however, that agreement on more detailed legal and technical definitions may ultimately be required.

II. Project Goals and Objectives

As a starting point, the Working Group may want to give consideration to the overall goals and objectives for the project. In light of the initial decision to focus on the use of IdM systems for commercial purposes, the Working Group may want to consider which of the following goals and objectives might be appropriate for this project:

- Promote the development of a private sector identity ecosystem;
- Identify and remove legal barriers to commercial identity transactions;
- Remove ambiguities regarding the applicability of existing law to commercial identity transactions;

- Encourage the commercial use of and reliance on third party digital identity credentials;
- Facilitate the trust needed for commercial online identity transactions;
- Assist private parties by providing a basis for deciding whether to trust digital identity information in commercial transactions;
- Identify and remove cross-border obstacles to e-authentication;
- Facilitate cross-border recognition of digital identity information; and
- Foster confidence in electronic commerce.

III. Nature of the Proposed WG IV Work Product

It might be useful to begin consideration of the type of product the Working Group would like to develop in the field of commercial identity management.

IV. Governing Principles

Regardless of the ultimate form of the work product to be produced by the Working Group, there are several general principles that the Working Group may want to consider, and where appropriate adopt, to guide its work with respect to IdM. As with the Model Law on Electronic Commerce and the UN Convention on the Use of Electronic Communications in International Contracts, such general principles can be used to guide the Working Group in its deliberations. Moreover, governing principles can be useful to help clarify the scope of work. Possible governing principles the Working Group may want to consider include the following:

A. Source of Legal Duty to Identify

As a starting point, the Working Group may want to consider whether any IdM legislation should contain obligations to identify a party in a commercial transaction independent of those that apply as a result of other legislation. If IdM legislation does not contain any obligations to identify a party, legal requirements to identify a party in a commercial transaction would be left to other existing laws such as laws governing notarization, “know your customer” requirements, anti-money laundering laws, or laws governing access to personal data. This was the approach the Working Group took with respect to electronic signatures when it developed the Model Law on Electronic Commerce and the UN Convention on the Use of Electronic Communications in International Contracts.

B. Party Autonomy

Because IdM systems will typically be governed by contract-based system rules agreed to by the participants in such systems, it may be important to consider whether, and the extent to which, any law governing IdM transactions should recognize and defer to such system rules.

Thus, the Working Group may want to consider whether the principle of party autonomy should apply to commercial identity systems to allow the parties to an identity system to vary by agreement the provisions of any legal rule, or of certain legal rules.

C. Technology Neutrality

Many different types of identity systems may be developed and implemented for use in commercial transactions. Such systems may use a wide variety of technologies. These may include simple usernames and passwords, more complex systems based on the PKI x.509 standard or other standards such as SAML or OpenID Connect. Additionally, systems are currently being developed using new technologies, such as Blockchain.

Thus, the Working Group may want to consider whether any work product relating to IdM should make clear that any IdM rules should not require the use of any particular technology.

The Working Group may want to further consider how UNCITRAL might best address the existence and use of multiple commercial identity systems.

Legislation other than that specific to IdM may, of course, require that parties use identity systems that meet certain requirements. And parties themselves may insist that the persons and entities with which they do business use a particular identity system. For example, a commercial entity could restrict access to its services to users that use one or more specific identity systems of which it is a member.

D. System Model Neutrality

In addition to variations among technologies deployed, commercial identity systems are currently the subject of a great deal of experimentation with respect to organizational and business structures and approaches deployed. We can probably expect to see quite a wide variation among identity system models in the future, even if they use the same underlying technology. These include broker or hub type arrangements, single identity provider models, single relying party models, organizational models, and many other different approaches.

Accordingly, the Working Group may want to consider whether it should adopt as a principle the concept of system model neutrality -- that is, a recognition that any work product developed should not be written in a way that assumes or requires the use of any particular identity system business, organizational, or structural model, and that can readily accommodate future changes in identity system approach, structure, and business model.

E. Non-Discrimination

The Working Group may also want to consider the applicability of the principle of non-discrimination in the context of the use of identity systems for commercial purposes. Under such a principle, for example, the legal effect (e.g., satisfaction of a legal requirement for identification) and admissibility as evidence in legal proceedings of an electronic identification should not be denied solely on the grounds that such identification was made in electronic form.

F. Relationship between Identity Management Law and Privacy Law

Commercial identity transactions involving the issuance or use of an identity credential will frequently involve some personal data. In such cases, privacy of such personal data may be important.

Privacy laws usually address the protection of personal data in accord with relevant public policy. Accordingly, the Working Group may want to consider the relationship between these laws and IdM systems.

G. Relationship between Identity Management Law and Data Security Law

Data security is critical to the proper functioning and trustworthiness of identity transactions, both from the perspective of protecting the confidentiality of the personal data involved in such transactions and for ensuring the proper functioning and trustworthiness of the credentials communications comprising the transaction itself.

Data protection laws often address the security of personal data in accord with relevant public policy. Similarly, other data security laws may do the same with respect to protecting other aspects of identity transaction communications. Accordingly, the Working Group may want to consider the relationship between these laws and IdM systems.

H. Relationship between Contract-Based System Rules and Other Law

Because IdM systems will typically be governed by contract-based system rules (i.e., trust frameworks) agreed to by the participants in such systems, the Working Group may want to discuss the relationship b5,etween these rules and applicable laws that are not directly related to identity.

V. Substantive Topics

A. Legal Recognition

The Working Group may want to consider the topic of legal recognition of identity information authenticated in a commercial transaction. In this regard, the Working Group may want to address what legal recognition is, what it seeks to achieve, and the requirements to obtain it; who provides legal recognition; the purposes for which legal recognition is provided; the relationship between legal recognition and laws that require some form of identification, such as laws governing notarization, “Know Your Customer,” anti-money laundering, access to personal data; and how, if at all, legal recognition applies to the identity of legal entities, devices, or digital objects.

B. Cross-Border Mutual Recognition.

The concept of mutual recognition is important to facilitate the commercial use of identity credentials, and reliance on those credentials, both across identity systems and across jurisdictional boundaries.

There are numerous issues that the Working Group may want to consider with respect to the subject of mutual recognition. Some of the more obvious issues include addressing: (a) whether there should be a requirement to recognize credentials, (b) if there is requirement to recognize credentials, who should be required to recognize the credentials, (c) if there is a requirement to recognize credentials, which party’s credentials should be recognized, (d) what is the purpose of such mutual recognition, (e) what exactly does “mutual recognition” mean, (f) what characteristics (e.g., levels of assurance) should be present for mutual recognition, (g) should there be limits on

when mutual recognition applies, and (h) should mutual recognition apply to identity of legal entities, devices, or digital objects?

C. Attribution of Identity Information to a Subject

Attribution of identity information to a subject (for inclusion in an identity credential) is often a critical element of identity management systems. A fundamental question governing attribution is when and under what circumstances is identity data in a credential to be attributed to a specific subject.

The Working Group may want to consider this issue from two perspectives. First, how should an identity provider ensure that the information about a subject that it includes in an identity credential does in fact describe the subject named in the credential? Second, when an identity credential is used, how can a relying party ensure that the information in the credential relates to the subject presenting the credential?

D. Reliance / Attribution of Action, Data Message, or Signature to a Subject

A key question for all participants in an identity system is when, and under what circumstances, reliance on an identity credential by a party is appropriate and reasonable. The reasonableness of reliance by a party can affect a variety of issues, including when an erroneous identity credential is relied upon.

For example, in the context of electronic signatures, this issue was addressed in Article 13 of the Model Law on Electronic Commerce.

E. Liability / Risk Allocation

Issues of liability and risk allocation are frequently cited as major barriers to the implementation of commercial identity systems. Issues include (a) concerns by identity providers and other participants in identity systems that the liability risk allocated to them under existing law is inappropriate or simply too onerous to allow them to proceed, as well as (b) concerns by participants in identity systems that the law is too vague, ambiguous or uncertain to allow them to properly assess their risks of participating.

The Working Group may want to consider whether it should address the issue of liability, and if so, for which identity system roles, and how. Examples of laws which address liability in the context of IdM systems include the European Union eIDAS regulation and the Virginia Electronic Identity Management Act.

F. Transparency

The processes, procedures, and technology used by an identity provider to issue and validate identity credentials can have a significant impact on the trustworthiness of any identity transaction using those credentials. Accordingly, it may be important that other participants in an identity system understand how those processes, procedures, and technology are implemented, so that they can make their own assessment as to the reliability and trustworthiness of the resulting identity transactions. To that end, the Working Group may want to consider whether there is an appropriate level of transparency on the part of certain participants within an identity system. Likewise, in the event of a breach or compromise in any of the processes, procedures, technology,

databases, or identity credentials maintained by a party in the context of an identity system, the Working Group may want to consider whether information regarding such compromise should be disclosed.

In some cases, transparency requirements have also been used as a substitute for regulation mandating certain processes, procedures, or technology. An approach based on transparency allows parties to make their own decisions regarding trustworthiness based on more complete information.

G. Trustworthiness / Levels of Assurance

Many identity systems define so-called “levels of assurance” to help the participants to address concerns regarding the trustworthiness of identity credentials and identity transactions. Several levels of assurance schemes exist, and they often involve differing gradations of assurance. For example, the EU defines three levels of assurance in its eIDAS Regulation (designated as “low,” “high,” and “substantial”), whereas four levels of assurance are utilized in the United States and elsewhere.

The Working Group may want to consider how best to facilitate trust by the participants in an identity system. While the concept of levels of assurance is commonly used, the Working Group may also want to consider whether other mechanisms, such as mandated transparency, third-party certification, or other approaches can be used to help facilitate trust.