United Nations A/CN.9/891

General Assembly

Distr.: General
3 May 2016

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Forty-ninth session
New York, 27 June-15 July 2016

Legal Issues Related to Identity Management and Trust Services

Note by the Secretariat

Contents

		Paragraphs	Page
I.	Introduction	1-5	2
II.	Legal Issues Related to Identity Management and Trust Services	6-55	3
	A. Current Legal Environment for Identity Management and Trust Services	6-30	3
	B. Promoting Confidence in the Use of Identity Management and Trust Services	31-43	7
	C. Relevant Issues for Future Work	44-55	8

V.16-02634 (E) 170516 180516

I. Introduction

1. At its forty-eighth session, in 2015, the Commission requested the Secretariat to conduct preparatory work on identity management and trust services, including through the organization of colloquiums and expert group meetings, for future discussion at the Working Group level following the current work on electronic transferable records on the basis of a proposal submitted to the Commission for its consideration (A/CN.9/854).[1]

2. At that session, the Commission also asked the Secretariat to share the result of such preparatory work with Working Group IV, with a view to seeking recommendations on the exact scope, possible methodology and priorities for the consideration of the Commission at its forty-ninth session.[2]

3. In furtherance of that request, the UNCITRAL Colloquium on Legal Issues Related to Identity Management and Trust Services was organized on 21 and 22 April 2016 in Vienna. Moreover, the Secretariat participated in a conference on "Open Issues on Electronic Commerce: the Digital Identity", organized by the University of Bologna (10 June 2015, Bologna, Italy); an "International Identity Management Law and Policy Meeting" co-organized by the American Bar Association (ABA) and the World Bank (Washington, United States of America, 14 January 2016); and a conference on "Identity Management and Trust Services since the eIDAS regulation" organized by the University of Namur (Namur, Belgium, 18 March 2016).[3]

4. This note provides a summary of the discussions at that Colloquium and at other relevant meetings. Materials used for presentations at the Colloquium are available on the UNCITRAL website.[4]

5. The Commission may wish to note that a document providing an overview of identity management had been submitted to Working Group IV (Electronic Commerce) at its forty-sixth session (A/CN.9/WG.IV/WP.120) and that additional considerations are contained in a document submitted to Working Group III (Online Dispute Resolution) at its thirty-second session (A/CN.9/WG.III/WP.136). The report on a prior colloquium on electronic commerce, which included a panel on identity management, is also available (A/CN.9/728, paras. 9-28).

---

[1] *Official Records of the General Assembly, Seventieth Session, Supplement No. 17* (A/70/17), paras. 354-355 and 358.

[2] Ibid., para. 358.

[3] The proceedings of that Conference have been published: Hervé Jacquemin (Dir.), *L'identification électronique et les services de confiance depuis le règlement eIDAS*, Brussels, 2016.

[4] Those materials, presented in the form they were submitted by speakers, are available at: www.uncitral.org/uncitral/en/commission/colloquia/idm2016-programme.html.

II. Legal Issues Related to Identity Management and Trust Services

A. Current Legal Environment for Identity Management and Trust Services

6. Electronic identity management (IdM) is a foundational issue for the use of electronic means. Verifying the identity of remote parties, such as determining who is seeking access to an online database of sensitive information, who is trying to initiate an online transfer of funds from an account, who signed an electronic contract, who remotely authorized a shipment of product, who is seeking access to online government services, or who sent an e-mail, is often a fundamental concern. Functionally, IdM aims at answering the basic questions: "Who or what is seeking to prove identity?" and "How reliably is identity proven?" in an electronic environment.[5]

7. In that respect, it should be noted that verifying in a trustworthy manner the identity of a remote party in an electronic environment is necessarily different from verifying in a trustworthy manner the identity of a present party in a physical environment. For instance, IdM may be used remotely and simultaneously in multiple applications, while traditional means of identification may not.

8. Paper-based identity documents have been used for centuries to identify natural persons and well-established practices were developed, so that users of such documents know their reliability as identification tools and the risks associated with their use. By contrast, IdM being a relatively new process that requires correlation of electronic identity information with a person not physically present, related business practices are not yet fully established and risk assessments vary. Therefore, promoting confidence in the use of IdM systems requires clarifying, among others, various technical and legal aspects, including liability issues.

9. Given its broad relevance, IdM may have an impact on cultural, political, social and economic inclusion.[6] IdM has several implications for the Sustainable Development Goals, being directly relevant for Target 16.9 (on providing legal identity for all, including birth registration, by 2030) and an enabler to a number of other targets such as Target 1.4 (on ensuring access of the poor to economic resources, including property and finance), Target 10c (on reducing remittance costs) and Target 16.5 (on reducing corruption).

10. The ongoing transition towards online-enabled and data-driven economies requires the use of IdM for multiple business and social uses. Policymakers suggest the adoption of user-centric IdM models where users have the choice of what identity credentials and level of assurance to use.[7]

11. In the current legal environment, IdM systems and trust services are subject, on the one hand, to requirements contained in laws drafted for other purposes

---

[5] A/CN.9/WG.IV/WP.120, paras. 6 and 8.

[6] In general, see the World Bank Identification for Development Programme at www.worldbank.org/en/programs/id4d.

[7] OECD, Digital Identity Management: Enabling Innovation and Trust in the Internet Economy, Paris, 2011, pp. 7 ff.

(e.g., commercial and civil code; privacy laws); and, on the other hand, to contractual agreements (often called “system rules”, “scheme rules” or “trust frameworks”), which aim at ensuring proper functioning and trustworthiness of the system by defining the obligations of the parties.

12. Although a majority of the world’s jurisdictions have adopted laws on electronic transactions and electronic signatures that often contain provisions relevant for IdM and trust services,[8] only a few laws specifically dealing with the use of IdM and trust services exist.[9] Additional legislative provisions may cater to specific industry needs, such as those of the banking sector and payments services.[10]

13. Several States have indicated interest for preparing legislation on IdM or have started doing so. Those initiatives are based on differing approaches and notions. There is therefore a clear, strong and urgent need to provide guidance to legislators in order to suggest desirable options and to prevent lack of harmonization.

The scope of IdM systems

14. A number of different IdM models are currently in use to discharge several functions, which may vary significantly in purpose and requirements. Since IdM systems may involve different types of applications, services and users, it is important that their legal analysis should not be limited to certain types of transactions, such as commercial ones. Similar considerations apply to trust services.

15. IdM systems may be used to identify natural and legal persons as well as physical and digital objects. However, not all of those entities have received equal attention in the study of legal issues related to IdM. In particular, work on legal aspects of identification of objects seems to require additional attention. In that respect, it should be noted that certain technologies (e.g. radio frequency identification (“RFID”) tags or other contactless technology) may be more suitable for identification of objects than others and therefore may provide user cases that could be useful to start that analysis.

16. Commercial users of IdM typically carry out an analysis of benefits and costs associated with technologies and methods used to conduct business and therefore require a significant level of flexibility. Moreover, those users require clarity and predictability on the allocation of obligations and related liability among concerned parties. The same considerations may not necessarily apply in case of use of IdM systems for providing public services.

17. IdM systems may be classified in a variety of manners, such as “commercial-driven” or “government-driven”, and “centralised” or “decentralised”.

---

[8] For an overview of the current status of legislation on electronic transactions and electronic signatures, see the UNCTAD Global Cyberlaw Tracker at http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx.

[9] E.g., Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market; Virginia Electronic Identity. Management Act, 2015 (SB 814).

[10] See the relevant provisions contained in the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.

Another classification refers to IdM systems providing foundational or core identities, i.e. identity attributes that typically do not change, such as birth name or date, which are supposed to be multipurpose; and to IdM systems providing functional identities, i.e. identity attributes that are issued for a specific purpose.

18. Although at a global level the commercial need for IdM is a major driver of IdM systems, the importance of government IdM systems should not be underestimated. It has to be noted that traditionally a number of functions related to identity management in the physical world have been performed by civil registration and vital statistics (CRVS) registries. Those registries have been, especially in the last two centuries, managed by governments. When performing CRVS-related functions, governments typically limit their liability in line with the legal regime applicable to governmental activities and ensure the reliability of the information contained in the registry with other legal mechanisms (e.g., criminal law provisions for providing or creating false identity-related information).

19. Commercial practices regarding the identification of parties developed over centuries on the basis of identity information available from CRVS and other registries and its associated legal framework. To date, CRVS registries play an important role in providing information used in IdM. In particular, CRVS registries may be used as the basis for "breeder documents" that commercial systems rely upon in establishing the identity of natural and legal persons.

20. Further, government-driven IdM systems may be designed as extensions and improvements of traditional CRVS registries. Those systems may stress security and other features relevant to their intended main use. Moreover, in line with the traditional approach of CRVS registry operators, their providers do not necessarily operate under a full liability regime in case of non-performance or partial performance of their services.

21. Commercial identity credentials issued for different purposes may rely on the same primary identity document. Yet, those different identity credentials may offer varying levels of reliability and will be used with different methods and technologies. Hence, legal analysis of the relationship between the various identity credentials and the primary breeder identity document requires careful examination.

22. The above considerations highlight that no single model or solution for IdM exists. On the contrary, many IdM systems with different purposes co-exist. Similarly, obligations and liability of the parties involved in IdM systems may vary. This, however, does not seem to preclude the possibility of identifying common elements and of building on those elements to promote legal interoperability.

Interaction and interoperability among IdM systems

23. IdM systems are often federated. According to that model, identity information verified by one entity is made available in an agreed-upon and managed fashion to multiple parties that need such identity information for different purposes.[11] Federated IdM systems achieve interoperability among their participants by using a common technical and legal framework defined by a set of system rules. Federation of an IdM system contributes to increasing the number of users and of applications and may assist in containing IdM-related costs.

[11] A/CN.9/WG.IV/WP.120, para. 10.

24. Currently, however, most IdM systems operate in an autonomous manner, with little or no interaction. Barriers to that interaction are both technical and legal. In particular, legal rules applicable to IdM systems may vary significantly. However, the value of an IdM system is proportional to the number of parties using it and to the number and diversity of applications in which it can be used. Hence, ideally the various IdM systems should interact seamlessly, thus implementing not only technical interoperability but also legal mutual recognition (referred to as "legal interoperability").

25. Since federation alone may not address all the issues posed by IdM, IdM systems would benefit from a harmonized legal framework. Whether federation of IdM systems as such poses specific legal challenges is a matter that requires further investigation.

26. Additional challenges to technical and legal interoperability may arise at the regional level, where specific trends may exist and where available capacity and resources may not always suffice.

27. A number of organizations aim at promoting the development and wider use of IdM systems.[12] That goal requires a combination of policy decisions, technical developments and legal provisions. Certainty and predictability of applicable legal rules — as well as, to the extent possible, their harmonization — could greatly contribute to removing barriers to the use of IdM across systems and national borders.

Trust services

28. Trust services encompass a number of different services aimed at promoting confidence in electronic transactions, including, but not limited to: digital archiving; time-stamping; signatures providing evidence of origin and integrity of the message; return receipt; guarantee to existence at a certain point in time; digital seals; authentication of electronic address (e.g. URL) and escrow.

29. UNCITRAL texts on electronic commerce contain a number of provisions relevant to trust services, such as provisions on electronic signatures, on integrity of data messages, on archiving of data messages, and on the attribution of data messages. As those texts have been widely adopted in the world,[13] a significant amount of uniform law already exists in this field.

30. Trust services may have elements in common with IdM services. However, significant differences also exist, in particular, in light of the function pursued with the use of each trust service. It remains to be determined whether it would be feasible and desirable to jointly consider legal aspects of IdM and trust services.

---

[12] See A/CN.9/WG.IV/WP.120, para. 5, for a list of several organizations engaged in the field.

[13] For the status of adoption of UNCITRAL texts on electronic commerce, see www.uncitral.org/uncitral/uncitral_texts/electronic_commerce.html.

B. Promoting Confidence in the Use of Identity Management and Trust Services

31. Ensuring trust in the operation of IdM systems and trust services is fundamental in order to promote their use (see paras. 6-8 above). Trust may be defined as "Firm belief in the reliability […] of […] something".[14] It is therefore an opinion influencing behaviour and the willingness to rely. In the case of IdM and trust services, trust is the opinion on the reliability of the service offered.

32. In turn, reliability may be defined as "the quality […] of performing consistently well"[15] and is the result of a process, rather than a product.

33. Lack of clarity on parties' liability is a major barrier to promoting trust in the use of IdM and trust services. Parties need to be able to clearly assess rights and obligations and to allocate risks. Currently, those terms can be clarified in contractual agreements (often contained in system rules) whose content may vary significantly. Moreover, the law may allocate liability, possibly on the basis of general rules, in absence of any agreement, or may also override those agreements. Provisions on limitation of liability contained in the law and in contractual clauses are also relevant to define risk allocation. Similarly relevant is the availability of commercial insurance to cover risks associated with the use of IdM and trust services.

34. It is of great importance that legislative and contractual provisions aimed at promoting trust should focus on the outcome of the process, e.g. providing reliable services, rather than prescribing specific processes, which could violate technology or identity system neutrality. This has important practical consequences, for instance, by ensuring that rules do not prevent use of IdM with any particular technology or method, such as mobile devices. Likewise, legislative requirements associated with reliability may refer to technical standards; however, caution is necessary to avoid favouring any technology, method or process, or to inhibit adaptability to change.

35. Specifically, the law may promote confidence in the reliability of IdM systems and trust services by rewarding compliance with certain requirements associated with reliability of the system or service.

36. In particular, the law may attach legal presumptions to the use of IdM systems or trust services that satisfy certain requirements. Such presumptions may shift the burden of proof on origin, integrity, time of despatch and receipt, etc. when electronic transactions are used with the assistance of compliant IdM systems or trust services. Parties are free to choose whether those systems and services are relevant and useful for their commercial operations, thus achieving desired flexibility.

37. Alternatively, the law may provide for limitation or exclusion of liability for certain parties involved in IdM systems and trust services as long as they comply with requirements set forth in legislation or contractual agreements. The law may

---

[14] Oxford English Dictionary Online, "Trust", sub 1.

[15] Oxford English Dictionary Online, "Reliability", sub 1.

also set forth that contractual agreements may not derogate or vary liability for gross negligence or wilful misconduct.

38. One important benefit arising from a clearer understanding of the obligations of the various parties in an identity system and of allocation of liability risk among them is improved assessment of cybersecurity needs, which, in turn, allows more efficient distribution of related resources in line with the parties' actual needs.

Cross-border use of IdM and trust services

39. An enabling legal environment for the use of IdM and trust services needs to take into full consideration also cross-border aspects of that use. Those aspects may pose additional challenges in the absence of a uniform legal framework promoting mutual recognition of the legal status of IdM systems and trust services. In dealing with such aspects, due consideration should be given to provisions on mutual legal recognition of authentication methods contained in international instruments such as free trade agreements.[16]

40. Currently, cross-border legal recognition may be achieved on the basis of private agreements stipulating contractually the terms of service as well as technical specifications.[17] That model is, however, subject to limits to freedom of contract set forth in applicable national law and does not apply to parties that are not contractually bound.

41. Another approach to cross-border legal recognition of IdM systems and trust services may foresee the establishment of a centralized accreditation system performing an assessment, whose result determines the legal status of the system or service and is binding on participating States. Assessment of conformity of systems and services is made before their actual use and along general categories. That model may be particularly useful when applied in the framework of regional economic integration since States pursuing that integration have an incentive to join it.

42. Yet another possibility would foresee the preparation of uniform legal provisions to pursue cross-border recognition, preferably on a multilateral basis. In that case, it would be possible to conduct the assessment of reliability only in case of actual dispute and on a case-by-case basis.[18]

43. One important consideration relates to the need for a uniform law text to interact with private international law rules. Analysis of that interaction may require special attention.

C. Relevant Issues for Future Work

44. Various stakeholders welcome UNCITRAL's decision to undertake work on legal aspects of the use of IdM systems and trust services and suggest that UNCITRAL should prepare provisions aimed at providing specific legislative

---

[16] See, e.g., article 14.6 of the Trans-Pacific Partnership.

[17] This model is used by the Pan-Asian E-Commerce Alliance.

[18] This approach is adopted in article 9, paragraph 3 of the United Nations Convention on the Use of Electronic Communications in International Contracts.

guidance. The outcome shall enhance parties' confidence in the use of IdM systems and trust services and promote legal interoperability among IdM systems. That work product would, on the one hand, fill the current gap between general legislation and system rules and, on the other hand, ensure uniformity in future legislation.

45. In conducting future work, it seems particularly important to ensure coordination with relevant organizations dealing with legal and technical aspects of IdM systems and trust services. This will allow focusing the exercise on concrete issues, drawing on existing experience and expertise as well as highlighting common elements in existing and prospective laws.

46. With respect to the form of future work by UNCITRAL, while the preparation of model legislation to be enacted at the national level may be envisaged, an international text may be more appropriate to cover cross-border aspects. Non-legislative texts, such as model contractual provisions, could adequately address certain issues. Mutually reinforcing texts could be drafted.

47. With respect to the content of provisions on IdM systems and trust services, the general principles underpinning UNCITRAL texts on the use of electronic communications (technology neutrality, non-discrimination of electronic communications, functional equivalence) and other general principles of uniform commercial law, such as freedom of contract, are relevant for defining the legal framework for the use of IdM systems and trust services.

48. Moreover, several provisions contained in UNCITRAL texts on electronic commerce (e.g., provisions on electronic signatures and on archiving) and in certain other texts[19] are directly relevant for IdM systems and trust services and may provide useful guidance. A thorough analysis of those texts may be useful for preparing future UNCITRAL work in this field.

49. In that respect, further clarification of the relationship between IdM systems and trust services, on the one hand, and electronic signatures, on the other hand, seems particularly useful. One element to consider in that analysis is that electronic signatures require an associated identity element that allows parties to rely on the signature by identifying reliably the signatory. Another element to be taken into account relates to the use of certain types of electronic signatures in delivering trust services.

50. Preparing definitions of the most relevant terms used in connection with IdM and trust services could be beneficial to clarify the various notions and ensure their uniform understanding. In doing so, existing technical standards, and definitions therein, need to be taken into consideration.[20]

51. In light of the above considerations it seems preferable that the scope of this legislative project shall cover all types of IdM systems and trust services, regardless of the nature of the provider and of the main intended purpose, function or use. It seems also desirable that it shall consider all possible entities that could be

---

[19] E.g., article 5, paragraph 2 of the UNCITRAL Model Law on International Credit Transfers, 1992.

[20] See documents ISO/IEC 24760-1:2011(en) and ISO/IEC 24760-2:2015(en) for examples of IdM-related definitions.

identified by an IdM system and all possible roles. Finally, the project should deal with both use of IdM systems and transactions between IdM systems.

52. With respect to specific topics, the following seem to be core issues to be discussed with respect to IdM: rights and obligations of the parties; reliability in the various steps of the IdM cycle; consequences of reliability on liability; system rules and other contractual agreements (such as service level agreements); mutual legal recognition and other matters related to legal interoperability.

53. An important aspect of IdM relates to privacy and data protection. Policy approaches to that complex topic may vary significantly and several initiatives aim at reconciling them. In practice, existing legislation on IdM recognizes the existence of specific privacy law and defers to its application. Against that background, and in view of the fact that work on IdM systems and trust services should not extend to matters outside UNCITRAL's mandate,[21] it is doubtful that UNCITRAL could efficiently deal in detail with those matters at the present stage.

54. Another aspect to be further analysed relates to the use of IdM systems and trust services in cloud computing. Cloud services may be used to provide identity management (identity as a service). Moreover, IdM (e.g., in the form of multifactor authentication) is commonly used to access cloud services, in particular to ensure compliance with privacy and other regulatory requirements. However, further investigation is needed in order to clarify whether those uses pose specific legal issues.

55. With respect to working methods, it seems particularly desirable to foster broad participation by all regions in future UNCITRAL work to better assess the current status of IdM systems and trust services as well as identify regional specific trends.[22] One possible tool to do so is the distribution of surveys. This could be done also through cooperation and coordination with relevant regional organizations, such as the Arab ICT Organization (AICTO).[23]

---

[21] *Official Records of the General Assembly, Seventieth Session, Supplement No. 17* (A/70/17), para. 355.

[22] For additional information on ASEAN member States, see Electronic Transactions Development Agency, Intra-ASEAN Secure Transactions Framework Final Report, Bangkok, July 2014.

[23] Specifically, the mandate of AICTO Working Group III (E-certification and Cybersecurity) may encompass IdM.