United Nations A/CN.9/WG.IV/WP.154

General Assembly

Distr.: Limited
12 September 2018

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Fifty-seventh session
Vienna, 19–23 November 2018

Legal Issues Related to Identity Management and Trust Services

Note by the Secretariat

Contents

V.18-05926 (E)

I. Introduction

1. This note illustrates certain aspects of some of the topics identified by the Working Group as relevant to its consideration of legal issues related to identity management ("IdM") and trust services (A/CN.9/936, para. 58) in order to facilitate further discussion. In particular, it aims at highlighting key issues and suggesting possible solutions and does not intend to limit the possibility of considering additional topics or of considering some topics together, as appropriate. Working paper A/CN.9/WG.IV/WP.153 illustrates certain aspects of other topics identified by the Working Group as relevant to its consideration of legal issues related to IdM and trust services.

2. Background information on the work of the Working Group on legal issues related to IdM and trust services may be found in working paper A/CN.9/WG.IV/WP.152, paras. 6–17. A list of additional relevant documentation may be found in working paper A/CN.9/WG.IV/WP.152, para. 18.

II. Relevant Issues for Future Work on Legal Aspects of Identity Management and Trust Services

A. Certification of IdM and trust services providers

3. Certification, including self-certification, accreditation and independent audits may significantly assist in establishing trust in IdM providers and trust services providers. The choice of the most appropriate form of certification may be influenced by the type of service involved, the cost and the level of assurance sought.

4. The eIDAS Regulation foresees a comprehensive system for supervision and certification of trust services. According to its article 17, each member State shall designate a body responsible for carrying out regular supervisory tasks on qualified trust service providers and occasional tasks on other trust service providers. Article 17(4) provides a list of the specific tasks to be carried out by the supervisory body.

5. It has to be noted that under the eIDAS Regulation the existence of a supervisory body is necessary for a trust service provider to be considered as qualified. In particular, according to article 20, qualified trust service providers must be audited at least every 24 months by a conformity assessment body, and the resulting conformity assessment report is to be submitted to the supervisory body. Failure to comply with requests from the supervisory body may result in withdrawal of the qualified status of the trust service provider or of any of its services.

6. In turn, under the eIDAS Regulation only qualified trust service providers may offer qualified trust services that are associated with certain legal effects, such as presumptions. For instance, according to article 25(2) eIDAS, a qualified electronic signature shall have the equivalent legal effect of a handwritten signature. In short, the existence of the supervisory body enables the offer of qualified trust services associated with legal effects.

7. With respect to trust services, article 10(e) and (f) MLES refer to the existence of accreditation, audits and self-certification as one element possibly relevant to assessing the trustworthiness of the systems used by the certification service provider. Hence, under this approach, the existence of a supervisory body and of accreditation schemes is optional and the appreciation of their existence discretionary.

8. In mutual legal recognition models that make use of trusted lists (see A/CN.9/WG.IV/WP.153, paras. 61–73 and 76–79), certification (including self-certification) is a necessary element to assess IdM schemes using outcome-based standards. It may be necessary to predefine a set of profiles to be used for the assessment.

9. The Working Group may wish to consider whether the existence of certification, including self-certification, accreditation and independent audits, should be associated with certain legal effects, and, if so, which effects, or rather be listed as elements possibly relevant to assessing the reliability, trustworthiness or other quality of IdM and trust services providers. In deliberating, the Working Group may also wish to indicate whether the use of certification, including self-certification, accreditation and independent audits, should be mandatory or optional.

B. Levels of assurance

1. IdM

10. The level of assurance is a measure of the reliability of an identity assertion that is based on the processes used. Different definitions of levels of assurance are available from public and private entities. Their formulation is regularly updated in light of developments in technology and business processes. In light of the adoption of the principle of technology neutrality, only levels of assurance formulated in a technology-neutral manner are taken into consideration.

11. The National Institute of Standards and Technology ("NIST") of the United States of America has identified three different levels of identity-related assurance: identity assurance level ("IAL"), authenticator assurance level ("AAL") and federation assurance level ("FAL").[1] IAL refers to the identity proofing process, AAL refers to the authentication process and FAL refers to the assertion protocol used in a federated environment to communicate authentication and attribute information (if applicable) to a relying party.

12. More precisely, IAL refers to the robustness of the identity proofing process to confidently determine the identity of an individual; AAL refers to the robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier; and FAL refers to the robustness of the assertion protocol the federation uses to communicate authentication and attribute information to a relying party if a federated identity architecture is used.[2]

13. Each level of identity assurance has its own degree of robustness associated with certain requirements. For instance, at IAL1, attributes, if any, are self-asserted or should be treated as self-asserted. At IAL2, either remote or in-person identity proofing is required. IAL2 requires identifying attributes to have been verified in person or remotely using, at a minimum, specified procedures. At IAL3, in-person identity proofing is required and identifying attributes must be verified by an authorized certification service provider representative through examination of physical documentation according to specified procedures.

14. Article 8 of the eIDAS Regulation establishes three assurance levels for IdM: low, substantial and high, as well as the respective criteria. In particular, assurance level "low" provides a limited degree of confidence in the claimed or asserted identity of a person; assurance level "substantial" provides a substantial degree of confidence in the claimed or asserted identity of a person; and assurance level "high" provides a higher degree of confidence in the claimed or asserted identity of a person than assurance level "substantial".

15. An implementing act of the eIDAS Regulation[3] establishes minimum technical specifications and procedures to be used to determine the reliability and quality of enrolment, electronic identification means management, authentication and

[1] NIST Special Publication 800-63-3, *Digital Identity Guidelines*, June 2017, section 2. Available at https://doi.org/10.6028/NIST.SP.800-63-3.

[2] NIST, *Digital Identity Guidelines*, cit., section 5.2.

[3] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means.

management and organization of cross-border IdM providers. Those technical specifications and procedures are described in a technology-neutral manner.

16. In light of the above, the Working Group may wish to consider whether the notion of levels of assurance should be used for purposes of satisfying legal requirements or determining legal effects. If so, it may also wish to discuss, in particular, the relationship between levels of assurance, on the one hand, and legal recognition requirements and mechanisms, on the other. The Working Group may also wish to discuss whether and to what extent it should engage in a discussion of the features of levels of assurance.

2. Trust services

17. A fundamental issue regarding trust services is whether the notion of levels of assurance should be applied also to them. A number of national laws on electronic signatures recognize two levels of electronic signatures. The first one encompasses all forms of electronic signatures. The second one associates certain legal consequences, such as a presumption of origin and integrity, to electronic signatures that satisfy certain requirements. This may be interpreted as introducing different levels of assurance with respect to electronic signatures.

18. With respect to trust services, article 24(1) of the eIDAS Regulation offers an illustration of use of levels of assurance in the context of satisfying an identification requirement for issuing a qualified certificate. Specifically, to satisfy the requirement that a qualified trust service provider verify the identity of the person to whom it issues a qualified certificate, the eIDAS Regulation allows such verification to be done remotely using an electronic identification means with level of assurance “substantial” or “high”.

19. The Working Group may wish to consider whether the notion of levels of assurance should be applied to trust services and, if so, in what manner.

C. Liability

20. The applicable liability regime may have a significant impact on promoting the use of IdM and trust services both for commercial and non-commercial uses. In that respect, it should be noted that, while legal remedies for wrongful identification in commercial transactions are generally available, wrongful attribution of foundational identity in paper-based documents may not give rise to liability if national law does not allocate liability to public entities for that service.

21. The Working Group has already identified certain issues relevant for its discussions on liability of IdM and trust services participants, namely: the entities that should be liable (issuers, providers, other parties), taking into account special liability regimes for public entities; the possibility to limit liability of parties complying with predetermined requirements; statutory mechanisms to limit liability, e.g. by exemption or reversal of burden of proof; and contractual limitations of liability (A/CN.9/936, para. 85).

22. In certain cases, it may not be easy to identify a liable entity, e.g., with respect to trusted attribute data provided by a trust service, when using distributed ledger technology for timestamping (A/CN.9/936, para. 86). In other cases, an insurance-based mechanism may be used for commercial transactions, under which the wrongful use of the electronic identification scheme or of the trust service may lead to compensation by the insurer. Yet another mechanism available foresees the automated release of pre-liquidated compensation or fixed penalties if certain conditions are met.

1. IdM

23. Article 9 of the eIDAS Regulation mandates submission, at the time of notification of an IdM scheme, of information on the liability regime applicable to

the issuer of the electronic identification means and to the party operating the authentication procedure.

24. Article 11 of the eIDAS Regulation allocates to the notifying member State liability for damages caused due to a failure to comply with its obligations to ensure that the person identification data uniquely representing the person in question are attributed to the appropriate person, and to ensure the online availability of authentication information used to confirm the person identification data. It also allocates to the party issuing the electronic identification means liability for damages arising from a failure to attribute electronic identification means to the person uniquely represented by the person identification data. Finally, it allocates to the party operating the authentication procedure liability for a failure to ensure the correct operation of the online authentication used to confirm the person identification data.

25. Article 11 of the eIDAS Regulation applies only to cross-border transactions and requires that the failure to comply is intentional or negligent. It is applied in accordance with national law with respect to issues such as definition of damages and allocation of burden of proof and without prejudice to additional liability arising from national law of the parties involved in the transactions where IdM schemes are used.

26. To sum up, the eIDAS Regulation allocates liability to the participants in the IdM scheme for their failure to comply with certain named obligations, if that failure is intentional or negligent, provided the transaction is cross-border and without prejudice to additional liability arising under national law.

27. Article 281 of the Law 2017-20 of Benin indicates that the IdM system operator is liable for the damages to users of IdM schemes if the damages were caused with intention or negligence.

28. Under section 1-552 of the Virginia Electronic IdM Act, an identity trust framework operator or an identity provider is not liable if the identity credential is issued or the identity attribute or trustmark is assigned in compliance with the IdM standards approved by the Secretary of Technology of the Commonwealth of Virginia, any contractual agreement, and any written rules and policies of the identity trust framework of which the identity provider is a member. According to section 1-550, a trustmark is "a machine-readable official seal, authentication feature, certification, licence, or logo that may be provided by an identity trust framework operator to certified identity providers within its identity trust framework to signify that the identity provider complies with the written rules and policies of the identity trust framework".

29. In short, the Virginia Electronic IdM Act exempts from liability identity trust framework operators and identity providers compliant with standards set by a public body, contractual representations and federation rules. Compliance with the minimum specifications and standards set forth by the Commonwealth of Virginia is established with the use of independent third-party certification authorities who provide objective, consistent, auditable compliance reviews based on clearly defined certification criteria.[4] The exemption does not operate if the identity trust framework operator or the identity provider has committed an act or omission with gross negligence or is guilty of wilful misconduct.

30. Section 1-555 of the Virginia Electronic IdM Act specifies that no provision of the Act or related act or omission by a public entity related to IdM shall be construed as a waiver of sovereign immunity of that public entity.

31. The Working Group may wish to discuss which entities should be held liable, under which liability regime, and whether a special liability regime should be introduced for public entities.

[4] Commonwealth of Virginia Identity Management Standards Advisory Council, *Guidance Document 5: Certification of Identity Trust Framework Operators* (draft), Section 7: Certification of Identity Trust Framework Operators.

32. In discussing the liability regime, the Working Group may wish to consider: (a) the possibility to limit liability of parties complying with predetermined requirements, e.g. by exemption or reversal of burden of proof; (b) whether different levels of assurance should be associated with different liability regimes; (c) the possibility to limit liability contractually; and (d) whether the provision of metadata describing the liability regime, including any limitation, should be required.

2. Trust services

33. According to article 13 of the eIDAS Regulation, trust service providers will be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under the Regulation. In other words, trust service providers that comply with the obligations under the Regulation are not held liable.

34. Moreover, article 13 introduces a rebuttable presumption of intention or negligence of a qualified trust service provider, while the burden of proving intention or negligence of a non-qualified trust service provider lies with the person claiming the damage. This provision aims at building users' trust in qualified providers given that, in case of damage, seeking redress is facilitated by the presumption. Finally, article 13 recognizes the possibility for trust service providers to limit their liability, provided that customers are informed in advance of those limitations and that those limitations are recognizable by third parties.

35. The MLES contains provisions dealing with liability arising from the conduct of the signatory (art. 8), of the certification service provider (art. 9) and of the relying party (art. 11). Those provisions stipulate the obligations for each entity involved in the electronic signature life cycle. The MLES acknowledges the possibility for certification service providers to limit the scope or extent of their liability.

D. Institutional cooperation mechanisms

36. Institutional cooperation mechanisms may assist in achieving mutual legal recognition and interoperability of IdM systems and trust services. They may be of a private or public nature.

37. Article 12 of the eIDAS Regulation provides an example of an institutional cooperation mechanism by indicating that member States should cooperate with regard to interoperability and security of IdM schemes. Cooperation may consist of exchanges of information, experience and good practice, in particular with respect to technical requirements and levels of assurance, peer review of IdM schemes and examination of relevant developments.

38. An eIDAS implementing act[5] provides additional details on exchange of information and peer review, including by indicating that the member State may not provide the required information if disclosure could violate matters of public security or national security, or business, professional or company secrets. It also establishes a Cooperation Network to facilitate the conduct of cooperation activities. It should be noted that, while peer review of an IdM scheme to be notified is voluntary, in practice its outcome may provide important insight into the possibility that the scheme meets the required standards, and therefore is an important step in the notification mechanism that lies at the core of the eIDAS Regulation institutional structure.

39. A different type of cooperation between IdM systems may be achieved with IdM systems federation. According to that model, identity information verified within one IdM system is made available in an agreed-upon and managed fashion to multiple parties within a different IdM system that need such identity information for different purposes (see also A/CN.9/WG.IV/WP.153, para. 47). IdM systems federation

[5] Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification.

achieves interoperability among their participants by using a common technical and legal framework defined by a set of system rules. Federation may therefore contribute to increasing the number of participating users and applications and containing IdM-related costs. Although federations are based on contractual agreements, statutory provisions may contribute to promote federation (see, e.g., the use of trustmarks in the Virginia IdM Act at para. 28 above).

E. Transparency

40. The Working Group identified the principle of transparency as relevant for future discussions on IdM and trust services (A/CN.9/936, para. 8). In so doing, it highlighted two duties related to that principle: the duty to disclose which IdM and trust services are offered and their quality; and the duty to notify security breaches.

41. With respect to the services offered and their quality, it should be noted that a significant amount of information would be disclosed by those identity and trust service providers participating in federations or otherwise obtaining a certification of their services. Minimum duties of disclosure may be established for other providers. For instance, article 9(1) MLES contains a list of information that the certification service provider should disclose to the relying party.

42. With respect to the duty to notify security breaches, it was noted that security breach notifications had elements in common with data breach notifications, but also significant differences. It was added that useful examples of mechanisms going beyond mere notification in case of security breach existed (A/CN.9/936, para. 89). Additional considerations may pertain to the possible use of cyberthreat intelligence for risk mitigation.

43. Article 10 of the eIDAS Regulation contains a duty for member States to notify breaches or compromises that affect the reliability of the cross-border authentication scheme. The concerned member State should also suspend or revoke without delay the compromised authentication or its compromised parts.

44. Article 19(2) of the eIDAS Regulation contains a similar obligation for trust service providers to notify the supervisory body and any other relevant bodies such as the data protection authority of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. The notification should be made without undue delay and in any event within 24 hours after becoming aware of the breach or loss.

45. Article 8(1)(b) of the MLES provides an optional notification mechanism that the signatory may use in case the signature creation data have been compromised, or there is a substantial risk that they may have been compromised.

46. A possible provision on the duty to disclose security breaches could read as follows:

> Identity providers and trust service providers shall, without delay [and, in any event, within … days after having become aware of it], notify [the oversight authority] [its affected clients and relying parties] of any breach of security or loss of integrity that has a [significant] impact on the services, identity credentials or authentication processes provided or on the personal data maintained therein.
>
> In case of significant breach of security or loss of integrity, identity providers and trust service providers shall suspend the provision of the affected services [until…].
>
> Users of identity and trust services shall notify the service provider in case the identity credentials, authentication processes or trust service creation data have been compromised, or in case the circumstances known to the user give rise to a substantial risk that the identity credentials, authentication processes or trust service creation data may have been compromised.

47. The draft provision has optional language to provide for a time limit in which the notification must be made, to identify the parties to be notified and to establish the level of impact on services, identity credentials or personal data that triggers the duty to notify. It is also possible to establish a duty to suspend the IdM system and the trust services until the breach or loss are contained, or, alternatively, a new certification or similar process is achieved.

F. Data retention

48. The Working Group has already emphasized the importance of harmonization and interoperability of data retention regimes for cross-border trade (A/CN.9/936, para. 91). In doing so, it has highlighted at least two possible profiles of interest. The first relates to data protection. The second refers to data storage and archiving.

49. Data protection is a topic that may raise particularly complex issues. The Working Group may wish to confirm that, in line with the general principle that UNCITRAL enabling texts on electronic commerce do not affect substantive provisions (see A/CN.9/WG.IV/WP.153, para. 48), law on data protection and related issues, such as privacy, should remain applicable in its entirety, and consider whether any additional specification or clarification would be useful.

50. Document storage and archiving is a function that may be fulfilled with the use of electronic means, as already indicated by article 10 MLEC, which establishes the requirements for functional equivalence between data messages and paper-based documents with respect to retention. Obligations to preserve documents arise from substantive law and are related to the time needed for the prescription of the various actions.

51. The provision of services for data storage and archiving may be the object of a dedicated trust service (see below, paras. 64–65). In the framework of interoperability of trust services, the Working Group may wish to discuss matters related to portability of electronic archives.

G. Supervision of service providers

52. In the event that the Working Group determines that it is appropriate to address IdM schemes and trust services systems rather than related transactions (see A/CN.9/WG.IV/WP.153, paras. 57–59), the establishment of a supervisory body may be useful or even necessary to create trust in the service providers and in the services provided. However, establishing such a body entails several administrative and financial consequences. Alternative or complementary mechanisms, such as third-party certification, may assist in achieving the goals pursued by supervision of service providers while reducing associated costs.

53. The legislation of Vermont and Virginia assigns supervisory authority over identity service providers to public bodies. Similarly, article 97 of the Law 2017-07 of Togo assigns supervisory functions on trust service providers to the national certification authority. According to article 283 of Law 2017-20 of Benin, identity service providers are appointed by a public authority. A supervisory mechanism on the management and provision of identity services is implicit also in the notification scheme established by the eIDAS Regulation.

54. With respect to trust services providers, a number of laws assign to a supervisory body the authority to grant a qualified status or to supervise how that status is granted by third parties. The eIDAS Regulation requires the designation by member States of a national supervisory body competent on trust service providers.

55. The MLES contains optional reference to the existence of supervisory bodies in light of its adoption of the principle of model neutrality, since the insertion of mandatory provisions on the existence of supervisory bodies may be understood as preventing the adoption of a market model based on self-regulation of trust services.

H. Issues specific to trust services

56. Work on legal issues relating to trust services is closely related to that on IdM. Accordingly, comments related to trust services in the context of the principle of functional equivalence (A/CN.9/WG.IV/WP.153, paras. 36–37), of legal recognition (A/CN.9/WG.IV/WP.153, paras. 93–98), of levels of assurance (paras. 17–19 above) and of liability (paras. 33–35 above) have been made in conjunction with the consideration of the same issues with respect to IdM.

57. However, the legal treatment of trust services may also pose peculiar challenges. One fundamental issue is the fact that each trust service is different, and thus, raises a different set of issues for consideration. Additionally, there is the question of whether the legal treatment of trust services should consider an open-ended list of trust services based on a common definition of "trust service" or rather provide common rules applicable to all trust services and specific rules applicable to each of them.

58. Moreover, it may be possible to refer to functional equivalence provisions to describe the functions to be pursued with the use of each trust service in a manner akin to UNCITRAL provisions on electronic signatures and retention of documents (see A/CN.9/WG.IV/WP.153, para. 36). The existence of a significant body of legislation dealing with electronic signatures[6] and the experience gathered in the application of that legislation may assist in considering this suggestion.

59. The eIDAS Regulation offers an example of comprehensive legislation on trust services. It contains general provisions on liability and burden of proof (art. 13; see above, paras. 23–26), supervision (art. 17; see above, para. 53) and security requirements (art. 19; see above, para. 44, on the duty of notification of breaches of security or loss of data), among others.

60. The eIDAS Regulation contains a specific section applicable to all qualified trust services. Qualified trust services are recognizable because of their insertion in a trusted list maintained by European Union member States. In that respect, the Working Group may wish to consider whether a distinction between trust services should be made on the basis of the level of assurance associated with a trust service and, in that case, which institutional mechanism should be used to distinguish trust services.

61. The eIDAS Regulation also contains specific provisions relating to the following trust services: electronic signatures; electronic seals; electronic time stamps; electronic registered delivery services and website authentication.[7] Each trust service may be delivered in qualified form. Electronic signatures and electronic seals may also be delivered in advanced form.

62. Law 045-2009/AN of Burkina Faso contains a section on provisions applicable to all trust service providers, as well as provisions on how to achieve accreditation, which is relevant to attain qualified trust service provider status. That Law also contains specific provisions for qualified electronic certificates, electronic archiving, electronic timestamps and electronic registered delivery services. It also features a dedicated chapter on electronic signatures.

63. Law 2017-20 of Benin contains a general part applicable to all trust service providers and specific provisions on the following trust services: electronic signatures; electronic seals; electronic timestamps and electronic archiving.

64. Article 301 of that law indicates that "electronic archiving guarantees the authenticity and the integrity of the documents, data and information stored in that

[6] The UNCTAD Global Cyberlaw Tracker indicates that 145 States, or 78 per cent of the total, have adopted laws on electronic transactions, which typically include provisions on electronic signatures.

[7] A definition of those trust services is available in document A/CN.9/WG.IV/WP.150.

manner". It also contains a functional equivalence provision similar to article 10 MLEC.

65. Article 302 of the Law 2017-20 of Benin further indicates that the purpose of electronic archiving is to preserve documents, data and information for further use, and that relevant data should be structured, indexed and stored in a manner to allow for preservation and migration (see also above, para. 51). Access should be possible regardless of technological evolution. The provision applies both to documents originating in electronic form and to documents originating on paper and subsequently digitized.

66. Law 2017-07 of Togo also contains a section on provisions applicable to all trust service providers, including procedures to attain the status of qualified trust service provider. That Law also contains specific provisions for electronic certificates, electronic archiving, electronic timestamps and electronic registered delivery services. It also features a dedicated chapter on electronic signatures.

67. Law 2017-07 of Togo is complemented by Decree no. 2018-062/PR that further establishes obligations common to all trust service providers. Those obligations relate to security and confidentiality of data, liability, financial resources, accessibility, data protection, transparency and risk management. Moreover, the Decree contains provisions related to each of the trust services identified by the Law 2017-07.

68. Additional trust services that have been identified but have yet to receive specific legislative treatment include electronic escrow accounts and electronic proof of presence. The latter trust service has been discussed with respect to electronic wills.[8]

69. The Working Group may wish to consider whether the same, or different mechanisms should be used for the legal treatment of IdM and trust services. Moreover, it may wish to consider whether the legal treatment of trust services should consider an open-ended list of trust services based on a common definition of "trust service" or rather provide common rules applicable to all trust services and specific rules applicable to each of them. In particular, the Working Group may wish to consider whether functional equivalence rules should be formulated for each trust service and whether reference to levels of assurance should also be made in the context of trust services.

[8] See, e.g., section 8 of the draft Electronic Wills Act being prepared by the National Conference of Commissioners on Uniform State Laws.