United Nations A/CN.9/WG.IV/WP.144

General Assembly

Distr.: Limited
30 January 2017
English
Original: English/French

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

Work in the field of electronic commerce — legal issues relating to electronic identity management and trust services

Proposal by Austria, Belgium, France, Italy, the United Kingdom and the European Union

Note by the Secretariat

The governments of Belgium, France, Italy and the United Kingdom, from the Austrian delegation and the European Union submitted to the Secretariat a paper for consideration at the fifty-fifth session of the Working Group. The text received by the Secretariat is reproduced as an annex to this note.

V.17-00408 (E)

Annex

Proposal by Austria, Belgium, France, Italy, the United Kingdom and the European Union

Date: 26 January 2017

Proposal from the Governments of Belgium, France, Italy and the United Kingdom of Great-Britain and Northern-Ireland, from the Austrian delegation and the European Union : work in the field of electronic commerce — legal issues relating to electronic identity management and trust services.

I. Introduction

1. Pursuant to the mandate of the 44th Session of the Commission in 2011, the Working Group IV on electronic commerce (hereinafter Working Group IV) undertook work in the field of electronic transferable records.[1] During the 49th session of the Commission, Working Group IV reported on its work undertaken during its 52nd and 53rd sessions. Work on the provisions of the draft Model Law on Electronic Transferable records is being finalised.

2. At its 44th session in 2011, the Commission also noted that some support was also expressed for dealing with legal issues relating to identity management (IdM) as a possible topic in the mandate of Working Group IV.[2] At its 48th session in 2015, the Commission instructed the Secretariat to conduct preparatory work on IdM and trust services, cloud computing and mobile commerce, including through the organization of colloquia and expert group meetings, for future discussion at the Working Group level following the current work on electronic transferable records. The Commission also asked the Secretariat to share the result of that 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.[3]

3. Further to this request, at its forty-ninth session, the Secretariat submitted to the Commission a note on the legal issues related to IdM and trust services, which provided a summary of the discussions held at the colloquium and at other relevant meetings on this subject.[4]

4. The Commission, at its forty-ninth session in 2016, reaffirmed the mandate given to Working Group IV to complete the preparation of the draft Model Law on Electronic Transferable Records and the accompanying explanatory note, and to consider the topics of IdM and trust services as well as of cloud computing upon completion of work on the draft Model Law.[5]

---

[1] Report of the United Nations Commission on International Trade Law, forty-fourth session (27 June-8 July 2011) - A/66/17, para. 238.
[2] Ibid., para. 236.
[3] Report of the United Nations Commission on International Trade Law on the work of its forty-eighth session (2015), UN document A /70/17, para. 358.
[4] Document A/CN.9/891.
[5] Report of the United Nations Commission on International Trade Law on the work of its forty-ninth session (2016), UN document A/71/17, para. 353.

5. In accordance with the reaffirmation of this mandate, during the 54th session of Working Group IV the draft model law on electronic transferable records was finalised and work on IdM and trust services started. Following fruitful discussions on the latter subject,[6] Working Group IV decided that the following session would be devoted in particular to clarifying the objectives of the project on IdM and trust services, to stressing its scope, identifying the applicable general principles, listing the concepts to be defined and making a first draft definition of these.[7]

6. In this context, this proposal aims to provide the Working Group IV with a contribution on the above mentioned elements with a view to supporting the discussions during the 55th session of this Group, while remaining open to additional proposals aimed at fuelling the discussions.

II. Context, scope and objectives of the project

7. The proposed work in the field of IdM and trust services is directly linked to the work carried out by Working Group IV (1) in the past (in particular with reference to the model law on electronic commerce, the model law on Electronic Signatures and the Convention on the Use of Electronic Communications in International Contracts), (2) currently (work on electronic transferable records), and (3) in the future, on other topics that have been discussed, such as cloud computing or mobile payments.

8. De facto, IdM is a fundamental requirement underpinning most of the work that has been (or is being) undertaken by Working Group IV. In addition, many requirements provided for in UNCITRAL texts which are applicable to e-commerce can be facilitated by the use of one or more trust services provided by trust service providers. A "trust service" may include electronic signatures, electronic seals to ensure the origin and integrity of a document, electronic time stamps to provide a document with a specific date, secure communication of a document between parties (electronic registered delivery service), or website authentication.

9. Reliable IdM and the use of reliable trustworthy services have become essential requirements for e-commerce activities because of the increasing importance and sensitivity of online transactions.

10. In many Internet transactions, verifying the identity of a website's owner is needed to ensure that the website belongs and is effectively managed by the legal person who claims to be behind it. Similarly, it is often important that parties identify themselves when starting interacting online. In addition, the electronic signature of a final agreement may also require identifying the different signatories, to ensure that they have expressed their consent to a content that will maintain its integrity, and stamping the document to provide it with a specific date and time. Finally, in some cases it is important that documents are transmitted to the other party through a secure channel that ensures the date of sending and receiving the document.

11. Identity authentication and trust services contribute significantly to a paperless commerce environment, since the daily operations of public administrations and businesses can be performed faster, more efficiently and at a lower cost. In this context, many entities, both public and private, develop (or would like to develop) economic models that provide, or make use of, IdM and trust services.

12. Today national and regional reflections and initiatives in the field of IdM and/or trust services are numerous and have now reached maturity. While sometimes

[6] Report of the 54th session of the Working Group IV on electronic commerce (16 November 2016), A/CN.9/897, para. 107 to 123.

[7] Ibid., para. 120.

adopting contradictory approaches, they allow identifying relevant issues and can guide the discussion on devising the appropriate legal frameworks at international level that could be transposed into the existing different legal systems.

13. Work in the field of IdM and trust services aims at:

- Facilitating the development of international trade law and addressing the need to provide economic players with the tools to ensure the legal certainty of their electronic transactions.
- Contributing to harmonising emerging legal aspects of the projects which are currently addressing in silos these questions at national or international level. The objective would be to provide for a general legal framework applicable to both IdM and trust services, including the appropriate provisions to foster international cross-border legal and technical interoperability.
- Raising public administrations' and businesses' awareness — who are not always aware of the legal issues at stake -, with a view to boosting trust in electronic commerce and transactions.
- Completing and providing practical solutions to existing documents produced by UNCITRAL. More specifically, work in this field would aim at drafting legal provisions with a view to making the "abstract" requirements drafted in the above mentioned UNCITRAL texts more "concrete and operational". Businesses would therefore take advantage of clear legal rules to better manage their risk in the context of the international electronic commerce and to ensure the legal certainty of their transactions in a simple and efficient manner.

14. Given the close relationship between the two topics, the work should be focusing from the outset on both IdM and trust services. The definition of the scope of the work and of the concepts should therefore include these two closely related topics. Such an approach does not prevent from working on these topics in a sequential manner at a later stage.

III. Identification of applicable general principles and possible orientations

15. The fundamental principles underpinning UNCITRAL texts should guide the work on IdM and trust services. These include:

- *The principle of party autonomy*. The use of the provided tools should remain optional and fully respect party autonomy. Parties should also remain free to decide the level of assurance/security to be used. Providers should remain free to offer one or more IdM and trust services, and among them to provide one or more levels of assurance/security. To sum up, the set legal rules should be considered as a "legal toolbox" to be put at the disposal of the market players.
- *The principle of neutrality both technological and of economic models*. Providing a legal framework should in no way hamper innovation and business opportunities by introducing strict rules that would favour a technical solution or an economic model over another.
- *The principle of non-discrimination*. The legal effect and admissibility as evidence in legal proceedings of an electronic identification (eID) or a trust service should not be denied solely on the grounds that such service is in an electronic form or that it does not meet the requirements of the assurance/security levels.

- *The principle of functional equivalence* aiming at ensuring comparable legal functions, whether we act in the physical or in the electronic environment.

16. The issues that should be addressed when drafting the legal provisions, both for IdM and for trust services, are the following:

(a) The definition of different levels of assurance/security on the basis of objective criteria: assurance/security of IdM and trust services is often a critical element. Defining and measuring assurance/security can be fundamental in some cases. What is the assurance/security of an identity service or management system or of a trust service? The absence of objective evidence to judge the actual quality and assurance of a service may be a significant problem for stakeholders, in particular as part of their risk management policy. A flexible model providing for different levels of requirements for IdM and/or trust services and identity and/or trust service providers would respect the diversity of the systems around the world.

(b) Distinct legal effects associated to the level of assurance: The legal effects of electronic identification and authentication as well as those of a number of trust services should be defined. The objective is to determine the legal effects stemming from electronic identification and trust services according to each defined level of assurance. Stakeholders could thus effectively manage their legal risks by opting for the most appropriate level of assurance and legal effect in line with their needs. In order to define these different legal effects, one could, in particular, take account — when appropriate — of the principle of non-discrimination, the principle of assimilation, the principle of mutual recognition, particular presumptions and/or mechanisms for reversing the burden of proof. The higher the level of assurance, the more favourable the legal effect would be to the user of the service.

(c) Liability regimes according to the level of assurance: Defining the liability regime of the providers of electronic identification systems and of trust services in order to foster the required clarity and predictability. This regime would vary depending on the provided level of assurance.

17. For the services of IdM in particular, the following guidelines should be followed:

- By applying the principle of the party autonomy, providers of an online service can decide whether to require an electronic identification and authentication to access their service and which level of assurance is required.
- Cross-border mutual recognition of electronic identification means which have an assurance level equal to or higher than the assurance level required for the online access. This principle would be based on the definition of the different assurance levels of electronic identification means. Each level would be characterised by harmonised objective criteria.
- In order to determine which systems for IdM should be taken into account in our work, the purpose/aim of the use of the electronic identification means should first be identified, i.e. whether this is intended to be used -fully or partially — for commercial transactions or not, and later to understand who has issued the electronic identification means (whether it is the public or private sector or both). Since the purpose of using eID means may be commercial, all eID means — even those fully or partially issued by the public sector — should be considered in our work.
- Our work should first focus on identification of natural and legal persons, initially leaving out the question of identifying material (e.g. servers, smartphones, terminals ...) or digital objects (software ...). Since we need to establish rules of law, priority should be given to identifying the subject of law

(whether natural or legal person) who has **rights and obligations and takes liability** (e.g. a website, a **copyright or a server owner**). Material or digital objects will always be linked to a natural or legal person. The identification of objects is essentially a technical and security issue rather than a legal one.

- eID means of a higher level should at least be attached to person identification data issued/managed by an **authoritative source**.

- For the higher assurance levels, an obligation should be established for the providers of eID means to notify any security breach to their system and, where necessary, to suspend it. The provider should notify in accordance with the provisions laid down in national law and, given the cross-border context, make the information publicly available.

- A presumption could be established by which objective criteria defining the assurance levels as well as the legal requirements should be respected if the provider is in line with the technical standards defined by an international authority.

18. For IdM, three assurance levels could be set: (a) low ; (B) substantial; And (C) high.

- Assurance levels would be based on technical specifications, standards and procedures related thereto.

- A cooperation mechanism and an interoperability framework could be foreseen to define the criteria underpinning the assurance levels as well as to exchange the information related to eID means and their assurance levels.

- A principle of cross-border mutual recognition would be envisaged for those eID means having an equivalent (or higher) assurance level (from the substantial level).

19. For trust services, the following guidelines should be followed:

- with a view to defining and harmonising security levels of trust services, there should be at least two levels:

  1. non-qualified trust services;

  2. Qualified trust services.

- The legal effects differ according to the security level of the trust service:

  1. If the trust service is NOT qualified: the legal effect is limited to the non-discrimination clause.

  2. If the trust service is QUALIFIED: the legal effect would include assimilation, presumption, reversal of the burden of proof.

- A principle of cross-border mutual recognition for trust services having an equivalent security level would be established.

- A general requirement on security, which is commensurate to the degree of risk, would be set for all providers (qualified or not).

- Specific requirements for qualified trust service providers and for the qualified trust services they provide would be provided for to ensure a high level of reliability/security.

- Liability regime would depend on whether the trust service provider is qualified or not.

- A requirement could be established for all trust service providers (at least qualified) to notify any breach of security to their system and, where necessary, to suspend it. The provider should notify in accordance with the provisions laid down in national law and, given the cross-border context, make the information publicly available.
- A presumption could be established by which objective criteria defining the security levels as well as the legal requirements should be respected if the provider is in line with the technical standards defined by an international authority.

IV. Identification of concepts and proposed draft definitions

20. In view of the forthcoming discussions on IdM and trust services, the following (non-exhaustive) list of concepts and definitions is proposed:

- ***Electronic identification:*** means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;
- ***Electronic identification means:*** means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;
- ***Person identification data*** means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;
- ***Electronic identification scheme*** means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;
- ***Authentication*** means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;
- ***Authoritative source*** means any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity;
- ***Trust service*** means an electronic service (normally provided for remuneration) which consists of:
  1. the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
  2. the creation, verification and validation of certificates for website authentication; or
  3. the preservation of electronic signatures, seals or certificates related to those services;
- ***Qualified trust service*** means a trust service that meets the applicable requirements laid down in this text [Convention, Model Law];
- ***Electronic signature*** means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
- ***Signatory*** means a natural person who creates an electronic signature;

- ***Electronic seal*** means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;
- ***Electronic time stamp*** means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;
- ***Electronic registered delivery service*** means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;
- ***Certificate for website authentication*** means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;
- ***Electronic document*** means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;
- ***Validation*** means the process of verifying and confirming that an electronic signature or a seal is valid;
- ***Relying party*** means a natural or legal person that relies upon an electronic identification or a trust service.

V. Linkages with practice

In order to better understand the scope of the work, concepts and links with practice, concrete projects set up in different countries or regions may be presented during the session(s) of Working Group IV. A presentation of CEF eID DSI and of the eIDAS node could be provided in order to illustrate how this works and is being implemented by the EU Member States.