United Nations A/CN.9/692

General Assembly

Distr.: General
15 April 2010

Original: English

United Nations Commission on International Trade Law
Forty-third session
New York, 29 June-9 July 2010

Present and possible future work on electronic commerce

Note by the Secretariat

Contents

V.10-52774 (E) 160410 190410

I. Introduction

1. At its fortieth session, in 2007, the Commission requested the Secretariat to continue to follow closely legal developments in the area of electronic commerce, with a view to making appropriate suggestions in due course.[1]

2. At its forty-first session, in 2008, the Commission requested the Secretariat to engage actively, in cooperation with the World Customs Organization (WCO) and the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), and with the involvement of experts, in the study of the legal aspects involved in implementing a cross-border single window facility with a view to formulating a comprehensive international reference document on the legal aspects of creating and managing a single window, and to report to the Commission on the progress of that work.[2] That request was reiterated by the Commission at its forty-second session, in 2009.[3]

3. Furthermore, at its forty-second session, in 2009, the Commission requested the Secretariat to prepare studies on electronic transferable records also in light of the written proposals received at that session (documents A/CN.9/681 and Add.1 and A/CN.9/682), and to organize colloquia on those topics, resources permitting, with a view to reconsidering those matters at a future session.[4]

4. In furtherance of the above, the present note contains an update on the progress of the work of the WCO-UNCITRAL Joint Legal Task Force on Coordinated Border Management Incorporating the International Single Window and provides information relating to electronic transferable records. Moreover, it contains an update on recent developments in the field of electronic commerce, with particular regard to identity management and electronic commerce conducted with mobile devices, including payments (m-payments).

II. Electronic single window facilities

5. The second meeting of the WCO-UNCITRAL Joint Legal Task Force on Coordinated Border Management incorporating the International Single Window (the "Joint Legal Task Force") took place from 8 to 11 February 2010 at the premises of the WCO in Brussels. Pursuant to the instructions received from its Permanent Technical Committee, the WCO secretariat involved WCO regional chairs in the preparation of that meeting.

6. The second Joint Legal Task Force meeting stressed once more the relevance of electronic single window facilities for trade facilitation. In particular, it was noted that such facilities were likely to play a significant role in shaping paperless trade, thus directly impacting electronic commerce procedures.

---

[1] *Official Records of the General Assembly, Sixty-second Session, Supplement No. 17* (A/62/17), part I, para. 195.

[2] Ibid., *Sixty-third Session, Supplement No. 17* (A/63/17), paras. 333-338.

[3] Ibid., *Sixty-fourth Session, Supplement No. 17* (A/64/17), para. 340.

[4] Ibid., *Sixty-fourth Session, Supplement No. 17* (A/64/17), para. 343.

7. The Joint Legal Task Force agreed that the analysis of legal issues arising from the implementation of single window facilities would greatly benefit from the availability of reference models, prepared on the basis of documents such as UN/CEFACT draft recommendation 35[5] and the APEC Single Window Implementation Guide and Working Group Phase 2 Final Report,[6] as well as of case studies. Such reference models would illustrate commercial transactions at the national and at the international level in the context of the trade clearance process and the technical models of electronic single window facilities, with particular attention to the parties involved and their location.

8. At that meeting, certain legal issues were identified as suitable for further study in the near future. Such issues included: legal validity of electronic communications, including via mobile devices; identification, authentication and authorization, in particular in the context of identity management; data use, retention and privacy; evidentiary value of electronic records and other enforcement-related issues; and legal implications of the various technical architectural options.

9. As an outcome of the meeting, the Joint Legal Task Force established a work plan to gather the necessary information from experts in customs procedures and to compile it so that it could be used for legal analysis. The work plan schedule took into account the desirability to interact with relevant UNCITRAL meetings, including possible future sessions of UNCITRAL Working Group IV.

10. Other work of the Secretariat relating to single window facilities included cooperating with the secretariat of the Eurasian Economic Community in the preparation of a legislative framework for the implementation of such facilities in member States of the Community, and providing comments, at the request of UN/CEFACT, on UN/CEFACT draft recommendation 35.

11. In light of the above, the Commission may wish to consider asking Working Group IV (Electronic Commerce) to review at its future sessions the work on single windows carried out by the Joint Legal Task Force and by other organizations, and to exchange views and formulate recommendations on possible legislative work in that domain.

III. Electronic transferable records

A. Introduction

12. The possibility of future work by UNCITRAL with regard to issues of negotiability and transferability of rights in goods in an electronic environment was first mentioned at the Commission's twenty-seventh session, in 1994,[7] and

---

[5] UN/CEFACT, *Establishing a Legal Framework for an International Trade Single Window – Draft Recommendation No. 35*. February 2009 (Public Review Draft); available from http://www.unece.org/cefact/recommendations/rec35/Rec35-PublicReviewDraftv9-Feb09.doc.

[6] APEC document #209-CT-01.3 (July 2009), available from http://publications.apec.org/publication-detail.php?pub_id=910.

[7] *Official Records of the General Assembly, Forty-ninth Session, Supplement No. 17* (A/49/17), para. 201.

subsequently discussed in various sessions of the Commission and of Working Group IV.[8] In this framework, two documents have dealt in depth with substantive aspects of the topic.

13. Document A/CN.9/WG.IV/WP.69 discussed both paper-based and electronic bills of lading and other maritime transport documents. In particular, that document provided an overview of the attempts to deal with bills of lading in the electronic environment, and made suggestions for model legislative provisions which were eventually adopted as articles 16 and 17 of the UNCITRAL Model Law on Electronic Commerce.[9]

14. Furthermore, that document contained a preliminary analysis of the conditions for establishing the functional equivalence of electronic and paper-based bills of lading. In this respect, it highlighted as a key issue the possibility to identify with certainty the holder of the bill, which would be entitled to delivery of the goods. Such issue brought into focus the need to ensure the uniqueness of the electronic record incorporating the title to the goods.[10]

15. Document A/CN.9/WG.IV/WP.90 discussed in general legal issues relating to transfer of rights in tangible goods and other rights. It offered a comparative description of the methods used for the transfer of property interests in tangible property and for the perfection of security interests, and of the challenges posed by the transposition of those methods in the electronic environment. It also provided an update on on-going efforts for the use of electronic means in transfer of rights in tangible goods.

16. With respect to documents of title and negotiable instruments, that document stressed the desirability to ensure control over the electronic transferable record in a manner equivalent to physical possession, and suggested that a combination of a registry system and adequately secure technology could assist in addressing issues relating to the singularity and authenticity of the electronic record.[11]

17. The use of electronic communications in international trade has gained further acceptance since the preparation of those two documents, including with respect to the use of registries for the creation and transfer of rights.

18. A notable example of such use in relation to security interests is provided by the Convention on International Interests in Mobile Equipment (Cape Town, 2001)[12] (the Cape Town Convention) and, in particular, its Protocol on Matters specific to Aircraft Equipment (Cape Town, 2001)[13] (the Aircraft Equipment Protocol to the Cape Town Convention).

19. Article 16 of the Cape Town Convention mandates the use of an electronic registry for the registration of international interests in mobile equipment and related transactions and notices, as described in that article. Interests registered

---

[8] See A/CN.9/484, paras. 87-93; *Official Records of the General Assembly, Fifty-sixth Session, Supplement No. 17* (A/56/17), paras. 291-293. For an historical record of previous sessions, see A/CN.9/WG.IV/WP.90, paras. 1-4.

[9] United Nations publication, Sales No. E.99.V.4.

[10] A/CN.9/WG.IV/WP.69, para. 92.

[11] A/CN.9/WG.IV/WP.90, paras. 35-37.

[12] United Nations, *Treaty Series*, vol. 2307, No. 41143.

[13] Ibid., vol. 2367, No. 41143.

under the Cape Town Convention have priority over those registrable but not registered in those cases falling under the scope of that Convention. Thus, registration may confer priority to the interest, with clear benefits for the interest holder, typically a financing entity.

20. The electronic registry system established by the Cape Town Convention is supervised by a supervisory authority and managed by a registrar. The Cape Town Convention contains further provisions on the electronic registry, including, in its article 28, rules on the liability of the registrar for malfunctioning of the registry.

21. In the case of the Aircraft Equipment Protocol to the Cape Town Convention, the International Civil Aviation Authority (ICAO) discharges the functions of the Supervisory Authority, and Aviareto Limited, an Irish-based company, was selected as the Registrar by the Supervisory Authority. The Supervisory Authority has adopted regulations on the operation of the registry.[14] Additional information on the Cape Town Convention, the Aircraft Equipment Protocol to the Cape Town Convention and its electronic registry is available from the Unidroit website[15] and from the Registrar's yearly reports on its activity.[16]

22. The use of electronic registries for security interests has attracted further attention and may be relevant for the future work of UNCITRAL Working Group VI (Security Interests).[17] In fact, the UNCITRAL Legislative Guide on Secured Transactions provides recommendations regarding the use of electronic communications reflecting the content of previous UNCITRAL legislative texts.[18] It also contains a chapter on the registry system, recommending that it should be in electronic form when possible and setting criteria for its operation,[19] and it further suggests a specific rule on the liability of the electronic registry operator.[20]

23. Moreover, the Seventh Inter-American Specialized Conference on Private International Law (CIDIP-VII) has adopted the "Model Registry Regulations under the Model Inter-American Law on Secured Transactions" which are also meant for use with electronic registries.[21]

---

[14] ICAO doc. 9864, *Regulations and Procedures for the International Registry*, Third Edition, 2009, available from http://www.icao.int/icao/en/leb/intl_registry/index.html.

[15] Available from https://www.internationalregistry.aero/irWeb/pageflows/work/Reports/DownloadAnnualReport/DownloadAnnualReportController.jpf.

[16] A select bibliography on the International Registry for Aircraft Objects is available from http://www.unidroit.org/english/conventions/mobile-equipment/bibliography/registryaircraft.htm.

[17] See document A/CN.9/702.

[18] *UNCITRAL Legislative Guide on Secured Transactions. Terminology and recommendations*, United Nations publication, Sales No. E.09.V.13. See, in particular, recommendations n. 11 and n. 12, on the functional equivalence between written and electronic form and between handwritten and electronic signatures.

[19] Ibid., recommendation n. 54.

[20] Ibid., recommendation n. 56: *Responsibility for loss or damage*. […] If the system is designed to permit direct registration and searching by registry users without the intervention of registry personnel, the responsibility of the registry for loss or damage should be limited to system malfunction.

[21] CIDIP-VII/RES.1/09, *Adoption of the Model Registry Regulations under the Model Inter-American Law on Secured Transactions* (9 October 2009).

24. With respect to electronic transferable records incorporating a right to goods, it should be noted that the United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (the "Rotterdam Rules")[22] contains a chapter devoted to electronic transport records. In particular, article 8 of the Rotterdam Rules provides for the use and effect of electronic transport records, article 9 indicates the procedures for use of negotiable electronic transport records and article 10 sets out rules for the replacement of negotiable transport documents with negotiable electronic transport records and vice versa. Moreover, the Rotterdam Rules define both the notion of electronic transport record (article 1 (18))[23] and that of negotiable electronic transport record (article 1 (19)).[24]

25. Finally, the Republic of Korea has recently enacted legislation enabling the use of electronic bills of lading. Since such legislation aims at addressing the issues of uniqueness and security that were often considered as fundamental in the creation and management of electronic transferable records, a detailed description of that system might provide useful insight for the consideration of future work in this field.

B. Legal framework for the operation of electronic bills of lading in the Republic of Korea

26. In the context of a broader legislative reform exercise, the Republic of Korea has introduced in its Commercial Act an article enabling electronic bills of lading.[25] The provisions of that article are complemented by those contained in a Presidential

---

[22] United Nations publication, Sales No. E.09.V.9.

[23] Rotterdam Rules, article 1 (18): "Electronic transport record" means information in one or more messages issued by electronic communication under a contract of carriage by a carrier, including information logically associated with the electronic transport record by attachments or otherwise linked to the electronic transport record contemporaneously with or subsequent to its issue by the carrier, so as to become part of the electronic transport record, that: (a) Evidences the carrier's or a performing party's receipt of goods under a contract of carriage; and (b) Evidences or contains a contract of carriage.

[24] Ibid., article 1 (19): "Negotiable electronic transport record" means an electronic transport record: (a) That indicates, by wording such as "to order", or "negotiable", or other appropriate wording recognized as having the same effect by the law applicable to the record, that the goods have been consigned to the order of the shipper or to the order of the consignee, and is not explicitly stated as being "non-negotiable" or "not negotiable"; and (b) The use of which meets the requirements of article 9, paragraph 1.

[25] Article 862 of the revised Korean Commercial Act, enacted on 3 August 2007 (Law n. 9746). This article on bills of lading. can be found in Part V (Marine Commerce), Chapter II (Transport and Charter), Section 6 (Seaway Bill) of the Commercial Act.

Decree.[26] Contractual agreements for access to the service may also be relevant to determine the legal framework applicable to electronic bills of lading.[27]

1. Scope and general provisions

27. Article 862 of the revised Korean Commercial Act establishes the legal equivalence between electronic and paper-based bills of lading managed in an electronic title registry ("the electronic title registry", or "the registry"). The adoption of the electronic form is voluntary.[28] All natural and legal persons wishing to use the electronic bills of lading system shall register with the registry operator by providing their name, address and company registration number, as appropriate, prior to obtaining access to the services.[29]

28. All communications among parties are exchanged in electronic form unless the law specifies otherwise.[30] In order to ensure the authenticity and integrity of the electronic communications, parties must sign the electronic document transmitted to the registry operator for issuance and transfer of electronic bills of lading with a digital signature provided by a Korea-based certification service provider.[31]

29. Article 862 of the revised Korean Commercial Act applies to bills of lading issued in connection with domestic or international carriage of goods by sea.[32] However, a practical difficulty may arise for non-Korean companies in obtaining Korea-based PKI certification as this requires a personal identification number or company registration number issued in Korea. In this respect, it should be further noted that article 27 bis of the Korean Electronic Signature Act[33] foresees cross-border recognition of digital signatures by virtue of a formal agreement between governments. Thus, in principle, foreign digital signatures may get recognition in the Korean legal system.

---

[26] In accordance with article 862 (5) of the Commercial Act, specific requirements for electronic bills of lading and other relevant matters for the implementation of the Commercial Act are defined in the Presidential Decree on the Implementation of the Electronic Bill of Lading Provisions of the Commercial Act ("the Presidential Decree"). The Presidential Decree went into effect on 4 August 2008. On 26 September 2008, the Korean Ministry of Justice designated Korea Trade Net (KTNET) as the registry operator in accordance with articles 3 and 4 of the Presidential Decree. KTNET started its service to the public on electronic bills of lading on 30 March 2009.

[27] Service Agreement of the e-B/L Korea Portal (the "Service Agreement").

[28] Commercial Act, article 862 (1).

[29] Presidential Decree, article 8 (5) prescribes that the transferees of electronic bill of lading shall register with the registry operator prior to the request for transfer.

[30] The registry operator communicates with the parties through the electronic addresses designated in the online platforms (Service Agreement, article 15).

[31] The carrier or its agent shall sign the request for issuance of electronic bills of lading with its digital signature (Presidential Decree, articles 6 (1) and 6 (1) (3)); the holder shall sign the request for transfer of electronic bills of lading with its digital signature (Ibid., article 8 (2) (3)).

[32] The Korean practice on paper-based bills of lading may extend their application to multimodal carriage of goods with a prevalent maritime leg. Based on this analogy, the e-B/L Korea Portal issues electronic multimodal transport bill of lading.

[33] Electronic Signature Act, last amended on 26 December 2008 (Law n. 9208).

2. Issuance of the electronic bill of lading

30. In order to issue an electronic bill of lading, the carrier needs to submit a request to the registry operator.[34] The message shall contain the same information required for paper-based bill of lading[35] and, in addition, indicate the place of receipt and of delivery of the goods.[36] The carrier or its agent shall also transmit the general terms and conditions of the electronic bill of lading.[37] The carrier shall further transmit the agreement of the parties on the use of the electronic form.[38] The shipper may express its consent on the use of the electronic form at the time of submitting the shipping request to the carrier.[39]

31. The request from the carrier to the registry operator constitutes the authorization to issue an electronic bill of lading. The registry operator creates an electronic record constituting the electronic bill of lading and assigns a unique identification number to it, thereby guaranteeing the singularity of the electronic record.[40]

32. The registry operator then informs the consignor of the creation of the record.[41] The consignor may begin to exercise the right of control on the electronic bill of lading upon receipt of this notification.[42]

3. Transfer of the electronic bill of lading

33. The holder may endorse an electronic bill of lading by transmitting to the registry operator a message communicating the intention to transfer the electronic

---

[34] Commercial Act, article 862 (1) and Presidential Decree, article 6 (1). In practice, all requests are submitted to the registry through online platforms by click-wrap method. Small-sized companies may use a web-based portal ("e-B/L Korea Portal"), while medium- and large-sized companies may implement customized solution or internal enterprise resource planning systems to submit requests directly to the registry and update the information contained therein.

[35] Commercial Act, article 853 (1).

[36] Presidential Decree, article 6 (1) (2).

[37] The carrier may register the general terms and conditions of the electronic bill of lading in the registry by uploading them in the e-B/L Korea Portal prior to the request (Service Agreement, article 8). In such case, the carrier does not need to transmit the general terms and conditions again upon issuance of each electronic bill of lading (Presidential Decree, article 6 (2)).

[38] This communication may be effected in paper form (Presidential Decree, article 6 (1)).

[39] In the e-B/L Korea Portal, the shipper may submit the shipping request through uTradeHub (a one-stop electronic trade service operated by KTNET), and, on that occasion, express its agreement to the use of the electronic bill of lading through a click-wrap agreement. The registry operator receives the shipping request, assigns a number to it and forwards it to the carrier.

[40] Actually, two electronic records are created in the implemented system. One identifies the holder of the electronic bill of lading, and is stored in the registry. The second contains the information submitted with the request and is stored in the uTrade Document Repository. The two records are uniquely identified, linked and synchronized daily.
The uTrade Document Repository is a platform operated by KTNET according to Article 16 of the Act on the Promotion of Electronic Trade establishing parameters for the management of the PKI infrastructure (Act on the Promotion of Electronic Trade, last amended on 22 May 2009 (Law n. 9705)). The uTrade Document Repository, the electronic title registry and the electronic bill of lading online platform (e-B/L Korea Portal) form the electronic bill of lading information system.

[41] Presidential Decree, article 6 (3).

[42] Commercial Act, articles 862 (2) and 862 (4).

record.[43] The transferor shall indicate in the message the transferee's information and the unique identification number of the electronic bill of lading assigned by the registry operator.[44]

34. The registry operator amends the electronic record by updating the information relating to the holder and informs the transferee and the transferor accordingly.[45] Upon receipt of this message, the transferee begins to exercise the right of control on the electronic bill of lading.[46]

4. Amendment of the electronic bill of lading

35. The holder of the electronic bill of lading or the carrier may amend the particulars of the electronic bill of lading by submitting a request to the registry operator.[47] The registry operator shall inform the non-requesting party of this request;[48] if that party accepts the suggested changes,[49] the registry operator amends the electronic record in line with the request and informs the parties accordingly.[50]

36. Only the holder may request splitting or combining electronic bills of lading.[51] The consent of the carrier is required if the splitting or combining results in the cancellation of an electronic bill of lading.

5. Replacement of the electronic bill of lading

37. The holder may request to the registry operator the replacement of an electronic bill of lading with a paper-based one.[52] In that case, the registry operator shall terminate the electronic record of the bill of lading and communicate the termination to the carrier.[53] The registry operator shall then issue a paper-based bill of lading and annotate on its back any previous endorsement of the electronic bill of lading.[54] This annotation has the same legal effect as an endorsement.[55]

---

[43] Presidential Decree, articles 8 (1).
[44] Ibid., articles 8 (2) (2).
[45] Ibid., articles 8 (3) and 8 (4).
[46] Commercial Act, articles 862 (3) and 862 (4).
[47] For the holder, see Presidential Decree, article 9 (1). The Service Agreement extends this right to the carrier (Service Agreement, article 19).
[48] Presidential Decree, article 9 (2).
[49] Ibid., article 9 (3).
[50] Ibid., article 9 (4). If the non-requesting party refuses the amendment, it shall submit the reasons for refusal to the registry operator, which shall then inform the requesting party.
[51] Service Agreement, article 19.
[52] Presidential Decree, article 12 (1). The holder shall submit a request through the online platform to obtain the paper-based bill of lading from the registry operator (Service Agreement, article 20).
[53] Ibid., article 12 (4). The registry operator is responsible for the accuracy of the information on the paper-based bill of lading (Presidential Decree, article 12 (5)).
[54] Ibid., article 12 (2).
[55] Ibid., article 12 (3). The Presidential Decree assigns to the registry operator the exclusive right to issue paper-based bill of lading in order to prevent multiple issuance. This represents an exception to the principle that the carrier should issue paper-based bills of lading. Moreover, article 7 of the Service Agreement gives the registry operator the right to define the format of paper-based bills of lading in accordance with its needs.

6. Delivery of goods and termination of the electronic bill of lading

38. The holder of the electronic bill of lading may request the delivery of the goods by transmitting a message to the registry operator.[56] The registry operator shall then amend the electronic record to prevent further circulation and transmit the delivery request to the carrier.[57]

39. The carrier shall verify that the requesting party corresponds to the party entitled to the delivery of the goods according to the electronic record and, in that case, shall communicate to the registry operator its acceptance of the delivery request and deliver the goods.[58]

40. After delivery of the goods, the carrier shall transmit to the registry operator the actual name of the recipient of the goods and date of delivery.[59] Upon receipt of this information, the registry operator shall terminate the electronic record and communicate the termination to the carrier and to the consignee.[60]

41. In case of refusal to deliver the goods, the carrier shall inform the registry operator of the reasons. In turn, the registry operator shall communicate the refusal to the holder of the electronic bill of lading and amend the electronic record so that the electronic bill of lading may be circulated again.[61]

7. Registry operator

42. The registry operator should be a legal entity with equipment and facilities capable of offering electronic bills of lading services, a net asset of more than 20 billion Korean won[62] and insurance liability coverage.[63] Particular importance is given to the adoption of adequate measures for data archival and security. Further, the registry operator shall employ at least 12 staff qualified in information technology, information management and trade operations, and shall adopt an internal regulation on the procedure and methods of operating and managing the equipments and facilities. The Ministry of Justice has the authority to supervise the registry operator and to audit its operations.[64]

8. Liability issues

43. Article 862 of the revised Korean Commercial Act and the Presidential Decree do not contain specific rules on the allocation of liability; therefore, the general rules on liability contained in the Commercial Act and the contractual provisions contained in the Service Agreement define the liability regime relating to the use of electronic bills of lading.

---

[56] Ibid., article 10 (1).

[57] Ibid., article 10 (2).

[58] Ibid., articles 11 (1) and 11 (2). The carrier is informed of the identity of the requesting party at the time of receipt of the delivery order, which is submitted by the requesting party to the registry through the online portal.

[59] Ibid., article 11 (2).

[60] The termination of the record prevents any deletion, change or addition of information in the electronic bill of lading (Ibid., article 2 (7)).

[61] Ibid., article 10 (3).

[62] Currently corresponding to circa 17 million USD.

[63] Ibid., article 3.

[64] Ibid., article 14.

44. In particular, under the contractual provisions contained in the Service Agreement, the registry operator shall be exempted from any liability and dispute arising from the shipment of the goods.[65] Moreover, the registry operator shall not be liable for any damage arising from the user's failure to keep its user id and password safely, from a user's violation of the Service Agreement, or from changes in user information. Finally, the registry operator shall not be liable for natural disasters.

45. The users of the e-B/L Korea Portal have a legal duty to verify any change in the status of the electronic bill of lading and to notify the registry operator of any discrepancy.[66]

9. Records retention

46. The registry operator shall retain the electronic records of the electronic bills of lading for ten years after the date of delivery of the goods, if that took place; for ten years after the date of issuance of the electronic bill of lading, if the delivery of the goods did not take place and, in case of replacement of electronic bill of lading with paper-based bill of lading, for ten years after the termination of the electronic record by the registry operator.[67]

47. In light of the above, the Commission may wish to discuss whether further work to establish a uniform legal framework for electronic transferable records should be undertaken.

IV. Identity management

48. An electronic identity for a person or entity is defined by a set of attributes (e.g., a name; an email address; a birth date), usually selected in light of their relevance in the specific context. Such attributes may be common to several persons or entities or may be unique. However, the aggregation of the attributes in each identity should be unique, at least in the context in which it is used, to allow secure authentication of that identity and legitimate access to a service by the user.

49. The business model currently prevailing in the electronic world requires service providers and other businesses to identify and authenticate users seeking access to services or databases. In turn, users need to establish a dedicated identity credential for each service they wish to access. This approach has led to the proliferation of identities referring to the same user, whose management may be burdensome. It has also led to redundancy of data stored by businesses, with increased costs as well as privacy risks. Attempts to streamline identity management, for instance with "single sign-on" systems, have not yet gained support on a broad scale, especially in open networks, due to concerns relating, inter alia, to privacy, security and technological neutrality.

50. Identity management systems have recently attracted significant attention as a tool to improve trust in electronic commerce and other electronic applications.

---

[65] Service Agreement, article 5.
[66] Ibid., article 14.
[67] Presidential Decree, article 13.

Indeed, the extensive reliance of businesses, governmental offices and consumers on electronic communications requires appropriate mechanisms for establishing mutual trust. Identity management systems aim at enabling identity portability across different applications by facilitating the secure exchange of identity credentials and eliminating redundant operations. They therefore may provide a significant contribution to establishing a trustworthy, secure and efficient electronic environment.

51. Identity management systems may operate using different technical processes, such as proprietary standards, open source technologies or public specifications which may be implemented in different manners. Their system architecture may also vary significantly.

52. Identity management systems may perform the identification, authentication and authorization of the user by a selective use of shared identity attributes, thus potentially addressing issues relating to the proliferation of electronic identities. Identity management systems are already being used both in the public sector[68] and in the private sector,[69] including for social networking.

53. Identity management involves the initial process of identifying a physical or legal entity ("identification"), and the process of later verifying that an entity claiming to be the one previously identified is, in fact, such entity ("authentication"). Once an entity is successfully authenticated, a third process, referred to as "authorization", is used by the party relying on the authentication to determine the rights and privileges granted to the authenticated identity — e.g., whether such identity should be granted access to a database, or to a online service.

54. In their simplest form, identity management systems envisage three main actors: the subject (i.e., the physical or legal person being identified), the identity provider, and the relying party. The function of the identity provider is to verify the identity of the subjects and to assert their identities vis-à-vis relying parties. Therefore, the identity provider may act as a trusted third party, receiving, storing, managing, redistributing and possibly aggregating the information submitted by subjects and relying parties.

55. A more complex scheme involves the existence of multiple identity providers federated under a trust framework provider. In this model, the trust framework provider would establish the minimum standards to be maintained in the federation and monitor the compliance of all identity providers with those standards. This

---

[68] For the US government identity management policy, see http://www.idmanagement.gov/ and, in particular, *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, Version 1.0 (10 November 2009). Moreover, the US government is preparing a National Strategy for Secure Online Transactions whose goal is "to improve the trustworthiness and security of online transactions by facilitating the establishment of interoperable trust frameworks and implementation of improved authentication and authorization technology and processes for all online transaction participants across federal, civil and private sectors" (see Federal News Radio, *White House works to change online transactions*, 25 March 2010, available from http://www.federalnewsradio.com/?nid=35&sid=1919771).

[69] See, for instance, the OpenID system at http://openid.net/, the Kantara system at http://kantarainitiative.org/ and the SAFE-BioPharma Association system at http://www.safe-biopharma.org/.

approach aims at ensuring competition among identity providers, thus possibly improving the quality of their services.

56. Identity management systems may provide significant benefits both to subjects and to relying parties. In particular, they could allow subjects to interact with different relying parties with a single identity, thus avoiding inputting and sharing redundant identifying information, and simplifying and expediting authentication procedures for access to services.

57. From the standpoint of relying parties, possible advantages stem from the fact that subjects would need to be identified only once by the identity provider. The identity provider would then authenticate subjects and share selectively the relevant attributes of their identity with the various relying parties when the subject wishes to obtain access to services. This could lead to significant savings for relying parties in human and technical resources due to scale economies, and could support easier interaction among relying parties through increased interoperability. It might also facilitate compliance with regulatory standards.

58. Inter-governmental organizations have already contributed to the study of this topic. On the technical side, the International Telecommunication Union has set up a Focus Group on Identity Management "to facilitate and advance the development of a generic [identity management] framework and means of discovery of autonomous distributed identities and identity federations and implementations".[70]

59. On the policy side, the Organisation for Economic Co-operation and Development (OECD) has prepared a first reference document.[71] That document identifies the need for "compatibility of regulatory compliance obligations across organisations" in order to facilitate legal interoperability. It also highlights the desirability, especially at the international level, of creating an enabling legal environment, rather than a regulatory one, with a view to fostering systems federation.[72] That document further lists accountability and transparency in the operation of the various components of the identity management system as elements relevant for an enabling legal environment. Moreover, the document highlights the need for clear rules regarding delivery of services, handling and storing personal information, in particular sensitive one, and allocation of liability risks among participants.

60. A more detailed discussion has classified the legal issues raised by identity management systems in four main categories: privacy, identification and authentication, liability and performance.[73]

61. Privacy and security risks have attracted significant attention from an early stage. Dangers relating to inappropriate use, undue disclosure and breach of identity information have been stressed. In this respect, it was suggested that the use of a

---

[70] More information on the ITU Focus Group on Identity Management is available from http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html.

[71] OECD Working Party on Information Security and Privacy, *The Role of Digital Identity Management in the Internet Economy: a Primer for Policy Makers*, DSTI/ICCP/REG(2008)10/FINAL (11 June 2009).

[72] Ibid., p. 12.

[73] T. J. Smedinghoff, *Federated Identity Management: Balancing Privacy Rights, Liability Risks, and the Duty to Authenticate* (21 August 2009), available from http://ssrn.com/abstract=1471599.

federated approach, and, in particular, the supervision of a trust framework provider, would increase the levels of privacy and security.[74] Reference has also been made to the desirability or necessity of setting international standards on the cross-border flow of identity information.

62. Identification and authentication are the key processes that underlie any identity management system. Identification allows establishing the relation between the subject and an electronic identity, while authentication permits validating the association between the subject claiming that identity and the identity claimed. Thus, a faulty identification would expose relying parties to abusive access to the services they provide in spite of strong authentication requirements. Similarly, a faulty authentication would expose relying parties to similar risks notwithstanding a correct identification. As the identity management environment favours identity portability, all parties might be particularly exposed to potential damages arising from such abusive accesses.

63. Compliance with proper procedures for authentication and identification might be relevant also for parties not included in the identity management scheme. For instance, where appropriate under applicable law, a financial institution might wish to rely on a identity provider in the framework of a identity management system to comply with legal duties under Know Your Customer (KYC) standards to prevent money-laundering and terrorism financing.

64. Discussion of rules for the allocation of liability, in particular in case of incorrect identification, unauthorized access to services or identity data, or for denial of access to legitimate services or identity data, might be particularly useful. Scenarios of concern might also involve misuse of identity information and illegal access to services. The allocation of liability would need to balance the various interests without hindering the broader adoption of the model. In order to do so, it might be desirable to define the performance standards of the various actors, which, in turn, might support establishing mutual trust.

65. Current standards are being shaped through self-regulation and contractual agreements. Calls have also been made for compiling a set of legal rules defining duties and obligations of participants in identity management systems.[75] Such rules might also have a statutory nature.

66. In light of the above, the Commission may wish to consider whether the current state of the matter warrants further study by the Secretariat, including by participating in or organizing expert meetings, as appropriate.

---

[74] Center for Democracy & Technology, *Issues for Responsible User-Centric Identity*, November 2009 – Version 1.0, p. 2, available from http://cdt.org/files/pdfs/Issues_for_Responsible_UCI.pdf.

[75] The American Bar Association has constituted a Federated Identity Management Legal Task Force whose goals are to: "identify and evaluate the legal issues that arise in connection with the development, implementation and use of federated identity management systems; identify and evaluate appropriate legal models to address those issues; develop model terms and contracts that can be used by parties". More information on the work of that Legal Task Force is available from www.abanet.org/dch/committee.cfm?com=CL320041.

V. Use of mobile devices in electronic commerce

67. The broad use of mobile devices, including mobile telephones, is a well-established reality in many developed countries. In the last years, it has seen high growth rates also in developing countries, where mobile devices are considered a particularly efficient tool to overcome limited communication infrastructures.[76] Indeed, the rapidly increasing number of users of mobile devices in developing countries proved to be instrumental in achieving the goal set by the World Summit on the Information Society (WSIS) Geneva Plan of Action "to ensure that more than half the world's inhabitants have access to ICTs within their reach"[77] well before its deadline of 2015.[78]

68. This trend has also led to increased offer of a broad range of services delivered through mobile devices. The technology used may differ in light of the available communication infrastructure. Thus, mobile devices may be used to send and receive electronic communications via Short Messaging Services (SMS), or to browse Internet through Wireless Application Protocol (WAP), or to perform contactless transactions based on Near Field Communication (NFC) applications. In most, if not all cases, the communication may be qualified as of electronic nature under the legislative standards adopted in UNCITRAL texts.

69. At a general level, the predictability of the legal status of transactions conducted with electronic means, including those effected with mobile devices, would be greatly enhanced by the adoption of appropriate legislation. However, on the one hand, several countries, especially least developed ones, have not yet adopted general electronic commerce laws; on the other hand, certain countries, having explicitly indicated that mobile commerce is among the forms of electronic commerce covered by technology-neutral legislation, have envisaged additional specific rules for its needs.[79] At the same time, industry organizations are active in presenting their views on various legislative issues.[80] Guidance on the adoption of appropriate legislative standards, with particular respect to the use of mobile devices, might therefore be useful.

70. One area where the importance of mobile technology has been stressed is payment services. In this field, too, it is possible to notice an increase not only in the quantity but also in the variety of the services offered, which is proportional to technological availability and affordability to users. Rapid changes in technology may give additional weight to the reasons for adopting technology-neutral legislation.

---

[76] UNCTAD, *Information Economy Report 2009*, United Nations publication, Sales No. E.09.II.D.18, p. 4-8.

[77] WSIS-03/GENEVA/DOC/0005.

[78] UNCTAD, *WSIS Follow-up Report 2008*, UNCTAD/DTL/STICT/2008/1, p. 2-4.

[79] France, *Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, article 28.

[80] See, for instance, the GSM Europe Working Group on M-Commerce, whose views are available from http://www.gsmeurope.org/work_groups/mcommerce.shtml.

71. Mobile payments are considered as a tool supportive of financial inclusion, especially in rural areas.[81] In fact, in a rapidly increasing number of developing countries, mobile network operators offer fee-based payment services through electronic communications transmitted via mobile devices, typically via SMS. This scheme may reach clients not having access to the services of traditional financial institutions for a number of reasons, including difficulty in accessing their physical facilities.[82] Cross-border payments may be common, for instance, in support of regional trade, especially in areas where trading communities are based on links other than nationality, and for remittances of expatriates.[83]

72. It should be noted that mobile network operators typically do not offer financial services, but simply facilitate money transfer; their services may therefore be defined as mobile payments (or m-payments). However, financial institutions may as well offer their services, which typically include access to credit and remuneration of money deposits, through mobile devices; in that case, the service may be qualified as mobile banking (or m-banking).[84] Since mobile banking often requires higher technological standards, including for security purposes, it is more commonly available in countries with advanced communications networks. Other relevant factors in the diffusion of mobile banking may include the sophistication of the financial markets and, in particular, the availability of multiple tools for interaction with financial services providers.

73. Mobile payments may pose peculiar challenges. For instance, the goal of financial inclusion may require adopting a lower threshold for the identification of clients in environments where formal identity documents may not be easily available. Therefore, lower identification standards could be applied to those clients. This might, in turn, suggest the adoption of flexible authentication standards in the context of a technology-neutral approach. A recent study by the OECD discusses some of the policy issues specific to mobile commerce, in particular, from the perspective of consumers.[85]

74. In light of the above, and taking into account the potential impact of mobile technologies for development, the Commission may wish to consider whether the current state of the matter deserves further study. With respect to mobile payments, the Commission may wish to recall the work already conducted in the area of international payments, for instance when drafting the UNCITRAL Model Law on

---

[81] Timothy R. Lyman, Mark Pickens, David Porteous, *Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance*, CGAP Focus Note no. 43, January 2008, available from http://www.cgap.org/p/site/c/template.rc/1.9.2583/.

[82] A well-known example of implementation of this business model is offered by Kenya: see Alliance for Financial Inclusion (AFI), *Case Study. Enabling mobile money transfer. The Central Bank of Kenya's treatment of M-Pesa*, February 2010, available from http://www.afi-global.net/downloads/AFI_case%20study_Mpesa.pdf.

[83] For additional consideration on the use of electronic means to promote financial inclusion, see document A/CN.9/698, *Microfinance in the context of international economic development*, in particular, para. 58.

[84] From the regulatory standpoint, it should be noted that one important difference between m-payments and m-banking may lie in the extent to which the service operator might fall under the scope of a central financial authority.

[85] OECD, *Policy Guidance for Addressing Emerging Consumer Protection and Empowerment Issues in Mobile Commerce*, June 2008.

International Credit Transfers,[86] with a view to considering whether that work should be revised and updated to accommodate the use of mobile devices.

[86] United Nations publication, Sales No. E.99.V.11.