



General Assembly

Distr.: Limited
8 September 2011

Original: English

**United Nations Commission
on International Trade Law**
Working Group IV (Electronic Commerce)
Forty-fifth session
Vienna, 10-14 October 2011

Legal issues relating to the use of electronic transferable records

Note by the Secretariat*

Contents

	<i>Paragraphs</i>	<i>Page</i>
Introduction	1-2	3
I. Subject matter: electronic transferable records.	3-5	3
II. Legal challenges for electronic transferable records	6-29	4
A. Writing and signature	6-11	4
B. Uniqueness and guarantee of singularity	12-18	5
C. Physical possession.	19-21	7
D. Transfer of rights by delivery.	22-23	7
E. Identification and authentication of holder.	24-26	8
F. Other issues	27-29	9
III. Functional equivalence and technology neutrality	30-35	9
IV. Functional equivalence for “uniqueness”	36-42	10
A. Technical uniqueness	37-39	11
B. Designation of authoritative copy	40-42	11

* The late submission of the document is due to the need to carry out consultations.



V.	Functional equivalence for “possession”: the concept of “control”	43-51	12
A.	Identifying the person in “control”	45-48	13
B.	Adoption of the “control” approach	48-51	14
VI.	The registry approach	52-63	15
A.	Examples of existing law utilizing registries	58-60	16
B.	Examples of existing registry systems	61-63	17
VII.	Possible methodology for the future work by the Working Group	64-69	17

Introduction

1. At its forty-fourth session in 2011, the Commission agreed that Working Group IV (Electronic Commerce) should be convened to undertake work in the field of electronic transferable records.¹ In particular, at that session it was recalled that such work would be beneficial not only for the generic promotion of electronic communications in international trade, but also to address some specific issues such as assisting in the implementation of the United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea, 2008 (“Rotterdam Rules”).² Similarly, it was noted, other transport business, such as aviation, could benefit directly from the formulation of uniform legal standards in the field. It was also noted that work regarding electronic transferable records may include certain aspects of the other topics discussed in documents A/CN.9/728 and A/CN.9/728/Add.1.

2. To assist the Working Group in its work, this note will provide a general overview and summary of key legal issues relating to the creation, use, and transfer of electronic transferable records. This note will focus on issues arising from the use of such records in electronic rather than the traditional paper form. It will not address substantive legal issues that would apply regardless of the medium used, such as wording requirements or rights of a holder of such a record.

I. Subject matter: electronic transferable records

3. The term electronic transferable record is used in this note as a general term to refer to the electronic equivalent of a transferable instrument (negotiable or non-negotiable) or a document of title:

(a) Transferable instruments are financial instruments that may contain an unconditional promise to pay a fixed amount of money to the holder of the instrument, or an order to a third party to pay the holder of the instrument. Examples of transferable instruments include promissory notes, bills of exchange, cheques, and certificates of deposit. They may also include chattel paper (e.g. retail instalment sales contracts, promissory notes secured by an interest in personal property, and equipment leases);

(b) Documents of title are documents which in the regular course of business or financing are treated as adequately evidencing that the person in possession of such document is entitled to receive, hold, and dispose of the document and the goods indicated therein (subject to any defences to enforcement of the document). Examples of documents of title include certain transport documents, bills of lading, dock warrants, dock receipts, warehouse receipts, or orders for the delivery of goods.

4. Each of these categories of documents evidences an obligation owed by the person issuing the document to another person named in the document or to bearer. For example, a promissory note is a transferable instrument that evidences an

¹ *Official Records of the General Assembly, Sixty-sixth Session, Supplement No. 17 (A/66/17)*, para. 250.

² United Nations publication, Sales No. E.09.V.9 (treaty not yet in force).

obligation to repay a debt. A negotiable warehouse receipt is a document of title that represents an obligation by the warehouse operator to deliver goods stored in the warehouse to the owner of the warehouse receipt. These documents can circulate independently of the underlying transaction.

5. Currently both transferable instruments and documents of title typically exist as paper documents. To distinguish an electronic transferable record from its paper equivalent, the term “transferable paper” is used in this note as a general term to refer to transferable instruments and documents of title in traditional paper form.

II. Legal challenges for electronic transferrable records

6. Transferable paper “reifies” the value or obligation they represent; that is, the obligation to pay a sum of money or to deliver goods is embodied in the written document, and the rightful possessor of the document (i.e., the holder) is entitled to enforce and obtain the benefit of it. The written document itself is tangible, but its value does not lie in its physical characteristics. Rather, its value is in the rights embodied in the paper. Thus, possession of the transferable paper is generally required to enforce the rights.

7. Because transferable paper is recognized as the single embodiment of those rights, the mechanism used to transfer the rights in transferable papers is physical delivery to the transferee of the paper itself, usually coupled with the transferor’s signed declaration of an intent to transfer (either written on the document or attached to it). This typically constitutes evidence of the transferee’s right to enforce the underlying obligation. Stated differently, title to transferable paper (and the rights it comprises) passes by endorsement (where necessary) and delivery of the original paper document.

8. These key characteristics of transferable paper raise several issues that represent obstacles to the creation, use, transfer, and enforcement of electronic transferable records and that must be addressed in order to create equivalent electronic transferable records. Those issues may be summarized as follows:

A. Writing and signature

9. Generally, transferable paper must be in writing and signed. While writing and signature requirements and the probative effect of electronic communications generally have been perceived as major legal barriers to the development of electronic commerce in the past, those concerns have now been settled in articles 5 to 10 of the UNCITRAL Model Law on Electronic Commerce (“Model Law on Electronic Commerce”).³ Matters pertaining to contract formation in an electronic environment are settled in articles 11 to 15 of the Model Law on Electronic

³ United Nations publication, Sales No. E.99.V.4. See Model Law on Electronic Commerce: Article 5, Legal recognition of data messages; Article 6, Writing; Article 7, Signature; Article 8, Original; Article 9, Admissibility and evidential weight of data messages; Article 10, Retention of data messages.

Commerce.⁴ Matters relating to electronic signatures are dealt with in the UNCITRAL Model Law on Electronic Signatures (“Model Law on Electronic Signatures”).⁵

10. Most of these issues are also similarly addressed in Articles 8, 9, 10 and 12 of the United Nations Convention on the Use of Electronic Communications in International Contracts, 2005 (the “Electronic Communications Convention”).⁶ However, the Electronic Communications Convention expressly excludes electronic transferable records from its scope.⁷ This was done “because the potential consequences of unauthorized duplication of ... any transferable instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of money make it necessary to develop mechanisms to ensure the singularity of those instruments,” and because the “need for ensuring their uniqueness go beyond simply ensuring the equivalence between paper and electronic forms, which is the main aim of the Electronic Communications Convention.”⁸

11. Thus, as suggested by an earlier study by the Secretariat,⁹ surmounting the issues of writing and signature in an electronic context does not solve the issue of negotiability, which may be perhaps the most challenging aspect of implementing electronic transferable records in international trade practices.

B. Uniqueness and guarantee of singularity

12. Since each transferable paper embodies the rights it represents, there typically must be a single unique document that represents the rights embodied in such transferable paper, and any transfer or assignment of such rights by the holder requires the physical transfer of the singular document physically representing such rights.

13. Thus, if a person is to receive possessory title of a transferable instrument or a document of title by receiving it as an electronic message, the addressee will need to be satisfied that no identical message could have been sent to any other person by any preceding party in the chain, thereby creating the possibility of other claimants to the title. In other words, the potential consequences of unauthorized duplication of any electronic transferable record that entitles the bearer or beneficiary to claim

⁴ See Model Law on Electronic Commerce: Article 11, Formation and validity of contracts; Article 12, Recognition by parties of data messages; Article 13, Attribution of data messages; Article 14, Acknowledgement of receipt; Article 15, Time and place of dispatch and receipt of data messages.

⁵ United Nations publication, Sales No. E.02.V.8.

⁶ United Nations publication, Sales No. E.07.V.2 (treaty not yet in force): article 8, Legal recognition of electronic communications; article 9, Form Requirements; article 10, Time and place of dispatch and receipt of electronic communications; article 12, Use of automated messages for contract formation.

⁷ Electronic Communications Convention, article 2, paragraph 2.

⁸ Electronic Communications Convention, Explanatory Note, paras. 80-81. Note that the Rotterdam Rules contain, in article 9, the requirements for the use of one category of electronic transferable records, that is negotiable electronic transport records. However, that text does not discuss the details of those documents.

⁹ A/CN.9/WG.IV/WP.69, para. 55.

the delivery of goods or the payment of a sum of money make it necessary to develop mechanisms to provide a guarantee of singularity of those records.

14. The concern regarding a guarantee of singularity arises from the fact that an electronic record generally can be copied in a way that creates a duplicate record identical to the first and indistinguishable from it. Absent special measures or widespread application of technologies today not in common use, there is little or no certainty that any electronic record is unique.

15. It is important to recognize that the requirement that transferable paper be unique (i.e., the requirement for a guarantee of singularity) is different from the requirement that such document be presented or retained in its original form. Both the Model Law on Electronic Commerce and the Electronic Communications Convention recognize this distinction and, for purposes of transposing these requirements in an electronic environment, address each of them separately.

16. Legal requirements that documents be made available or retained in their original form are addressed by the Model Law on Electronic Commerce (article 8) and the Electronic Communications Conventions (article 9, paragraph 4) essentially as evidentiary requirements aimed at ensuring document integrity and availability. This is achieved by providing that an electronic communication will satisfy the requirement that it be made available or retained in its original form if: (1) there exists a reliable assurance as to the integrity of the information, and (2) the information is capable of being displayed to the appropriate persons. Under this approach, multiple copies of the same electronic communication can qualify as being in original form.

17. Ensuring that a document is unique typically requires that it be the only one in existence (or alternatively, that any copies be clearly identifiable as a copy). Article 17 of the Model Law on Electronic Commerce recognizes the need to address the issue of uniqueness in the context of electronic transport documents, but does not specify how this is to be done: it simply requires that “a reliable method is used to render such data message or messages unique.” Article 9 of the Rotterdam Rules also indirectly addresses the issue by requiring that “The use of a negotiable electronic transport record shall be subject to procedures” defined by the parties and by identifying four categories of issues intended in part to address uniqueness concerns. However, like the Model Law on Electronic Commerce, the Rotterdam Rules do not specify how those procedures are to be accomplished. By contrast, while the drafters of the Electronic Communications Convention also recognized that uniqueness is a critical requirement for electronic transferable records, they acknowledged that finding a solution for that problem required a combination of legal, technological and business solutions, which had not yet been fully developed and tested. Thus the Electronic Communications Convention dealt with the issue by excluding electronic transferable records from the scope of the Convention.¹⁰

18. As a consequence, a key challenge to be faced in designing a legal regime to accommodate electronic transferable records is to define a functionally equivalent mechanism to address the requirement of uniqueness or singularity of those records. In this respect, it is important to note that the function of uniqueness or singularity

¹⁰ See Electronic Communications Convention, article 2, paragraph 2; see also A/CN.9/571, para. 136.

is to provide adequate assurance that only one creditor may claim the entitlement to the performance of the obligation embodied in the document. This is done by eliminating the possibility that multiple enforceable documents embodying the same entitlement could circulate.

C. Physical possession

19. With transferable paper, the requirement for a guarantee of singularity is coupled with the requirement for physical possession of the paper document that represents the obligation. It is possession of the unique document embodying such rights and obligations¹¹ that is generally required in order to become a person entitled to enforce it.¹² Rights to the delivery of goods represented by documents of title are typically conditioned on the physical possession of a unique paper document (e.g., the bill of lading, warehouse receipt, or other similar document). Likewise, rights to the payment of a sum of money represented by transferable instruments are also typically conditioned on the physical possession of a unique paper document (e.g., a promissory note, bill of exchange, cheque, or other similar document).

20. Possession is important not because tangible paper documents are per se valuable, but because only one person can possess a unique tangible object at one time. The possession requirement coupled with the singularity requirement protects the issuer from multiple liabilities on the same instrument, helps to provide assurance to a transferee (i.e., the holder) that it has acquired good title, and protects the transferee from a fraudulent transfer of a duplicate.

21. Thus, in addition to addressing the singularity requirement, a key challenge for the implementation of electronic transferable records is to define a functionally equivalent mechanism to address the requirement for possession of the electronic transferable record. This requires devising a process whereby a holder who claims due negotiation of an electronic transferable records will feel assured that there is a unique electronic transferable record in existence, and that there is a means to take control of that electronic transferable record in a manner that is functionally equivalent in law to physical possession.

D. Transfer of rights by delivery

22. Transfer by delivery is the norm for the effective circulation of transferable papers. Negotiable instruments, such as bills of exchange and promissory notes, are typically negotiated by transfer of possession of the instrument by a person other than the issuer to a person who thereby becomes its holder. Except for negotiation by a remitter, if an instrument is payable to an identified person, negotiation requires transfer of possession of the instrument and its endorsement by the transferor. If an instrument is payable to bearer, it may be negotiated by transfer of possession alone. Article 13 of the United Nations Convention on International Bills

¹¹ The person legally in possession of the transferable paper is typically referred to as the holder, and the holder is the person entitled to enforce the document.

¹² There may, however, be special rules for enforcing lost, destroyed, or stolen transferable papers.

of Exchange and International Promissory Notes, 1988¹³ reflects this principle by providing that an instrument is transferred by endorsement and delivery of the instrument by the endorser to the endorsee; or by mere delivery of the instrument if the last endorsement is in blank. The same principle can be found in articles 11 and 16 of Annex I to the Convention Providing a Uniform Law on Bills of Exchange and Promissory Notes, 1930.¹⁴

23. As noted above at paragraphs 9-11, existing electronic commerce laws surmounting the issues of writing and signature in an electronic context facilitate the use of various processes by which an electronic transferable record might be signed for endorsement but they do not solve the issue of delivery required for a transfer of the value inherent in an electronic transferable record.

E. Identification and authentication of holder

24. Another significant challenge faced in adapting transferable paper legal regimes to accommodate electronic transferable records lies in the identification and authentication of the person who is considered to have possession (or, in an electronic environment, control) of the electronic record that represents the obligation (i.e., the holder) and who thus constitutes the creditor or beneficiary of the value it represents. This is in addition, of course, to the underlying need to reliably identify and authenticate the other parties to an electronic transferable record — e.g., the original issuer and the transferor.

25. Establishing the identity of the issuer who signs the original electronic transferable record and of the transferor who endorses the electronic transferable record to transfer it to another party is required for a valid electronic signature under article 7 of the Model Law on Electronic Commerce, article 6 of the Model Law on Electronic Signatures and article 9, paragraph 3, of the Electronic Communications Convention. However, those provisions merely require the use of a method to identify the signatory, leaving it to the parties to determine how that may be accomplished.

26. With respect to the holder, however, the identification problem is a different one. The holder is the person entitled to enforce the electronic transferable record, yet the identity of the holder may not be noted on the transferable record itself, and the holder may change from time-to-time as the record is transferred from one person to another. Thus a mechanism must be in place to identify the person that, at any particular point in time, is considered to be the holder. In a paper environment the person in possession of the unique transferable paper may be presumed to be the holder. But in an electronic environment, where the concept of possession may need to be replaced with a functional equivalent such as control (see paragraphs 43-51 below), a mechanism must be in place to establish the identity of such person.

¹³ United Nations publication, Sales No. E.95.V.16 (treaty not yet in force).

¹⁴ League of Nations, *Treaty Series*, vol. CXLIII, p. 259, No. 3313 (1933-1934).

F. Other issues

27. A critical element in the acceptance and diffusion of electronic transferable records relates to their acceptance by third parties, which, in turn, depends on their level of trust in the underlying processes, as well as their trust in third-party providers of trust services, such as registries and trust platform operators.

28. Generally, electronic records can be easily altered in a manner that is not detectable. Thus, the usability and general trustworthiness of an electronic transferable record as well as its use as evidence in court require procedures to ensure the continuing integrity and availability of both the electronic record and its electronic signature. This necessitates providing appropriate data security for both the electronic transferable record and its related processes in order to guarantee their accuracy and completeness and to guard against unauthorized transfers or alterations whether intentionally or accidentally made.

29. The establishment of electronic equivalents to transferable paper raises a number of additional issues. These may include the satisfaction of legal requirements on record-keeping, the adequacy of certification and authentication methods, possible need of specific legislative authority to operate electronic registry systems, the allocation of liability for erroneous messages, communication failures, and system breakdowns; the incorporation of general terms and conditions; and the safeguarding of privacy.

III. Functional equivalence and technology neutrality

30. Historically, UNCITRAL has addressed the problems created by paper-based form requirements through the principle of “functional equivalence.”¹⁵ Under this principle, the Model Law on Electronic Commerce, the Model Law on Electronic Signatures and the Electronic Communications Convention, as well as legislation implementing the principles set forth in those documents, establish requirements that are intended to replicate in the electronic world the objectives achieved by each form requirement in the paper world.

31. The functional equivalence approach is based on an analysis of the purposes and functions of the traditional paper-based requirements in order to determine how those purposes or functions could be fulfilled through electronic techniques.¹⁶ This approach “does not attempt to define a computer-based equivalent to any particular kind of paper document.” Instead, it singles out the basic functions of the primary paper-based form requirements, and sets out criteria that, if satisfied, enable electronic records to enjoy the same level of legal recognition as corresponding paper documents.¹⁷ By doing so, it also allows States to enforce electronic transactions in accordance with existing laws “without necessitating the wholesale removal of the paper-based requirements themselves or disturbing the legal concepts and approaches underlying those requirements.”¹⁸

¹⁵ See, e.g., Electronic Communications Convention, Explanatory Note, para. 133.

¹⁶ Electronic Communications Convention, Explanatory Note, para. 51.

¹⁷ Electronic Communications Convention, Explanatory Note, para. 51.

¹⁸ See, e.g., Electronic Communications Convention, Explanatory Note, para. 52.

32. This principle of functional equivalence goes beyond the concept of non-discrimination¹⁹ and requires that paper-based and electronic documents should be treated equally by the law so long as the electronic document satisfies the requirements for equivalence specified in the law.

33. To facilitate the development of electronic alternatives to transferable paper, it is essential to transpose to the electronic world the paper-based requirements of uniqueness, possession, and negotiation by delivery. This requires defining equivalents that are able to achieve the same results as those paper-based requirements, and doing so in a manner compatible with the electronic medium.

34. The need to establish criteria for equivalence for those functions fulfilled by transferable paper may be met by adopting a single broad and flexible standard that could satisfy all the functions of the paper document in the electronic environment, or by separate standards aiming at fulfilling each individual function of the paper document.

35. In addressing the requirements for functional equivalence, the Working Group should also keep in mind the principle of “technology neutrality” reflected in prior UNCITRAL texts, including the Model Law on Electronic Commerce, the Model Law on Electronic Signatures and the Electronic Communications Convention. This principle holds that the law should not discriminate between different technologies, i.e., the law should neither require nor assume the adoption of a particular technology. The goal of technology neutrality is important from the standpoint of not stifling development of any technology or unfairly favouring one technology over another. Strictly adhering to the principle of technology neutrality will maximize the ability to accommodate all possible present and future models.

IV. Functional equivalence for “uniqueness”

36. Electronic records — even if signed with “qualified” or “secure” signatures — do not inherently possess a characteristic of uniqueness when used with most current technologies. In fact, as noted above (paragraph 14), most electronic records can be copied without the “copy” being easily distinguishable from the “original”. To overcome this, several alternate approaches for achieving the electronic functional equivalent of a unique paper document have been proposed or implemented.

¹⁹ The principle of non-discrimination provides that “A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.” Electronic Communications Convention, Article 8 (1). This principle is key to most e-commerce laws. See, e.g., Model Law on Electronic Commerce (Article 5), the European Union Electronic Signatures Directive (Article 5 (2)), and UETA (Section 7 (a)) and E-SIGN (Section 101 (a)(1)) in the U.S.A. While the principle of non-discrimination is designed to eliminate the nature of the medium as a reason to deny effect or enforceability to an electronic communication, signature, or contract, it may leave open the concern that an electronic communication does not satisfy certain form requirements.

A. Technical uniqueness

37. In theory it may be technically possible to create a truly unique electronic document that cannot be copied (at least without the copy being distinguishable as a copy) and that can be transferred. If and when technology that is capable of ensuring the uniqueness of an electronic record and of enabling its transfer is widely available, it would provide a basis for rendering an electronic record unique, so that it can mimic a unique paper document. Technologies possibly relevant for achieving technical uniqueness might include digital object identifiers (DOI) and digital rights management (DRM).

38. Most existing electronic transferable record laws, however, have been written on the assumption that the problem of guaranteeing the uniqueness of a record cannot be solved at the level of the design of the record itself, or in any event, that the concept of a truly unique electronic record is not a reality, and that a different approach is required. Generally, such laws take the view that it is not necessary that an electronic transferable record possess any intrinsic characteristic that makes it truly “unique” in the sense that identical copies cannot exist. Instead, they focus on establishing the functional equivalence of uniqueness through requirements designed: (1) to ensure the integrity and availability of at least one copy of the electronic transferable record by designating an authoritative copy (i.e., to specify and determine the terms of the electronic transferable record), and (2) to identify the owner or holder (i.e., person in control) of such electronic transferable record.

39. Stated differently, two issues must be addressed: (1) what are the terms of the electronic transferable record?, and (2) who is the person entitled to the benefit of its value or obligation? In some jurisdictions, the terms of the electronic transferable record are established by designation of an authoritative copy, and the identity of the person entitled to the benefit of its value or obligation is established through the concept of control (used as a functional equivalent for possession).

B. Designation of authoritative copy

40. Designating an authoritative copy of an electronic transferable record (without regard to how many other copies may exist), can address concerns regarding the integrity of the record (i.e., establishing “what” the holder owns an interest in) without the need for the existence of a unique record. Approaches to designation of an authoritative copy include:

(a) Designation based on storage in a specific secure system. One approach involves storing a copy of the electronic transferable record designated as the authoritative copy on a specific secure computer system designed for such purpose and protected by appropriate security and access controls. This might involve, for example, the use of an information system that is specifically designed to store and keep track of a particular type of electronic transferable record, perhaps for a particular business sector. The designated authoritative copy of the electronic transferable record remains on the system for its life cycle, and a related registry tracks the identity of the holder. Under this approach, uniqueness of an electronic record is established through the design of a secure environment within which a copy of the electronic record can be kept. Controls on the system ensure that the

integrity of such electronic transferable record remains assured, regardless of where or how the record is stored on the system, or how many copies the system maintains;

(b) Designation based on verifiable content or location. An alternative approach allows the specific copy that constitutes the authoritative copy, and the computer system on which it is stored, to change over time. This is often done through the use of a registry that tracks the location where the authoritative copy is stored, and/or that maintains a digital fingerprint (e.g., the hash value or digital signature) of the authoritative copy so that it can be readily determined whether the integrity of the copy maintained by or for the holder is intact and matches the original. Sometimes referred to as a registry model, this approach allows for the creation, issuance, storage and transfer of the electronic transferable record on a variety of distributed information systems, with certain information transmitted to and recorded in a central registry. The designated authoritative copy of the electronic transferable record is not necessarily stored in the registry, but any copy can be verified as accurate by reference to the registry. Thus, in some systems the registry holds the authoritative copy as well as the identity of the person in control of it. In other systems, the registry simply holds only the digital signature of the authoritative copy, which is then available to verify the integrity of any copy the person in control later seeks to enforce.

41. Other approaches may also be devised that use technology, process or agreement as a substitute for uniqueness.

42. Finally, it should be noted that while some laws authorize or require one or more of the approaches above, other laws have left the approach to this issue unresolved. For example, as noted in paragraph 17 above, neither the Model Law on Electronic Commerce nor the Rotterdam Rules specify the method whereby such a singularity requirement can be satisfied, and leave it to the parties to agree on the method to be used for this purpose.

V. Functional equivalence for “possession”: the concept of “control”

43. In most legal models governing electronic transferable records, the concept of “control” over an electronic record is used as the functional equivalent of possession. That is, the person in control of the electronic transferable record is considered the holder capable of enforcing the electronic transferable record. Where control of an electronic transferable record is used as a substitute for possession of transferable paper, transfer of control serves as the substitute for delivery of the electronic transferable record, just as transfer of possession (plus endorsement where required) serves as delivery of transferable paper.

44. As noted above at paragraphs 38-39, in the absence of technical uniqueness for electronic records, the control approach can also help to address the singularity requirement of transferable paper. By providing a process for designating the identity of the person in control of the electronic transferable record (along with a

process to establish “what” it is that the holder owns an interest in),²⁰ the concern regarding the existence of multiple copies of the electronic transferable record is eliminated, since ownership (i.e., holder status) is not determined by possession of any copy of the electronic transferable record itself and transfer does not involve altering or endorsing those copies.

A. Identifying the person in “control”

45. Where control is used as a substitute for possession, there must be a method for identifying the current party in control of a specific electronic transferable record. This may be accomplished by having evidence of the identity of such person integrated into the authoritative copy itself, or by having the authoritative copy logically associated with a method for tracking the identity of such person (such as a registry), so that a person viewing the authoritative copy is also alerted, and has access, to the evidence of control

46. Thus, the concept of “control” is typically defined in a manner that focuses on the identity of the person entitled to enforce the rights embodied in the electronic transferable record. For example, under United States law: “A person has control of [an electronic] transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.”²¹ The key point is that a system, whether involving third-party registry or technological safeguards, must be shown to reliably establish the identity of the person entitled to payment of a sum of money or delivery of goods.²²

47. Legal systems using “control” as a replacement for “possession” often specifically recognize that the control requirements may be satisfied through the use of a trusted third-party registry system (see below, paragraphs 58-60). Other technological approaches may also be available to achieve the same goal.

48. In general, the primary approaches that have been advanced to establish the identity of the person to whom the electronic transferable record was issued or transferred [i.e., the person in control] include the following:

(a) Person in control identified in electronic transferable record itself (token model). Under the token model approach, the identity of the person in control of the electronic transferable record (the holder) is contained in the electronic transferable record itself, and changes in ownership (e.g., assignments) are noted by modifications made directly to the electronic transferable record. With this approach, establishing the owner of the electronic transferable record requires a system to maintain careful control over the electronic record itself, as well as the process for transfers of control. In other words, like transferable paper, there may be a need for technological or security safeguards to ensure the existence of a unique “authoritative copy,” that cannot be copied or altered,²³ and that can be referenced

²⁰ See discussion of uniqueness at paragraphs 36-42 above.

²¹ UETA § 16 (b); 15 U.S.C. § 7021 (b).

²² UETA Section 16, Official Comment 3.

²³ This might be accomplished by the technology used to create the record (which may not yet exist), or by keeping the record under such security that no one can copy or modify it.

to determine the identity of the owner (as well as the terms of the electronic transferable record itself);

(b) Person in control identified in a separate registry (registry model). Under the registry model, the identity of the owner of the electronic transferable record is contained in a separate independent third-party registry. Under this approach, reliably establishing the owner of the electronic transferable record requires careful control over the registry, and the uniqueness of a copy of the electronic transferable record itself becomes less important or irrelevant as long as a means is in place to verify the integrity of the electronic transferable record. The electronic transferable record merely contains a reference to the registry where the identity of the person with control can be found, and does not change over time or in the event of an assignment. The primary concern regarding the copies of the electronic transferable record is that there is a mechanism to determine whether any particular copy is accurate (i.e., that its integrity is intact) so that anyone viewing the copy is on notice as to where the owner is identified, and so that the true owner identified in the registry can enforce it. In this kind of system, the concept of control and the associated concerns regarding security focus primarily on the registry rather than the transferable record itself;

(c) Person in control defined as person with exclusive access. Where the authoritative copy of an electronic transferable record is stored on a specific secure computer system designed for such purpose and protected by appropriate security and access controls, it may also be possible to define the person in control (i.e., the holder) as the single person given access to the electronic transferable record in question. In such case, a transfer of control would require a transfer of the exclusive means of secure access, such as a unique access token.

B. Adoption of the “control” approach

49. Existing legislative examples relating to electronic transferable records that refer to the notion of “control” include article 1, paragraphs 21 and 22, and articles 50 and 51 of the Rotterdam Rules; article 862 of the revised Korean Commercial Act, enacted on 3 August 2007 (Law No. 9746) (article enabling electronic bills of lading);²⁴ and rule 7 of the Comité Maritime International (CMI) Rules for Electronic Bills of Lading.²⁵

50. Several electronic transferable record laws in the United States of America also make use of the notions of an “authoritative copy” and of “control” to establish the conditions for equivalence to the notions of “uniqueness” and “possession.” They include Uniform Commercial Code (UCC) articles 7-106 (Control of Electronic Document of Title), 7-501 (b) (Warehouse Receipts and Bills of Lading: Negotiation and Transfer) and 9-105 (Control of Electronic Chattel Paper), the Uniform Electronic Transactions Act (UETA), 1999, section 16 (Transferable Records), and the Electronic Signatures in Global and National Commerce Act (E-SIGN), 2000, section 201 (Transferable Records).

²⁴ For a description of the Korean law enabling electronic bills of lading, see A/CN.9/692 at paragraphs 26-47.

²⁵ Available at <http://comitemaritime.org/Rules-for-Electronic-Bills-of-Lading/0,2728,12832,00.html>.

51. Systems that allow the transfer of rights over the goods and against the carrier while cargo is in transit have also emerged in recent years. They operate on the basis that possession of a paper document is replaced by “exclusive control” of an electronic record. Three notable examples are the Bill of Lading Electronic Registry Organisation (Bolero) system, the Electronic Shipping Solutions (ESS) Databridge system, and the Korea Trade Net (KTNET) Registry system. Bolero²⁶ and KTNET²⁷ achieve exclusive control through a title registry. ESS Databridge achieves exclusive control through limiting access to the electronic record in question.²⁸

VI. The registry approach

52. A registry model allows for the creation, issuance and transfer of electronic transferable records based on information transmitted to and recorded in a central registry. Access to the registry might be controlled and might be subject to acceptance of contractual provisions.

53. A registry can be used to assist in the designation of the authoritative copy of an electronic transferable record for purposes of providing a functionally equivalent approach to uniqueness (see paragraph 40 (b) above), and can also be used to identify the person that controls an electronic transferable record for purposes of providing a functionally equivalent approach to possession (see paragraphs 47-48 above).

54. Registry systems, including in electronic form, are currently being discussed by UNCITRAL Working Group VI (Security Interests) in the framework of its work on registration of security rights in movable assets.

55. Registries are also a common feature of most recent initiatives involving electronic transferable records. See, e.g., paragraphs 58-63 below, and A/CN.9/WG.IV/WP.90 December 2000 at paragraphs 39-94.

56. Registry systems may be divided into three main categories:²⁹

(a) Governmental registries. An agency of the State records transfers as public records, and may authenticate or certify such transfers. For public policy reasons, the State agency is usually not liable for any errors, and the cost is borne through user fees;

(b) Central registries. Central registries are established where a commercial group conducts its transactions over a private network (such as SWIFT), accessible

²⁶ Bolero is set up under English Law and is governed by its own private law framework, the Bolero Rulebook. For a description of Bolero, see A/CN.9/WG.IV/WP.90, paras. 75-86.

²⁷ This system was designated as the registry operator for the purposes of the South Korean Presidential Decree on the Implementation of the Electronic Bill of Lading Provisions of the Commercial Act of 2008. For a discussion of the content and workings of this legislation see A/CN.9/692, paras. 26-47.

²⁸ Like Bolero, this system operates under a private law framework, the ESS-Databridge Services and Users Agreement (DSUA). The DSUA is governed by English law but where the contract of carriage in question is governed by US law, transfer of title under the DSUA is governed by the law of the State of New York including the New York Uniform Commercial Code and the United States Uniform Electronic Transactions Act 1999 (T&C 8.1).

²⁹ A/CN.9/WG.IV/WP.67, Annex.

only to its members. This type of registry, which has been used for the various securities settlement systems, is preferred where security and speed are critical, since limited access permits efficient and quick party verification. Access to the actual records of the transactions is usually limited to the users, but summaries of the transactions can be reported publicly in summary form (e.g., in securities trading). The rules of the network usually govern the liabilities and costs. Depending on the jurisdiction concerned, such rules may be of a contractual nature or may have legislative character;

(c) Private registries. These registries are conducted over open or semi-open networks, where the issuer of the document, its agent (as in the systems of electronic warehouse receipts in the United States) or a trusted third party (as in the Bolero System) administers the transfer or negotiation process. The records are private and costs may be borne by each user. Liability parallels the present practice with paper, in that the administrator is obliged to deliver to the proper party unless excused by another party's error, in which case local law may apply. Such systems may be based exclusively or primarily on contractual arrangements (as in the Bolero System) or be derived from enabling legislation (as in the systems of electronic warehouse receipts in the United States).

57. International experience has shown that these categories of registry are complementary, rather than mutually exclusive. Indeed, different types of transactions may require the development of different registry systems. Therefore, a possible desirable approach may focus on the areas that are more likely to benefit from an internationally harmonized legislative framework rather than on the type of registry system used.

A. Examples of existing law utilizing registries

58. Several legal systems for electronic transferable records have adopted, or accommodate, a registry model. One example under United States law is section 16 UETA (governing electronic transferable instruments), which accommodates systems based on registries, and notes in its Official Comments that "A system relying on a third party registry is likely the *most effective way* to satisfy the requirements ... that the [electronic] transferable record remain unique, identifiable and unalterable, while also providing the means to assure that the transferee is clearly noted and identified."³⁰ Another example is article 9-105 UCC (governing electronic chattel paper) which was enacted as a response to requests from the auto financing industry to foster wider use of electronic chattel paper.

59. The Convention on International Interests in Mobile Equipment ("Cape Town Convention")³¹ utilizes an international registry system for registration of various interests in mobile equipment. The Cape Town Convention and the protocols thereto deal in an industry-specific way with remedies upon default of the debtor and introduce a priority regime based on international, equipment-specific registries.

³⁰ UETA Section 16, Comment 3 (emphasis added).

³¹ www.unidroit.org/english/conventions/mobile-equipment/main.htm. See also A/CN.9/692, paras. 18-21.

60. Another recent example is article 862 of the revised Korean Commercial Act, enacted on 3 August 2007 (Law No. 9746), which enables electronic bills of lading.³² It establishes the legal equivalence between paper-based and electronic bills of lading managed in an electronic title registry.

B. Examples of existing registry systems

61. Notable examples of registry systems include the Bill of Lading Electronic Registry Organisation (Bolero) system and the Korea Trade Net (KTNET) Registry system noted at paragraph 51 above. Each of these systems works on the basis that possession of a paper document is replaced by “exclusive control” of an electronic record, where exclusive control is achieved through a title registry.

62. Other examples of registry systems include the MERS eRegistry in the U.S. MERS is an independent industry utility that is intended to track and maintain information on electronic promissory notes in support of home loans. The MERS eRegistry serves as the central (and only) location to identify (i) the current holder of the electronic promissory note, and (ii) the current location of the authoritative copy of the electronic promissory note.³³ It functions as the system of record of rights holders to electronic promissory notes. Any and all subsequent transfers of the electronic promissory notes — i.e., changes in the identity of the entity that owns the note and/or changes of the identity of the entity that maintains the authoritative copy — must also be reflected in the MERS eRegistry.

63. In addition, dematerialized securities systems typically utilize a registry.³⁴ In such systems, the central registry contains a record of the holdings of dematerialized securities and of the rights and restrictions arising therefrom, which are held by depository participants on behalf of investors at any time. Trading intermediaries are normally financial institutions, brokers and other entities authorized to be members of the depository and who hold accounts with the depository.

VII. Possible methodology for the future work by the Working Group

64. With regard to the scope of its work, the Working Group may want to consider whether that work should encompass all types of electronic transferable records in all sectors, or some subset thereof (whether based on type of electronic transferable record, industry sector, or some other criteria). This discussion would allow also for an assessment of the actual market demand for electronic equivalents.³⁵

65. While the progress of its work will allow the Working Group to clarify the final desirable outputs (e.g., a guidance document or uniform law provisions), once the Working Group has determined the scope of its work it might be useful to

³² For a description of the Korean law enabling electronic bills of lading, see A/CN.9/692, paras. 26-47.

³³ From MERS eRegistry Integration Handbook Volume I (Release 2.75 – 7/31/06), Overview of the MERS eRegistry, at p. 4.

³⁴ A/CN.9/WG.IV/WP.90, paras. 45-60.

³⁵ See A/CN.9/728/Add.1, para. 11.

develop a clear set of high-level principles to be incorporated in any international system for electronic transferable records. Such principles will need to address issues relating to cross-border use of electronic transferable records, too.

66. The identification and promotion of such harmonized principles would facilitate the later development of rules for the legal processes involved in the creation, use, negotiation, and enforcement of electronic transferable records. Mechanisms for the transfer or negotiation of rights, including those based on the flow of written documents, show a very similar structure irrespective of the area in which they take place and of the nature and content of the rights concerned. Such similarities will probably increase as the use of electronic means for this purpose becomes more widespread.

67. Moreover, the use of electronic transferable records may vary by sector or business application. Electronic transferable records may, for example, have differing requirements, depending on the application, for authentication, security, access by third parties, conversion from electronic to paper and vice-versa, system cost constraints, transaction ranges, volumes and scalability, mobility, negotiability, party capabilities, automated transaction processing, timeliness and transaction finality, single registries vs. multiple registries (and interoperability and transfers between systems), fraud risk, and evidentiary and regulatory concerns. In addressing these factors, many sectors will rely to a significant extent on private system rules, with associated legislation to address such areas as third-party property rights.

68. Such differing requirements highlight the need to clarify the fundamental considerations in this area as well as to rationalize approaches to solving specific problems. Accordingly, the Working Group could develop basic principles and considerations that will be common to all unique implementation systems, and offer a means to allow the specific needs of each system to be adequately addressed. Those principles could be refined with respect to particular sectors, as appropriate.

69. Within the scope of work it determines appropriate, topics the Working Group may want to consider addressing include:

(a) The ways in which rights in electronic transferable records should be created, transferred, and enforced so as to achieve functional equivalence with transferable paper;

(b) Whether and how electronic transferable records can be converted to transferable paper documents, and vice versa;

(c) The requirements for identifying and verifying the holder of the rights in an electronic transferable record, and the requirements for protecting and verifying the integrity of electronic transferable record;

(d) The use of electronic registries or other third party service providers, recognizing that specific solutions may vary based on sector and application requirements;

(e) The extent to which the issuer of the underlying obligation should be involved in the transfer, negotiation, or conversion of an electronic transferable record and its consequences;

(f) The impact of different modes of transferring of rights an electronic transferable record on the protection to be enjoyed by a third-party transferee in good faith, vis-à-vis both the issuer and other third parties;

(g) The responsibilities of third-party entities such as registries, transaction platform operators, identity providers, certifying authorities and other third-party participants involved in the storage or transfer of an electronic transferable record or identification of the person in control of such a record.
