RESTRICTED

CEFACT/2013/ITXXX
May 2013

UNITED NATIONS
CENTRE FOR TRADE FACILITATION AND ELECTRONIC BUSINESS
(UN/CEFACT)

INTERNATIONAL TRADE PROCEDURES DOMAIN GROUP
Trade and Transport Programme Development Area

Recommendation 14

Authentication of Trade Documents
~~By Means Other Than (a Manual-Ink) Signature~~

SOURCE: **Recommendation 14 Revision Project Team**
ACTION: **Finalized draft (recent changes or points pending discussion in red)**
STATUS: **Draft v0.12**

Foreword

Introduction

The exchange of accurate, complete and timely information is fundamental to the efficient and effective conduct of domestic and international trade. Traditionally the exchange has been conducted by the use of paper-based documents. Increasingly, electronic equivalents to paper have improved the speed and efficiency of data exchange for trading partners, trade services providers, government and other regulatory authorities and agencies.

A constant and continuing objective of the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) is the reduction of documents used in the supply chain between business partners both domestic and international. Where removal is not possible because of legal obligation, regulatory requirement or business need, UN/CEFACT has pursued the objective that the document should NOT require a signature to convey the intent of the party originating it or for the recipient to act on the information contained ion it.

UN/CEFACT recognizes ~~that~~ the aim of removing signature from all trade documents that remain in the supply chain is probably unattainable. Some trade documents will of legal necessity continue to require a signature. The requirements for a signature are tied to the use of paper documents. The ever increasing use of electronic or other automatic means of data transfer makes it desirable to find alternative authentication methods, some of which may eliminate the need for a signature entirely and some may provide the electronic equivalent of a manual-ink signature. Since the first version of this recommendation in 1979, a number of alternative methods of authentication have appeared and will probably continue to appear in the years ahead.

Part ONE: Recommendation 14 on Authentication of Trade Documents ~~by Mean Other Than a Manual-ink Signature~~

1. Scope

This Recommendation seeks to encourage the use of electronic data transfer in international trade by recommending that Governments review national and international requirements for signatures on trade documents in order to eliminate the need for paper-based documents by meeting the requirement for manual-ink signatures through authentication methods that can be electronically transmitted.[1]

Similarly, this Recommendation encourages the trading community and trade services providers to examine business processes to identify where signatures (of any kind) ~~are not required and~~ may be eliminated and for those processes ~~in those~~ where this is not possible, to pursue the electronic transfer of trade data and the adoption of ~~trade related data could be transferred electronically and paper-based documents could be eliminated by adopting~~ authentication methods other than the manual-ink signature.

2. Use of International Standards

The use of international standards can play a key role in larger acceptance of chosen solutions and eventually, interoperability. In so far as possible, governments and private actors who

[1] For the transition from paper documents to electronic equivalents in the various functions of an international trade transaction, see Lauri Railas, The Rise of the Lex Electronica and the International Sale of Goods, Facilitating Electronic Transactions Involving Documentary Credit Operations, Forum Iuris, University of Helsinki, 2004, especially Chapter VIII.

intend to electronically exchange data using an authentication method should try to make use of existing international standards. Technical standards ~~which were able to be~~ identified during the development of this recommendation are referenced in Annex B.

This document is part of a package of recommendations on trade standardization and facilitation (see A~~a~~nnex A3). Electronic data exchange has many aspects which are the subject of several United Nations Economic Commission for Europe (UNECE) current and future recommendations.

The legal codification work in electronic commerce and electronic signature, undertaken by the United Nations Commission on International Trade Law (UNCITRAL) should be taken into account and used, whenever possible as a foundation for developing electronic authentication legal infrastructure for both national and international transactions.

3. Recommendation

~~The United Nations Centre for Trade Facilitation and Electronic Business (~~UN/CEFACT~~)~~ recommends that governments and those engaged in the international trade and movement of goods:

- ~~Should~~ A~~a~~ctively consider the removal of the requirement for a signature (manual-ink or its electronic equivalent) from trade documents except where essential for the function of the document or the activity and refrain from requiring a signature in new rulings or practices.

Further, the UN/CEFACT, recognizing the importance of authentication methods in electronic exchange of trade-related documents, recommends that governments and those engaged in the international trade and movement of goods:

- ~~Should~~ C~~c~~onsider the introduction of electronic methods to authenticate trade documents;
- ~~Should c~~Create a legal or contractual framework that permits and gives equal status to such authentication methods.

In order to achieve this objective, UN/CEFACT recommends:

- A regular review of the documentation used for domestic and cross border trade by a joint public and private sector working party (or sector-specific working parties). The goal ~~aim~~ of the working party would be to ~~aim at~~ eliminat~~e~~~~ing~~ the requirements for a manual-ink signature and where this is not possible, replace the manual-ink signature ~~e it~~ with other authentication methods.

Part TWO: Guidelines for Implementing Recommendation 14

1. Introduction

These Guidelines, which are complementary to UN/CEFACT Recommendation Number 14 on Authentication of Trade Documents ~~by Means Other Than a Manual Ink Signature~~, are designed to assist Governments and Trade in identifying the function and use of signature. They provide an overview of the main issues that should to be addressed, some of the tools that are available and the steps to be taken when moving ~~going~~ towards electronic methods of authentication.

This recommendation will be accompanied by two Annexes ~~which are~~ aimed at assisting Governments and Trade to envision ~~see~~ ways in which electronic methods of authentication have been put in place or are currently implemented. Special attention is made to identify existing standards within these A~~a~~nnexes.

2. Signature

2a. Definition of Signature

The word "signature" in today's vocabulary encompasses both manual-ink signature and its electronic equivalent. The original 1979 version of this recommendation makes no distinction in the title because at that time, a signature was considered to always be manual-ink. As such, ~~This is thus the reason which r~~this term requires further precision in the current recommendation title and throughout this document.

In its broadest sense, a signature (manual-ink or its electronic equivalent) creates a link between a person (physical or legal) and the content (document, transaction, procedure, or other). This link can be considered as ~~having~~ three inherent functions: an identification function, an evidentiary function and an attribution function.[2]

In international business relations, one of the basic foundations is trust between the parties; the requirements of a signature will, in many cases, most likely reflect that trust.

2b. Functions of a Signature

- The i~~I~~dentification function of a signature confirms or allows the establishment ~~o establish~~ of the identity of that signatory; identification can include: the claimed/asserted identity of the person, the veracity of the identity claims, the credentials of any verifying organism, the proof of origin, the time and date, and any other aspect which identifies the related persons or the content.
- The e~~E~~videntiary function of a signature will involve legal implications and can include: integrity, consent, acknowledgement, and detection of any changes in the document after it was signed. It can reflect any level of commitment which the act of signing might have indicated.

---

[2] These ideas of functions are developed in paragraph 7, page 5, UNCITRAL "Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods," United Nations, Vienna 2009. Available as of March 2013 at http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf.
See also "Review of definitions of "Writing," "Signature" and "Document" employed in multinational conventions and agreements relating to international trade, submitted by the Legal Working Group (LWG), Revision of Document Trade/WP.4/R.1096 dated 22 July 1994; TRADE/CEFACT) Geneva, October 2001, ECE/TRADE/240."

- The a~~A~~ttribution function of a signature is the link between the signatory and the document which is signed. This can include the authority granted within the role (i.e. within a company, within a government authority, within the market…) of the signatory.

These three functions can be considered to be on variable levels. There can be more or less of each of these functions inherent in any signature.

2c. Methods of Authentication

A signature or its functional equivalent is a common method of authentication and as such the terms "to sign" and "to authenticate" are used as synonyms in these guidelines.[3]

The usage or the requirement of a manual signature presents major problems for modern high-technology data transfer in those instances where the data is~~are~~ transmitted from the country of purchase to the country of (final) destination and where the manual signature must be available at the clearance of the goods. National legislation and international conventions should be changed wherever they impose a manual signature as a guarantee for the authenticity of information transmitted in this way.

3. Requirement for Signatures on Trade Documentation

In general, there are various uses of a signature on trade documentation. When considering a transaction from a manual-ink signature process to its electronic equivalent, it is necessary to consider the context of the transaction itself.

3a. Considering the L~~l~~egal C~~c~~ontext of the T~~t~~ransaction

Generally, for business to business transactions, the legal requirements can be within the framework of commercial ~~civil and public~~ law. The requirements or trade practices may further be developed or defined by trade organizations for their members. Finally, many requirements within transactions between two independent trading partners will be explicitly defined in bilateral or multilateral agreements.

For transactions with government authorities or among government authorities, the legal requirements are defined almost exclusively within the framework of public law.

There may be several layers of public and private law to be considered: at a federal level, at a state level, at a ministerial level, at an agency level, ~~… a~~at a regional level, at an international level, etc. ~~…~~ It may also be necessary to consider several types of public regulations: commercial regulations, transport regulations, health regulations, customs regulations, etc.

---

[3] Care should be taken when considering the terms presented here in S~~s~~ection 2 (signature, function of signature and authentication). There are often different understandings of these terms depending on the environment (legal or technical). There can be further differences based on the region of the world these terms are being used. In general, signature and authentication in an Information Technology (IT) environment often encompass some inherent functions which can vary from integrity, genuineness, proof, security, etc. ~~…~~ Again, all of these terms can have differing interpretation based on ~~the~~ environment and geography. ~~the region of the world~~.
This recommendation has been prepared to align itself with the works of UNCITRAL while remaining consistent ~~herent to~~with the use of these terms in other UNECE Trade Recommendations.
When reading or drafting any text on the subject, ~~or when drafting any text on the subject~~, clear identification of which approach is being used, is ~~it is~~ recommended ~~to clearly identify which approach is being used~~. For legislators who will probably use a legal definition, ~~it is recommended to make~~ reference to UNCITRAL documents on the subject is recommended in order to clearly identify the legal use of these terms.

Furthermore, a same document may be used by several agencies of a same government, or even of different governments. This may happen for instance, in the framework of single window facilities or coordinated border management. In these cases, the requirements of authentication will need to be aligned so as not to put into doubt the validity of the data which is being communicated.

Legislation must not create stringent requirements which would put in doubt the validity and enforceability of otherwise legitimate transactions.

3b. Trade documents

Several interests can be affected by a chosen method of authentication; these include commercial, transport, financial and official interests. Problems may arise in documents that cross borders as they must be used in two different countries or regions. It should also be ~~recalled~~ noted that the information in some documents may be of interest to more parties than the original and the final recipient of the documents.

Commercial documents can include the commercial invoice, quality and quantity certificate, ~~regarding quality and quantity~~, and shipping advice/notification.~~.~~ ~~The main practice applied in international trade law there are few formal requirement for a signature. Subject to possible requirements of signature in national law, documents required for the practical performance of a contract need not therefore be signed.~~

The use of transport documents often involves a number of parties apart from the carrier, as for example: ~~themselves:~~ exporters, importers, financers, insurers and authorities. The documents can include Bill of Lading, Air Waybill, etc. Many of these documents are covered by international conventions.~~; the tendency is that requirements for a signature are not necessary.~~

Financial documents can include insurance policies or certificates, documents issued for the issue of documentary credit or collections, etc.

Official documents can include customs declarations, import certificates, agricultural certificates, CITES certificates, etc. The acceptance and responsibility to meet official demand often occurs at import in the country of final destination. These needs~~,~~ however, often have a direct bearing on action in the country of purchase at the time of dispatch, or subsequently thereafter.

3c. Determining the N~~n~~eeds of A~~a~~uthentication in the C~~c~~ontext of a T~~t~~ransaction

For transactions with government authorities, it is recommended that a joint public and private sector working party (or sector-specific working parties) be established in order to perform a regular review of the documentation used for domestic and cross border trade. The goal ~~aim~~ of the working party would be to eliminate the manual-ink signature whenever possible and either eliminate~~s~~ its necessity completely, if this is safe and reasonable in the context of the transaction, or replace~~s~~ it with other authentication methods. A list of considerations is proposed in Annex B.1.

For business to business transactions, the two parties can likewise study the needs of authentication in the context of individual transactions. The list of considerations proposed in Annex B.1 should also provide guidance in this context.

4. Use of Eelectronic Aauthentication Mmethods

The choice of other authentication methods will depend on the business process and a risk assessment of the needs of that process. A list of considerations when choosing an electronic authentication method is proposed in Annex B.1.

4a. Technology Neutrality

In so far as possible, legislation should remain technology neutral; it should not discriminate between forms of technology. Technological guidance, when provided, should be based on minimal requirements perhaps with examples, but with the possibility of responding to these requirements with other solutions which would be functionally equivalent. A study of minimal requirements is proposed in Annex B.2.

4b. Levels of Rreliability

As described above, depending on the relationship between the parties and the context of the legal environment, some processes may require more or less security. Not every transaction needs to be the highest level of security. Likewise, technological methods vary and may provide more or less security as required.

The chosen method of authentication should be "as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement."[4]

Efforts should be made to ~~try to~~ avoid creating electronic solutions which are more cumbersome or costly than the manual process. Technology can provide implementations with very high levels of reliability. Implementation choice should be in line with the level of reliability required by the process and existing legal constraints.

4c. Typologies of Eelectronic Aauthentication Mmethods

A number of alternative methods exist that can replace a manual-ink signature. Technology is constantly evolving. Illicit or fraudulent activity is also constantly evolving, finding ways to undermine the level of reliability that might be placed in some aspects of a given method. For this reason, technical standards and technical implementations are further discussed in Annex B of this recommendation in order to facilitate its updating to correspond to current best practices and standards.

Depending on risks, security needs, and other considerations, an authentication method used alone ("single factor authentication") may suffice. In high-risk situations~~,~~ however, an appropriate combination of authentication methods and other techniques may be needed ("multi-factor authentication"). For example, a registration and verification process may be based on an ID/Password for identification accompanied by a Virtual Private Network (VPN) or other electronic method.

4d. Electronic Signature

Almost without exception, all of these methods can generally be referred to as an electronic signature. An electronic signature can be defined as "data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in

[4] Article 7.1, UNCITRAL "Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998" United Nations, New York, 1999, p.5-6. Available as of March 2013 at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html.

relation to the data message and to indicate the signatory's intention in respect of the information contained in the data message."[5]

It should be noted that an electronic signature in this broad sense does not inherently call for a specific form of technology. An electronic signature will serve the same functions as a manual-ink signature, again on a sliding scale ~~so~~ with more or less of each of these functions (that is, identification, evidentiary and attribution).

An electronic signature should not be discriminated because of its origin. It should also not be discriminated ~~just~~merely because it is an electronic authentication method. However, it may be discriminated because of its intrinsic qualities.

A distinction should be made between "electronic signature" as it is used in this guideline and relevant UNCITRAL texts on electronic commerce and "digital signature" which is addressed in the Annex B of this recommendation. For the sake of clarity, it is underlined that these two terms are not interchangeable. The generic term, which makes no reference to any technological choice, and used in UNCITRAL texts on electronic commerce, is "electronic signature," ~~.~~ "Digital signature," ~~,~~ as discussed in UNCITRAL documents, implies that a technological choice has been made (for solutions with asymmetrical encryption, Public Key Infrastructure (PKI) signature technology being the main example).[6] Regulators and those drafting contracts or technical documents, should bear this distinction in mind and ~~prefer~~use the term "electronic signature" unless they intend to imply such a technological choice has been made.

5. Aspects for C~~c~~onsideration of E~~e~~lectronic A~~a~~uthentication M~~m~~ethods

These are some aspects that should be considered depending on the chosen methods of authentication.

5a. Use of T~~t~~hird P~~p~~arty S~~s~~ervices

The parties may prefer or need to call upon a third party to perform any aspect of transmission, archival, retrieval, verification etc. involved in the authentication method. In some cases, third party services are mandated or validated by a government authority (issuing encryption keys, for example). In some cases, third party services offer options to trading partners for full plug-and-play solutions, ~~for~~ data compilation and transmission services, ~~for~~ enhancement of security, ~~for~~ archiving/retrieval services, etc.

In a very general sense, authorization to use a third party service should ~~be able to~~ be granted by either trading partner. In this case, the third party service would be considered an 'intended party' / 'authorized party' in the transaction process. Any limitations to this authorization or the possibility to use a third party service should be clearly outlined in the appropriate legal text, the bilateral agreement between trading partners or agreements with the third party services.

---

[5] Cf Article 2a of the UNCITRAL "Model Law on Electronic Signature with Guide to Enactment 2001," ~~,~~ United Nations, New York 2002, page 1. Available as of March 2013 at: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html. ~~To n~~Note that the original definition in this 2002 document cites the "signatories approval," ~~,~~ Further UNCITRAL work has evolved towards the "signatories intention." ~~,~~ Reference needed?

[6] Cf for example paragraph 21, page 15, UNCITRAL "Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods," ~~,~~ United Nations, Vienna 2009. Available as of March 2013 at http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf.

Where third party services are mandated or validated by a government authority, the requirements to become mandated should be transparent and the process should be open to all.

5b. Security of Dd~~d~~ata

Access to the data should be limited to the intended parties (authorized parties). This can in part be determined by the legal responsibilities of the parties involved.

The requirements of the security of the data will correspond with the level of reliability required by the transaction which should have been determined by a risk assessment considering the process, the operational constraints, the legal constraints and the relationship of trust between the parties. If a trusted third party is acting within the process, they should ensure this same level of reliability. Depending on the determined level of reliability, parties' interests in the event of litigation should be protected.

Depending on the level of reliability, security of the data may encompass ensuring protection and ensuring that data is not deleted or destroyed.

5c. Transmission of Dd~~d~~ata

The aspects of the actual transmission of data will depend on the electronic method chosen. These are presented in the Annex B of this recommendation.

For private business to business exchanges, the two parties should explicitly agree on the method of communication and the method of authentication. They should consider the level of reliability required when establishing this agreement. This could, for example, be part of an Interchange Agreement between the two parties as per the model of UN/CEFACT Recommendation 26.

Depending on the level of reliability, an audit trail may be necessary. In some cases it may be useful or legally necessary to obtain confirmation of transmission / confirmation of receipt, ensuring the order of messages, time stamp, the various headers, etc. This may be required under certain trading partner agreements or in a particular legal context.[7]

5d. Archiving / R~~r~~etrieval

In most cases, trade documents will need to be archived either for later use for other processes, for a trace of the operations, etc. or in order to respond to legal obligations or regulatory requirements (for example the legal requirements to archive electronic invoices or customs declarations). When considering the archiving of trade documents, the party should consider the ~~respect of~~ archiving period, archiving place, and access control. Authentication method for archiving documents could be very different depending on long-term archiving or short-term archiving. Documents archived for long periods may require special attention, as existing authentication methods commonly weaken or even become obsolete over time due to new technologies. Governments or bilateral agreements may want to foresee migration from one technology to another during archiving.

[7] In this regard, reference may be made to article 15 of the UNCITRAL Model Law on Electronic Commerce and article 10 of the Electronic Communication Convention which provide rules on the time and place of dispatch and receipt of data messages.

Archiving methods are expected to correspond to at least an equivalent level of reliability as the authentication/signature method used. The method of archiving should be auditable; in other words, it must be possible to check its reliability to see whether it works or not, to check the correctness of retrieved data and its readability (format used), and to verify that it encompasses the functional aspects of an authentication which is being accepted between the parties and authorities.

The trading partners may wish to call upon a third party service to assist in archival and retrieval of the data; this may be dependent on many factors including technological capabilities and costs. In this case, the third party services should take into consideration the above points. Third party solutions may also have the possibility to issue a certificate with legal effect proving that an authorized party retrieved the data and when it was retrieved, if the level of reliability calls for such provisions.[8]

6. Recommendation Review Process

The present recommendation is divided into the recommendation text, guidelines and annexes (which include repositories). It is suggested that the annexes and repositories are updated every three to five years. This will entail contacting each initial contributor to verify that the information is still pertinent / up-to-date (absence of a response should result in the elimination of the submission from the annex). Following the response from the contributor, the information in the annex should be confirmed, revised or eliminated as the case may be. This will also be an opportunity to request new submissions for the annexes and integrating any other contributions.

Once all of the annexes and repositories have been updated, it is suggested that ~~to verify the~~ the content of the recommendation and its guidelines be verified against the revised annexes. If there are no (or very minor) modifications, ~~then~~ it may be best not to update the recommendation in the interest of trying to keep a stable version. If there are elements from the annexes and repositories which contradict or render obsolete / erroneous the recommendation text, then it should be modified.

This procedure being said, if Governments or Trade bring substantive concerns as to the pertinence of the text of the recommendation, this should be considered for purposes of text revision even outside of the updating periods.

7. Other Options than a Manual-Ink Signature

This chapter aims to bring further precision to the three main recommendations of this document.

7a. Removal of Manual-Ink Signatures and their Electronic Equivalent When Possible

It is recommended ~~to~~that Governments and ~~to~~ all organizations concerned with the facilitation of international trade procedures ~~to~~ examine current commercial documents~~,~~ to identify those where manual-ink signatures and their electronic equivalent could safely be eliminated and to mount an extensive program of education and training in order to introduce the necessary changes in commercial practices.

[8] In this context, reference may be made to article 10 of the UNCITRAL Model Law on Electronic Commerce which provides a rule on retention of data messages.

This removal of the requirements for a signature should be studied on a case-by-case basis for each given commercial document. Where signature is not essential for the function of the document or the transaction, then it is recommended that these requirements be removed.

Furthermore, when creating new trading environments or documents, it is recommended to naturally refrain from introducing requirements for signatures in new regulations, rulings, contracts or practices.

7b. Enabling Eelectronic Mmethods of Rreplacing a Mmanual-Iink Ssignature

It is recommended to Governments and international organizations responsible for relevant intergovernmental agreements to study national and international texts which embody requirements for signature on documents needed in international trade and to give consideration to amending such provisions, where necessary, so that the information which the documents contain may be prepared and transmitted by electronic means.

Amending the relevant provisions in every legal text where a signature is mentioned is not feasible given the very high number of occurrences. In order to resolve this at the national level, it is recommended to adopt legislation establishing functional equivalence between electronic and paper-based signatures such as that based on the UNCITRAL Model Law on Electronic Commerce and on the UNCITRAL Model Law on Electronic Signatures. This blanket provision would reinterpret any reference to signature or authentication as meaning the possibility to allow for their functional electronic equivalent. At the international level, the same result may be achieved with the adoption of the United Nations Convention on the Use of Electronic Communications in International Contracts, 2005 (article 9(3)).[9] Since the Convention applies to international transactions only, it is also recommended to create a concurrent legal text for domestic transactions with such a blanket provision which would reinterpret any reference to signature or authentication as encompassing their functional electronic equivalent.

It is suggested that the paper-based process be identified and that this process be detailed step-by-step. Risk-assessment should be a guiding principle, considering the context of the transaction/service, the legal constraints, the operational constraints, etc. ... Parties should be permitted and encouraged to fulfill functional requirements of a manual-ink signature by using other methods.

7c. Creation of Legal Framework

Examples of legally enabling environments are provided in Annex A. The operational capability of replacing a manual-ink signature by an electronic method must be accompanied by appropriate legislation which gives equal status to those authentication methods. This legal framework should foresee the acceptability in court of alternative transmission methods and archiving processes. Two main aspects may need to be addressed either jointly or separately: the legal framework for private-sector operations and the legal framework for operations between the private sector and government agencies.

Concerning operations between private businesses and between business and consumers, governments should undertake a study (including e-Commerce legal benchmarking and "gap analysis" studies) to determine an appropriate set of measures that may need to be taken to

[9] "United Nations Convention on the use of Electronic Communications in International Contracts" (Electronic Communications Convention [ECC]) United Nations, New York, 2007. Available as of March 2013 at: http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf

address legal issues related to authentication of national and cross-border exchange of trade data.

Concerning operations between business and government agencies, the government, at the highest level, must first provide the legislative mandate for agencies to provide the option for electronic maintenance, submission, or disclosure of information, when practicable as a substitute for paper. As part of this mandate, the Government should, in consultation with other agencies and the private sector, develop practical guidance on the legal considerations related to agency use of electronic filing and record keeping so that the agency can in return, make the appropriate assessment for its mission. Consideration should be given by the agency on how to design the process to protect the agency's legal rights and how best to minimize legal risks to the agency.

Government should, when possible, provide guidance to the private community on this issue. Any guidance provided by the Government and/or the specific agency should also take into consideration current legal requirements pertaining to the use, storage and disclosure of information, and its use as evidence in courts or administrative bodies.

The legislative frameworks should be reviewed regularly in order to correspond to actual business practices. Public law should aim, whenever possible, to align with current way of doing business and with current best practices and standards.

Annex A – Legally Enabling Environment.

1. Recommended checklist for government agencies when reviewing their legal environment~~?~~

- Compliance with applicable laws and regulations?
- Compliance under confidentiality laws?
- Comprehensive plan to address all issues raised by moving to an electronic system?
- Consultation with impacted parties, including other relevant offices and agencies?
- Is any information used in the process required by law or regulation to be in a particular form, paper or otherwise? If part of the process is paper, how will this be satisfied?
- Is there a legal requirement or an agency need to maintain the information? And if so, for how long?
- Is the information of importance to national security, public health or safety, public welfare, the protection of the environment, or other important public purposes?
- Is there impact to the public if this information is not available?
- What is the importance of the information to the agency's mission/ programs?
- Is there a revenue impact to the agency?
- Might the information be needed for use in criminal proceedings or other legal proceedings?

2. Virtuous Circle for the Review of Commercial Documents

To achieve the objective of removing the requirement for a signature on commercial documents, or where that is not immediately possible, to consider other methods of authentication, Recommendation 14 recommends a regular review of the documents used in domestic and cross border trade. The review would be conducted by a joint public and private sector working party to ensure that the regulatory and official requirements and the business needs of the trading community are fully considered in an open, transparent and inclusive way.

The suggested methodology of the working party is shown in the figure below:

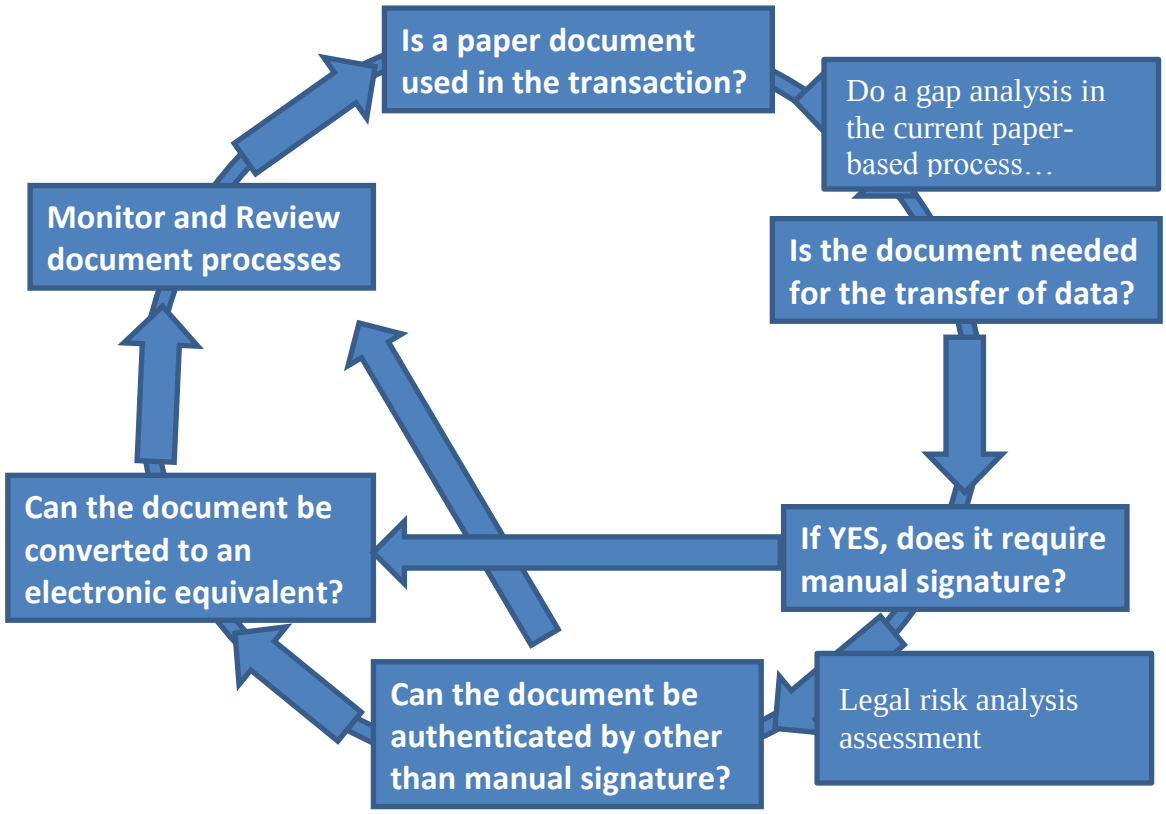

Figure 1

The 'virtuous circle' diagram envisages a rolling programme of review for all documents used in domestic and international trade conducted every three to five years. For ease of conducting the programme and utilizing the expertise of the participants in the working party, the documents should be divided into specific functional groups, for example Commercial, Transport, Financial (including international payments) and Official. The suggested divisions are indicative and not exhaustive.

A schedule or calendar for the document groups should be agreed by an oversight or supervisory committee to ensure consistency of methodology and outputs from each group. Adopting this approach should make the review programme manageable, efficient and effective. Equally a structured programme should reduce the time and burdens on participants of the individual review groups.

The outcome from the rolling programme would be an action plan to remove the requirement for a signature from a significant number of trade documents. Where this is not immediately possible the action plan should offer imaginative an innovative ways of replacement by other authentication methods. In this respect the members of the review groups should embrace the concept of simpler, easier trade processes through radical yet well informed and considered solutions.

3. Trade Documents Standards Package

UN/CEFACT provides a suite of products that offer recommendations, guidance, advice and good practices for the design, preparation and presentation (including electronic submission) of trade documents used in domestic and cross-border trade. Recommendation 14 is one of the instruments in this suite of products and the diagram below, figure 2, gives a graphical

representation of its related position in the integrated package of standards for trade documents.

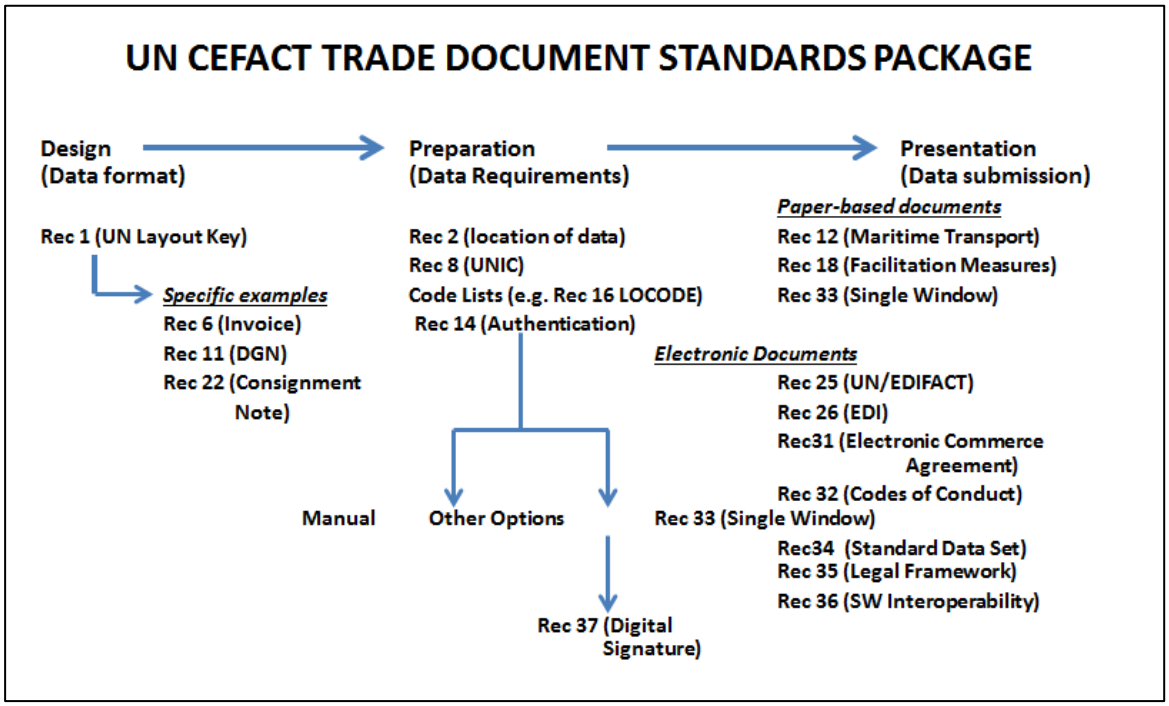

Figure 2

4. Examples from countries in ISO-country alphabetical order.
5. Examples from industries and other

Annex B – Technical Implementations.

1. Checklist of C~~c~~onsiderations to D~~d~~etermine the N~~n~~eeds of A~~a~~uthentication in the C~~c~~ontext of a G~~g~~iven T~~t~~ransaction

~~It is suggested to take into consideration~~ T~~t~~he following key points should be taken into consideration when determining the needs of authentication. This list should be applicable to transactions with government authorities as well as business to business transactions.

- Context considerations
  - Is a signature required at all to authenticate the commercial document?
  - Is an electronic transmission of the document suitable?
  - Kind of transaction
  - Volume (number of) transaction
  - Volume (value of the) transaction
  - Frequency at which the commercial transactions take place
  - Nature of the trade activity (who are the parties, the sector of activity)
  - Cost and benefits
  - Compliance with trade customs and practice
  - ~~(after reviewing the paper-based process)?~~
    - ~~Assessment of whether the current paper based process requires improvement/change, and incorporating those changes in the electronic environment~~
- Technological considerations
  - System and equipment capabilities and their possible interaction (hardware/software)
  - When using an intermediary, the authentication procedures made available and set forth by them~~;~~ (audit procedure?)
  - What are the potential threats / risks / vulnerabilities to attacks?
  - What are the strengths of each alternative authentication method?
  - Compatibility issues of authentication methods
  - Analysis of existing technology and usability of that technology for purposes of data retention and/or future access
- Legal considerations
  - Legal context (national [local, federal…], regional, international, sectorial, jurisprudence, private law… as described above in point 3a)
  - Adherence to the UNCITRAL Model Law on Electronic Commerce or Electronic Signature which enable mutual recognition of authentication methods.
  - International agreements / bilateral or multilateral mutual recognitions (for example recognition of standards, of financial arrangements, interoperability issues, etc.)
  - Awareness of legal concerns and/or regulatory restrictions in each trading parties' environment
  - Does the transaction require legal validity or is the authentication merely for enhancing security?
  - The existence of insurance coverage mechanisms against unauthorized communications~~;~~
- Relationship considerations
  - Determination of the level of protection needed and the potential of risk of liability for the agency / trading party

- ~~the~~ Iimportance and the value of the information contained in the electronic communication~~;~~
- ~~the~~ dDegree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the electronic communication was communicated~~;~~
- Relationship between the trading parties (trust, etc.)

2. Overview of Mminimal Rrequirements

Proposed chart of minimal requirements study

	Minimal requirements															
Authentication typologies																
Biometric methods																
"Click through process"																
Communication channel																
Devices (smart phone)																
Digital Signatures																
Electronic seals																
ID/Password																
Registration / Verification																
Scanned signature																
"Something I know"																
Structural agreement																
3rd party validation																
Tokens																
Typed signature																

[For each minimal requirement, each typology should respond if it is (0) impossible to comply; (1) sometimes possible to comply depending on the system; (2) possible to comply; (3) recommended to be an attribute of this typology, so it will comply; (4) an inherent quality of this typology, so it will comply]

3. Typologies of Eelectronic Eequivalents to a Mmanual-Iink Dsignature

The different typologies of electronic equivalents to a manual-ink signature can include (this is a non-exhaustive list and there is no promotion intended in any of these methods):

- Biometric methods
- "Click through process"
- Communication channel (for example VPN)
- Devices (authentication with a smart phone, for example)
- Digital signatures (encryption, PKI)
- Electronic seals
- ID/Password
- PGP
- Registration & verification process
- Scanned signatures
- Signatures on PADs
- "Something I know"
- Structural agreement enabling electronic data exchange with no authentication

- Third-party validation / Trusted-third parties
- Tokens
- Typed signatures

Recommendation 14 "Authentication of Trade Documents by Means Other Than a Manual-Ink Signature"

Template for comments and observations

Please return completed templates to Working Group Chair, Lance THOMPSON: lance.thompson@conex.net

Date submission:	

Please make all comments using this template.
Please propose suggested changes in order to make the Recommendation Draft align with your comments.

Ref. (leave blank)	Draft version number	Line numbers	Type of comment[1]	Comments	Proposed changes	Working Group Observations (leave blank)

[1] Types of comments: ge = general; te = technical; le = legal; ed = editorial
(This document is inspired by the ISO/IEC/CEN/CENELEC electronic balloting commenting template/version 2012-03)