RESTRICTED
CEFACT/2013/ITXXX
April 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: **Nearing a finalized draft for experts' consideration**
STATUS: **Draft v0.9**

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 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 on it.

Obviously, UN/CEFACT recognizes that the aim of removing the signature from all documents that remain in the supply chain is probably unattainable. Some documents will of legal necessity continue to require authentication. The requirements for a signature are tied to the use of paper documents; it is unlikely that paper documents will be eliminated completely in the near future. That said, the ever increasing use of electronic or other automatic means of data transfer makes it desirable to find alternative ways of authentication, 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 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 or guarantees that can be electronically transmitted.

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 trade related data could be transferred electronically and eliminate paper-based documents by adopting other methods of authentication 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 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.

The United Nations 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 actively consider the removal of the requirement for a signature (manual-ink or its electronic equivalent) from trade documentation except where essential for the function of the document or the activity and refrain from requiring the signatures in new rulings or practices.

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 aim of the working party would be to eliminate the manual-ink signature and replace it with other authentication methods.

Further, the United Nations Centre for Trade Facilitation and Electronic Business (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 consider the introduction of methods to authenticate trade documents electronically;
- Should create a legal or contractual framework that permits and gives equal status to authentication methods other than manual-ink signature.

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 available and the steps to be taken when going towards electronic methods of authentication.

This recommendation will be accompanied by two Annexes which are aimed at assisting Governments and Trade to 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 annexes.

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. This is thus the reason which 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 content (document, transaction, procedure, or other). This link can be considered having three inherent functions: an identification function, an evidentiary function and an attribution function.[1]

With very few exceptions, a signature is not self-standing. 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

- Identification function of a signature is a process & data that confirms or allows to establish the identity of that signatory and/or the content. The 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.
- Evidentiary function of a signature. This usually will involve the 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.
- Attribution function of a signature. This is the link between the signing party or that which is authorized by 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.

[1] 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.

These three functions can be considered to be on variable scales. There can be more or less of each of these functions inherent in every signature (manual-ink or its electronic equivalent).

2c. Authentication of a document

(Illustrate what authentication achieves in the paper world – functional equivalent in electronic world).

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 parties involved in the transaction

In a business environment, considering two trading partners, trade documents can be summarized into the following categories:

- Documents authenticated by both trading partners, principally used by both trading partners
  - For example: Commercial contracts, Service agreements…
- Documents authenticated by one trading partner, principally used by the other trading partner
  - For example: Authorization requests, Written guarantees, Transport Orders, Lodging an appeal, Purchase order, Order to pay, …
- Documents authenticated ~~by a 3rd party~~, principally used by one or both of the trading partners
  - For example: Audit report, Legal statement, Certificate of origin, Bank guarantee, Authorizations, Permits, Formal Publications

Of course, any of these documents may be used or referenced by a 3rd party for a number of reasons such as fiscal or trade control purposes.

The relationship between these two trading partners will probably also entail some level of inherent trust which most likely is reflected in their bilateral exchanges.

3b. Considering the legal context of the transaction

Generally, for business to business transactions, the legal requirements can be within the framework of 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… at a regional level, at an international level… It may also be necessary to consider several types of public regulations: commercial regulations, transport regulations, health regulations, customs regulations, etc.

Furthermore, in the framework of single window initiatives, a same document may be used by several agencies of a same government, or even of different governments. 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.

3c. Determining the needs of authentication in the context of a ~~given~~ transaction

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 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 any given transaction. The list of considerations proposed in Annex B.1 should also provide guidance in this context.

4. Use of electronic authentication methods

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 at the (highest?) general level should remain technology neutral; such laws should not discriminate between forms of technology. It is suggested that technological guidance should be based on minimal requirements perhaps with examples, but with the possibility of responding to these requirements with other solutions which would be semantically equivalent. A study of minimal requirements is proposed in Annex B.2.

4b. Levels of reliability that a document is authentic

Not every transaction needs to be the highest level of security. 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. 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."[2]

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 electronic methods

[2] 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.

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 VPN or other electronic method.

4d. Electronic Signature

Almost without exception, all of these methods can generically 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 relation to the data message and to indicate the signatory's intention in respect of the information contained in the data message."[3]

Please note 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 more or less of each of the 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 because it is an electronic method of authentication. However, it may be discriminated because of its intrinsic qualities.

A distinction should be made between "electronic signature" as it is defined here (and in UNCITRAL documents) and a "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, used within UNCITRAL documents is "electronic signature". "Digital signature", as defined in UNCITRAL documents implies that a technological choice has been made (for solutions with asymmetrical encryption, PKI signature technology being the main example).[4] Regulators and those drafting contracts or technical documents, should bear this distinction in mind and prefer the term "electronic signature" unless they intend to imply such a technological choice has been made.

5. Aspects for consideration of electronic methods of document authentication

---

[3] 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 note that the original definition in this 2002 document cites the "signatories approval". Further UNCITRAL work has evolved towards the "signatories intention". Reference needed?

[4] 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.

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

5a. Use of third party services

The parties may prefer or need to call upon a third party to perform any aspect of transmission, archival, retrieval, etc. involved in the authentication method. In some cases, the third party services are mandated or validated by a government authority (issuing encryption keys, for example). In some cases, the third party services offer options to trading partners for full plug-and-play solutions, 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 either in the appropriate legal text or the bilateral agreement between trading partners.

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 data

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.

5b. Transmission of data

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, the history of the data should be traceable. In some cases it may be useful or legally necessary to obtain confirmation of sending / confirmation of receipt of the transmission. This may be required under certain trading partner arrangements or in a given legal context.

5c. Archiving / retrieval

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 (for example the legal requirements to archive electronic invoices or customs declarations). When considering electronic methods of transmission and the authentication methods used, the archival duration period must be taken into consideration. Any specific technology used, or their functional equivalents, must be maintained during the entire archival period. Governments or bilateral agreements may want to foresee migration from one technology to another during archiving. Documents archived for long periods may require special attention, as existing authentication methods commonly weaken over time due to new technologies and heightened computing power.

Archiving methods must 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), to verify that it encompasses the functional aspects of an authentication which is being accepted between the parties.

Only authorized parties should be able to archive and retrieve the data. In this case, the third party solution 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.

6. Recommendation review process

The present recommendation is split into the recommendation text 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 to verify the content of the recommendation and its guidelines 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 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 Governments and to all organizations concerned with the facilitation of international trade procedures to examine current commercial documents, to identify those

where 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.

This removal of the requirements for a signature should be studied on a case-by-case basis for each given commercial document. Where the manual-ink signature or its electronic equivalent 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 electronic means of replacing a manual-ink signature

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 (apply to) 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)).[5] 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 (apply to) 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… Parties should be permitted and encourage 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 these other 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

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

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

Annex B – Technical Implementations.

1. Checklist of considerations to determine the needs of authentication in the context of a given transaction

It is suggested to take into consideration the following points 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 trade document?
  - Is an electronic transmission of the data suitable (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
  - (b) the nature of their trade activity;
  - (c) the frequency at which commercial transactions take place between the parties;
  - (d) the kind and size of the transaction;
  - (i) compliance with trade customs and practice;
- Technological considerations
  - (a) the sophistication of the equipment used by each of the parties;
  - (f) the capability of communication systems;
  - (g) compliance with authentication procedures set forth by intermediaries;
  - (h) the range of authentication procedures made available by any intermediary;
  - Assessment of costs and benefits / (l) the availability of alternative methods of identification and the cost of implementation;
  - (m) the degree 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;
  - What are the potential threats / risks?
    - Have vulnerabilities or attacks been experienced or identified under existing systems? Does a move to a new system create additional vulnerabilities?
  - 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
  - Does the transaction require legal validity or is the authentication merely for enhancing security?
  - Context of national civil and public laws on all levels described above / (e) the function of signature requirements in a given statutory and regulatory environment;
  - International conventions
  - Awareness of legal concerns that might restrict the process
  - Awareness of current legislative and/or regulatory restrictions
  - (j) the existence of insurance coverage mechanisms against unauthorized communications;
  - Determination of the level of protection needed and the potential of risk of liability for the agency / trading party
- Relationship considerations

- (k) the importance and the value of the information contained in the electronic communication;
- Relationship between the trading parties (trust, etc.)

2. Overview of minimal requirements

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 electronic equivalents to a manual-ink signature

The different typologies of electronic equivalents to a manual-ink signature can include (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
- "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)