Part 1	Authentication of Trade Documents by Means Other Than a (Manual-Ink) Signature
1.	Introduction
2.	Scope
3.	Benefits
4.	Recommendation

Part 2	Guidelines for going towards electronic methods
1.	Introduction

2.	Definition and function of a signature

Link between a person and a document & having the following functions

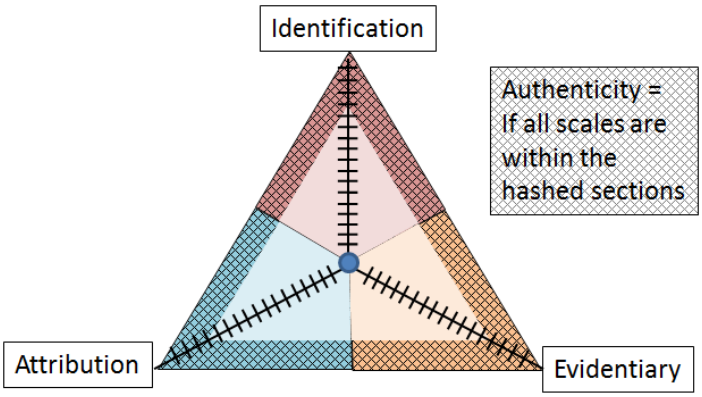
FUNCTIONS of a signature

- Identification
- Evidentiary
  - (Depending on the legal implications can involve: integrity, consent/commitment, acknowledgment)
- Attribution
  - (link between signature and signatory) / (link between signature to the content)

These three functions are on a variable scale (there can be more or less of each of these inherent in each signature)

If a certain level of all three of these are correctly fulfilled, then authenticity can be achieved

Suggestions of graphic explanation of this variable scale (This or another suggestion, or no graphic):



Definition of an Electronic Signature

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.

An electronic signature should not be discriminated because of its origin. (but may be discriminated because of their intrinsic qualities).

Document authenticity (as opposed to signature of a moral/physical person)

Origin & integrity of the document (but does not necessarily look at the signatory)

Authenticity = quality of the document / data

Authenticity & integrity can be improved in the electronic environment.

3. Requirements for signatures on trade documentation

Considering the requirements for signature on trade documentation

Regular review of documentation used for domestic and cross border trade, possibly by a joint public and private sector effort.

Organizational decision to be made (*Consensus so far for Suggestion 2*):

Suggestion 1:	Suggestion 2:	Suggestion 3: Eliminate examples from this section
Organize by doc types (like 1979 version) • Commercial doc • Transport doc • Financial doc • Official doc	Organize by typology • B2B, • B2C (business to consumer), • B2G/G2B, • G2G…	(Citing specific procedures will inevitably lead to leaving some out… and will necessitate a more regular review of the recommendation for updates)

OR

OR

4. Other options than a manual-ink signature

Removal of the requirements for a signature

Removal of the requirement for a signature except where essential for the function of the document

Recommends to all organizations concerned with the facilitation of international trade procedures to examine current commercial documents, to identify those where signature could safely be eliminated and to mount an extensive program of education and training in order to introduce the necessary changes in commercial practices.

(Perhaps bring in the idea to "avoid" a signature instead of remove)

Need more explanation of the "removal" in order to be avoid misinterpretation. The current text is perhaps not sufficient.

Introduction of other methods to authenticate documents

Recommends 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 or other automatic means of data transfer

Governments should seek to meet any such requirements through authentication methods or guarantees that can be electronically transmitted

Identify paper-based process for which conversion to dematerialization is sought and map out the process including associated risks

Use risk-assessment as a guiding principle

Parties should ("feel free" / "be permitted") to fulfill functional requirements of a signature by using other methods.

Creation of a legal framework that permits and gives equal status to authentication methods other than [manual-ink] signature

Government should create and maintain appropriate legislative frameworks

Governments should provide the private community guidance on this issue

Policies can be catalyst for change in the area of electronic exchanges

The legislative frameworks should be reviewed regularly (10 years?) in order to correspond to actual business practices

Public law need to be aligned with current way of doing business & with current best practices and standards

5. Use of other authentication methods

Choice of other authentication methods will depend on the business process and a risk assessment of the needs of that process

Technology Neutrality

Common understanding of semantics of information being exchanged
Must not create stringent requirements which would put in doubt the validity and enforceability of transaction (UNCITRAL, Promoting Confidence, p.30§66)
To achieve the technology neutrality, the law should not discriminate between forms of technology.

Levels of Assurance

Check for alignment with ISO/IEC 29115 "Entity Authentication Assurance Framework" (4 levels of assurance)

Not every process needs to be "certified mail". Some processes require more or less security…
Based on risk assessment
Should consider the context of the process (trade document)
Should consider not only operational constraints but also legal constraints.

These levels are not necessarily straightforward. An electronic method may be high for some functions of signature, but not for all functions…

Check if a matrix can use the three functions of a signature described elsewhere (identification, evidentiary, attribution), or if other aspects must be considered?

Typologies of electronic methods that can replace a manual-ink signature for purpose of authentication of trade documents

The structure of this typology will most likely be the organization of the future Annex B / Repository of actual implementations

Authentication can be any combination of these (one single method or a combination of methods)

Digital signatures (encryption)
Electronic seals
Biometric methods
Devices (authentication with a smart phone, for example)
Tokens
ID/Password
Scanned signatures
Typed signatures
"Click through process"
"Something I know"
3rd party validation
Communication channel (for example VPN)
Registration & verification process (can result in ID/Passwords, VPN or other electronic method)

6. Security of data, transmission, archiving, retrieval

Security of data

Access to data should be limited to intended parties
Legal responsibilities of the parties involved
Depending on the level of assurance required by the transaction, parties' interests in the event of litigation should be protected

Depending on the level of assurance required, trusted third parties should guarantee the corresponding level of confidence.

Transmission of data

Whenever possible, use of international standards

In a bilateral exchange, the two parties should explicitly agree on the method of communication and the method of authentication.

They should consider the level of assurance required when establishing this agreement.

Minimal requirements for data transmission are presented in Annex 2 with the appropriate technological solutions with an aim towards promoting interoperability.

Confirmation of sending / Confirmation of receipt of the transmission.

Archiving / retrieval

Must take into account archival duration period

The technology used must be maintained during the entire period (or functional equivalent)

Migration from one technology to another during archiving.

Archiving method must correspond to at least an equivalent level of assurance as the authentication/signature method used

The method of archiving should be auditable (checking the reliability – whether it works or not; checking correctness of retrieved data, readability [format used]; & encompassing the functional aspects of a authentication which is being accepted between the parties …)

Only authorized parties should be able to retrieve the data.

Possible use of third-party archiving solutions which take into consideration the above points.

The 3rd party archiving system can issue a certificate with legal effect proving that an authorized party retrieved the data.

7. Recommendation review process

Suggestions for future review of the present recommendation

The present recommendation is split up into the recommendation text, annexes and repository.

It is suggested that the annexes and repository is 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 response should result in eliminating the submission from the annex). And confirming, revising or eliminating the information as the case may be.

This will also be an opportunity for other contributors to be integrated into this work.

Then once all of the annexes and repository have been updated, verify if the updated content modifies in any way the text of the recommendation. If there are no (or very minor) modifications, then the recommendation should not be updated. Otherwise, it should be modified.

This procedure being said, if the industry brings concerns as to the pertinence of the text of the recommendation, this should be considered for revision even outside of the updating periods.

Annexe A Legally Enabling Environment

1. Checklist for the creation of a Legally Enabling Environment

2. Template for submission of Legally Enabling Environments

3. Legally Enabling Environments (organized in alphabetical order by country code, followed by any international organizations)

Annexe B	Technical implementations that allow the elimination of a (manual-ink) signature from trade documents
1.	**Existing international standards in the domain**
2.	**Guidelines for submissions to the "Actual Implementation Repository"**
3.	**Actual Implementation Repository (organized into sections according to the typologies of electronic methods outlines within Part 2, chapter 5)**
	Each section of the repository to be composed of: Checklist of functional requirements / minimal requirements (based on international standards and submissions) Suggestions of ways forward towards interoperability within the method of the section Actual implementation submissions (organized in order of receipt)