United Nations ECE/TRADE/C/CEFACT/2013/MISC.2

Economic and Social Council

Distr.: General
17 May 2013

Original: English

Economic Commission for Europe

Committee on Trade

Centre for Trade Facilitation and Electronic Business

Nineteenth session
Geneva, 5-7 June 2013
Item 3 of the provisional agenda
Bureau overview of developments

Follow-up to decision 12-11: issues concerning a possible framework for the governance of digital signature interoperability standards and recommendations

Submitted by the UN/CEFACT Bureau for information

Summary

This informal note for information follows up on Decision 12-11 of the eighteenth session of the UN/CEFACT Plenary. It addresses issues concerning a possible framework for the governance of digital signature interoperability standards and recommendations. As requested by the Plenary, it has been prepared by the Vice-Chair with Programme Development Area responsibilities for Methodology and Technology.

Contents

I. Introduction

1. This informal note is submitted to the nineteenth session of UN/CEFACT for information. As requested by the Plenary, it was prepared by the Bureau Vice-Chair with Programme Development responsibilities for Methodology and Technology in response to UN/CEFACT decision 12-11 as recorded in the summary report of the eighteenth session (ECE/TRADE/C/CEFACT/2012/12, p.5, para. 30):

> "The Plenary discussed draft Recommendation No. 37 on Signed Digital Document Interoperability (ECE/TRADE/C/CEFACT/2010/14/Rev.1 available in English, French and Russian). The Plenary recognized that the project team had completed the Open Development Process (ODP) before submitting draft Recommendation 37 to the December 2010 Plenary and subsequent revisions 2 up until November 2011. The Plenary thanked the team for their work. The Plenary decided:
>
> - that the process would continue under the direction of the Bureau Vice-Chair responsible for Methodology and Technology;
> - to initiate work to establish a framework for the on-going governance of digital signature interoperability in coordination with the United Nations Commission on International Trade Law (UNCITRAL), ISO and other relevant organizations;
> - to request that the structure of this framework be established by November 2012, and;
> - to include in the structure a plan that will enable Draft Recommendation 37 [Signed Digital Document Interoperability] to be put before the Plenary for intersessional approval. (Decision12-11)."

2. To summarize the events since February 2012, the Bureau Vice-Chair drafted this information note, and in preparing it pursued informal contacts with the United Nations Commission on International Trade Law (UNCITRAL), the International Organization for Standardization (ISO) and other organizations. As the discussions remain ongoing, it was not possible to conclude them by the Plenary's requested date of November 2012.

3. On the other hand, the last point raised by the Plenary has already been addressed; as the Project Team for the revision of Recommendation 14 (Authentication of Trade Documents by Means Other Than Signature) envisages that the work on draft Recommendation 37 will be included as one of the annexes to Recommendation 14 when it is published.

4. This informal document is presented under item 3 of the draft agenda of the nineteenth session of UN/CEFACT as part of the Bureau overview of recent developments. Following any Plenary discussion, further steps may be taken towards addressing Decision 12-11.

II. Scope

5. This document proposes a possible framework for the governance of digital signature interoperability recommendations and standards. Possible coordination with UNCITRAL, ISO and other organizations may be considered later on.

6. The framework mainly aims to set out possible conditions for achieving the interoperability of digital signatures for international trade by describing the roles and responsibilities for the governance of relevant standardization efforts.

7. It is based on three fundamental principles: non-discrimination, technology and geographic neutrality and functional equivalence. However, it should be pointed out that as some of the issues discussed refer to the application of a specific type of technology – digital signatures – the focus is, by definition, not technology-neutral.

8. It does not promote or endorse the use of digital signatures. Its purpose is to raise awareness of work going on in relevant standardization organizations which may encourage greater interoperability of digital signatures if used for cross-border trade.

9. The proposed framework could be applied when developing all UN/CEFACT Recommendations and Business Standards in the areas of authentication, security, integrity, non-repudiation and reliability for the exchange of business documents used in international trade.

10. It also identifies possible roles and responsibilities that may involve others outside of UN/CEFACT.

11. It could be promoted to organizations with those roles and responsibilities.

12. A key condition of such arrangements would be the provision of standards unencumbered by licence fees.

III. Terminology

13. In this documentation, the following terms are defined:

(a) An **electronic signature** is data in electronic form, 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 (see Article 2 (a) of UNCITRAL Model Law on Electronic Signatures and Article 9 of United Nations Convention on the Use of Electronic Communications in International Contracts).

(b) A **digital signature** is one type of electronic signature. "Digital signature" is a name for technological applications using asymmetric cryptography, also referred to as public key encryption systems, to ensure the authenticity of electronic messages and guarantee the integrity of the contents of these messages. This is commonly implemented using a set of services collectively known as a Public Key Infrastructure (or PKI). The digital signature is widely regarded as a particular technology for "signing" electronic documents. However, it is at least questionable whether, from a legal point of view, the application of asymmetric cryptography for authentication purposes should be referred to as a digital "signature", as its functions go beyond the typical functions of a handwritten signature. The digital signature offers means both to "verify the authenticity of electronic messages" and to "guarantee the integrity of the contents." Furthermore, digital signature technology does not merely establish origin or integrity with respect to individuals as is required for signing purposes, but it can also authenticate, for instance, servers, websites, computer software or any other data that is distributed or stored digitally, which gives digital signatures much broader use than an electronic alternative for handwritten signatures.[1]

[1] Babette Aalberts and Simone van der Hof, *Digital Signature Blindness: Analysis of Legislative Approaches toward Electronic Authentication* (November 1999), p. 8, available at

IV. Digital signature interoperability

14. Interoperability of digital signatures aims at increasing the level of interoperability of digitally signed information as a means of facilitating paperless international trade. This includes the cross-border recognition of foreign digital signatures.

15. Recent activities in the area of standardization to support interoperability of digital signatures have led the UN/CEFACT Plenary to realize that the international trade environment lacks a recognized framework for developing these standards and recommendations.

16. This document provides the Plenary with a possible framework based on the principles of interoperability being identifiable as separate layers: legal, business requirement and technical.

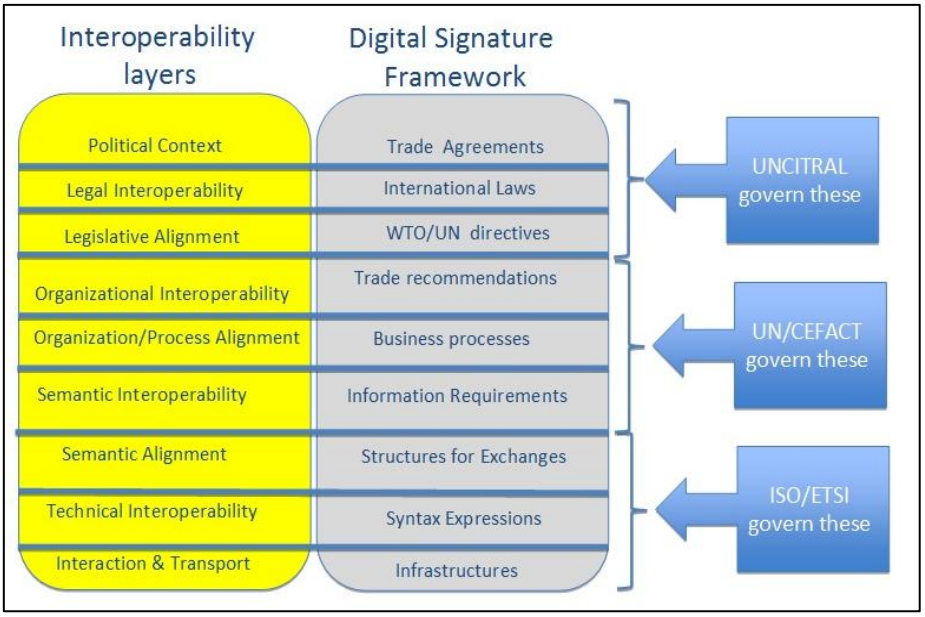
17. The principal requirements for trust in the exchange of business documents used in international trade are summarized in the following table and shown diagrammatically in the figure:

Area	*Responds to the question*	*Possible Agency Responsible*	*Examples*
Legal	Is this enforceable in law? Do the signed digital data and the electronic signature meet the legal requirements?	UNCITRAL	UN Electronic Communications Convention[2], Model Law on Electronic Signatures
Business requirements	**Are these data acceptable to my business operations?**	**UN/CEFACT**	**UNECE Recommendation 14**
Process	**Is this a valid business relationship?**	**UN/CEFACT**	**Business Document Header**
Semantics	**Is the content consistent with my understanding?**	**UN/CEFACT**	**UNTDED**
Technical	Are these data acceptable to my information system?	ISO (and ETSI)	ISO 14533-1 and 14533-2, XAdES, CAdES, PAdES

http://panel.bogor.net/idkf-wireless/aplikasi/hukum/digital-signature-blindness-11-1999.pdf (accessed on 8 May 2013).

[2] Official title: United Nations Convention on the Use of Electronic Communications in International Contracts. It came into force on 1 March 2013.

Figure: Possible governance model



18. Such a framework may be further developed as a candidate for inclusion as an annex to the Memorandum of Understanding on eBusiness.

A. Legal and cross-border recognition

Proposed possible overall responsible role:
United Nations Commission on International Trade Law

Aim: To review proposed standards and recommendations regarding the legal aspects of using digital signatures (including cross-border recognition of digital signatures) for consistency with UN international texts and documents

19. UNCITRAL is the core legal body of the United Nations system in international trade law. One of its aims is to harmonize rules on commercial transactions by providing legislative guidance. It has been a pioneer in developing legal standards on electronic commerce and many of its texts have influenced a great number of jurisdictions.[3]

20. These texts include the 1995 UNCITRAL Model Law on Electronic Commerce, 2001 UNCITRAL Model Law on Electronic Signatures and 2005 United Nations Convention on the Use of Electronic Communications in International Contracts. With the increased use of electronic communications in international trade, almost all of the UNCITRAL Working Groups (currently six) have considered or are considering related issues when deliberating their respective topics.

21. The increased use of electronic authentication techniques as substitutes for handwritten signatures and other traditional authentication procedures has created a need

[3] See http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce.html

for a specific legal framework to reduce uncertainty as to the legal effect that may result from the use of electronic signatures. The risk of diverging legislative approaches to electronic signatures in various countries calls for uniform provisions to foster their legal harmonization, as well as their interoperability.

22. In considering uniform rules on electronic signatures, UNCITRAL has examined various electronic signature techniques currently being used or still under development. The common purpose of those techniques is to provide functional equivalents to (a) handwritten signatures and (b) other kinds of authentication mechanisms used in a paper-based environment (e.g. seals or stamps).

23. Article 9, paragraph 3, of the Electronic Communications Convention is based on the recognition of the functions of a signature in a paper-based environment. It considers the following functions of a signature: (a) to identify a person; (b) to provide certainty as to the personal involvement of that person in the act of signing; and (c) to associate that person with the content of a document.

24. Alongside the traditional handwritten signature, several procedures (e.g. stamping and perforation)—sometimes also referred to as "signatures"—provide varying levels of certainty. In theory, it may seem desirable to develop functional equivalents for the different types and levels of signature requirements. In this way, users would know exactly the degree of legal recognition that could be expected from the use of the various means of authentication.

25. Any attempt, however, to develop rules on standards and procedures to be used as substitutes for specific instances of "signatures" could create the risk of tying the legal framework to a given state of technical development.

26. The Convention, therefore, does not attempt to identify specific technological equivalents to particular functions of handwritten signatures. Instead, it establishes the general conditions under which electronic communications would be regarded as authenticated with sufficient credibility and would thus be enforceable in the face of signature requirements.

27. Paragraph 3(a) of article 9 establishes the principle that in an electronic environment the basic legal functions of a signature are performed by a method that not only identifies the originator the communication but also indicates the originator's intention vis-à-vis the information it contains.

28. UNCITRAL texts relating to electronic commerce, as well as a large number of other legislative texts, are based on the principle of technological neutrality and therefore aim at accommodating all forms of electronic signature.

29. Given the pace of technological innovation, the Convention provides criteria for the legal recognition of electronic signatures irrespective of the technology used. The following are some examples:

- digital signatures relying on asymmetric cryptography
- biometric devices
- symmetric cryptograph
- use of PINs
- use of "tokens" as a way of authenticating electronic communications through a smart card or other device held by the signatory
- digitized versions of handwritten signatures
- signature dynamics

- other methods, such as clicking an "OK box".

30. Electronic signatures may take the form of "digital signatures", often generated within a public-key infrastructure where the functions of creating and verifying the digital signature are supported by certificates issued by a trusted third party.

31. Although the use of such "digital signatures" may be prevalent in some countries, various other devices, also covered in the broad notion of "electronic signature", may currently be used or considered for future use, with a view to fulfilling one or more of the functions of handwritten signatures.

32. Therefore, a piece of legislation that requires digital signature as a general standard for all transactions would not be technology neutral. And this could also hinder cross-border recognition of electronic signatures and their interoperability.

33. Such difficulties may be avoided with the broader definition of electronic signature as adopted in UNCITRAL texts, encompassing all existing or future "electronic signature" methods.

34. As long as the methods used are "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", they should be regarded as meeting legal signature requirements.

35. Paragraph 3(b) of article 9 establishes a flexible approach to the level of security to be achieved by the method of identification used under paragraph 3(a).

36. Legal, technical and commercial factors that may be taken into account in determining whether the method used under paragraph 3(a) is appropriate, include the following:

(i) sophistication of the equipment used by each of the parties;

(ii) nature of their trade activity;

(iii) frequency at which commercial transactions take place between the parties;

(iv) kind and size of the transaction;

(v) function of signature requirements in a given statutory and regulatory environment;

(vi) capability of communication systems;

(vii) compliance with authentication procedures set forth by intermediaries;

(viii) range of authentication procedures made available by any intermediary;

(ix) compliance with trade customs and practice;

(x) existence of insurance coverage mechanisms against unauthorized communications;

(xi) importance and the value of the information contained in the electronic communication;

(xii) availability of alternative methods of identification and the cost of implementation;

(xiii) 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;

(xiv) any other relevant factor.

37. Paragraph 3(b)(i) establishes a "reliability test" with a view to ensuring the correct interpretation of the principle of functional equivalence for electronic signatures. The test, which also appears also in article 7, paragraph 1(b), of the UNCITRAL Model Law on Electronic Commerce, reminds courts of the need to take into account factors other than technology. These could include the purpose for which the electronic communication was generated or communicated, or a relevant agreement of the parties, in ascertaining whether the electronic signature used was sufficient to identify the signatory.

38. Paragraph 3(b)(ii) also contains a safety clause to ensure that electronic signatures that have indeed satisfied the function they were meant to serve may not be repudiated.

39. Therefore, a flexible approach based on technological neutrality would probably be most appropriate to foster interoperability of electronic signatures. Relevant provisions can be found, for instance, in article 9, paragraph 3 of the Electronic Communications Convention and article 12, paragraph 3 of the Model Law on Electronic Signatures.

B. Business process and semantics

Proposed possible overall responsible role:
United Nations Centre for Trade Facilitation and Electronic Business

Aim: Providing instruments to promote consistent business practices in the use of digital signatures for verifying authenticity and guaranteeing integrity of trade documents used in electronic data exchange

40. A long-held and continuing ambition of UN/CEFACT is to reduce the number of documents used in the supply chain between business partners both domestic and international. Where this 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. This is also complementary to the World Customs Organization's recent Recommendation on the Dematerialization of Supporting Documents[4].

41. The use of signatures in general (not specifically digital signatures) is mentioned in a number of United Nations recommendations:

- Recommendation 1. United Nations Layout Key for Trade Documents
- Recommendation 6. Aligned Invoice Layout Key for International Trade
- Recommendation 8. Unique Identification Code Methodology
- Recommendation 14. Authentication of Trade Documents by means other than Signature
- Recommendation 26. The Commercial Use of Interchange Agreements for Digital data Interchange

42. In August 2012, the Bureau approved a project to revise Recommendation 14. This project aims first and foremost to remove the requirements for a signature when it is not essential for the trade document and/or transaction. It further recommends that equal status be given to other methods to authenticate documents when the signature is considered necessary.

[4] http://www.wcoomd.org/en/about-us/legal-instruments/recommendations/~/media/B45AE03562BF4B2EA06DEEECE556EAC3.ashx

43. The revised Recommendation 14:

- Establishes a base vocabulary on the subject (in close alignment with UNCITRAL works).
- Studies the use of signatures on trade documents both from a business and a legal point of view and advocates for the establishment of a regular review of trade documents and the needs for authentication on these documents.
- Identifies aspects of electronic authentication methods and key elements to consider in choosing these.

44. The revised Recommendation 14 also includes the following:

- Removal of the requirement for a signature except where essential for the function of the document.
- Introduction of other methods to authenticate documents.
- Creation of a legal framework that permits and gives equal status to authentication methods other than signature.
- Regular review of documentation used for domestic and cross-border trade, possibly by a joint public and private sector effort.

45. Moreover, the revisions to Recommendation 14 also aim at providing a recommendation text that would be universal and durable in time, accompanied by two different types of annex to be updated in the light of any future evolutions of the legal framework or technical advances. In particular, the Recommendation and its guidelines will be accompanied by:

- Checklists for the implementation of electronic signatures and other means of electronic authentication (legally enabling environment, functional requirements, etc.).
- Repository of case studies of existing technological solutions— either from the point of view of a legal framework or their functional implementation —or ideally both.

46. The work on Signed Digital Document Interoperability (previously known as draft Recommendation 37) identified rules for parties who have mutually agreed to use digital signatures. To achieve this goal, the draft Recommendation defined a set of requirements that addressed the organization and relationships between the signed content, signatories' certificates and signatures. These requirements will be incorporated into examples of best practice for inclusion in the annex of case studies of existing technological solutions as part of the revisions to Recommendation 14. Therefore they do not need to be provided as a separate Recommendation.

47. As well as having the reliable identification, authentication and authorization of the digital data involved in cross-border trade documents, it is also critical to establish trust in the reliability, traceability and integrity of the various data exchange services (such as message handling systems) that may be used to transport the digital data.

48. This level of trust addresses issues such as:

- If a trading party receives electronic data from a foreign infrastructure or service, how can they trust that the data is from whom it claims to be from and that the information is authentic?
- If a trading party sends electronic data to a third party, how can they trust that it will be securely delivered without corruption and only to the intended recipient?

49. To address this requirement, UN/CEFACT is also preparing a proposal to develop a "Recommendation for enabling interoperability between electronic data exchange systems in domestic and cross border trade".

50. This project will formulate basic principles and prepare a recommendation on enabling interoperability between different organizations providing existing and new electronic trade document data-exchange infrastructures. The goal is to enable global trust when exchanging electronic trade documents across different trans-boundary scenarios.

51. These recommendations (together with other UN/CEFACT instruments) are intended to address the governance of specifications relating to the use of digital signatures as part of the overall business requirements for trusted electronic data exchange of trade documents (see annex II).

C. Technical recognition

Proposed possible overall responsible role: ISO (and ETSI)

Aim: To establish a set of digital signature format standards required that enable technical recognition of digital signatures across borders

52. The situation related to standards for technical interoperability of digital signatures is multi-faceted (there are many standards for certificates, hash algorithms, etc). The multiplicity of electronic signature standards may make it difficult for a recipient to technically verify digital signatures. It could sometimes affect the ability of businesses and administrations to exchange digital data securely among themselves and with their administrative and financial counterparts.

53. This has resulted in a market where there is:

- A lack of truly interoperable digital signature applications
- A lack of trust in existing frameworks
- Problems with mutual recognition and cross**-**border interoperability

54. To address the problem, the European Commission has issued a standardization mandate (M/460) aiming at achieving the interoperability of digital signatures throughout Europe by providing a rationalized European digital signature standardization framework to allow mutual recognition and cross-border interoperability. Annex I describes the scope of M/460.

55. Mandate M/460 addresses the same issues faced outside of Europe in the global marketplace. It seeks to create the conditions for interoperability of digital signatures at a cross-border level by defining and providing a rationalized digital signature standardization framework. The scope of the M/460 framework is described in annex I.

56. The international community should evaluate the findings of Europe's M/460 mandate and consider adapting and applying it to global cross-border trade.

57. The standard digital signature implementation formats most pertinent to trade documents are currently developed and published by ETSI. In particular the focus has been on three types of digital signature implementations:

- CAdES, CMS Advanced Electronic Signature
- XAdES, XML Advanced Electronic Signature
- PAdES, PDF Advanced Electronic Signature.

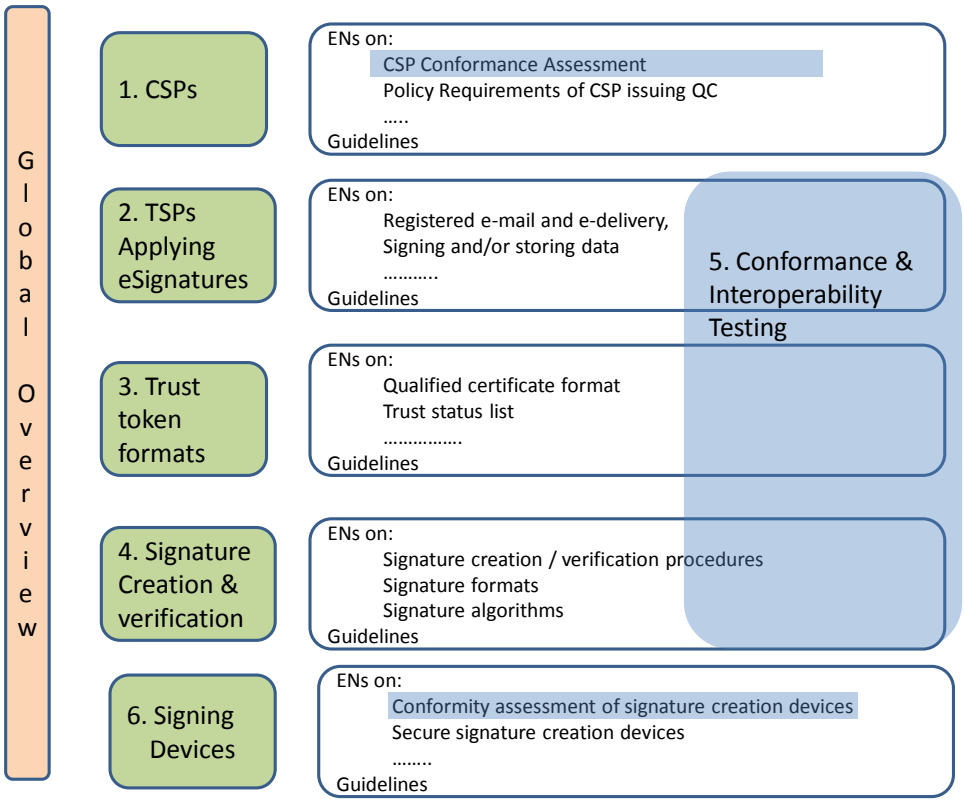
58. ETSI standards through liaison with ISO are developed in coordination with ISO/TC 154, as well as other ISO TCs working in this area, including ISO/IEC JTC/1 SSCs.

59. This has resulted in ISO 14533 - "Long Term Signature profiles for EDI Data and Electronic Documents" from ISO/TC 154. It neither specifies new technical specifications about digital signatures nor restricts usage of the technical specifications about digital signatures that already exist. It defines selected elements from the CMS Advanced Electronic Signatures (CAdES) and XML Advanced Electronic Signature (XADES) standards that enable verification of a digital signature over a long period of time.

60. UN/CEFACT has liaison arrangements with ISO and ETSI that can be used to ensure that business requirements from UN/CEFACT stakeholders are supported through the technical standardization process.

Annex I

European digital signature standardization framework



Key:

CSP:	Certificate Service Provider: Providers of Certificates for Trust Services not only relating to Digital Signatures.
QC:	Qualified Certificate: Certificate provided by a trusted Certification Service Provider.
TSP	Trust Service Provider: Providers of Trust Services not only relating to Digital Signatures.
EN	European Norm: European Standard recognized by the European Commission.

Annex II

How UN/CEFACT addresses the business requirements for trusted electronic data exchange of trade documents