Economic and Social Council

Distr.: General
5 December 2011

Original: English

Economic Commission for Europe

Committee on Trade

Centre for Trade Facilitation and Electronic Business

Eighteenth session
Geneva, 15-17 February 2012
Item 5 of the provisional agenda
UN/CEFACT recommendations and standards

Recommendation No. 37: Signed Digital Document Interoperability

Prepared by the by the Security for XML documents and messages project team of the Supply Chain Programme Development Area and submitted for information by the Bureau

Summary

The original draft UNECE Recommendation 37 on Signed Digital Evidence Interoperability was submitted to UN/CEFACT at its sixteenth session and subsequently by decision 10-04 submitted to intersessional approval. Comments received during the intersessional process were discussed at the seventeenth session. It was decided to go back to Step 4 "Public Review" of the Open Development Process until 12 September 2011.

The Supply Chain Project Development Area is now submitting an updated draft of this recommendation for information.

The Bureau has also prepared an explanatory note (ECE/TRADE/C/CEFACT/2012/8) as background for the Plenary's deliberations on this topic.

Previous documentation:

ECE/TRADE/C/CEFACT/2010/14 Recommendation No. 37: Signed Digital Evidence Interoperability

Contents

Page

1. Foreword ... 3
2. Executive summary ... 4
    2.1. Context ... 4
    2.2. Recommendation ... 4
    2.3. Benefits and objectives ... 5
3. Introduction ... 5
    3.1. Scope ... 5
    3.2. Objective ... 6
    3.3. Audience ... 7
4. Definitions ... 7
5. Recommendation ... 8
    5.1. The Recommendation’s signed digital document profile ... 8
    5.2. Functional requirements of the profile ... 9
    5.3. Differences between signed digital documents and signed paper documents ... 10
6. Conclusion ... 10
7. References ... 10

1. Foreword

The Signed Digital Documents Interoperability Recommendation (SDDIR) aims at increasing the level of interoperability of electronically signed digital documents as one option in particular situations to facilitate the development of paperless international trade.

To achieve this goal, the Recommendation defines a set of functional rules for signed digital documents that address the organization and relationships between the signed content, purported signatories’ digital identities and signatures.

The Recommendation is intended for use by organizations or individuals who agree to utilize signed digital documents.

Legal issues affected by this Recommendation should be coordinated with other international organizations.

The Recommendation does not deal with the legal aspects of electronic signatures, which are addressed at the international level by other documents such as those published by the United Nations Commission of International Trade Law (UNCITRAL). Neither does it deal with usability or interpretation of the signed content.

This Recommendation is not intended to conflict with UNECE Recommendation 14 “Authentication of trade documents by means other than signature”.

2. Executive summary

2.1 Context

The multiplicity of electronic signature standards may make verification of signed digital documents by a recipient technically or legally difficult. This may in some cases have a direct impact on the ability of businesses and administrations to securely exchange digital documents between themselves and with their administrative and financial counterparts.

Applying these recommended standards in particular situations would also present compliance application issues and increased cost, as well possibly the need for regulatory or other legal mechanisms, which need to be taken into account as to the overall benefits projected to be achieved.

To address this issue, a functional rather than a technical approach to signed digital documents has been taken in this Recommendation, by focusing first on the “what” instead of on the “how”.

The verification of signed digital documents should not require from the parties any prior process agreement to give the verifier a clear view of the following reasonable list of information:

- The signatures’ parameters (date, place, type of commitment).
- The integrity of the signed content where that is expressly intended.
- The integrity and validity of the purported signatories’ digital identities and the level of assurance they are designed to provide, in accordance with purported certifying parties’ practice statements, agreements between users, and applicable regulatory requirements.
- The trustworthiness of the purported certification service providers.

This Recommendation offers a set of functional requirements for creating and verifying signed digital documents to improve their interoperability while keeping in mind that its adoption might elicit requests for changes over time.

Aside from the particular issues raised here, the Recommendation focuses on functional interoperability and has not been reviewed from a legal perspective generally or as to particular national laws, and compliance with these standards does not provide any assurances of the admissibility or enforceability of any signed digital document in any jurisdiction.

From the perspective of governments, legislatures, judiciaries, implementers, users, or others, the Recommendation is not intended to resolve the issue of whether its use will be legally cognizable under national law in any country or for use in cross-border transactions. The use of approaches developed under this Recommendation may not necessarily have any greater effect as evidence in any legal proceeding than other cognizable methods for providing or authenticating such information as evidence.

2.2 Recommendation

This Recommendation encourages any organization or party that chooses to exchange signed digital documents with others to apply the following principles in order to maximize interoperability:

Signed digital documents:

- MUST contain one and only one identifiable content
- MUST be signed by one or more signatures
- MUST contain all digital identities involved in an unambiguous way

Each signature contained in the digital document:

- MAY contain a date of signature and other properties
- MUST sign the entire content
- MAY be signed by one or many counter-signatures

The keywords "MUST" and "MAY" used in this section are to be interpreted as follows:

- MUST: means that the requirement is an absolute requirement of the specification.
- MAY: means that the requirement is optional. An implementation that does not include a particular option must be prepared to interoperate with another implementation that does; though perhaps with reduced functionality.

  Similarly, an implementation that does include a particular option must be prepared to interoperate with another implementation that does not (except, of course, for the feature the option provides.)

2.3 Benefits and objectives

This Recommendation provides business, administrative, and financial organizations with a proposed set of standard functional requirements to improve the interoperability of the creation and verification of signed digital documents, if compliant standards and technology solutions are agreed to and applied taking into account the regulatory, infrastructure development and operations costs for users.

These benefits can be achieved with currently and widely available technologies and products, including open source projects.

Its objectives are to:

- Improve efficiency and reliability for the creation and verification of signed digital document received from another party.
- Increase interoperability of signed digital document which, in turn, will increase trust and confidence.
- Provide a wide, yet coordinated path to increase the rate of adoption of paperless technologies.

3. Introduction

3.1 Scope

Since the early 1990s, numerous technical standards for signed digital documents have been designed, proposed and adopted. Examples of such standards are shown in Section 7 - References.

However, as a result, this multiplicity of standards with many possible options and lack of guidance on how to apply digital signatures to digital documents has led to a lack of interoperability of signed digital documents from a syntactic, semantic and processing perspective.

The aim of this Recommendation is to propose a particular approach to signed digital documents creation and verification, focusing on their functional aspects, as opposed to their technical aspects.

By focusing on the functional aspects, for those sectors for which this Recommendation is concluded to be an appropriate solution, and where acceptable to participating parties, it allows the definition of a common functional signed digital document profile. This sectoral implementation profile of the Recommendation, subject to other factors such as cost, regulatory infrastructure, sector practices, etc., can simplify and facilitate the creation and verification of signed digital documents.

This Recommendation does not affect the ability of parties to select other methodologies which systems or parties may choose to accomplish comparable purposes.

This Recommendation offers a set of functional requirements to promote interoperability for the creation and verification of signed digital documents to the extent applicable to particular sectors and agreed to by parties involved.

3.2 Objective

The objective of this Recommendation is to facilitate the exchange and verification of signed digital documents that may have significant value for business by ensuring or promoting their interoperability, to the extent applicable to particular sectors and to the extent agreed to by parties involved. Its use is expected to increase the rate of dematerialization of digital documents, by facilitating the creation, validation and interoperability of signed digital documents.

From an end-user's point of view, the use of digital signatures involves three main processes:

- Determining the extent of content to be subject to digital signature;
- Signing appropriate document(s) or portions thereof;
- Verifying the document's signature(s) including the discovery of its parameters.

Particular regional practices in the eTendering and eInvoicing domains show that a number of interoperability problems must be solved when a party signs a document with its identity and signature software:

- Signature format interoperability: the verifying software is often unable to deal with the digital signature format received or unable to understand to which file the signature corresponds, or where the signature is.
- Semantic value of the signature: the verifying software or the format of the signature may not allow understanding the signatory’s intention (for instance if the signature was made by the signatory for integrity purposes or as an approval of the signed content, or otherwise).
- Digital identity validity: the verifying software may not able to determine if the digital identity is trustworthy or if it was valid at the date and time of signature.

Signature verification failures are of importance, for instance, at the pre-award and award phases of the process domain of Public Procurement, since tenders might be considered invalid and be rejected mistakenly or verification procedures used which can affect delay and lessen the cost-savings to be achieved through the use of digital signatures.

To solve the first two categories of problems, all signatures produced may be required to be presented in a format that all software packages used to verify these signatures will be able to manage.

As a consequence, the main benefits of the proposed signed digital documents profile are to:

- Facilitate trust by offering generic functionality to create, verify and easily manage signed digital documents.
- Promote interoperability of signed digital documents by means of a functional common denominator and independence regarding the technical format used.
- Simplify the integration of digital signatures in business and archiving applications, so as to more easily replace a "print" function by a "sign" or "certify" function.

3.3 Audience

This document is intended primarily for organizations, parties and systems which have the following concerns:

- Exchanging signed digital documents.
- Choosing a format for signed digital documents suitable for a particular dematerialization project.
- Monitoring information technology with respect to the fields of digital signatures and digital archiving.
- Ensuring the interoperability of signed digital documents.

4. Definitions

This section provides a brief definition of the terms and abbreviations used in this document.

AdES: Advanced Electronic Signature

CAdES: CMS Advanced Electronic Signature

Signed digital document: a digital document or other information, which may be used to demonstrate reliability or non-corruption of signed information, or an agreement between parties or use by a system of procedures to accomplish that. It does not identify a particular party having actually taken action absent additional procedures and technology.

CMS: Cryptographic Message Syntax

Cosignature: a signature, which applies to the same content as another signature, or comparable means to identify a related party in accordance with applicable sector practices

Counter-signatory: person that holds counter-signature creation data and acts either on its own behalf or on behalf of the person it represents, or comparable means to identify a related party in accordance with applicable sector practices

Counter-signature: a signature which applies to a signature (the signed content of a counter-signature is itself a signature); may also be called "hierarchical signature"

Data Message: Information generated, sent, received or stored by electronic, magnetic, optical or similar means, including, but not limited to, electronic data interchange, electronic mail, telegram, telex or telecopy. (Article 4. Definitions, UN E-Commerce Convention)

Digital document: a document in digital form used to convey information to be either presented to or processed by its user.

ECC or UN E-Commerce Convention: 2005 United Nations Convention on the Use of Electronic Communications in International Contracts, Official Records of the General Assembly, 60th Session, A/RES/60/21 (referred to as the UN E-Commerce Convention or ECC).

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 approval of the information contained in the data message (Reference 1)

ETSI: European Telecommunications Standards Institute

EU: European Union

Information: Includes all types of digital files [need a definition of "files"?] and content, including but not limited to "documents as well as any type of data message."

IETF: Internet Engineering Task Force

ISO: International Organization for Standardization

PAdES: PDF Advanced Electronic Signature

PDF: Portable Data Format

PKCS: Public Key Cryptographic Standard

RFC: Request For Comment

Signatory: Person who holds signature creation data and acts either on its own behalf or on behalf of the person it represents

Signed content: data contained in the signed digital document which is signed by the purported signatory (ies)

TS: Technical Specification

UNCITRAL: United Nations Commission on International Trade Law

XAdES: XML Advanced Electronic Signature

XML: eXtensible Markup Language

XMLDSIG: XML Digital Signature

5. Recommendation

This section describes the Recommendation.

5.1 The Recommendation's signed digital document profile

The Recommendation proposes a signed digital document profile designed to maximize interoperability between the creation and verification of signed digital documents.

The profile is described by a set of functional requirements.

5.2 Functional requirements of the profile

The functional requirements of the proposed signed digital document profile are described in this paragraph.

The keywords "MUST" and "MAY" used in this section are to be interpreted as follows:

- MUST: This word means that the requirement is an absolute requirement of the specification.
- MAY: This word means that the requirement is truly optional. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein, an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

A signed digital document compliant to the proposed signed digital document profile:

- MUST contain one and only one identifiable content along with its type and an optional name
- MUST be signed by one or more signatures
- MUST contain all digital identities involved in an unambiguous way

Each signature contained in the signed digital document compliant to the proposed signed digital document profile:

- MUST sign the entire content
- MAY contain attributes, which must be signed by the signature, such as:
    - Date of signing: specifies the time at which the purported signatory claims to have performed the signing process.
    - Signatory location: specifies a mnemonic for an address associated with the purported signatory at a particular geographical (e.g. city) location.
    - Reference to a signature policy which describes the precise role and commitments that the purported signatory intends to assume with respect to the signed document.
    - Type of commitment associated with the signature: explicitly indicates to a verifier that by signing the document, it illustrates a specific type of commitment on behalf of the purported signatory.
    - Role(s) of the purported signatory: specifies the role(s) or position(s) claimed by the purported signatory when signing the document.
    - References to the digital identity of the purported signatory and its purported certifiers.
- MAY be signed by one or many counter-signatures
- MAY contain a timestamp

5.3 Differences between signed digital documents and signed paper documents

Many features are common to both types of signed documents, but there are certain important differences, such as:

- The identities of the purported signatories are not always present in paper-based documents.
- The identities of the purported certifiers of the purported signatory are generally not present in paper-based documents.
- Conversely, signed paper-based documents often include a handwritten signature although stamped or affixed signatures are common as well in commerce, while a digital signature on an electronic digital document is not intended to be represented graphically unless other technologies such as signature dynamics are also employed. Usually, only a computer program is capable of performing the complex mathematical calculations needed to verify a digital signature.

6. Conclusion

The signed digital document profile presented in this document, to the extent adopted by organizations, systems or parties, aims (a) to contribute to the development of dematerialization of paper documents by simplifying (while taking into account the regulatory and infrastructure mechanisms and costs associated therewith) and facilitating the creation and verification of signed digital documents and (b) to contribute to their integration into business applications in contexts or situations where this is required or agreed.

7. References

PKCS#7: http://www.rsa.com/rsalabs/node.asp?id=2129

S/MIME: http://www.ietf.org/rfc/rfc3851.txt

CMS: http://www.ietf.org/rfc/rfc3852.txt

XMLDSIG: http://www.w3.org/TR/xmldsig-core/

CAdES (ETSI TS 101 733): http://www.etsi.org

EANCOM digital signature:
http://www.gs1.org/docs/ecom/eancom/eancom_Digital_Signature.pdf

Signed PDF (ISO/DIS 32000): http://www.adobe.com/devnet/pdf/pdf_reference.html

or otherwise

http://www.iso.org/iso/fr/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51502

XAdES (ETSI TS 101 903): http://www.etsi.org

PAdES (ETSI TS 102 778): http://www.etsi.org