UNITED NATIONS **E**

Economic and Social Council

Distr.
GENERAL
ECE/TRADE/TBG/CEFACT/2010/xx
19 February 2010

Original: ENGLISH
ECONOMIC COMMISSION FOR EUROPE
COMMITTEE ON TRADE

Centre for Trade Facilitation and Electronic Business

TBG "Security Project" hosted by TBG6

Recommendation No. 37

Digital Evidence Certification Recommendation

SOURCE: **The Chair**

ACTION: **Review before further iteration of Open Development Process Step 5 – Public Review**

STATUS: **Proposed Publication Draft**

Table of Contents

1. Acknowledgements

Editors:

- François Devoret (UN/Cefact Security Project Editor, Lex Persona / France),
- Andrea Caccia (AITI, Member of ETSI/ESI),
- Michel Entat (Axemio / France),
- Julien Pasquier (Lex Persona / France).

Contributors:

- Sujeet Bhatt (UN/Cefact Security Project Leader, NexTenders / India),
- Paul Burrows (BCIS / United Kingdom),
- Andrew Hudson (Kern CM Ltd / United Kingdom).
- Bernard Longhi (UN/Cefact TBG6 Chair, BLC-Consultants / France),
- Ajit Menon (NexTenders / India),
- Kevin Smith (Cloud Data Technologies / United Kingdom).

Reviewers:

- Gordon Cragge (Sitpro / United Kingdom),
- Chris Hassler (DOD-DCMA / USA).

2. Introduction

2.1. Scope

Since the early nineties, numerous technical standards for digital evidence certification have been designed, proposed and adopted[i].

However, as a result, this multiplicity of signature formats with many possible options and lack of guidance on how to apply digital signatures to documents has led to a lack of interoperability of certified digital evidences from a syntactic, semantic and processing aspect.

The aim of this document is to propose a new, normative approach to digital evidence certification, focusing on their functional aspects, as opposed to their technical aspects.

By focusing on the functional aspects of certified digital evidences, it is possible to define a common, functional digital evidence profile, which will simplify and facilitate the exchange and verification of electronic documents with legal or probative value.

This recommendation offers a set of functional requirements to help the design of interoperable digital evidence certification applications. In addition, it offers sample implementations of this recommendation, applied to the most recent digital evidence technical standards.

To ease the referencing of this recommendation in this document, the name DEC-R will be used. The “DEC-R” acronym stands for Digital Evidence Certification (would be) Recommendation.

2.2. Objective

The objective of this profile is to increase the rate of dematerialization of paper documents, by facilitating the creation, validation and interoperability of electronic documents with legal or probative value, and their integration into business applications.

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

- Signing a document
- Verifying a document's signature.

The real practice, both in eTendering and eInvoicing domains, shows that a number of interoperability problems must be solved, when a party signs a document with its certificate and signature software:

- Signature format interoperability: the verifying software is often not able to deal with the digital signature format received or not able 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 if the signature was made by the signer for integrity purpose or as an approval of the signed content.

[i] Examples of such standards are: PKCS#7 (1), S/MIME (2), CMS (3), XMLDSIG (4), CAdES (5), EANCOM signature (6), Signed PDF (7), XAdES (8), PAdES (9), etc.

- Certificate validity: the verifying software may not able to determine if the certificate is trustworthy or if it was revoked at the date of signature.

Signature verification failures are of critical 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.

To solve the first two categories of problems, it is necessary to ensure that all signatures produced will be presented in such a format that all verifying software packages liable to be used to verify these signatures will be able to manage this format.

As a consequence, the main benefits of the proposed certified digital evidence profile are the following:

- Facilitate trust by offering generic functionality to create, verify and easily manage certified digital evidences;
- Ensure interoperability of certified digital evidence by means of a functional common denominator and independence vis-à-vis 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.

2.3. Audience

This document is intended primarily for IT consultants, project managers, information systems managers, information systems security officers, who have the following concerns:

- Choosing a format for certified digital evidences, suitable for a particular dematerialization project;
- Information Technology watch with respect to the fields of digital signatures and legal archiving;
- Evaluating the interoperability, reversibility and validity of digital evidences.

3. References and definitions

3.1. References

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

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

(3). CMS: http://www.ietf.org/rfc/rfc3852.txt

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

(5). CAdES (ETSI TS 101 733): http://pda.etsi.org/exchangefolder/ts_101733v010704p.pdf (may require authentification)

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

(7). 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

(8). XAdES (ETSI TS 101 903): http://pda.etsi.org/exchangefolder/ts_101903v010401p.pdf (may require authentication)

(9). PAdES (ETSI TS 102 778): http://pda.etsi.org/exchangefolder/ts_10277801v010101p.pdf (may require authentication)

(10). Keywords: http://www.faqs.org/rfcs/rfc2119.html

(11). Council Directive 2001/115/EC: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0115:EN:HTML (7)-2-c)

(12). CWA 14171 on electronic signature verification: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14171-00-2004-May.pdf

(13). TSP Status List (ETSI TS 102 231): http://pda.etsi.org/exchangefolder/ts_102231v030101p.pdf (may require authentication)

(14). ETSI work on Attached Signature (work in progress): http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=31946

(15). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

(16). ISO TC 154 : http://www.iso.org/iso/iso_technical_committee.html?commid=53186

(17). ISO/CD 14533-2: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56025

(18). ISO/CD 14533-1: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56024

(19). ISO 32000-2 http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?ics1=37&ics2=100&ics3=99&csnumber=53041

(20). XAdES digital signature profile of the French Administration: http://www.references.modernisation.gouv.fr/sites/default/files/FormatdeSignature_Xades_V1_0.pdf

(21). PAdES Basic (ETSI TS 102 778-2): http://pda.etsi.org/exchangefolder/ts_10277802v010201p.pdf

(22). RFC 2315: http://www.ietf.org/rfc/rfc2315.txt

(23). RFC 3161: http://www.ietf.org/rfc/rfc3161.txt

(24). Online Certificate Status Protocol: http://www.ietf.org/rfc/rfc2560.txt

(25). Certificate Revocation List: http://www.ietf.org/rfc/rfc5280.txt

(26). Algorithm recommendations: ETSI TS 102 176

3.2. Definitions

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

AdES: Advanced Electronic Signature.

BES: Basic Electronic Signature.

CAdES: CMS Advanced Electronic Signature.

CEN: Comité Européen de Normalisation

Certified digital evidence: a digital document which can be produced as evidence in court.

CMS: Cryptographic Message Syntax.

CRL: Certificate Revocation List.

CWA: CEN workshop agreement

Cosignature: a signature which signs the same content as the signature it cosigns.

Counter signature: a signature which signs a signature (the signed content of a counter signature is itself a signature); may also be called “hierarchical signature”.

DEC-R: Digital Evidence Certification Recommendation.

EPES: Explicit Policy based Electronic Signature.

ETSI: European Telecommunications Standards Institute.

EU: European Union.

Identity: digital information that can identify unambiguously the signer and that contains data that can uniquely link the signer with the signature.

ISO: International Standards Organization.

OCSP: Online Certificate Status Protocol.

PAdES: PDF Advanced Electronic Signature.

PDF: Portable Data Format.

PKCS: Public Key Cryptographic Standard.

PKI: Public Key Infrastructure.

RFC: Request For Comment.

Signed content: data contained in the digital evidence which is signed by the signer(s).

SSCD: Secure Signature Creation Device.

Trust anchor: designates a certificate which is trusted by a verifier. It is often called a “root” certificate.

TS: Technical Specification.

TSL: TSP Status List.

TSP: Trusted Services Provider.

XAdES: XML Advanced Electronic Signature.

XML: eXtensible Markup Language

XMLDSIG: XML Digital Signature.

4. DEC-R specification

This chapter describes the functional characteristics and management rules which make the DEC-R specification.

4.1. The DEC-R certified digital evidence profile

The proposed DEC-R digital evidence profile describes a set of functional features unique to the certification and verification of digital evidences, which must follow specific rules.

4.2. Key functional features of the common certified digital evidence profile

The functional features of the proposed certified digital evidence profile are the following:

- One and only one signed content with its type and an optional name.
- Signatures and co signatures of the signed content.
- Counter signatures (i.e. “hierarchical” signatures) as unsigned properties of a signature or counter signature.
- Signature (and counter signature) signed properties:
    - Date of signing: specifies the time at which the signer claims to have performed the signing process;
    - Signer location: specifies a mnemonic for an address associated with the signer at a particular geographical (e.g. city) location;
    - Reference to a signature policy which describes the precise role and commitments that the signer intends to assume with respect to the signed data;
    - Type of commitment associated with the signature: explicitly indicates to a verifier that by signing the data, it illustrates a specific type of commitment on behalf of the signer;
    - Role(s) or the signer: specifies the role(s) or position(s) claimed by the signer when signing the data;
    - References to the identity of the signer and its certifiers.
- Timestamps as unsigned properties of a signature or counter signature.
- Identities of the signers (and counter signers) and their certifiers.

4.3. Differences between digital and paper evidences

Many features are present in both types of evidence, but certain important differences exist, such as:

- The identities of the signer are not always present on paper-based evidences.
- The identities of the ancestors of the signer are generally not present on paper-based evidences.
- Conversely, paper-based evidence generally includes a handwritten signature, while a digital signature on an electronic document is not intended to be represented graphically. Usually, only a computer program is capable of performing the complex mathematical calculations needed to verify a digital signature.

4.4. DEC-R specification levels

The DEC-R specification provides different levels to differentiate the strength of the DEC-R requirements. In this version, two levels have been defined:

- Core, which is the level which provides the greatest flexibility; it is the default level of DEC-R requirements;
- Level 1, which is a more constrained version of DEC-R, specifically imposing a signed date of signature for every signature, as well as signed references of all certifiers and their identities.

4.5. DEC-R specification keywords

The keywords "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "SHALL", "RECOMMENDED", "MAY", and "OPTIONAL" in this document (in uppercase, as shown) are to be interpreted as described in RFC 2119 (10).

4.6. DEC-R application profiles

The DEC-R specification makes provision for two different application profiles:

- DEC-R compliant creation applications
- DEC-R compliant verification applications

A DEC-R compliant verification application, when verifying a DEC-R digital evidence MUST return a status, whose value is:

- PASSED: the evidence has passed verification
- FAILED: the evidence has failed verification
- INCOMPLETE: the evidence has neither passed nor failed verification

4.7. DEC-R requirements

The DEC-R requirements are described below, with requirements numbered R1 through R19[ii].

R1. A certified digital evidence MUST contain one and only one signed content composed of data and type and an OPTIONAL name.

R2. A certified digital evidence MUST contain at least one signature. At least five (co) signatures of a certified digital evidence MUST be supported by a compliant creation or verification application. If additional cosignatures are present and the verification application does not support them, the verification MUST be declared incomplete.

R3. Each signature MUST sign the whole signed content, i.e. its data together with its type and OPTIONAL name.

R4. A signature MAY be signed by one or more counter signatures. At least five counter signatures of a signature MUST be supported by a compliant creation or verification application. If additional counter signatures are present and the verification application does not support them, the verification must be declared incomplete.

R5. A counter signature MUST sign one and only one signature or counter signature, and MUST NOT sign the signed content or anything else. A counter signature MUST be included as an unsigned property of the signature or counter signature it counter signs.

[ii] The requirements below are not implemented by all the digital signature technical standards available at the time of publication of this document. Hence it is recommended to the reader to check if the technical standard chosen for implementation supports the chosen requirements. Please refer to Part 2 of this document for details of some proposed technical implementations of the DEC-R requirements.

R6. A counter signature MAY be signed by one or more counter signatures. At least one counter signature of a counter signature MUST be supported by a compliant creation or verification application. If additional levels of counter signature are present and the verification application does not support them, the verification must be declared incomplete.

R7. A signature or counter signature MAY be time stamped by at most one timestamp. The timestamp MUST be included as an unsigned property of the signature or counter signature.

R8. A certified digital evidence MUST contain the identities of the signers and counter signers pointed by the signed references mentioned in [R9].

R9. A signature or counter signature MUST contain a signed unambiguous reference to the signer's or counter signer's identity. This constraint is to link unambiguously the signer with its signature and make sure that the verifier does not need to "guess" the identity of the signer or counter signer so as to be able to verify the signature.

R10-Core. A certified digital evidence MAY contain the identities of signers' or counter signers' certifiers pointed or not by the signed references mentioned in [R11-Core].

R10-Level 1. A certified digital evidence MUST contain the identities of all signers' and counter signers' certifiers pointed by the signed references mentioned in [R11-Level 1].

R11-Core. A signature or counter signature MAY contain signed references to the signer's or counter signer's certifiers' identities. This possibility is to provide the verifier with information in order to verify the identity of the signer or counter signer.

R11-Level 1. A signature or counter signature MUST contain all signed references to the signer's or counter signer's certifiers' identities. This constraint is to make sure that the verifier does not need to "search for" the identity of any certifier in order to verify the identity of the signer or counter signer.

R12-Core. A signature or counter signature MAY contain one signed date of signature.

R12-Level 1. A signature or counter signature MUST contain one signed date of signature.

R13. A signature or counter signature MAY contain at most one signed signer location.

R14. A signature or counter signature MAY contain at most one signed signature policy.

R15. A signature or counter signature MAY contain one or more signed claimed roles associated with the signer.

R16. A signature or counter signature MAY contain at most one signed type of commitment.

R17. A type of commitment MUST be one of the following:

R17-1. Proof of creation, indicating that the signer has created the signed content, but not approved it, nor that is it the sender. This particular type of consent is important in light of the necessity to sometimes guarantee the integrity and authenticity of a document without implying any other kind of commitment. This is the case for electronic invoices(11), which only need to be protected in their integrity and authenticity. Another example, where this type of commitment is useful, are contracts which must only be protected in their integrity and authenticity by their originator in the first place but approved by its recipient in the second place (such as a work contract for example).

R17-2. Proof of approval, indicating that the signer has approved the signed content.

R17-3. Proof of origin, indicating that the signer recognizes to have created, approved and is the sender of the signed content.

R17-4. Proof of sender, indicating that the entity providing that indication is the sender of the signed content but has not necessarily created it.

R17-5. Proof of receipt, indicating that the signer recognizes to have received the signed content.

R17-6. Proof of delivery, indicating that the time stamp authority providing that indication has delivered the signed content in a local store accessible to the recipient of the signed content.

R18-Core. A signature or counter signature MAY contain other signed properties. Support of these other signed properties by a DEC-R compliant verification application is OPTIONAL.

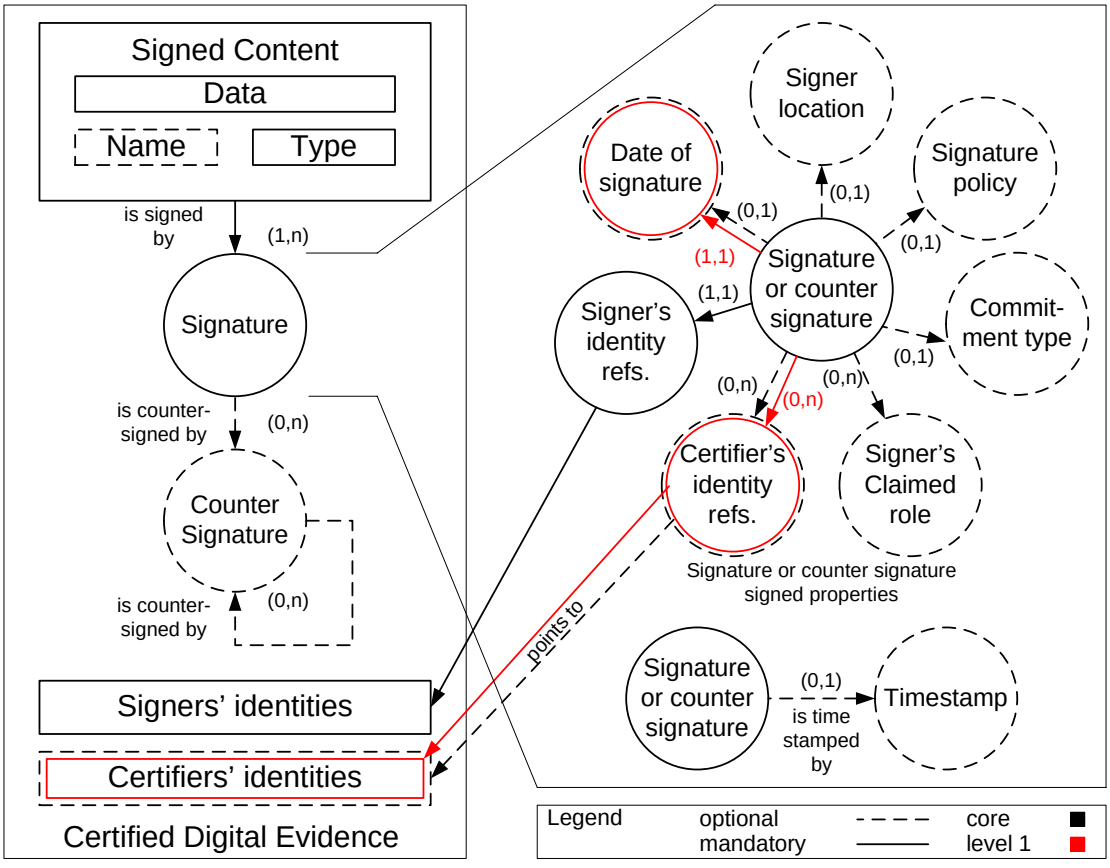
R18-Level 1. A signature or counter signature MUST NOT contain other signed properties.

R19. A signature or counter signature MAY contain other unsigned properties. Support of these other unsigned properties by a DEC-R compliant verification application is OPTIONAL. The presence of unsupported unsigned properties MUST NOT impact the verifier's interpretation of the signature.

4.8. DEC-R digital evidence schematic representation

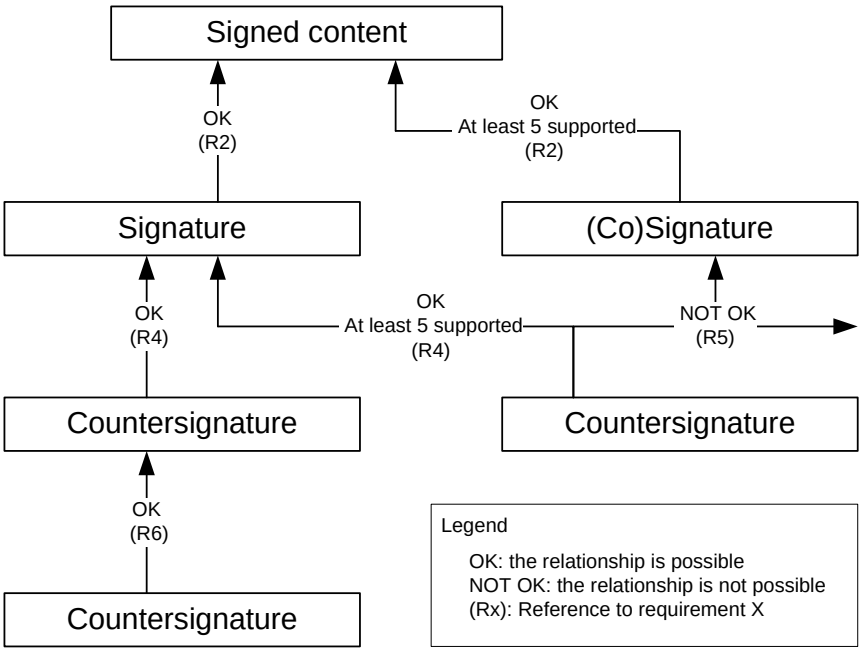
This section provides a schematic representation of the DEC-R digital evidence structure and organization.

The figure below illustrates the overall structure and organization of a DEC-R digital evidence. Requirements 18 and 19 are not represented.



DEC-R digital evidence: Overall structure and organization representation

The figure below represents the relationships between signatures, cosignatures and counter signatures of a DEC-R digital evidence.



DEC-R digital evidence: Signature relationships representation

4.9. Version numbering scheme of the DEC-R specification

The version numbering scheme of the DEC-R specification is in the form of [version].[status].

[version] is an integer describing the major version number of the specification.

[status] is an integer describing the version's status of the specification, which can take the following values:

- 0: alpha status
- 1: draft status
- 2: general availability status

4.10. Current version of the DEC-R specification

The current version of the DEC-R specification is 1.1.

Note: the version of the DEC-R specification is in no way related, and should not be confused with the revision of this document.

4.11. Backward compatibility

Any change in the profile must ensure backward compatibility with earlier versions. Indeed, it is not possible to conceive evolutions to the profile which would render evidences, created in compliance with previous versions of the profile, incompatible, illegal, or non interoperable.

4.12. Possible evolutions of the DEC-R profile

Many developments may enhance the DEC-R certified digital evidence profile in the future.

Such developments may provide support for incorporation of data necessary for long-term verification of the evidence such as AdES-A(12) (level 2), or mechanisms for verifying the validity of the identities of the signers such as TSL(13) (level 2).

Future versions of DEC-R should also be able to take into account the properties of the identity itself (qualified certificates, SSCD and so on).

Also, future enhancements of DEC-R may provide support for:

- attached signature (detached signature and multiple signed contents packaging)(14);
- signature kinematics.

.

5. Technical implementation guidelines of the DEC-R recommendation

The DEC-R profile is necessarily used in conjunction with a technical implementation which implements and supports its rules and characteristics.

5.1. Overview of sample implementations

Three digital signature standards have already been studied and successfully evaluated for DEC-R implementations:

- A XAdES implementation based on ETSI TS 101 903 v1.4.1. When implemented the format of the digital evidence is referred to as X-DEC-R in the rest of this document. This implementation is described in 7Annex A: X-DEC-R description.
- A CAdES implementation based on ETSI TS 101 733 v1.8.1. When implemented the format of the digital evidence is referred to as C-DEC-R in the rest of this document. This implementation is described in 7Annex B: C-DEC-R description.
- A PAdES implementation based on ETSI TS 102 778 v1.1.1. When implemented the format of the digital evidence is referred to as P-DEC-R in the rest of this document. This implementation is described in 7Annex C: P-DEC-R description.

The main reasons which led to the study of these digital signature standards, as DEC-R technical implementations are the following:

- They conform to the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures(15).
- They are referenced as ETSI standards.
- Work is being conducted by an ISO technical committee (ISO TC 154 (16)) to make these formats ISO standards:
    - XAdES: ISO/CD 14533-2 (17)
    - CAdES: ISO/CD 14533-1 (18)
    - PAdES: ISO 32000-2 (19)

5.2. Comparison of the sample implementations

The availability of several technical implementations gives application developers the freedom of choosing the most appropriate digital evidence format to meet their needs.

X-DEC-R is particularly suited to XML content (stored in clear text) and to the need for integrating digital signatures into business applications. The X-DEC-R format is compatible with the XAdES signature format referenced by the General Repository for Interoperability of the French Administration(20).

C-DEC-R is particularly well suited for signing binary content (stored without transformation). The ability to easily detach the signed content of signatures provides flexibility for storage and the verification of the evidence.

P-DEC-R is particularly suited for applications that emphasize access to the content of the document from a signature verification standpoint. The P-DEC-R format however is reserved for signed content of type PDF.

6. Conclusion

The certified digital evidence profile presented in this document aims to contribute to the development of dematerialization of paper documents, by simplifying and facilitating the creation, verification and exchange of secure digital messages with legal or probative value and their integration into business applications.

7. Annex A: X-DEC-R description

7.1. Generalities

The XAdES signature structure used as DEC-R implementation is based on the XAdES enveloping structure with the `<ds:Object>` element of the signed content moved outside the `<ds:Signature>` element in order to be shared by all signatures within the document. Other reasons why this structure has been chosen are to ensure that it is independent from any specific application or XML structure and to ensure reversibility of the signatures.

However, unlike the CAdES and PAdES signature formats, XAdES is a single signature format.

To enable the creation of certified digital evidences containing a XAdES signature and co-signatures, it is necessary to implement an XML schema acting as a container of XAdES signatures. The additional benefit of defining such a schema is the ability to create a digital evidence structure which contains a single instance of the signed content, with multiple signatures cosigning the same content.

The namespace of this schema is to be published and available at a URL such as http://www.uncefact.org/X-DEC-R#.

The forms of XAdES signatures accepted by the container MUST be at least XAdES-BES and MUST have the following characteristics so as to be compliant with DEC-R:

- XAdES-BES; this characteristic MUST be present in all DEC-R signature. Additionally, to be compliant with DEC-R level 1, the signature MUST contain a reference to the complete certificate chain of the signer, and the evidence MUST contain all the certificates referenced.
- XAdES-EPES; if a signature policy is to be used then the signature format should be compliant with XAdES-EPES and SHOULD be provided with the combination of OID, URI and the imprint and its algorithm of the policy document referenced by the URI.
- XAdES-T; if a signature must contain a timestamp then it SHOULD take the form XAdES-T.
- Other forms of XAdES MAY be used but their specific information MAY be ignored.

7.2. X-DEC-R Schema

The proposed schema is the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema targetNamespace="http://www.uncefact.org/X-DEC-R#"
            xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
            xmlns="http://www.uncefact.org/X-DEC-R#"
            elementFormDefault="qualified">

<!-- Start CertifiedEvidenceType -->
<xsd:element name="CertifiedEvidence" type="CertifiedEvidenceType"/>
<xsd:complexType name="CertifiedEvidenceType">
  <xsd:sequence>
    <xsd:element ref="ds:Signature" maxOccurs="unbounded"/>
    <xsd:element ref="ds:Object" maxOccurs="1"/>
  </xsd:sequence>
  <xsd:attribute name="Version" type="xsd:string" use="required"/>
</xsd:complexType>
<!-- End CertifiedEvidenceType -->
```

```
</xsd:schema>
```

7.3. X-DEC-R schema description

7.3.1. CertifiedEvidence

The required `Version` attribute contains the version of the X-DEC-R document. Its value MUST be set to 1.1.

The `ds:Signature` elements contain signatures of the X-DEC-R document (cf. 7.3.3 Signatures).

The `ds:Object` element is the signed content itself which is the same for each signature (cf. 7.3.2 SignedContent).

This root `CertifiedEvidence` element MUST only contain the following X-DEC-R name space declaration: xmlns:xdecr ="http://www.uncefact.org/X-DEC-R#".

7.3.2. SignedContent

The `ds:Object` element MUST contain the signed content itself. It MUST respect the following constraints:

- The `Id` attribute is MANDATORY. Value of this Id attribute is referenced from a `ds:Reference` element in the ds:SignedInfo element of each cosignature contained in the X-DEC-R document.
- The `MimeType` attribute is MANDATORY. It specifies the MIME type of the signed content.
- The `Encoding` attribute is OPTIONAL. It specifies the method by which the signed content is encoded. If this attribute is present, its value MUST be http://www.w3.org/2000/09/xmldsig#base64 (to specify that the signed content is encoded in base64).

7.3.3. Signatures

To be compliant with DEC-R Core, each XAdES signature contained in an X-DEC-R evidence MUST satisfy all the following conditions:

- The `ds:SignedInfo` element MUST contain two `ds:Reference` elements (order is not important):
  - A `ds:Reference` pointing to the `xad:SignedProperties` element with these constraints:
    - The `Type` attribute is MANDATORY and its value is set to http://uri.etsi.org/01903#SignedProperties.
    - The `URI` attribute is MANDATORY and its value contains an XPointer reference to the `Id` attribute of the `xad:SignedProperties` element.
    - The `ds:Transforms` element is MANDATORY and MUST contain one `ds:Transform` element. This element MUST contain an `URI` attribute with its value set to http://www.w3.org/2001/10/xml-exc-c14n#.
  - For cosignatures:
    - A `ds:Reference` element pointing to the `ds:Object` of the `SignedContent` element with these constraints:

- The Type attribute is MANDATORY and its value is set to http://www.w3.org/2000/09/xmldsig#Object.
- The URI attribute is MANDATORY and its value contains an XPointer reference to the Id attribute of the `ds:Object` element.
- The `ds:Transforms` element is MANDATORY and MUST contain one `ds:Transform` element which contains the canonicalization algorithm applied on the signed content.

For counter signatures:

- A `ds:Reference` element pointing to the `ds:SignatureValue` element of the signature which is counter signed with these constraints:
  - The `Type` attribute is MANDATORY and its value is set to http://uri.etsi.org/01903#CountersignedSignature.
  - The `URI` attribute is MANDATORY and its value contains an XPointer reference to the `Id` attribute of the `ds:SignatureValue` element of the signature which is counter signed.
  - The `ds:Transforms` element is MANDATORY and MUST contain one ds:`Transform` element with the exclusive canonicalisation algorithm http://www.w3.org/2001/10/xml-exc-c14n#.

- The `ds:Signature` element MUST contain one `ds:KeyInfo` element. This element MUST contain one `ds:X509Data` element which MUST only contain a set of `ds:X509Certificate` elements with a `ds:X509Certificate` element which contains the signer's certificate.
- The `ds:Signature` element MUST contain one `ds:Object` element which contains one `xad:QualifyingProperties` element which contains the XAdES signed and unsigned properties.
- The `ds:SignatureValue` element MUST contain an `Id` attribute to be referenced by counter signatures.
- The `xad:SignedProperties` element MUST respect the following constraints:
  - The `xad:SigningCertificate` element is MANDATORY and MUST reference the signer's certificate.
  - The `xad:SigningTime` element MAY be present to contain the time at which the signer claims to have performed the signing process.
  - The `xad:SignatureProductionPlace` element MAY be present to contain a mnemonic for an address associated with the signer at a particular geographical (e.g. city) location.
  - The `xad:SignaturePolicy` element is OPTIONAL. If it is present, this element can contain either the `xad:SignaturePolicyImplied` element (for implicit policy) or the `xad:SignaturePolicyId` element (for explicit policy). If `xad:SignaturePolicyId` is present, the `xad:SigPolicyQualifiers` child element is OPTIONAL but if it is present, it MUST contain one `xad:SPURI` element to specify the URL where a copy of the signature policy MAY be obtained.
  - The `xad:SignerRole` element is OPTIONAL. If it is present, this element MUST contain the `xad:ClaimedRoles` element which contains a sequence of roles claimed by the signer but not certified. The `xad:ClaimedRole` elements MUST contain the role claimed by the signer in a TEXT NODE.

- The `xad:CommitmentTypeIndication` element is OPTIONAL. If it is present, this element MUST contain the `xad:AllSignedDataObjects` element and the type of commitment made by the signer from the following values:

  - http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin
  - http://uri.etsi.org/01903/v1.2.2#ProofOfReceipt
  - http://uri.etsi.org/01903/v1.2.2#ProofOfDelivery
  - http://uri.etsi.org/01903/v1.2.2#ProofOfSender
  - http://uri.etsi.org/01903/v1.2.2#ProofOfApproval
  - http://uri.etsi.org/01903/v1.2.2#ProofOfCreation

- The `xad:DataObjectFormats` element MUST NOT be present in counter signature but is OPTIONAL in cosignature. If it is present, it MUST contain the same MimeType and Encoding as the corresponding attributes of the `ds:Object` element which is contained in the `Document` element. The signed content file name is RECOMMENDED to be added in the `xad:Description` child element.
- The `xad:AllDataObjectsTimeStamp` element MUST NOT be present.
- The `xad:IndividualDataObjectsTimeStamp` element MUST NOT be present.

- The `xad:UnsignedProperties` element MUST respect the following constraints:
  - The `xad:CounterSignature` elements MAY be present. These elements contain the counter signatures of the corresponding signature.
  - Only one `xad:SignatureTimeStamp` element MAY be present.
  - All other elements MAY be present.

In addition to the characteristics of an X-DEC-R Core signature, an X-DEC-R Level 1 signature MUST comply with the following additional specifications:

- The `ds:X509Data` element of the `ds:KeyInfo` element MUST contain a set of `ds:X509Certificate` elements containing all certificates of the signer's certificate path.
- The `xad:SignedProperties` MUST contain the `xad:SigningTime` to specify the time at which the signer (purportedly) performed the signing process.
- The `xad:SigningCertificate` MUST reference all certificates of the signer's certificate path.

7.4. Reversibility

The proposed X-DEC-R implementation guarantees the reversibility of the digital evidence: it is always possible to extract, from the XML container document, a XAdES signature of the signed content, and conversely, it is always possible to create an X-DEC-R digital evidence from a XAdES signature if this signature respects the following conditions:

1. the signature is compliant with the X-DEC-R requirements ;
2. if the signature contain an exclusive canonicalization form in the transform algorithm of the ds:Reference pointed to the signed content, then the <ds:Signature> element of this signature MUST only contain the XMLDSIG and the X-DEC-R namespace declarations (i.e. <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xdecr ="http://www.uncefact.org/X-DEC-R#" />).

The Banking Commission of the French National Bank, which verifies digital evidences produced by banks for their regulatory reporting, has helped validate the feasibility of an X-DEC-R technical implementation.

Since no specific syntax is specified in this specification it must be noted that any application capable of verifying a XAdES signature is capable of validating an X-DEC-R digital evidence.

7.5. Examples

This section provides an example of an X-DEC-R document with 2 cosignatures which complies with the DEC-R Level 1 requirements. This example also shows one of the signatures exported as an independent signature, to demonstrate the reversibility between the X-DEC-R document and its signatures. Conversely, the X-DEC-R document can be viewed as the merger of two independent signatures.

The file below contains an X-DEC-R compatible document containing two cosignatures.

```
<?xml version="1.0" encoding="UTF-8"?>
<xdecr:CertifiedEvidence xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xdecr="http://www.uncefact.org/X-DEC-R#" Version="1.1">[iii]
  <ds:Signature Id="S1">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <ds:Reference Id="S1-REF-1" Type="http://uri.etsi.org/01903#SignedProperties" URI="#S1-
       SignedProperties">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>FuNzsMXA2dnUP2+QoL4GxsPDFdQ=</ds:DigestValue>
      </ds:Reference>
      <ds:Reference Id="S1-REF-2" Type=http://www.w3.org/2000/09/xmldsig#Object
       URI="#SignedContent-E26526FD">[iv]
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>DfKzaZViDw9+pIzCR1n9Hi61AUE=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue Id="S1-SignatureValue">
      MWg59PLtvR7D7S/aMaAfwWfgLo0RcJ5Ua2LrXUtvmtdVs8y4za4t2JjCuc2wseukTf9X/DLN/9GF
      […]
      GIo1Yr6cJxoM+McwwZXaIVQpv2+FVSr6wx8sPg==
    </ds:SignatureValue>
    <ds:KeyInfo>[v]
      <ds:X509Data>
        <ds:X509Certificate>
          MIIGYTCCBcqgAwIBAgIQf/2X2OiJ6FpZeK+bvtlryTANBgkqhkiG9w0BAQQFADBxMRwwGgYDVQQK
          […]
          HNbFjkb7DJgzzZzOKFBsuOFKom51PqPvsMFH0vX3aQKYzPjiB9LRmnY=
        </ds:X509Certificate>
        <ds:X509Certificate>
          MIIDhTCCAm2gAwIBAgIQARorxTn0YWafZ1OFtXbvszANBgkqhkiG9w0BAQUFADAsMRwwGgYDVQQK
          […]
          7LnNkGY8JjGjECOQ1OK9SxYWcIZCDT4B+oCIthQwI8ePAkBBiVlx7+Wdpg7D2lhis/Y=
        </ds:X509Certificate>
        <ds:X509Certificate>
          MIIDiDCCAnCgAwIBAgIQLTlHhbmrvQvFFCfjqDwNdjANBgkqhkiG9w0BAQUFADAsMRwwGgYDVQQK
          […]
          Uo3xm4tY0KhswtXnCATei/NCh+4JnE53aCb8LtAsPspEmfade+v5QSyhXl7f4zMuftZgwtY=
        </ds:X509Certificate>
      </ds:X509Data>
      <ds:KeyValue>
        <ds:RSAKeyValue>
```

[iii] This element refers to the X-DEC-R namespace.
[iv] The signed content pointed by the URI is outside the two Signature elements.
[v] The KeyInfo element provides all the certificates of the certificate chain of the signer including the signer's certificate itself (level 1).

```
        <ds:Modulus>
          wTpTkbnpmM95iGbaB+bSbM5pvCAgzPEBe5Bc5t6+crC3sc//xMDdvpxuaqFnY/OFQHiL107YMOE1
          NJ/x4nhJIUcOIV4Y/Ix38ys9Z4SZh4AB3f36YQ==
        </ds:Modulus>
        <ds:Exponent>AQAB</ds:Exponent>
      </ds:RSAKeyValue>
    </ds:KeyValue>
  </ds:KeyInfo>
  <ds:Object>
    <xad:QualifyingProperties xmlns:xad="http://uri.etsi.org/01903/v1.3.2#" Target="#S1">
      <xad:SignedProperties Id="S1-SignedProperties">
        <xad:SignedSignatureProperties>
          <xad:SigningTime>2010-05-21T16:51:56+02:00</xad:SigningTime>[vi]
          <xad:SigningCertificate>
            <xad:Cert>[vii]
              <xad:CertDigest>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>GmO/4S2oxE9sNE0gOavxF4uJu+njzMfSk4NtZh1IpbI=</ds:DigestValue>
              </xad:CertDigest>
              <xad:IssuerSerial>
                <ds:X509IssuerName>CN=CSF - Classe III - Sign et Crypt,OU=Certification
                 Professionnelle,O=Autorite Consulaire</ds:X509IssuerName>
                <ds:X509SerialNumber>170128686398994124103649996950004657097</ds:X509SerialNumber>
              </xad:IssuerSerial>
            </xad:Cert>
            <xad:Cert>[viii]
              <xad:CertDigest>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>733jcwPtnpMzSQOkz40UTBfHZVaEvcHmRHQDUrEj9kI=</ds:DigestValue>
              </xad:CertDigest>
              <xad:IssuerSerial>
                <ds:X509IssuerName>CN=CSF,O=Autorite Consulaire</ds:X509IssuerName>
                <ds:X509SerialNumber>146511548360387714555394914307636830 7</ds:X509SerialNumber>
              </xad:IssuerSerial>
            </xad:Cert>
            <xad:Cert>
              <xad:CertDigest>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>yZchWoxASR81aAqMTpXmJcVSZj9jylraQ0L57XR75/g=</ds:DigestValue>
              </xad:CertDigest>
              <xad:IssuerSerial>
                <ds:X509IssuerName>CN=CSF,O=Autorite Consulaire</ds:X509IssuerName>
                <ds:X509SerialNumber>601126713771475189977379620600170448 54</ds:X509SerialNumber>
              </xad:IssuerSerial>
            </xad:Cert>
          </xad:SigningCertificate>
          <xad:SignaturePolicyIdentifier>
            <xad:SignaturePolicyImplied>
            </xad:SignaturePolicyImplied>
          </xad:SignaturePolicyIdentifier>
          <xad:SignatureProductionPlace>
            <xad:City>Troyes</xad:City>
            <xad:StateOrProvince/>
            <xad:PostalCode>10000</xad:PostalCode>
            <xad:CountryName>France (FR)</xad:CountryName>
          </xad:SignatureProductionPlace>
        </xad:SignedSignatureProperties>
        <xad:SignedDataObjectProperties>
          <xad:DataObjectFormat ObjectReference="#S1-REF-2">
            <xad:Description>test.xml</xad:Description>
            <xad:MimeType>application/xml</xad:MimeType>
          </xad:DataObjectFormat>
        </xad:SignedDataObjectProperties>
      </xad:SignedProperties>
    </xad:QualifyingProperties>
  </ds:Object>
</ds:Signature>
<ds:Signature Id="S2">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <ds:Reference Id="S2-REF-1" Type="http://uri.etsi.org/01903#SignedProperties" URI="#S2-
```

[vi] The signing time is included as qualifying property (level 1).
[vii] The signer's certificate is included as qualifying property.
[viii] The certifiers' certificates of the signer's certificate are included as qualifying properties (level1).

```
    SignedProperties">
     <ds:Transforms>
       <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
     </ds:Transforms>
     <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
     <ds:DigestValue>NDfLTcaKDVsn63vzvWDxT6on3pQ=</ds:DigestValue>
   </ds:Reference>
   <ds:Reference Id="S2-REF-2" Type="http://www.w3.org/2000/09/xmldsig#Object"
    URI="#SignedContent-E26526FD">
     <ds:Transforms>
       <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
     </ds:Transforms>
     <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
     <ds:DigestValue>DfKzaZViDw9+pIzCR1n9Hi61AUE=</ds:DigestValue>
   </ds:Reference>
 </ds:SignedInfo>
 <ds:SignatureValue Id="S2-SignatureValue">
   bQAgehSceTyA4vyC6ig1NR+ZyfK3TLPwK5yUYtzk4808PzMXIjU4QLn7NMxMZyheMWCKHKjUy+Xd
  […]
   F4BZYrJtHd48js5CFxUzwKEvcDCHdBfOvNXddA==
 </ds:SignatureValue>
 <ds:KeyInfo>
   <ds:X509Data>
     <ds:X509Certificate>
       MIIFozCCBIugAwIBAgISIiHTBC2TsDVWjeLnMAcmycciMA0GCSqGSIb3DQEBBQUAMF4xCzAJBgNV
       […]
       dP+2w9yiHmEzy9/znu7EzD4692jHgg==
     </ds:X509Certificate>
     <ds:X509Certificate>
       MIIExDCCA6ygAwIBAgISESD4VkAj7qL5kQgtsE4CyTchMA0GCSqGSIb3DQEBBQUAMFoxCzAJBgNV
       […]
       VpjKDy+sjJ2wcvFF5MxGFHJtJrZNp3VzTo4x
     </ds:X509Certificate>
     <ds:X509Certificate>
       MIIFdjCCBF6gAwIBAgIEPhy+AzANBgkqhkiG9w0BAQUFADBpMQswCQYDVQQGEwJVUzEjMCEGA1UE
       […]
       Gd2K5ruRtOftLDHvhIZiVO4dNKZQQsOAbguM/QOvn9mg2Q==
     </ds:X509Certificate>
     <ds:X509Certificate>
       MIIEoTCCA4mgAwIBAgIEPhy9KDANBgkqhkiG9w0BAQUFADBpMQswCQYDVQQGEwJVUzEjMCEGA1UE
       […]
       QFEtnptH20KlfB/Cpkiw176SaU2k9ilXxXgRGNyHUcoTsmKdTysyvTGlwfpSqwWIyA==
     </ds:X509Certificate>
   </ds:X509Data>
   <ds:KeyValue>
     <ds:RSAKeyValue>
       <ds:Modulus>
         q3rqKYp30gUcsFwofC7XivkLi38lwtwPiovdjRbpvlvJT3DTisgDVxt5Od9++vp/TAnnHduJUGXM
         Rg8H+EE6INeJTx6Sf16dGKdYe6sAkepvI/X4bw==
       </ds:Modulus>
       <ds:Exponent>AQAB</ds:Exponent>
     </ds:RSAKeyValue>
   </ds:KeyValue>
 </ds:KeyInfo>
 <ds:Object>
   <xad:QualifyingProperties xmlns:xad="http://uri.etsi.org/01903/v1.3.2#" Target="#S2">
     <xad:SignedProperties Id="S2-SignedProperties">
       <xad:SignedSignatureProperties>
         <xad:SigningTime>2010-05-21T16:52:53+02:00</xad:SigningTime>
         <xad:SigningCertificate>
           <xad:Cert>
             <xad:CertDigest>
               <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
               <ds:DigestValue>hq1E/GUxqP5MKCuiz9U/YJO+xUHkIdd/WyRea88aRo4=</ds:DigestValue>
             </xad:CertDigest>
             <xad:IssuerSerial>
               <ds:X509IssuerName>CN=KEYNECTIS K.Sign CDS,OU=KEYNECTIS for
                Adobe,O=KEYNECTIS,C=FR</ds:X509IssuerName>
              <ds:X509SerialNumber>297332752858894691256545704408534442323331 4</ds:X509SerialNumber>
             </xad:IssuerSerial>
           </xad:Cert>
           <xad:Cert>
             <xad:CertDigest>
               <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
               <ds:DigestValue>8JWfW3cSiibWv7OrA0252eQd7qz6Vw6eccnbr3qoum8=</ds:DigestValue>
             </xad:CertDigest>
             <xad:IssuerSerial>
               <ds:X509IssuerName>CN=KEYNECTIS CDS CA,OU=KEYNECTIS for
                Adobe,O=KEYNECTIS,C=FR</ds:X509IssuerName>
```

```
            <ds:X509SerialNumber>14921279929627997717336615148453914975414O9</ds:X509SerialNumber>
          </xad:IssuerSerial>
        </xad:Cert>
        <xad:Cert>
          <xad:CertDigest>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>/3nJ3azjr/aRf/4B7ELGnmMlhS70gHAPbf2yFo1nq8A=</ds:DigestValue>
          </xad:CertDigest>
          <xad:IssuerSerial>
            <ds:X509IssuerName>CN=Adobe Root CA,OU=Adobe Trust Services,O=Adobe Systems
             Incorporated,C=US</ds:X509IssuerName>
            <ds:X509SerialNumber>1042071043</ds:X509SerialNumber>
          </xad:IssuerSerial>
        </xad:Cert>
        <xad:Cert>
          <xad:CertDigest>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>lE5mqpZ705CVLSJCa/HfzTeaLIeiG5QvvKefQfA1Sqw=</ds:DigestValue>
          </xad:CertDigest>
          <xad:IssuerSerial>
            <ds:X509IssuerName>CN=Adobe Root CA,OU=Adobe Trust Services,O=Adobe Systems
             Incorporated,C=US</ds:X509IssuerName>
            <ds:X509SerialNumber>1042070824</ds:X509SerialNumber>
          </xad:IssuerSerial>
        </xad:Cert>
      </xad:SigningCertificate>
      <xad:SignaturePolicyIdentifier>
        <xad:SignaturePolicyImplied>
        </xad:SignaturePolicyImplied>
      </xad:SignaturePolicyIdentifier>
      <xad:SignerRole>
        <xad:ClaimedRoles>
          <xad:ClaimedRole>Project Manager</xad:ClaimedRole>
        </xad:ClaimedRoles>
      </xad:SignerRole>
    </xad:SignedSignatureProperties>
    <xad:SignedDataObjectProperties>
      <xad:DataObjectFormat ObjectReference="#S2-REF-2">
        <xad:Description>test.xml</xad:Description>
        <xad:MimeType>application/xml</xad:MimeType>
      </xad:DataObjectFormat>
    </xad:SignedDataObjectProperties>
  </xad:SignedProperties>
 </xad:QualifyingProperties>
 </ds:Object>
</ds:Signature>
<ds:Object Id="SignedContent-E26526FD" MimeType="application/xml">
 <invoice>
  <reference>
   <number>123456</number>
   <date>2006/06/27</date>
  </reference>
  <customer>
   <name>Goodfellow</name>
   <address>15, Center street</address>
   <city>Boomsville</city>
   <zip>80001</zip>
   <state>Texas</state>
   <country>USA</country>
  </customer>
  <item>
   <description>Pilsner Beer</description>
   <qty>6</qty>
   <unitPrice>1.68</unitPrice>
  </item>
  <item>
   <description>Sausage</description>
   <qty>3</qty>
   <unitPrice>0.59</unitPrice>
  </item>
  <item>
   <description>Portable Barbecue</description>
   <qty>1</qty>
   <unitPrice>23.99</unitPrice>
  </item>
  <item>
   <description>Charcoal</description>
   <qty>2</qty>
   <unitPrice>1.19</unitPrice>
```

```
      </item>
    </invoice>
  </ds:Object>
</xdecr:CertifiedEvidence>
```

In the XML file below, the first signature has been exported from the previous document.

```
<?xml version="1.0" encoding="UTF-8"?>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xdecr="http://www.uncefact.org/X-DEC-R#"
Id="S1">[ix]
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <ds:Reference Id="S1-REF-1" Type="http://uri.etsi.org/01903#SignedProperties" URI="#S1-
     SignedProperties">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>FuNzsMXA2dnUP2+QoL4GxsPDFdQ=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference Id="S1-REF-2" Type="http://www.w3.org/2000/09/xmldsig#Object" URI="#SignedContent-
     E26526FD">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>DfKzaZViDw9+pIzCR1n9Hi61AUE=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue Id="S1-SignatureValue">
    MWg59PLtvR7D7S/aMaAfwWfgLo0RcJ5Ua2LrXUtvmtdVs8y4za4t2JjCuc2wseukTf9X/DLN/9GF
     […]
    GIo1Yr6cJxoM+McwwZXaIVQpv2+FVSr6wx8sPg==
  </ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate>
        MIIGYTCCBcqgAwIBAgIQf/2X2OiJ6FpZeK+bvtlryTANBgkqhkiG9w0BAQQFADBxMRwwGgYDVQQK
         […]
        HNbFjkb7DJgzzZzOKFBsuOFKom51PqPvsMFH0vX3aQKYzPjiB9LRmnY=
      </ds:X509Certificate>
      <ds:X509Certificate>
        MIIDhTCCAm2gAwIBAgIQARorxTn0YWafZ1OFtXbvszANBgkqhkiG9w0BAQUFADAsMRwwGgYDVQQK
         […]
        7LnNkGY8JjGjECOQ1OK9SxYWcIZCDT4B+oCIthQwI8ePAkBBiVlx7+Wdpg7D2lhis/Y=
      </ds:X509Certificate>
      <ds:X509Certificate>
        MIIDiDCCAnCgAwIBAgIQLTlHhbmrvQvFFCfjqDwNdjANBgkqhkiG9w0BAQUFADAsMRwwGgYDVQQK
         […]
        Uo3xm4tY0KhswtXnCATei/NCh+4JnE53aCb8LtAsPspEmfade+v5QSyhXl7f4zMuftZgwtY=
      </ds:X509Certificate>
    </ds:X509Data>
    <ds:KeyValue>
      <ds:RSAKeyValue>
        <ds:Modulus>
          wTpTkbnpmM95iGbaB+bSbM5pvCAgzPEBe5Bc5t6+crC3sc//xMDdvpxuaqFnY/OFQHiL107YMOE1
          NJ/x4nhJIUcOIV4Y/Ix38ys9Z4SZh4AB3f36YQ==
        </ds:Modulus>
        <ds:Exponent>AQAB</ds:Exponent>
      </ds:RSAKeyValue>
    </ds:KeyValue>
  </ds:KeyInfo>
  <ds:Object Id="SignedContent-E26526FD" MimeType="application/xml">
    <invoice>
      <reference>
        <number>123456</number>
        <date>2006/06/27</date>
      </reference>
      <customer>
        <name>Goodfellow</name>
        <address>15, Center street</address>
```

[ix] The X-DEC-R namespace must be referenced to maintain compatibility between the exported the signature and the DEC-R compliant certified digital evidence.

```
      <city>Boomsville</city>
      <zip>80001</zip>
      <state>Texas</state>
      <country>USA</country>
    </customer>
    <item>
      <description>Pilsner Beer</description>
      <qty>6</qty>
      <unitPrice>1.68</unitPrice>
    </item>
    <item>
      <description>Sausage</description>
      <qty>3</qty>
      <unitPrice>0.59</unitPrice>
    </item>
    <item>
      <description>Portable Barbecue</description>
      <qty>1</qty>
      <unitPrice>23.99</unitPrice>
    </item>
    <item>
      <description>Charcoal</description>
      <qty>2</qty>
      <unitPrice>1.19</unitPrice>
    </item>
  </invoice>
</ds:Object>
<ds:Object>
  <xad:QualifyingProperties xmlns:xad="http://uri.etsi.org/01903/v1.3.2#" Target="#S1">
    <xad:SignedProperties Id="S1-SignedProperties">
      <xad:SignedSignatureProperties>
        <xad:SigningTime>2010-05-21T16:51:56+02:00</xad:SigningTime>
        <xad:SigningCertificate>
          <xad:Cert>
            <xad:CertDigest>
              <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
              <ds:DigestValue>GmO/4S2oxE9sNE0gOavxF4uJu+njzMfSk4NtZh1IpbI=</ds:DigestValue>
            </xad:CertDigest>
            <xad:IssuerSerial>
              <ds:X509IssuerName>CN=CSF - Classe III - Sign et Crypt,OU=Certification
                Professionnelle,O=Autorite Consulaire</ds:X509IssuerName>
              <ds:X509SerialNumber>170128686398994124103649996950004657097</ds:X509SerialNumber>
            </xad:IssuerSerial>
          </xad:Cert>
          <xad:Cert>
            <xad:CertDigest>
              <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
              <ds:DigestValue>733jcwPtnpMzSQOkz40UTBfHZVaEvcHmRHQDUrEj9kI=</ds:DigestValue>
            </xad:CertDigest>
            <xad:IssuerSerial>
              <ds:X509IssuerName>CN=CSF,O=Autorite Consulaire</ds:X509IssuerName>
              <ds:X509SerialNumber>146511548360387714555394914307636830 7</ds:X509SerialNumber>
            </xad:IssuerSerial>
          </xad:Cert>
          <xad:Cert>
            <xad:CertDigest>
              <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
              <ds:DigestValue>yZchWoxASR81aAqMTpXmJcVSZj9jylraQ0L57XR75/g=</ds:DigestValue>
            </xad:CertDigest>
            <xad:IssuerSerial>
              <ds:X509IssuerName>CN=CSF,O=Autorite Consulaire</ds:X509IssuerName>
              <ds:X509SerialNumber>601126713771475189977379620600170448 54</ds:X509SerialNumber>
            </xad:IssuerSerial>
          </xad:Cert>
        </xad:SigningCertificate>
        <xad:SignaturePolicyIdentifier>
          <xad:SignaturePolicyImplied>
          </xad:SignaturePolicyImplied>
        </xad:SignaturePolicyIdentifier>
        <xad:SignatureProductionPlace>
          <xad:City>Troyes</xad:City>
          <xad:StateOrProvince/>
          <xad:PostalCode>10000</xad:PostalCode>
          <xad:CountryName>France (FR)</xad:CountryName>
        </xad:SignatureProductionPlace>
      </xad:SignedSignatureProperties>
      <xad:SignedDataObjectProperties>
        <xad:DataObjectFormat ObjectReference="#S1-REF-2">
          <xad:Description>test.xml</xad:Description>
```

```
            <xad:MimeType>application/xml</xad:MimeType>
          </xad:DataObjectFormat>
        </xad:SignedDataObjectProperties>
      </xad:SignedProperties>
    </xad:QualifyingProperties>
  </ds:Object>
</ds:Signature>
```

8. Annex B: C-DEC-R description

The different forms of CAdES signatures MUST have the following characteristics so as to be compliant with DEC-R:

- CAdES-BES; this characteristic MUST be present with a reference to the signer's certificate to be compliant with DEC-R Core. Additionally, to be compliant with DEC-R level 1, the signature MUST contain a reference to the complete certificate chain of the signer, and the evidence MUST contain all the certificates referenced.
- CAdES-EPES; if a signature policy is to be used then the signature format SHOULD be compliant with CAdES-EPES and SHOULD be provided with the combination of OID, URI and the imprint and its algorithm of the policy document referenced by the URI.
- CAdES-T; if a signature must contain a timestamp then it should take the form CAdES-T.

To be compliant with DEC-R Core, the `SignedData` contained in the C-DEC-R evidence MUST satisfy all the following conditions:

- The `encapContentInfo` field MUST contain the signed content in the `eContent` field.
- The `certificates` field MUST contain the signer's certificate of each signature.
- The `clrs` field MUST NOT contain certificate revocation lists (CRLs).
- The `signerInfos` field MUST contain the signature and, if present, the cosignatures.
- The `signedAttrs` field of each `SignerInfo` MUST respect the following constraints:
    - One `contentType` attribute MUST be present and MUST contain the `id-signedData` object identifier (1.2.840.113549.1.7.2).
    - One `messageDigest` attribute MUST be present.
    - One `signing-certificate-v2` attribute MUST be present and MUST reference the signer's certificate.
    - One `content-hints` attribute MUST be present. The `contentType` field MUST contain the `id-data` object identifier (1.2.840.113549.1.7.1) and the `contentDescription` field MUST respect the following constraints:
        - One content type information MUST be present and MUST contain the MIME type of the signed content (e.g. Content-Type: text/plain);
        - One content description is OPTIONAL. If it is present, it MUST contain the file name of the signed content (e.g. Content-Description: JCFV201.txt).
    - One `signing-time` attribute MAY be present to contain the time at which the signer claims to have performed the signing process.
    - One `signer-location` attribute MAY be present to contain a mnemonic for an address associated with the signer at a particular geographical (e.g. city) location.
    - One `signature-policy-identifier` attribute MAY be present to contain the signature policy. If it is present, this attribute can contain either the `signaturePolicyImplied` field (for implicit policy) or the `signaturePolicyId` field (for explicit policy). If `signaturePolicyId` is present, the `sigPolicyQualifiers` field is OPTIONAL but if it is present, it MUST contain one `spuri` qualifier to specify the URL where a copy of the signature policy MAY be obtained.

  - One `signer-attributes` attribute MAY be present. If it is present, this attribute MUST contain the `claimedAttributes` field which contains a sequence of roles claimed by the signer but not certified. Each claimed role MUST be encoded in an `UTF8String`.
  - One `commitment-type-indication` attribute MAY be present. If it is present, the `commitmentTypeidentifier` field MUST contain one of the following values:

    - id-cti-ets-proofOfOrigin OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 1}
    - id-cti-ets-proofOfReceipt OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 2}
    - id-cti-ets-proofOfDelivery OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 3}
    - id-cti-ets-proofOfSender OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 4}
    - id-cti-ets-proofOfApproval OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 5}
    - id-cti-ets-proofOfCreation OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 6}

  - Other attributes MUST NOT be present.

- The `unsignedAttrs` field of each `SignerInfo` MUST respect the following constraints:
  - One `counter-signature` attribute MAY be present. If it is present, it MUST contain one or more counter signatures of the corresponding signature.
  - One `signature-time-stamp` attribute MAY be present. If it is present, it MUST contain one time stamp token.
  - Other attributes MAY be present.

In addition to the characteristics of a C-DEC-R Core signature, a C-DEC-R Level 1 signature MUST comply with the following additional specifications:

- The `certificates` field MUST contain all certificates of the signer's certificate path of each signature.
- For each `SignerInfo`:
  - The `signing-time` signed attribute MUST be present.
  - The `signing-certificate-v2` signed attribute MUST reference all certificates of the signer's certificate path.

Since no specific syntax is specified in this specification it must be noted that any application capable of verifying a CAdES signature is capable of validating a C-DEC-R digital evidence.

9. Annex C: P-DEC-R description

9.1. Generalities

A PDF document can embed multiple digital signatures and offers all the necessary qualities of a DEC-R digital evidence. This section details the specific characteristics of the PDF digital signatures needed to satisfy the DEC-R Core and DEC-R level 1 requirements.

The PDF signature profile compliant with DEC-R is the PAdES Basic signature profile as defined by ETSI TS 102 7786-2[21] and is equivalent to the PDF signature format as defined by the ISO/DIS 32000-1 standard.

It must be noted that this implementation does not provide support for:

- countersignatures (DEC-R requirement R4),
- signature policy (DEC-R requirement R14),
- claimed roles (DEC-R requirement R15).

Implementation notes:

- If the document has to be printed, additional data should be printed on the document so that the reader can check the authenticity and integrity of the document.
- Regarding visible signatures, ongoing work is conducted by ETSI and OASIS on this aspect, but are not currently in the scope of DEC-R.

9.2. P-DEC-R PAdES Basic signature format specifications

The signature format supported by P-DEC-R matches two different types of PDF invisible signatures as defined in paragraph 8.7 of the ISO 32000-1 reference:

- A DEC-R signature with no commitment type or a commitment type different from “Proof of Creation” MUST be implemented as a “Document (or ordinary) signature”;
- A DEC-R signature with a commitment type equal to “Proof of Creation” MUST be implemented as an “MDP (modification detection and prevention) signature, also referred to as an author or certifying signature”. The type of the MDP signature is type 2.

Since no specific syntax is specified in this specification it must be noted that any application capable of verifying a PAdES Basic signature is capable of verifying a P-DEC-R Core certified digital evidence.

9.2.1. P-DEC-R Core specifications

The characteristics of a P-DEC-R Core signature are the following (in conformity with the ISO 32000-1 reference):

1. The signature is encoded in CMS as defined by PKCS#7 format (see RFC 2315 [22]);
2. The "SubFilter" used is “adbe.pkcs7.detached”;
3. The signature MAY contain a time stamp as defined in RFC 3161 (23);
4. The signature MUST NOT contain any OCSP [24] token or CRL [25] as a signed attribute;
5. The signature MUST contain the signer's certificate;

6. The signature MUST sign the signing certificate. Possible ways of doing this are:

    - Adding an additional signed attribute (not defined in the ISO 32000-1) containing the ESS signing certificate V2. This attribute MUST contain a reference to the signer's certificate;
    - Adding the fingerprint of the signing certificate manually inside the document itself.

7. The signature MAY contain the date of signature, the signature's production place and a reason;
8. The reason MUST match the value of the commitment type used for certifying the digital evidence in the form of [CommitmentType=<CommitmentTypeIdentifier>] <Label>, where Label is a string describing the commitment type in the language of the signer, and where CommitmentTypeIdentifier can take the following values: proof_of_origin, proof_of_receipt, proof_of_delivery, proof_of_approval, proof_of_sender. Example: "[CommitmentType=proof_of_receipt] Proof of Receipt".

9.2.2. P-DEC-R Level 1 specifications

In addition to the characteristics of a P-DEC-R Core signature, a P-DEC-R Level 1 signature MUST comply with the following additional specifications:

- Requirement 5 of section 9.2.1 applies to all the certificates of the signer's certificate certification path;
- Requirement 6 of section 9.2.1 applies to all the certificates of the signer's certificate certification path.

10. Annex D (normative): cryptographic algorithms

Because the strength of cryptographic algorithms is evolving over time, it is important for implementers of DEC-R compliant applications to take these evolutions into account.

This annex provides guidance for providing and maintaining algorithms for signature creation and verification.

For signature creation, DEC-R compliant applications SHOULD at a minimum support the following algorithms:

- Hashing algorithms: SHA-256
- Signature algorithms: RSA 2048

For signature verification, DEC-R compliant applications MUST at a minimum support the following algorithms:

- Hashing algorithms: SHA-256
- Signature algorithms: RSA 2048

For signature verification, DEC-R compliant applications SHOULD at a minimum support the following algorithms:

- Hashing algorithms: SHA-1
- Signature algorithms: RSA 1024

If a specific implementation of DEC-R is required using particular algorithms (i.e. elliptical curves), it is recommended to refer to ETSI TS 102 176[(26)].