United Nations ECE/TRADE/C/CEFACT/2010/14

# Economic and Social Council

Distr.: General
27 September 2010

Original: English

## Economic Commission for Europe

Committee on Trade

**Centre for Trade Facilitation and Electronic Business**
**Sixteenth session**
Geneva, 8-10 December 2010
Item 7 of the provisional agenda
**New and revised standards and recommendations**

# Recommendation No. 37: Signed Digital Evidence Interoperability Recommendation

**Submitted for approval by the Architecture, Engineering and Construction Working Group – TBG6**

*Summary*

The Recommendation defines a set of functional rules that signed digital evidence should follow, in terms of the organization and the relationships between the signed content, signatories' certificates and signatures. The TBG6 submits the Recommendation to the Plenary for approval.

# Contents

# Foreword

The Signed Digital Evidence Interoperability Recommendation aims at increasing the level of interoperability of electronically signed digital evidence in order to facilitate the development of paperless international trade.

To achieve this goal, the Recommendation defines a set of functional rules that signed digital evidence should follow, in terms of the organization and the relationships between the signed content, signatories' certificates and signatures.

The Recommendation does not deal with the legal aspects of electronic signatures, which are dealt with at the international level by other documents such as those published by UNCITRAL[1, 2, 3]. Neither does it does deal with the semantics, usability or interpretation of the signed content. This Recommendation does not conflict with UNECE Recommendation 14 "Authentication of trade documents by means other than signature".

To facilitate the implementation of these rules, annex B gives examples of technical implementations using some of the most recent digital evidence standards. This annex may be updated in the future to take into account other proposed technical implementations.

Due to the urgent need for improved interoperability in digital evidence verification, the Recommendation and its annexes are delivered simultaneously to facilitate the rapid deployment of the Recommendation.

# Executive summary

A digital document, unlike a paper document, has little evidence value until it is reinforced by a mechanism, such as an electronic signature, which guarantees its integrity and authenticity.

However, because of the multiplicity of electronic signature standards, verification of signed digital evidence by a recipient may be impossible. This has a direct impact on the ability of businesses and administrations to securely exchange digital documents between themselves and with their administrative and financial counterparts.

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

The verification of signed digital evidence must, at least, give the verifier a clear view of:

- The signatures' parameters (date, place, type of commitment)
- The integrity of the signed content
- The integrity and validity of the signatories' certificates
- The trustworthiness of the certification service providers.

This Recommendation thus defines simple and generic requirements for creating and verifying signed digital evidence to improve its interoperability while keeping in mind that its adoption will elicit requests for changes over time.

# 1. Recommendation No. 37: Signed Digital Evidence Interoperability Recommendation

This Recommendation encourages any organization that wishes to exchange signed digital evidence with others to maximize the interoperability of such evidence by following a set of proposed principles:

Signed digital evidence:

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

Each signature contained in the evidence:

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

## 1.1. Benefits

This Recommendation provides business, administrative and financial organizations with a set of simple and standard requirements for exchanging secure documents, which can be matched by a variety of standard technologies and products, including open source projects.

Its objectives are to:

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

# 2. Context

## 2.1. Scope

1. Since the early 1990s, numerous technical standards for signed digital evidence have been designed, proposed and adopted. Examples of such standards are shown in endnotes from 4 to 12[4, 5, 6, 7, 8, 9, 10, 11, 12].

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

3. The aim of this document is to propose a new approach to signed digital evidence creation and verification, focusing on their functional aspects, as opposed to their technical aspects.

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

5. This Recommendation offers a set of functional requirements to help the design of interoperable signed digital evidence creation and verification applications. It also offers sample implementations of this Recommendation, applied to some of the most recent signed digital evidence technical standards.

6. To ease the referencing of this Recommendation in this document, the abbreviation SDEIR will be used. This stands for “Signed Digital Evidence Interoperability Recommendation”.

### 2.2. Objective

7. 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 probative value and their integration into business applications.

8. 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.

9. 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 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).
- 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.

10. 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.

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

12. As a consequence, the main benefits of the proposed signed digital evidence profile are to:

- Facilitate trust by offering generic functionality to create, verify and easily manage signed digital evidence.
- Ensure interoperability of signed 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

13. This document is intended primarily for organizations and individuals who have the following concerns:

- Exchanging signed digital evidence in an open environment.
- Choosing a format for signed digital evidence, suitable for a particular dematerialization project.
- Monitoring information technology with respect to the fields of digital signatures and probative archiving.
- Ensuring the interoperability, reversibility and validity of signed digital evidence.

## 3. Definitions

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

AdES: Advanced Electronic Signature

BES: Basic Electronic Signature

CAdES: CMS Advanced Electronic Signature

CEN: Comité Européen de Normalisation

Certificate: data message or other record confirming the link between a signatory and signature creation data (Reference 2)

Signed digital evidence: a digital document which can be produced as evidence

CMS: Cryptographic Message Syntax

CRL: Certificate Revocation List

CSP: Certification Service Provider: means a person that issues certificates and may provide other services related to electronic signatures (Reference 1)

CWA: CEN workshop agreement

Cosignature: a signature which applies to the same content as another signature

Counter-signatory: person that holds counter-signature creation data and acts either on its own behalf or on behalf of the person it represents

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”

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)

EPES: Explicit Policy based Electronic Signature

ETSI: European Telecommunications Standards Institute

EU: European Union

ISO: International Organization for Standardization

OASIS: Organization for the Advancement of Structured Information Standards

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

SDEIR: Signed Digital Evidence Interoperability Recommendation

Signatory: person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents (Reference 1)

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

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. SDEIR user guidelines

14. This section describes the functional characteristics and management rules that constitute the SDEIR recommendation.

### 4.1. The SDEIR signed digital evidence profile

15. The Recommendation consists in a signed digital evidence profile designed to maximize interoperability between the creation and verification of signed digital evidence.

16. The profile is described by a set of functional rules.

### 4.2. Functional features of the profile

17. The functional features of the proposed signed 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 as unsigned properties of a signature or counter-signature.
- Signature and counter-signature signed properties:
    - Date of signing: specifies the time at which the signatory claims to have performed the signing process.

- Signatory location: specifies a mnemonic for an address associated with the signatory at a particular geographical (e.g. city) location.
- Reference to a signature policy which describes the precise role and commitments that the signatory 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 signatory.
- Role(s) of the signatory: specifies the role(s) or position(s) claimed by the signatory when signing the data.
- References to the certificate of the signatory and its certifiers.

- Timestamps as unsigned properties of a signature or counter-signature.
- Certificates of the signatories and counter-signatories and their certifiers.

### 4.3. Differences between digital and paper evidence

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

- The identities of the signatories are not always present in paper-based evidence.
- The identities of the ancestors of the signatory are generally not present in paper-based evidence.
- Conversely, signed 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. SDEIR implementation

19. For user guidelines regarding the implementation of the SDEIR recommendation, please refer to annexes A and B.

## 5. Conclusion

20. The signed 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 probative value and to their integration into business applications.

# Annex A (not normative): Functional implementation rules

## A.1. Levels

The SDEIR specification makes use of levels to differentiate the strength of certain SDEIR requirements. In this version, two levels have been defined:

- "Core" is the level that is simpler to implement.
- "Level 1" is a more constrained version of SDEIR and provides better interoperability, for example by imposing a signed date of signature for every signature, as well as signed references of all certifiers and their certificates.

## A.2. 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 defined in RFC 2119 [13].

## A.3. Application profiles

The specification makes provision for two different application profiles:

- SDEIR-compliant creation applications.
- SDEIR-compliant verification applications.

## A.4. Requirements

The 18 SDEIR requirements are described below. These 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 the technical annex for details of some proposed implementations of the SDEIR requirements.

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

R2. Signed digital evidence MUST contain at least one signature. At least five (co) signatures of signed digital evidence MUST be supported by a compliant creation or verification application. If additional co-signatures 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 countersigns.

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. Signed digital evidence MUST contain the certificates of the signatories and counter signatories pointed by the signed references mentioned in [R9].

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

R10-Core. Signed digital evidence MAY contain the certificates of signatories' or counter-signatories' certifiers pointed or not by the signed references mentioned in [R11-Core].

R10-Level 1. Signed digital evidence MUST contain the certificates of all signatories' and counter-signatories' certifiers pointed by the signed references mentioned in [R11-Level 1].

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

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

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 signatory's 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 signatory.

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

R16-Level 1. If present, the type of commitment MUST be one of the following: (The commitment types listed in this requirement have been taken from the CAdES and XAdES standards. This list may evolve in the future.)

- Proof of creation, indicating that the signatory has created the signed content, but has neither approved it, nor is the sender. This particular type of consent is important in the 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[14], which need to be protected only in their integrity and authenticity. Another example, where this type of commitment is useful are contracts that must only be protected in their integrity and authenticity by their originator in the first place but approved by the recipient in the second place (such as, for example, a work contract).

- Proof of approval, indicating that the signatory has approved the signed content.
- Proof of origin, indicating that the signatory acknowledges to have created, approved and be the sender of the signed content.
- Proof of sender, indicating that the entity providing that indication is the sender of the signed content but has not necessarily created it.
- Proof of receipt, indicating that the signatory acknowledges to have received the signed content.
- Proof of delivery, indicating that the timestamp authority providing that indication has delivered the signed content in a local store accessible to the recipient of the signed content.

R17-Core. A signature or counter-signature MAY contain other signed properties. Support of these other signed properties by a SDEIR-compliant verification application is OPTIONAL.

R17-Level 1. A signature or counter-signature MUST NOT contain other signed properties.

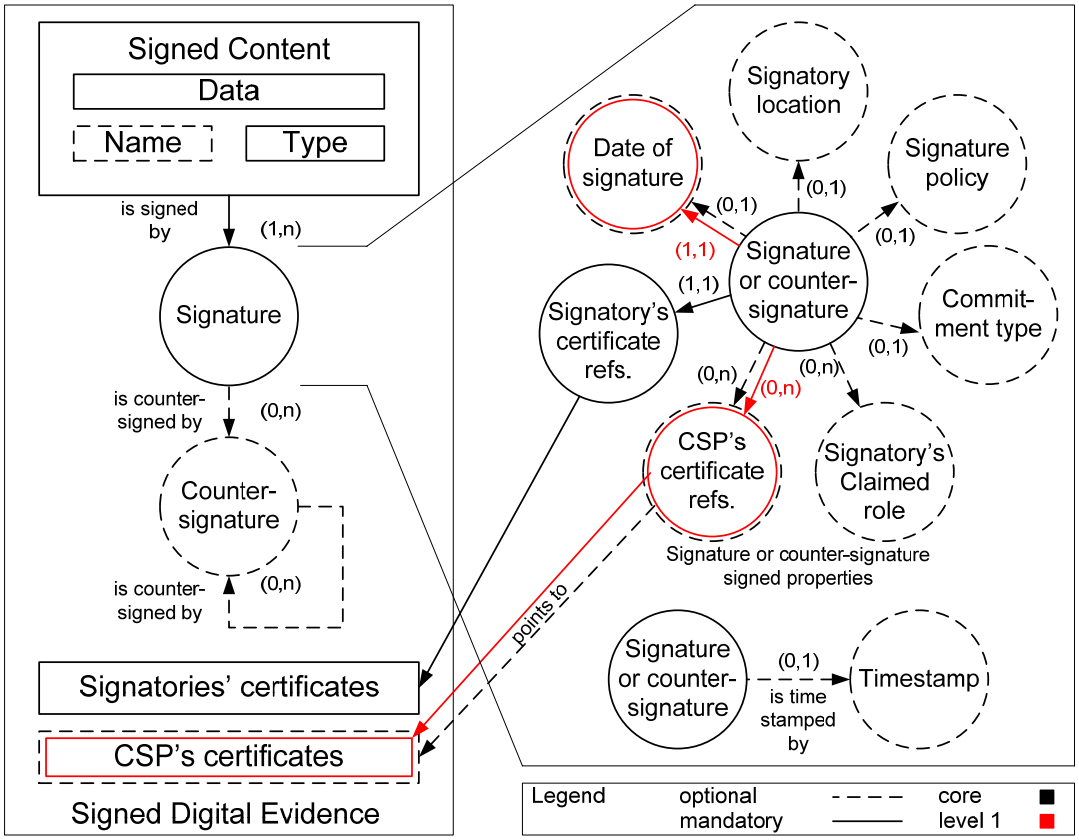
R18. A signature or counter-signature MAY contain other unsigned properties. Support of these other unsigned properties by a SDEIR-compliant verification application is OPTIONAL. The presence of unsupported unsigned properties MUST NOT impact the verifier's interpretation of the signature.

### A.5. SDEIR digital evidence schematic representation

This section provides a schematic representation of the SDEIR digital evidence structure and organization.

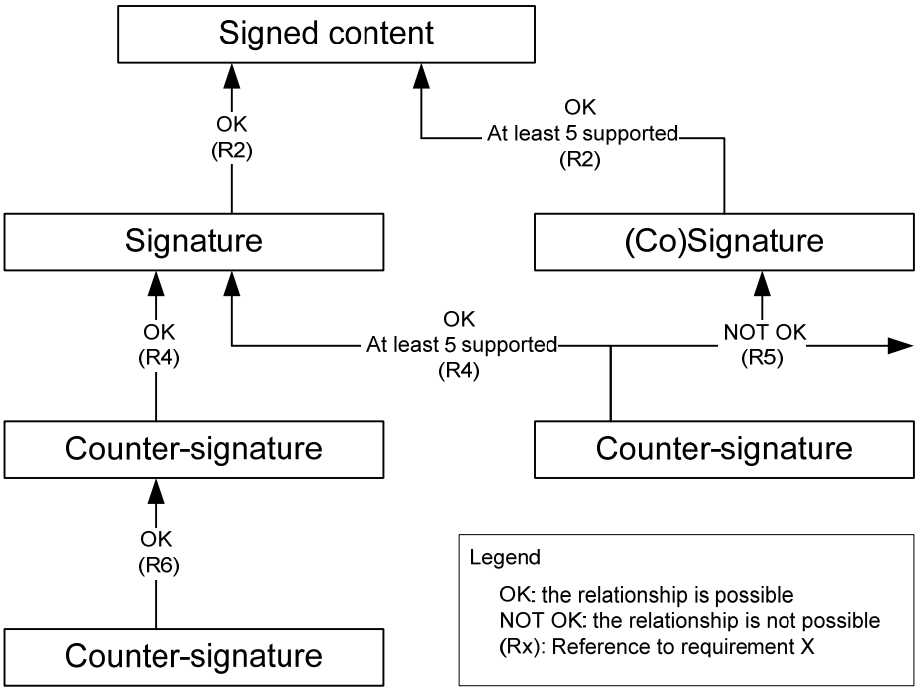
The figure below illustrates the overall structure and organization of SDEIR-compliant signed digital evidence. Requirements 17 and 18 are not represented.

**SDEIR digital evidence: Overall structure and organization representation**



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

**SDEIR digital evidence: Signature relationships representation**




## A.6. SDEIR verification process

The verification of signed digital evidence can be performed by the signatory, the receiver of the message or any interested third party.

### *A.6.1. SDEIR verification status*

The verification of the signed digital evidence includes two verification steps:

- Verification of requirements R1 and R2, which apply to the signed digital evidence as a whole.
- Verification of each signature applied to the signed digital evidence.

The result of the signed digital evidence verification MUST return a status, whose value is:

- PASSED: the signed digital evidence has passed verification; this means that requirements R1 and R2 are met and all signatures have their verification process completed with PASSED.
- NOT PASSED: when requirements R1 and/or R2 are not met and/or one or more signatures or counter-signatures do not pass the verification process, all the failure reasons MUST be returned.

*A.6.2. Signature verification process*

The time reference information used during the verification process of a signature is used to ascertain the validity of the signature at the time the signature is created. This time reference varies according to the signature validation policy applied. Among the possible values used for this time reference are:

- A timestamp provided by a trustable source.
- The time at which the signatory claimed to have performed the signing process.
- A time supplied by the verifier.

The recommended verification process for each signature or counter-signature present in the signed digital evidence includes the following steps:

1. Extract from the signature the certificate of the signatory and verify that it applies to the signature. Verify the integrity of the signed content.
2. Set the signature verification time reference according to the chosen signature validation policy.
3. If the signature verification time reference is given by a timestamp, the signature of the timestamp must be verified.
4. Check the integrity of all certificates involved in the signature using the certificates present in the signature or any other means available to the verifier.
5. Check that all certificates involved in the signature are valid in relation to the signature verification time reference as set in step 2.
6. Check revocation information, valid in relation to the signature verification time reference as set in step 2, of each certificate involved in step 4, using the information in the signature if present and appropriate.
7. Report to the verifier the result of the verification process including the signature time reference used (as set in step 2) and the signatory's certificate and, when present, the following information:
    - Date and time of signature.
    - Signatory's location.
    - Claimed role(s) associated with the signatory.
    - Signature policy or a reference to it.
    - Type of commitment.

Appropriate revocation information SHOULD take into account a grace period, i.e. the time needed for revocation information to be publicly available.

During the signature verification process, requirements R3 through R18 MUST also be met when applicable.

If any additional requirement on the verification process is present in the signature policy or in the signatory's certificate service provider policy, it SHOULD be taken into account.

The result [15] of the signature verification process is:

- PASSED when all the verification steps have passed correctly.
- FAILED when one or more of the verification steps have failed to pass.
- INCOMPLETE when some information required to the verification process is not available.

When the signature verification process fails or cannot be completed, a clear statement about the reason(s) of the failure MUST be reported to the verifier. The verification procedure SHOULD try to complete the verification process even in case of error and SHOULD give a complete report of the problem found.

### A.7. Backward compatibility

Any change in the profile must ensure backward compatibility with earlier versions. It is not possible to conceive evolutions to the profile that would render signed digital evidence created in compliance with previous versions of the profile incompatible, illegal, or non-interoperable.

### A.8. Possible evolutions of the SDEIR profile

Many developments may enhance the SDEIR signed digital evidence profile in the future.

Such developments may provide support for incorporation of data necessary for long-term verification of the signed digital evidence such as AdES-A (Reference 15) (level 2), or mechanisms for verifying the validity of the certificates of the signatories such as TSL [16] (level 2).

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

Also, future enhancements of SDEIR may provide support for:

- Attached signature (detached signature and multiple signed contents packaging) [17].
- Signature kinematics.

# Annex B (not normative): Technical implementation guidelines of the SDEIR recommendation

The SDEIR profile is necessarily used in conjunction with a technical implementation that implements and supports its rules and characteristics.

## B.1. Overview of sample implementations

Three digital signature standards have already been studied and successfully evaluated for SDEIR implementations:

- A XAdES implementation based on ETSI TS 101 903 v1.4.1. When implemented, the format of the signed digital evidence is referred to as X-SDEIR in the rest of this document. This implementation will be described in a future update of this technical annex.
- A CAdES implementation based on ETSI TS 101 733 v1.8.1. When implemented, the format of the signed digital evidence is referred to as C-SDEIR in the rest of this document. This implementation is described in B.4: C-SDEIR description.
- A PAdES implementation based on ETSI TS 102 778 v1.1.1. When implemented, the format of the signed digital evidence is referred to as P-SDEIR in the rest of this document. This implementation is described in B.5.: P-SDEIR description.

The main reasons that led to the study of these digital signature standards as SDEIR 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 [18].
- They are referenced as ETSI standards.
- Work is being conducted by an ISO technical committee (ISO TC 154 [19]) to make these formats ISO standards:
    - XAdES: ISO/CD 14533-2 [20]
    - CAdES: ISO/CD 14533-1 [21]
    - PAdES: ISO 32000-2 [22]

## B.2. Comparison of the sample implementations

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

X-SDEIR is particularly suited to XML content (stored in clear text) and to the need for integrating digital signatures into business applications. The X-SDEIR format is compatible with the XAdES signature format referenced by the General Repository for Interoperability of the French Administration [23].

C-SDEIR 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 signed digital evidence.

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

### B.3. X-SDEIR description

This description will be provided in a future version of this technical annex.

### B.4. C-SDEIR description

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

- CAdES-BES: this characteristic MUST be present with a reference to the signatory's certificate to be compliant with SDEIR Core. Additionally, to be compliant with SDEIR level 1, the signature MUST contain a reference to the complete certificate chain of the signatory, and the signed digital 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, it should take the form CAdES-T.

To be compliant with SDEIR Core, the SignedData contained in the C-SDEIR digital 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 signatory'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 signatory's certificate.
    - One content-hints attribute MUST be present. The content Type field MUST contain the id-data object identifier (1.2.840.113549.1.7.1) and the content Description 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 signatory claims to have performed the signing process.
    - One signer-location attribute MAY be present to contain a mnemonic for an address associated with the signatory at a particular geographical 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 signatory but not signed. 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 present, it MUST contain one or more counter-signatures of the corresponding signature.
    - One signature-timestamp attribute MAY be present. If present, it MUST contain one timestamp token.
    - Other attributes MAY be present.

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

- The certificates field MUST contain all certificates of the signatory’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 signatory's certificate path.

Since no specific syntax is specified in this specification, that any application capable of verifying a CAdES signature is capable of validating C-SDEIR digital evidence.

## B.5. P-SDEIR description

### *B.5.1. Generalities*

A PDF document can embed multiple digital signatures and offer all the necessary qualities of SDEIR digital evidence. This section details the specific characteristics of the PDF digital signatures needed to satisfy the SDEIR Core and Level 1 requirements.

The PDF signature profile compliant with SDEIR is the PAdES Basic signature profile as defined by ETSI TS 102 7786-2 [24] 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:

- Counter-signatures (SDEIR requirement R4).
- Signature policy (SDEIR requirement R14).
- Claimed roles (SDEIR 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 being conducted by the European Telecommunications Standards Institute (ETSI) and the Organization for the Advancement of Structured Information Standards (OASIS) on this aspect, but this is not currently in the scope of SDEIR.

### *B.5.2. P-SDEIR PAdES Basic signature format specifications*

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

- An SDEIR signature with no commitment type or a commitment type different from "Proof of Creation" MUST be implemented as a "Document (or ordinary) signature";
- An SDEIR 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 MDP signature is type 2.

Since no specific syntax is specified, any application capable of verifying a PAdES Basic signature is capable of verifying a P-SDEIR Core signed digital evidence.

#### *B.5.2.1. P-SDEIR Core specifications*

The characteristics of a P-SDEIR 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 [25]);
2. The "SubFilter" used is "adbe.pkcs7.detached";

3. The signature MAY contain a timestamp as defined in RFC 3161 [26];

4. The signature MUST NOT contain any OCSP [27] response or CRL [28] as a signed attribute;

5. The signature MUST contain the signatory'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 signatory'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 signed digital evidence in the form of [CommitmentType=<CommitmentTypeIdentifier>] <Label>, where Label is a string describing the commitment type in the language of the signatory, 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".

*B.5.2.2. P-SDEIR Level 1 specifications*

A P-SDEIR Level 1 signature MUST additionally comply with the following specifications:

- Requirement 5 of section 0 applies to all the certificates of the signatory's certificate certification path.
- Requirement 6 of section 0 applies to all the certificates of the signatory's certificate certification path.

## Annex C (normative): Cryptographic algorithms

Because the strength of cryptographic algorithms is evolving over time, it is important for implementers of SDEIR 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, SDEIR-compliant applications SHOULD at a minimum support the following algorithms:

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

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

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

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

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

If a specific implementation of SDEIR is required using particular algorithms (i.e. elliptical curves), it is recommended to refer to ETSI TS 102 176 [29].

## References


[1] Model Law on Electronic Commerce Adopted by the United Nations Commission on International Trade Law: http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

[2] Model Law on Electronic Signatures of the United Nations Commission on International Trade Law: http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf

[3] Promoting Confidence in Electronic Commerce: Legal Issues on the International Use of Electronic Authentication and Signature Methods: http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf

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

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

[6] CMS: http://www.ietf.org/rfc/rfc3852.txt

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

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

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

[10] 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

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

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

[13] Keywords: http://www.faqs.org/rfcs/rfc2119.html

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

[15] CWA 14171 on electronic signature verification: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14171-00-2004-May.pdf

[16] TSP Status List (ETSI TS 102 231): http://www.etsi.org

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

[18] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

[19] ISO TC 154 : http://www.iso.org/iso/iso_technical_committee.html?commid=53186

[20] ISO/CD 14533-2: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56025

[21] ISO/CD 14533-1: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56024

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

[23] XAdES digital signature profile of the French Administration: http://www.references.modernisation.gouv.fr/sites/default/files/FormatdeSignature_Xades_V1_0.pdf

[24] PAdES Basic (ETSI TS 102 778-2): http://www.etsi.org

[25] RFC 2315: http://www.ietf.org/rfc/rfc2315.txt

[26] Timestamping: RFC 3161: http://www.ietf.org/rfc/rfc3161.txt & X9.95: http://www.x9.org/news/pr050701

[27] Online Certificate Status Protocol: http://www.ietf.org/rfc/rfc2560.txt

[28] Certificate Revocation List: http://www.ietf.org/rfc/rfc5280.txt

[29] Algorithms and Parameters for Secure Electronic Signatures (ETSI TS 102 176): http://www.etsi.org