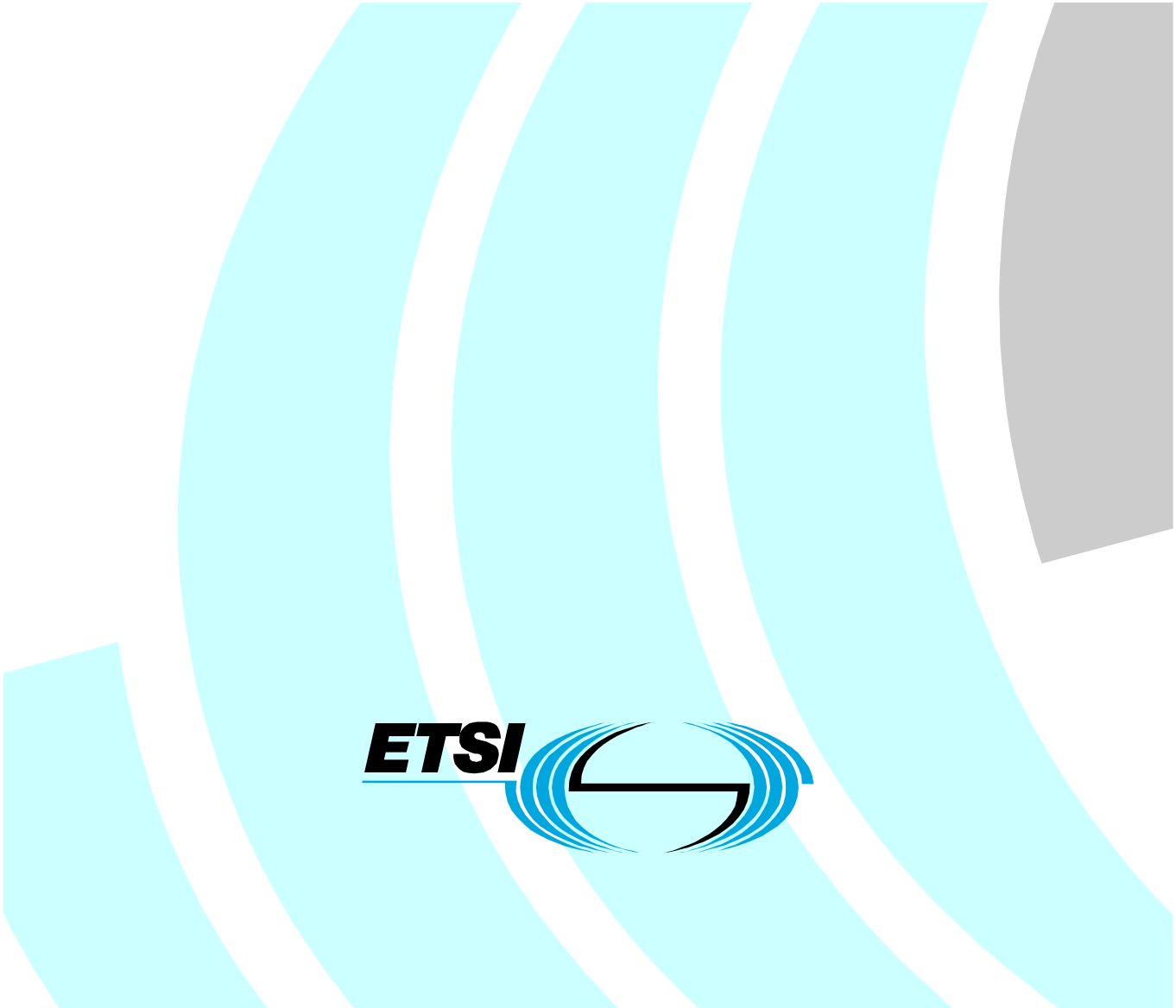
ETSI TS 102 734 V1.1.1 (2007-02)

Technical Specification

Electronic Signatures and Infrastructures;
Profiles of CMS Advanced Electronic Signatures
based on TS 101 733 (CAdES)



Reference
DTS/ESI-000042

Keywords
electronic signature, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Introduction

TS 101 733 [1] (CAdES henceforth) specifies formats for Advanced Electronic Signatures built on CMS [2]. That document defines a number of signed and unsigned optional signature attributes, resulting in support for a number of variations in the signature contents and powerful processing requirements.

In order to maximize interoperability in communities applying CAdES to particular environments it is necessary to identify a common set of options that are appropriate to that environment. Such a selection is commonly called a profile.

The present document defines three profiles that minimize the differences between implementations and so maximize interoperability. The two first profiles are suitable for specific business areas, namely e-Invoicing and e-Government, respectively. The third profile provides a baseline for other application areas.

Profiles specified in clauses 5, 6 and 7 are based on the actual usage of the CMS [2] and CAdES [1] options, as emerged from a survey conducted by ETSI over a substantial number of prominent European actors in the electronic signature domain.

Therefore the following provisions represent a general consensus of the use of these standards and hence provide a reliable basis for maximizing interoperability. Nevertheless, in particular business areas and niches there may be specific needs and/or regulations that may require variations to these profiles.

1 Scope

The present document profiles the use of TS 101 733 (CAdES) [1] signatures, based on CMS [2] for its use within the following specific environments as follows:

- e-Invoicing area.
- e-government area.
- a baseline for other application areas.

These profiles do not repeat the base requirements of the referenced standards, but their aim is to maximize interoperability of CMS-based advanced electronic signatures in the e-Invoicing and e-Government business areas. In addition to that, the baseline profile is given as basis for interoperability profiles in other application areas.

Optional elements defined in CAdES [1] but not specified in the current document are treated as optional for both generator and verifiers.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

[1] ETSI TS 101 733 (V1.7.3): "Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)".

[2] IETF RFC 3852: "Cryptographic Message Syntax (CMS)".

[3] IETF RFC 2634: "Enhanced Security Services for S/MIME".

[4] draft-ietf-smime-escertid-01.txt (October 2006): "ESS Update: Adding CertID Algorithm Agility".

[5] ITU-T Recommendation X.509 / ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[6] IETF RFC 3280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[7] CEN Workshop Agreement 15579 to be published: "E-invoices and digital signatures".

NOTE: As a fault has been identified in the 2006 version CWA 15579, it will be updated soon after publication of this TS. Implementations should refer to this revised version

[8] IETF RFC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[9] ETSI TS 102 176-1(V1.2.1): "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

[10] CEN Workshop Agreement 14171 (2004): "General guidelines for electronic signature verification".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

generator: any party which creates, or adds attributes to, a signature

NOTE: This may be the signatory or any party which initially verifies or further maintains the signature.

long term signatures: signatures that are expected to be verified beyond the signers' certificate expiration date and, possibly, even after the expiration date of the certificate of the signers' certificate-issuing CA

NOTE: Refer to CWA 14171, clause 5.1 [10].

protocol element: element of the protocol which may be including data elements and / or elements of procedure

service element: element of service that may be provided using one or more protocol elements

NOTE: All alternative protocol elements provide an equivalent service to the users of the protocol.

short term signatures: signatures that are to be verified for a period of time that does not go beyond the signers' certificate expiration date

NOTE: Refer to CWA 14171, clause 5.1 [10].

verifier: entity that validates or verifies an electronic signature

The present document makes use of certain key words to signify requirements. Below follows their definitions:

may: Means that a course of action is permissible within the limits of the present document.

shall: Means that the definition is an absolute requirement of the present document. It has to strictly be followed in order to conform to the present document.

should: Means that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required. Implementers may know valid reasons in particular circumstances to ignore this recommendation, but the full implications must be understood and carefully weighed before choosing a different course.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CA	Certification Authority
CAdES	CMS Advanced Electronic Signatures

NOTE: As per TS 101 733 [1].

CEN	European Committee for Standardization
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
CWA	CEN Workshop Agreement
ESS	Enhanced Security Services
OCSP	Online Certificate Status Protocol
TSP	Trusted Service Providers
TST	Time-Stamp Token

4 General requirements

4.1 Algorithm requirements

Implementers are strongly recommended to take into account TS 102 176-1 [9] when selecting algorithms and key lengths.

4.2 Compliance requirements

Profiles in the present document define separated requirements for both generator and verifier of CAdES signatures. Requirements are grouped in three different categories, each one having its corresponding identifier. Table 1 defines these categories and their identifiers.

Table 1: Requirement categories

Identifier	Requirement on generator	Requirement on verifier
M	Generator shall include the element in the signature.	Verifier shall process the element.
R	Generator should include the element in the signature.	Verifier shall process the element if present.
O	Generator may include the element in the signature.	Verifier may either process or ignore this element and process the rest of the signature.

Clauses 5 to 7 specify additional requirements on signature formats that must be taken into account along with those ones already present in TS 101 733 (CAdES) [1] and CMS [2].

Systems claiming to support the CAdES profile for e-Invoicing shall be compliant with requirements in clauses 5.1, 5.2, 5.3 and 5.5. Systems claiming to support the CAdES profile for e-Invoicing with support for long term signatures shall also be compliant with requirements in clause 5.4.

Systems claiming to support the CAdES profile for e-Government shall be compliant with requirements in clauses 6.1, 6.2, 6.3 and 6.5. Systems claiming to support the CAdES profile for e-Government with support for long term signatures shall also be compliant with requirements in clause 6.4.

Systems claiming to support the CAdES baseline profile shall be compliant with requirements in clauses 7.1, 7.2, 7.3 and 7.5. Systems claiming to support the CAdES baseline profile with support of long term signatures shall also be compliant with requirements in clause 7.4.

Optional elements defined in CAdES [1] but not specified in the current document are treated as "O" as above for both generator and verifiers. In certain cases, elements are marked with an "O" for both generator and verifier to bring the readers" attention to the fact that their processing is optional.

Certain service elements may be provided by different protocol elements at user's choice. In these cases the semantics of M, R and O defined in the table above depend on the requirement for the service element itself. Tables 2 to 4 (each one applies to a different requirement on the service element) define these semantics.

Table 2: Requirements for mandatory service with choices

Requirement Identifier for the Service / Protocol element	Requirement on generator	Requirement on verifier
Service = M	Generator shall provide the service by including one protocol element chosen from the list of choices.	Verifiers shall be able to process at least one of the protocol elements in the list of choices.
Protocol Choice = R	Generator should use this protocol element for providing the mandatory service element.	Verifiers shall process this protocol element if present.
Protocol Choice = O	Generator may use this protocol element for providing the mandatory service elements.	Verifiers may ignore this protocol element.

Table 3: Requirements for recommended service with choices

Requirement Identifier for the Service / Protocol element	Requirement on generator	Requirement on verifier
Service = R	Generator should provide the service by including one protocol element chosen from the list of choices.	Verifiers shall be able to process at least one of the protocol elements in the list of choices.
Protocol Choice = R	If the generator decides to provide the service, then she should use this protocol element.	Verifiers shall process this protocol element if present.
Protocol Choice = O	Generator may use this protocol element for providing the service elements.	Verifiers may ignore this protocol element.

Table 4: Requirements for optional service with choices

Requirement Identifier for the Service / Protocol element	Requirement on generator	Requirement on verifier
Service = O	Generator may provide the service by including one protocol element chosen from the list of choices.	Verifiers may ignore protocol elements providing this service.
Protocol Choice = R	If the generator decides to provide the service, then she should use this protocol element.	If supporting this service verifiers shall process this protocol element if present.
Protocol Choice = O	If the generator decides to provide the service, then she MAY use this protocol element.	Verifiers may ignore this protocol element.

The present document shows new requirements for each service and protocol element in tabular form. Below follows the structure of the table:

Table 5: Requirements for optional service with choices

Service / Protocol element	Reference	Requirement on generator	Requirement on verifier	Notes / Additional requirements
Service:				
Choice 1				
Choice 2				

Column **Service / Protocol element** will identify the service element or protocol element the requirement applies to. Service elements that may be implemented by different protocol elements (i.e. users may make a choice on several protocol elements) build tables with more than one row.

Column **Reference** will reference the relevant clause of the standard where the element is first defined. The reference is to CAdES [1], except where explicitly indicated otherwise.

Column **Requirement on generator** will contain an identifier of the requirement, as defined in table 1, bound to the corresponding protocol element for the generator.

Column **Requirement on verifier** will contain an identifier, as defined in table 1, of the requirement bound to the corresponding protocol element for the verifier of the signature.

Column **Notes / Additional requirements** will contain numbers referencing notes and/or letters referencing additional requirements. Both notes and additional requirements are listed below the table.

Profiles may be affected by applicable regulations; hence implementers should check, and abide by as appropriate, any applicable regulation that may affect these profiles.

5 CAdES profile for e-Invoicing

This clause defines a profile for CAdES signatures to be applied to electronic signatures applied on e-Invoices.

5.1 Elements defined in CMS

5.1.1 Placement of the signature

Table 6

Service / Protocol element	CMS [2] Reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Service: signature		M	M	
Enveloping with data	Clause 5.2	R	R	
Detached Signature	Clause 5.2	O	R	

5.1.2 Signer identifier

Table 7

Service / Protocol element	CMS [2] Reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Service: signer identifier	Clause 5.3	M	M	
`issuerAndSerialNumber`	Clause 5.3	R	R	
`subjectKeyIdentifier`	Clause 5.3	O	O	

5.1.3 Content type

Table 8

Service / Protocol element	CMS [2] Reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
`ContentType`	Clause 11.1	M	M	

5.1.4 Message digest

Table 9

Service / Protocol element	CMS [2] Reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Message digest	Clause 11.2	M	M	

5.1.5 Signing time

Table 10

Service / Protocol element	CMS [2] Reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
`signing-time`	Clause 11.3	O	O	

5.1.6 Countersignature

Table 11

Service / Protocol element	CMS [2] Reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
`counterSignature`	Clause 11.4	O	O	a

Additional requirement:

a) Use of countersignatures should be agreed upon in a prior arrangement between the generator and the verifier so that the verifier is aware of the presence, number and meaning of the countersignature.

5.1.7 Parallel signatures

Table 12

Service / Protocol element	CMS [2] reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
`SignerInfos`	Clause 5.3	O	O	a

Additional requirement:

a) Use of parallel signatures should be agreed upon in a prior arrangement between the generator and the verifier so that the verifier is aware of their presence, number and meaning.

5.2 Elements defined in ESS

5.2.1 Signing certificate

Table 13

Service / Protocol element	ESS [3] and [4] reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Service: protection of signing certificate		M	M	
`ESS signing-certificate`	ESS [3], Clause 5.4	R	R	a
`ESS signing-certificate` v2	ESS [4], Clause 3	O	R	a

Additional requirement:

a) Generators should migrate to the use of `ESS signing-certificate` v2 in preference to `ESS signing-certificate` in line with the guidance regarding limited lifetime for the use of SHA-1 given in clause 9.4 of TS 102 176-1 [9].

5.3 Additional attributes defined in CAdES

5.3.1 Signature time-stamp / time-mark

Table 14

Service / Protocol element	Reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Service: Trusted signing time		R	R	
signature-time-stamp	Clause 6.1.1	R	R	
Time-mark	Clause 4.4	O	O	

NOTE: The signature time-stamp assists in making the difference between valid and invalid electronic signatures in case the signer's certificate has been revoked.

5.4 Additional attributes defined in CAdES for long term signatures

The requirements specified in all 5.4 clauses are only applicable to systems managing long term signatures. Further details of procedures for the management of signatures over the long term may be found in CWA 14171, clause 5.1 [10].

5.4.1 Certificate references

Table 15

Service / Protocol element	Reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Complete-certificate-references	Clause 6.2.1	R	R	

5.4.2 Revocation status references

Table 16

Service / Protocol element	Reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Service: complete revocation status references	Clause 6.2.2	R	R	
complete-revocation-references.crlidss	Clause 6.2.2	O	R	a
complete-revocation-references.ocspids	Clause 6.2.2	O	R	a

NOTE 1: The generator is recommended to make use of this service, using either CRLs or OCSP Responses. The verifier should be able to handle both.

NOTE 2: This attribute should be generated and added when the meaningful issue of the required component of revocation and validation data become available. This may require taking into account a grace period. A grace period permits certificate revocation information to propagate through the revocation processes. This period could extend from the time an authorized entity requests for a certificate revocation, to when the revocation information is available for the relying to use. In order to make sure that the certificate was not revoked at the time the signature was time-marked or time-stamped, the generation of this attribute should wait until the end of the grace period.

NOTE 3: `complete-revocation-references.crlidss requires use of` CRLs [5] and `complete-revocation-references.ocspids` requires use of OCSP [8] Responses.

Additional requirement:

a) The revocation status information shall be the one that encompasses the time of signing.

5.4.3 Certificate values

Table 17

Service / Protocol element	Reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Service: certificate values		R	R	
`certificate-values`	Clause 6.3.3	O	O	
Certificates maintained by CA or other trusted service		O	O	a

Additional requirement:

a) If a Certification Authority (CA), or other trusted service, is trusted to keep certificates not already held within the signature for the archiving period and it is known where and how to obtain them, there is no need to hold them within the signature. This requires prior agreement between the verifier and the trust service provider / CA.

5.4.4 Revocation status values

Table 18

Service / Protocol element	Reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Service: revocation status values		R	R	
`revocation-values.crlVals`	Clause 6.3.4	O	O	a
`revocation-Values.ocspVals`	Clause 6.3.4	O	O	a
Revocation status values maintained by CA or other trusted service		O	O	a, b

NOTE: `revocation-values.crlVals requires use of` CRLs [5] and `revocation-Values.ocspVals` requires use of OCSP [8] Responses.

Additional requirements:

a) A verifier should be able to process a CRL and an OCSP Response regardless of where it fetches this revocation status information.

b) If a Certification Authority (CA) or other trusted service is trusted to keep revocation status information for the archiving period and it is known where and how to obtain them, then there is no need to hold revocation information within the signature. This requires prior agreement between the verifier and the trust service provider / CA.

5.4.5 Archive time-stamp

Table 19

Service / Protocol element	Reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
`archive-time-stamp`	Clause 6.4.1	O	O	a

Additional requirement:

a) The requirement for verifiers becomes R if there are no alternative technical or organizational mechanisms to maintain the validity of the signed document over the period of storage.

5.5 Other standards

5.5.1 X.509 Certificates

Table 20

Service / Protocol element	Reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
X.509 Certificate Profile	RFC 3280 [6]	M	M	1

NOTE 1: ETSI has defined suitable certificate profiles (TS 101 862 and TS 102 280).

NOTE 2: RFC 3280 [6] is a profile of X.509 [5].

5.5.2 Certificate key usage for e-Invoicing

Table 21

Service / Protocol element	CWA on e-Invoices and digital signatures [7] Reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Certificate extended Key Usage id= `kp-eInvoicing` (non critical)	Clause 5.7.2	R	O	

NOTE: As a fault has been identified in the 2006 version CWA 15579, it will be updated soon after publication of this TS. Implementations should refer to this revised version

5.5.3 Naming

Table 22

Service / Protocol element	CWA on e-Invoices and digital signatures [7] reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Certificate `Subject.Organization`	Clause 5.7	R	R	a

Table 23

Service / Protocol element	CWA on e-Invoices and digital signatures [7] reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Certificate `Subject.CommonName`	Clause 5.7	R	O	b, c

Table 24

Service / Protocol element	CWA on e-Invoices and digital signatures [7] reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Certificate `Subject.OrganizationalUnit`	Clause 5.7	O	O	d

Additional requirements:

a) The subject organization should identify the organization issuing the invoice.

b) If the invoice is signed by a human the Subject Common Name should identify the physical person signing the invoice within the issuing organization.

c) If the invoice is signed by a system the Subject Common Name should identify that system using, for example, the Internet Domain Name of that system.

d) Where more than one department in an organization independently issue invoices, Subject Organizational Unit should identify that department.

6 CAdES profile for e-Government

This clause defines a profile for CAdES signatures to be applied to electronic signatures applied on e-Government.

In addition to the general warning in the last sentence of clause 4.2, it should be noted that relationships with Governmental agencies may be governed by specific rules that address also technical provisions related to exchanging electronic communications.

6.1 Elements defined in CMS

6.1.1 Placement of the signature

Table 25

Service / Protocol element	CMS [2] reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Service: signature		M	M	
Enveloping with data	Clause 5.2	R	R	
Detached Signature	Clause 5.2	O	R	

6.1.2 Signer identifier

Table 26

Service / Protocol element	CMS [2] reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Service: signer identifier	Clause 5.3	M	M	
`issuerAndSerialNumber`	Clause 5.3	R	R	
`subjectKeyIdentifier`	Clause 5.3	O	O	

6.1.3 Content type

Table 27

Service / Protocol element	CMS [2] reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
`ContentType`	Clause 11.1	M	M	

6.1.4 Message digest

Table 28

Service / Protocol element	CMS [2] reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Message digest	Clause 11.2	M	M	

6.1.5 Signing time

Table 29

Service / Protocol element	CMS [2] reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
`signing-time`	Clause 11.3	O	O	

6.1.6 Countersignature

Table 30

Service / Protocol element	CMS [2] reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
`counterSignature`	Clause 11.4	O	R	a

Additional requirement:

a) Use of countersignatures should be agreed upon in a prior arrangement between the generator and the verifier so that the verifier is aware of the presence, number and meaning of the countersignature.

6.1.7 Parallel signatures

Table 31

Service / Protocol element	CMS [2] reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
`SignerInfos`	Clause 5.3	O	R	a

Additional requirement:

a) Use of parallel signatures should be agreed upon in a prior arrangement between the generator and the verifier so that the verifier is aware of their presence, number and meaning.

6.2 Elements defined in ESS

6.2.1 Signing certificate

Table 32

Service / Protocol element	ESS [3] [4] reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Service: protection of signing certificate		M	M	
`ESS signing-certificate`	ESS [3], Clause 5.4	R	R	a
`ESS signing-certificate` v2	ESS [4], Clause 4	O	R	a

Additional requirement:

a) Generators should migrate to the use `ESS signing-certificate` v2 in preference to `ESS signing-certificate` in line with the guidance regarding limited lifetime for the use of SHA-1 given in clause 9.4 of TS 102 176-1 [9].

6.3 Additional attributes defined in CAdES

6.3.1 Signature time-stamp / time-mark

Table 33

Service / Protocol element	Reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
Service: Trusted signing time		R	R	
`signature-time-stamp`	Clause 6.6.1	O	R	1
Time-mark	Clause 4.4	O	O	2

NOTE 1: The signature time-stamp assists in making the difference between valid and invalid electronic signatures in case the signer's certificate has been revoked.

NOTE 2: Governmental agencies or other trust service providers (TSP) may act in practice as "trusted signed documents storage providers" for the documents they send or receive. In this case there is no need to add time stamp tokens (or at least to add a TST chain) to these documents since the Governmental agency or TSP provides the necessary trust on the signature time, implementing in practice a "time mark".

6.4 Additional attributes defined in CAdES for long term signatures

The requirements specified in all 6.4 clauses are only applicable to systems managing long term signatures. Further details of procedures for the management of signatures over the long term may be found in CWA 14171, clause 5.1 [10].

6.4.1 Certificate references

Table 34

Service / Protocol element	Reference	Generator requirement	Verifier requirement	Additional requirements / notes
`complete-certificate-references`	Clause 6.2.1	R	R	

6.4.2 Revocation status references

Table 35

Service / Protocol element	Reference	Generator requirement	Verifier requirement	Additional requirements / notes
Service: complete revocation status references	Clause 6.2.2	R	R	
`complete-revocation-references.crlidss`	Clause 6.2.2	O	R	a
`complete-revocation-references.ocspids`	Clause 6.2.2	O	R	a

NOTE 1: The generator is recommended to make use of this service, using either CRLs or OCSP Responses. The verifier should be able to handle both.

NOTE 2: This attribute should be generated and added when the meaningful issue of the required component of revocation and validation data become available. This may require taking into account a grace period. A grace period permits certificate revocation information to propagate through the revocation processes. This period could extend from the time an authorized entity requests for a certificate revocation, to when the revocation information is available for the relying to use. In order to make sure that the certificate was not revoked at the time the signature was time-marked or time-stamped, the generator of this attribute should wait until the end of the grace period.

NOTE 3: `complete-revocation-references.crlidss requires use of` CRLs [5] and `complete-revocation-references.ocspids` requires use of OCSP [8] Responses.

Additional requirement:

a) The revocation status information shall be the one that encompasses the time of signing.

6.4.3 Certificate values

Table 36

Service / Protocol element	Reference	Generator requirement	Verifier requirement	Additional requirements / notes
Service: certificate values		R	R	
`certificate-values`	Clause 6.3.3	O	O	
Certificates maintained by CA or other trusted service		O	O	a

Additional requirement:

a) If a Certification Authority (CA), or other trusted service, is trusted to keep certificates not already held within the signature for the archiving period and it is known where and how to obtain them, there is no need to hold them within the signature. This requires prior agreement between the verifier and the trust service provider / CA.

6.4.4 Revocation status values

Table 37

Service / Protocol element	Reference	Generator requirement	Verifier requirement	Additional requirements / notes
Service: revocation status values		R	R	
`revocation-values.crlVals`	Clause 6.3.4	O	O	a
`revocation-Values.ocspVals`	Clause 6.3.4	O	O	a
Revocation status values maintained by CA or other trusted service		O	O	a, b

NOTE: `revocation-values.crlVals` `requires use of` CRLs [5] and `revocation-Values.ocspVals` requires use of OCSP [8] Responses.

Additional requirements:

a) A verifier should be able to process a CRL and an OCSP Response regardless of where it fetches this revocation status information.

b) If a Certification Authority (CA) or other trusted service is trusted to keep revocation status information for the archiving period and it is known where and how to obtain them, then there is no need to hold revocation information within the signature. This requires prior agreement between the verifier and the trust service provider / CA.

6.4.5 Archive time-stamp

Table 38

Service / Protocol element	Reference	Generator requirement	Verifier requirement	Additional requirements / notes
`archive-time-stamp`	Clause 6.4.1	O	O	a

Additional requirement:

a) The requirement for verifiers becomes R if there are no alternative technical or organizational mechanisms to maintain the validity of the signed document over the period of storage.

6.5 Other standards

6.5.1 X.509 Certificates

Table 39

Service / Protocol element	Reference	Generator requirement	Verifier requirement	Additional requirements / notes
X.509 Certificate Profile	RFC 3280 [6]	M	M	1

NOTE 1: ETSI has defined suitable certificate profiles (TS 101 862 and TS 102 280).

NOTE 2: RFC 3280 [6] is a profile of X.509 [5].

7 CAdES baseline profile

The present clause defines a profile for CAdES signatures which provides a baseline for other application areas.

7.1 Elements defined in CMS

7.1.1 Placement of the signature

Table 40

Service / Protocol element	CMS [2] reference	Generator requirement	Verifier requirement	Additional requirements / notes
Service: signature		M	M	
Enveloping with data	Clause 5.2	R	R	
Detached Signature	Clause 5.2	O	R	

7.1.2 Signer identifier

Table 41

Service / Protocol element	CMS [2] reference	Generator requirement	Verifier requirement	Additional requirements / notes
Service: signer identifier	Clause 5.3	M	M	
`issuerAndSerialNumber`	Clause 5.3	R	R	
`subjectKeyIdentifier`	Clause 5.3	O	O	

7.1.3 Content type

Table 42

Service / Protocol element	CMS [2] reference	Generator requirement	Verifier requirement	Additional requirements / notes
`ContentType`	Clause 11.1	M	M	

7.1.4 Message digest

Table 43

Service / Protocol element	CMS [2] reference	Generator requirement	Verifier requirement	Additional requirements / notes
Message digest	Clause 11.2	M	M	

7.1.5 Signing time

Table 44

Service / Protocol element	CMS [2] reference	Generator requirement	Verifier requirement	Additional requirements / notes
`signing-time`	Clause 11.3	O	O	

7.1.6 Countersignature

Table 45

Service / Protocol element	CMS [2] reference	Generator requirement	Verifier requirement	Additional requirements / notes
`counterSignature`	Clause 11.4	O	O	a

Additional requirement:

a) Use of countersignatures should be agreed upon in a prior arrangement between the generator and the verifier so that the verifier is aware of the presence, number and meaning of the countersignature.

7.1.7 Parallel signatures

Table 46

Service / Protocol element	CMS [2] reference	Generator Requirement	Verifier Requirement	Additional requirements / notes
`SignerInfos`	Clause 5.3	O	O	a

Additional requirement:

a) Use of parallel signatures should be agreed upon in a prior arrangement between the generator and the verifier so that the verifier is aware of their presence, number and meaning.

7.2 Elements defined in ESS

7.2.1 Signing certificate

Table 47

Service / Protocol element	ESS [3] [4] reference	Generator requirement	Verifier requirement	Additional requirements / notes
Service: protection of signing certificate		M	M	
ESS signing-certificate	ESS [3], clause 5.4	R	R	a
ESS signing-certificate v2	ESS [4], clause 4	O	R	a

Additional requirement:

a) Generators should migrate to the use of ESS signing-certificate v2 in preference to ESS signing-certificate in line with the guidance regarding limited lifetime for the use of SHA-1 given in clause 9.4 of TS 102 176-1 [9].

7.3 Additional attributes defined in CAdES

7.3.1 Signature time-stamp / time-mark

Table 48

Service / Protocol element	Reference	Generator requirement	Verifier requirement	Additional requirements / notes
signature-time-stamp	Clause 6.6.1	O	O	

NOTE: The signature time-stamp assists in making the difference between valid and invalid electronic signatures in case the signer's certificate has been revoked.

7.4 Additional attributes defined in CAdES for long term signatures

The requirements specified in all 7.4 clauses are only applicable to systems managing long term signatures. Further details of procedures for the management of signatures over the long term may be found in CWA 14171, clause 5.1 [10].

7.4.1 Certificate references

Table 49

Service / Protocol element	Reference	Generator requirement	Verifier requirement	Additional requirements / notes
complete-certificate-references	Clause 6.2.1	R	R	

7.4.2 Revocation status references

Table 50

Service / Protocol element	Reference	Generator requirement	Verifier requirement	Additional requirements / notes
Service: complete revocation status references	Clause 6.2.2	R	R	
`complete-revocation-references.crlidss`	Clause 6.2.2	O	R	a
`complete-revocation-references.ocspids`	Clause 6.2.2	O	R	a

NOTE 1: The generator is recommended to make use of this service, using either CRLs or OCSP Responses. The verifier should be able to handle both.

NOTE 2: This attribute should be generated and added when the meaningful issue of the required component of revocation and validation data become available. This may require taking into account a grace period. A grace period permits certificate revocation information to propagate through the revocation processes. This period could extend from the time an authorized entity requests for a certificate revocation, to when the revocation information is available for the relying to use. In order to make sure that the certificate was not revoked at the time the signature was time-marked or time-stamped, the generation of this attribute should wait until the end of the grace period.

NOTE 3: `complete-revocation-references.crlidss requires use of` CRLs [5] and `complete-revocation-references.ocspids` requires use of OCSP [8] Responses.

Additional requirement:

a) The revocation status information shall be the one that encompasses the time of signing.

7.4.3 Certificate values

Table 51

Service / Protocol element	Reference	Generator requirement	Verifier requirement	Additional requirements / notes
Service: certificate values		R	R	
`certificate-values`	Clause 6.3.3	O	O	
Certificates maintained by CA or other trusted service		O	O	a

Additional requirement:

a) If a Certification Authority (CA), or other trusted service, is trusted to keep certificates not already held within the signature for the archiving period and it is known where and how to obtain them, there is no need to hold them within the signature. This requires prior agreement between the verifier and the trust service provider / CA.

7.4.4 Revocation status values

Table 52

Service / Protocol element	Reference	Generator requirement	Verifier requirement	Additional requirements / notes
Service: revocation status values		R	R	
`revocation-values.crlVals`	Clause 6.3.4	O	O	a
`revocation-Values.ocspVals`	Clause 6.3.4	O	O	a
Revocation status values maintained by CA or other trusted service		O	O	a, b

NOTE: `revocation-values.crlVals` `requires use of` CRLs [5] and `revocation-Values.ocspVals` requires use of OCSP [8] Responses.

Additional requirements:

a) A verifier should be able to process a CRL and an OCSP Response regardless of where it fetches this revocation status information.

b) If a Certification Authority (CA) or other trusted service is trusted to keep revocation status information for the archiving period and it is known where and how to obtain them, then there is no need to hold revocation information within the signature. This requires prior agreement between the verifier and the trust service provider / CA.

7.4.5 Archive time-stamp

Table 53

Service / Protocol element	Reference	Generator requirement	Verifier requirement	Additional requirements / notes
`archive-time-stamp`	Clause 6.4.1	O	O	a

NOTE: `revocation-values.crlVals` `requires use of` CRLs [5] and `revocation-Values.ocspVals` requires use of OCSP [8] Responses.

Additional requirement:

a) The requirement for verifiers becomes R if there are no alternative technical or organizational mechanisms to maintain the validity of the signed document over the period of storage.

7.5 Other standards

7.5.1 X.509 Certificates

Table 54

Service / Protocol element	Reference	Generator requirement	Verifier requirement	Additional requirements / notes
X.509 Certificate Profile	RFC 3280 [6]	M	M	1

NOTE 1: ETSI has defined suitable certificate profiles (TS 101 862 and TS 102 280).

NOTE 2: RFC 3280 [6] is a profile of X.509 [5].

NOTE 3: `complete-revocation-references.crlidss` requires use of CRLs [5] and `complete-revocation-references.ocspids` requires use of OCSP [8] Responses.

Annex A (informative): Bibliography

- ETSI TS 101 862: "Qualified certificate profile".
- ETSI TS 102 280: "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons".

History

Document history		
V1.1.1	February 2007	Publication