PKCS7 and CMS Signature Profile

Version 1.0

Sep 2015

Controller of Certifying Authorities
Department of Information Technology
Ministry of Communications and Information Technology

Document Control

Document Name	PKCS7 and CMS Signature Profile
Status	Release
Version	1.0
Last update	10 Sep 2015
Document Owner	Controller of Certifying Authorities, India

Table of Contents

This document provides a profile for Public Key Cryptography Standards 7(PKCS-7) and Cryptographic Message Syntax (CMS) signatures.

1. Introduction

1.1. Scope

While PKCS-7 permits many content types, the scope of this document is limited to signed data only.

We have used PKCS 7 Version 1.5 for the profiles since Version 1.6 is not commercially implemented. In addition, the rationale for PKCS Version 1.5 is that Cryptographic Message Syntax (CMS) is also based on this version. Note that primary change from Version 1.5 to Version 1.6 is to change the ASN.1 SET to ASN.1 SEQUENCE and change the ASN.1 Version number from 1 to 2.

The values produced according to this profile are Basic Encoding Rules (BER) encoded data. Additional encoding such as base 64 encoding may have to be applied while transmitting the signed data.

The scope of this work includes profiles for the signer, multiple signers (i.e., parallel signatures), and counter signatures. Each of these three profiles can have detached signatures or attached, resulting in six profiles. Note that counter signer could sign single signed or parallel signed payload. In addition counter signatures can be recursively applied.

1.2. Approach

Since the number and size of differences between PKCS 7 and CMS and among various signature types (detached, attached, parallel, and counter) are small, we first profile the general structure and then for each instance we list the options to create the structure to be used.

While CMS definition of eContent (encapsulated content) is more restrictive (it is OCTET STRING), this definition is used since both the S/MIME and CMS use it.

Note that structure naming differences between PKCS-7 and CMS such as digestEncryptionAlgorithm Vs. signatureAlgorithm and encryptedDigest Vs. signature are immaterial; they do not cause any interpretation or interoperability concerns. The PKCS-7 terminology is narrower as encrypting a hash only applies to RSA and not to ECDSA. Thus, CMS terminology is chosen for both of them.

2. General Signature Profile

```
ContentInfo ::= SEQUENCE {
        contentType OBJECT IDENTIFIER = {1 2 840 113549 1 7 2} – signed data,
        content signedData
}

signedData ::= SEQUENCE {
        Version = INTEGER 1 or 3,
        digestAlgorithms DigestAlgorithmIdentifiers,
        econtentInfo EContentInfo,
        certificates [0] IMPLICIT Certificates,
        signerInfos SignerInfos
}

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier – set contains only one element

DigestAlgorithmIdentifier ::= SEQUENCE {
    Algorithm OBJECT IDENTIFIER = { 2 16 840 1 101 3 4 2 1 } – SHA 256,
    parameters = NULL
}

EContentInfo ::= SEQUENCE {
  contentType OBJECT IDENTIFIER = {1 2 840 113549 1 7 1} – data,
  eContent [0] EXPLICIT OCTET STRING OPTIONAL
}


Certificates ::= SET OF Signers' X.509 certificate

SignerInfos ::= SET OF SignerInfo

SignerInfo ::= SEQUENCE {
  version = INTEGER 1 or 3,
  sid SignerIdentifier,
  digestAlgorithm DigestAlgorithmIdentifier,
  signedAttributes [0] IMPLICIT SignedAttributes OPTIONAL,
  signatureAlgorithm SignatureAlgorithmIdentifier,
  signature SignatureValue,
  unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL
}

SignerIdentifier ::= CHOICE {
 issuerAndSerialNumber IssuerAndSerialNumber,
 subjectKeyIdentifier [0] SubjectKeyIdentifier
}

IssuerAndSerialNumber ::= SEQUENCE {
      issuer = DN of CA issuing signer certificate,
      serialNumber = INTEGER serial number of signer certificate
}
```

SubjectKeyIdentifier ::= OCTET STRING

SignedAttributes ::= SET {Attribute 1, Attribute 2, Attribute 3}

Attribute 1 ::= SEQUENCE {
    Attribute OBJECT IDENTIFIER {1 2 840 113549 1 9 3} – Content Type Attribute,
    ContentType OBJECT IDENTIFIER {1 2 840 113549 1 7 1} – OID for encapsulated content type
}

Attribute 2 ::= SEQUENCE {
    Attribute OBJECT IDENTIFIER {1 2 840 113549 1 9 4} – Message Digest Attribute,
    Digest = OCTET STRING
}

Attribute 3 ::= SEQUENCE {
    Attribute OBJECT IDENTIFIER {1 2 840 113549 1 9 5} – Signing Time attribute,
    time Time
}

Time ::= CHOICE {
      utcTime UTCTime,
      generalizedTime GeneralizedTime }

SignatureAlgorithmIdentifier :: SEQUENCE {
    Algorithm OBJECT IDENTIFIER {1 2 840 113549 1 1 11} – RSA using SHA-256,
    parameters = NULL
 }

SignatureValue ::= OCTET STRING

UnsignedAttributes ::= SET (Attribute 4)

Attribute 4 ::= SEQUENCE {
OBJECT IDENTIFIER {1 2 840 113549 1 9 6} – Counter Signature Attribute,
SignerInfo'
}

-- Having counter signature tied to SignerInfo makes it possible to having counter signatures independenly for each parallel signer.

-- SignerInfo' is same as SignerInfo except the signedAttributes field if present MUST NOT contain a content-type attribute; there is no content type for countersignatures. Thus, SignerInfo' becomes the following:

SignerInfo' ::= SEQUENCE {
  version = INTEGER 1 or 3,
  sid SignerIdentifier,
  digestAlgorithm DigestAlgorithmIdentifier,
  signedAttributes [0] IMPLICIT SignedAttributes' OPTIONAL,
  signatureAlgorithm SignatureAlgorithmIdentifier,
  signature SignatureValue,

```
  unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL
}
```

SignedAttributes' ::= SET {Attribute 2, Attribute 3}

-- Having UnsignedAttributes in counter signature SignerInfo makes possible having any number of (or layers of) counter signatures.

3. PKCS 7 Signatures

While we have left signedAttributes optional to provide flexibility, we strongly recommend that the signedAttributes as enumerated in the ASN.1 above (i.e., content type, message digest, and signing time) be present in compliant PKCS-7 signatures.

3.1 Detached PKCS 7 Signatures

The detached signatures do not carry contents with them.

3.1.1. PKCS 7 Detached Single Signature

The following choices from the General Signature Profile (Section 2) give us detached single signer for PKCS-7:

1. The Version number for both the signedData and signerInfo is 1.
2. OPTIONAL econtent is absent.
3. SET OF Signers' X.509 certificate and certificate chain(OPTIONAL).
4. SET OF SignerInfo has one SignerInfo structure (for the signer).
5. SignerIdentifier is populated using the following CHOICE: IssuerAndSerialNumber
6. UnsignedAttributes is absent, i.e., no counter signatures.

3.1.2. PKCS 7 Detached Parallel Signature

The following choices from the General Signature Profile (Section 2) give us detached parallel signers for PKCS-7:

1. The Version number for both the signedData and signerInfo is 1.
2. OPTIONAL econtent is absent.
3. SET OF Signers' X.509 certificate and the certificate chain for each signer (OPTIONAL).
4. SET OF SignerInfo has one SignerInfo structure for each signer.
5. SignerIdentifier is populated using the following CHOICE: IssuerAndSerialNumber
6. UnsignedAttributes is absent, i.e., no counter signatures.

3.1.3. PKCS 7 Detached Counter Signature

The following choices from the General Signature Profile (Section 2) give us detached counter signatures for PKCS-7:

1. The Version number for both the signedData and signerInfo is 1.
2. OPTIONAL econtent is absent.
3. SET OF Signers' X.509 certificates and certificate chain for each signer (OPTIONAL.
4. SET OF SignerInfo has one SignerInfo structure for each signer.
5. SignerIdentifier is populated using the following CHOICE: IssuerAndSerialNumber
6. UnsignedAttributes is present, and contains the countersigner's SignerInfo. While we have left signedAttributes optional to provide flexibility, we strongly recommend that the signedAttributes as enumerated in the ASN.1 above (i.e., message digest and signing time) be present in compliant PKCS-7 countersignatures. Note that countersignatures do not contain Content Type signedAttribute.

3.2 Attached PKCS 7 Signatures

The attached signatures carry contents with them. That is the only difference between detached and attached signatures

3.2.1 PKCS 7 Attached Single Signature

The following choices from the General Signature Profile (Section 2) give us attached single signer for PKCS-7:

1. The Version number for both the signedData and signerInfo is 1.
2. OPTIONAL econtent is present.
4. SET OF Signers' X.509 certificates and certificate chain (OPTIONALSET OF SignerInfo has one SignerInfo structure (for the signer).
5. SignerIdentifier is populated using the following CHOICE: IssuerAndSerialNumber
6. UnsignedAttributes is absent, i.e., no counter signatures.

3.2.2 PKCS 7 Attached Parallel Signature

The following choices from the General Signature Profile (Section 2) give us attached parallel signers for PKCS-7:

1. The Version number for both the signedData and signerInfo is 1.
2. OPTIONAL econtent is present.
4. SET OF Signers' X.509 certificates and certificate chain for each signer (OPTIONALSET OF SignerInfo has one SignerInfo structure for each signer.

5. SignerIdentifier is populated using the following CHOICE: IssuerAndSerialNumber
6. UnsignedAttributes is absent, i.e., no counter signatures.

3.2.3 PKCS 7 Attached Counter Signature

The following choices from the General Signature Profile (Section 2) give us attached counter signatures for PKCS-7:

1. The Version number for both the signedData and signerInfo is 1.
2. OPTIONAL econtent is present.
4. SET OF Signers' X.509 certificates and certificate chain for each signer (OPTIONALSET OF SignerInfo has one SignerInfo structure for each signer.
5. SignerIdentifier is populated using the following CHOICE: IssuerAndSerialNumber
6. UnsignedAttributes is present, and contains the countersigner's SignerInfo. While we have left signedAttributes optional to provide flexibility, we strongly recommend that the signedAttributes as enumerated in the ASN.1 above (i.e., message digest and signing time) be present in compliant PKCS-7 countersignatures. Note that countersignatures do not contain Content Type signedAttribute.

4. Cryptographic Message Syntax (CMS) Signatures

The primary difference between CMS and PKCS-7 profile we have provided is the SignerIdentifier, which in turn also results in a change in version number.

While we have left signedAttributes optional to provide flexibility, we strongly recommend that the signedAttributes as enumerated in the ASN.1 above (i.e., content type, message digest, and signing time) be present in compliant CMS signatures.

4.1 Detached CMS Signatures

The detached signatures do not carry contents with them.

4.1.1 CMS Detached Single Signature

The following choices from the General Signature Profile (Section 2) give us detached single signer for CMS:

1. The Version number for both the signedData and signerInfo is 3.
2. OPTIONAL econtent is absent.
3. SET OF Signers' X.509 certificate has one or more certificates in it (signer certificate- MANDATORY, certificate chain - OPTIONAL).
4. SET OF SignerInfo has one SignerInfo structure (for the signer).
5. SignerIdentifier is populated using the following CHOICE: SubjectKeyIdentifier
6. UnsignedAttributes is absent, i.e., no counter signatures.

4.1.2 CMS Detached Parallel Signature

The following choices from the General Signature Profile (Section 2) give us detached parallel signers for CMS:

1. The Version number for both the signedData and signerInfo is 3.
2. OPTIONAL econtent is absent.
3. SET OF Signers' X.509 certificate has one or more certificates for each signer. (signer certificate- MANDATORY, certificate chain - OPTIONAL)
4. SET OF SignerInfo has one SignerInfo structure for each signer.

5. SignerIdentifier is populated using the following CHOICE: SubjectKeyIdentifier
6. UnsignedAttributes is absent, i.e., no counter signatures.

4.1.3 CMS Detached Counter Signature

The following choices from the General Signature Profile (Section 2) give us detached counter signatures for CMS:

1. The Version number for both the signedData and signerInfo is 3.
2. OPTIONAL econtent is absent.
3. SET OF Signers' X.509 certificate has one or more certificates for each signer. (signer certificate- MANDATORY, certificate chain - OPTIONAL)
4. SET OF SignerInfo has one SignerInfo structure for each signer.
5. SignerIdentifier is populated using the following CHOICE: SubjectKeyIdentifier
6. UnsignedAttributes is present, and contains the countersigner's SignerInfo. While we have left signedAttributes optional to provide flexibility, we strongly recommend that the signedAttributes as enumerated in the ASN.1 above (i.e., message digest and signing time) be present in compliant CMS countersignatures. Note that countersignatures do not contain Content Type signedAttribute.

4.2 Attached CMS Signatures

The attached signatures carry contents with them. That is the only difference between detached and attached signatures.

4.2.1 CMS Attached Single Signature

The following choices from the General Signature Profile (Section 2) give us attached single signer for CMS:

1. The Version number for both the signedData and signerInfo is 3.
2. OPTIONAL econtent is present.
3. SET OF Signers' X.509 certificate has one or more certificates in it (signer certificate- MANDATORY, certificate chain - OPTIONAL).

4. SET OF SignerInfo has one SignerInfo structure (for the signer).
5. SignerIdentifier is populated using the following CHOICE: SubjectKeyIdentifier
6. UnsignedAttributes is absent, i.e., no counter signatures.

4.2.2 CMS Attached Parallel Signature

The following choices from the General Signature Profile (Section 2) give us attached parallel signers for CMS:

1. The Version number for both the signedData and signerInfo is 3.
2. OPTIONAL econtent is present.
3. SET OF Signers' X.509 certificate has one or more certificates for each signer. (signer certificate- MANDATORY, certificate chain - OPTIONAL)
4. SET OF SignerInfo has one SignerInfo structure for each signer.
5. SignerIdentifier is populated using the following CHOICE: SubjectKeyIdentifier
6. UnsignedAttributes is absent, i.e., no counter signatures.

4.2.3 CMS Attached Counter Signature

The following choices from the General Signature Profile (Section 2) give us attached counter signatures for CMS:

1. The Version number for both the signedData and signerInfo is 3.
2. OPTIONAL econtent is present.
3. SET OF Signers' X.509 certificate has one or more certificates for each signer. (signer certificate- MANDATORY, certificate chain - OPTIONAL)
4. SET OF SignerInfo has one SignerInfo structure for each signer.
5. SignerIdentifier is populated using the following CHOICE: SubjectKeyIdentifier
6. UnsignedAttributes is present, and contains the countersigner's SignerInfo. While we have left signedAttributes optional to provide flexibility, we strongly recommend that the signedAttributes as enumerated in the ASN.1 above (i.e., message digest and signing time) be present in compliant CMS countersignatures. Note that countersignatures do not contain Content Type signedAttribute.

5. References

- [RFC2315] PKCS #7: Cryptographic Message Syntax Version 1.5, RFC 2315, March 1998. https://tools.ietf.org/rfc/rfc2315.txt
- [PKCS7] PKCS #7: Cryptographic Message Syntax Standard, Version 1.5, November 1993. http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-7-cryptographic-message-syntax-standar.htm
- [PKCS7ASN1] ASN.1 for PKCS-7, http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-7-cryptographic-message-syntax-standar.htm
- [CMS] Cryptographic Message Syntax (CMS), RFC 5652, September 2009, https://tools.ietf.org/rfc/rfc5652.txt

****