Digital Signature Format for E-Invoice System

Signature Creation Guide

Version 1.0

26th of April 2020

E-Signature Competence Center

Information Technology Industry Development Agency

Table of Contents

1 Scope

The scope of this document covers Cades Basic Electronic Signature format expected by ITIDA Validation Module integrated into Egyptian tax authority E-Invoice system.
An electronic signature can be used for arbitration in case of a dispute between the signer and verifier. The present document is based on the use of public key cryptography to produce digital signatures, supported by public key certificates.
The present document describes a format for advanced electronic signatures using ASN.1. This format is based on CMS defined in RFC 3852 Electronic signatures are thus called CAdES, for "CMS Advanced Electronic Signatures".

2 Audience

This document is written and intended for technical engineers or technical managers, software engineers, software developers, solutions architects, IT specialists, IT managers.

3 Abbreviations

ASN.1	Abstract Syntax Notation 1
RFC	Request for Comments
CAdES	CMS Advanced Electronic Signature
CAdES-BES	CAdES Basic Electronic Signature
OID	Object Identifier

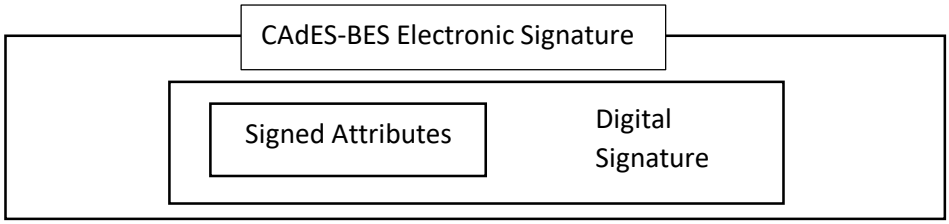
4 CAdES Basic Electronic Signature (CAdES-BES)

A CAdES Basic Electronic Signature (CAdES-BES), in accordance with the present document contains:

- a collection of mandatory signed attributes, as defined in CMS (RFC 3852)
- the digital signature value computed on the user data and, on the signed attributes, as defined in CMS (RFC 3852 [4])
- an additional mandatory signed attributes

A CAdES Basic Electronic Signature (CAdES-BES), in accordance with the present document may NOT contain any unsigned attributes.

The structure of the CAdES-BES is illustrated in the figure below



4.1 The mandatory signed attributes

- Content-type. It specifies the type of the EncapsulatedContentInfo value being signed. The syntax of the content-type attribute type is as defined in CMS (RFC 3852), clause 11.1.

- Message-digest. It is defined in RFC 3852 and specifies the message digest. The syntax of the message-digest attribute type of the ES is as defined in CMS (RFC 3852). Note that for the scope of this document the only supported algorithm for hashing is SHA-256.

- ESS signing-certificate-v2. The ESS signing-certificate attribute is defined in Enhanced Security Services (ESS), RFC 2634 The ESS signing-certificate-v2 attribute is defined in "ESS Update: Adding CertID Algorithm Agility", (published as RFC 5035). Note that in the scope of this document only ESS signing-certificate-v2 should be supported. The hash algorithm used should be SHA-256 algorithm.

  Note: certHash : Mandatory field
  issuerAndSerialNumber : OPTIONAL field

- Signing-time: as defined in CMS (RFC 3852), indicates the time of the signature, as claimed by the signer. NOTE: RFC 3852 states that "dates between January 1, 1950 and December 31, 2049 (inclusive) must be encoded as UTCTime.

5 CAdES Signature Syntax and Requirements for E-invoice

In this section, the expected CAdES-BES Signature syntax is identified as well as the required ASN.1 attributes values.

```
SignedData ::= SEQUENCE {
  version CMSVersion,
  digestAlgorithms DigestAlgorithmIdentifiers,
  encapContentInfo SEQUENCE {
        eContentType,
        eContent [0] EXPLICIT OCTET STRING OPTIONAL, //Should not be present
  },
  certificates [0] IMPLICIT CertificateSet OPTIONAL, //Only Signer Certificate
  crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
  signerInfos SET OF SEQUENCE {                        //Only One SignerInfo
    version CMSVersion,
    sid SignerIdentifier,
    digestAlgorithm DigestAlgorithmIdentifier,
    signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL, //4 Attributes
    signatureAlgorithm SignatureAlgorithmIdentifier,
    signature SignatureValue,
    unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL //Should not be
   present
     }
}
```

The table below identifies the expected values in generating SignedData values.

	Fields	Expected Values	Notes
SignedData	version	CMSVersion equals 3	In case of using third-party libraries to build a CAdES Object, CMSVersion may be auto-generated based on the values set in the digital signature.
	digestAlgorithms	This field should contains OID of SHA256 Algorithm which is "2.16.840.1.101.3.4.2.1"	

	encapContentInfo	• ContentType should be set to DigestData OID which is "1.2.840.113549.1.7.5". • eContent should **not** be present	eContent field should not be present as the expected digital signature format should be detached which means that it does not contain the data.
	Certificates	CertificateChoice field is a Choice of multiple fields. The expected field is Certificate that will contain X.509 Certificate of the signer	This field must be present & contain the signer certificate only.
	SignerInfos	This field is a SET of SignerInfos. It should contain **one** SignerInfo in the signature.	
SignerInfo	Version	CMSVersion equals to 1	In case of using third-party libraries to build a CAdES Object, CMSVersion may be auto-generated based on the values set in the digital signature.
	Sid	SignerIdentifier field is a Choice which will be IssuerAndSerialNumber.This field contains the serial number of the certificate and issuer name.	
	digestAlgorithms	This field should contains OID of SHA256 Algorithm which is "2.16.840.1.101.3.4.2.1"	
	signedAttrs	Signed Attributes should contain **4** mandatory attributes by ITIDA a. **ContentType** should be set to DigestData b. **MessageDigest** should contain Der Octet String format for SHA256 Hash of the date to be signed c. **ESSSigningCertificateV2** should contains SHA256 hash of the signer certificate. d. **SigningTime** should use the machine time in UTC	OID of Signed Attributes: • **ContentType:** 1.2.840.113549.1.9.3. • **MessageDigest:** 1.2.840.113549.1.7.5 • **SigningTime:** 1.2.840.113549.1.9.5 • **ESSSigningCertificatV2:**1.2.840.113549.1.9.16.2.47. For more info, see RFC 5035
	signatureAlgorithm	SignatureAlgorithmIdentifier should be set to sha256WithRSAEncryption OID which is 1.2.840.113549.1.1.11	
	Signature	Signature value computed on the user data and, on the signed attributes using the signer private key with Algorithm sha256WithRSAEncryption	
	unsignedAttrs	This field should **not** be present	

6 References

[1] IETF RFC 3852 (2004): "Cryptographic Message Syntax (CMS)".

[2] IETF RFC 2634 (1999): "Enhanced Security Services for S/MIME".

[3] IETF RFC 2045 (1996): "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

[4] IETF RFC 5035 (2007): "Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility".

[5] Recommendation ITU-T X.208 (1988): "Specification of Abstract Syntax Notation One (ASN.1)".