NemLog-in

AdES Signature Profile

Contents

Version	Change	Date
0.1	Draft	06-07-2020
0.2	Minor updates	1-10-2020
1.0	Version updated for release	12-11-2020
1.0.1	Updated with review from Digst	23-11-2020
1.0.2	Devoloper branding removed	29-03-2020
1.0.3	Language correction	19-05-2020
1.0.4	Minor corrections to XAdES signature format • X509 only contains the signing certificate • Canocalisation is the only transform of the DTBS.	03-03-2022

References

eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Available here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN
PAdES	ETSI EN 319 142-1: AdES digital signatures; Part 1: Building blocks and PAdES baseline signatures, ETSI ESI. Available here: https://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.01_60/en_31914201v010101p.pdf
XAdES	ETSI EN 319 132-1: XAdES digital signatures; Part 1: Building blocks and XAdES baseline signature, ETSI ESI. Available here: https://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.01.01_60/en_31913201v010101p.pdf
CAdES	ETSI EN 319 122-1: CAdES digital signatures; Part 1: Building blocks and CAdES baseline signature, ETSI ESI. Available here: https://www.etsi.org/deliver/etsi_en/319100_319199/31912201/01.01.01_60/en_31912201v010101p.pdf
CMS	IETF RFC 5652 (2009): "Cryptographic Message Syntax. Available here: https://tools.ietf.org/html/rfc5652
PDF	ISO 32000-1, Document management – Portable document format – Part 1: PDF 1.7. Available here: https://www.adobe.com/content/dam/acom/en/devnet/pdf/pdfs/PDF32000_2008.pdf

1 Signature classes

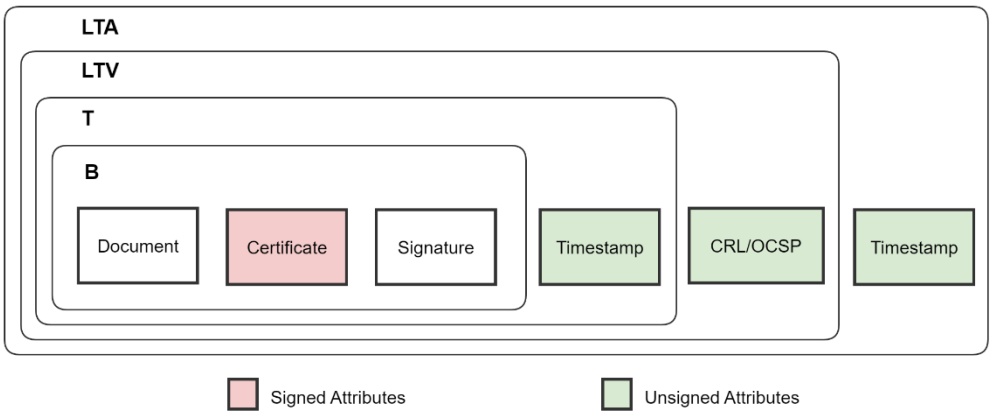
The signature format created by the NemLog-ins signing service is aimed for long term archival (LTA), which provides enough data to validate the signature for a period after the signature has been generated.

The PDF Advanced digital Electronic Signature PAdES [PADES] and XML Advanced digital Electronic Signature XAdES [XADES] are categorised in four groups each adding, on top of the others, specific data to the signature to create a signature format, which meets a posed requirement.

In increasing order of complexity and data, the four groups are:

Group	Data	Security properties
Basic (B)	Original document Signed attributes (incl. signing certificate) Signature	The signature can be used to prove that the identity in the signing certificate has produced a signature over the original document.
Time Stamp (T)	Basic (B) Time Stamp Token	The addition of the Time Stamp Token can be used to prove that the signature existed at the time specified in the token.
Long Term Validation (LTV)	Time Stamp (T) Revocation Information	The inclusion of Revocation Information proves that the signing certificate was not revoked at the time indicated in the information.
Long Term Archival (LTA)	Long Term Validation (LTV) Time Stamp Token	The Time Stamp Token proves that the Revocation Information was available at the time specified in the token.

The illustration below, describes how the classes are related.



2 PAdES

This section profiles the elements from [PADES], table 1 to describe the PAdES format produced by the NemLog-in3 signature service.

A PAdES LTA consists of elements:

- Original PDF/A to be signed
  - It will be extended with a Signature Directory and Document Security Store
- CMS object which contains the basic signature and signature time stamp token, which forms the PAdES-T signature
- A Signature Dictionary containing data including a CMS object
- Document Security Store Dictionary containing data that extends the basic signature to LTA.
  - Extending PAdES-T to PAdES-LTV
- Document Time-Stamp Dictionary
  - Extending PAdES-LTV to PAdES-LTA

2.1 Original PDF/A

The PDF to be signed shall be conformant to PDF/A-2 as described in [PDF].

2.2 CMS

The CMS structure has the following attributes:

Attributes	Description
ContentInfo	
.ContentType	OID 1.2.840.113549.1.7.2 for Signed Data
.content	Contains SignedData
SignedData	
.version	
.digestAlgorithms	Contains one digest algorithm with • OID 2.16.840.1.101.3.4.2.1 for SHA256. • Algorithm parameter is absent.
.encapContentInfo	Describes the object to be signed. • The eContentType shall be OID 1.2.840.113549.1.7.1 for id-data • The eContent shall be absent to indicate the PDF is external to the CMS structure.
.certificates	• The signing certificate is included. • The intermediate certificate is included for simplicity even though it is available through Authority Information Access in the signing certificate. • The root certificate is not included. It is available through the EU Trusted Lists.
.SignerInfos	Contains one SignerInfo
SignerInfo	
.version	Since SignerIdentifier is IssuerAndSerialNumber version is 1.

.sid	SignerIdentifier with IssuerAndSerialNumber
.digestAlgorithm	Contains the digest algorithm with • OID 2.16.840.1.101.3.4.2.1 for SHA256. • Algorithm parameter is absent.
.signedAttrs	Includes the following signed attributes: • SigningCertificateV2 identified by OID 1.2.840.113549.1.9.16.2.47. The value is a Set Of with value SigningCertificateV2. • ContentType identified by 1.2.840.113549.1.9.3 and value Set Of with Object Identifier 1.2.840.113549.1.7.1 (as above for eContentType). • MessageDigest identified by 1.2.840.113549.1.9.4 and value a Set Of with Octet String containing the hash of the PDF identified by ByteRange.
.signatureAlgorithm	AlgorithmIdentifier with: • ECDSA with SHA256
.signature	OctetString with signature value
.unsignedAttrs	• signature-time-stamp identified by 1.2.840.113549.1.9.16.2.14
SignerIdentifier	
.issuer	Name of issuer
.serialNumber	Certificate serial number
signing-certificate-v2	
.certs	Contains one ESSCertIDv2
ESSCertIDv2	
.hashAlgorithm	AlgorithmIdentifier with: • OID 2.16.840.1.101.3.4.2.1 for SHA256. • Algorithm parameter is absent.
.certHash	Octet String with hash of certificate.
.issuerSerial	Used to identify the certificate. However, this is available in the SignerIdentifier

2.3 Signature Dictionary

The Signature Directory which embeds the CMS object into the PDF and describes the part of the PDF that was covered by the signature shall have the following fields:

Field	Description
Type	Sig
M	Date in UTC format of signing
Contents	Byte string containing the DER encoded CMS object

Filter	Adobe.PPKLite
ByteRange	The range covers the entire file including the Signature Dictionary but excluding the entry with Contents
SubFilter	ETSI.CAdES.detached

2.4 Document Security Store Dictionary

The Document Security Store Dictionary extends the Signature Dictionary and forms a PAdES-LTV by adding revocation information to the PDF shall the following fields:

Field	Description
Type	DSS
VRI	This optional field is only relevant if the document shall be signed more than one time. We do not need to support that, so this is not included.
Cert	The following certificates shall be included • Trust anchor (root certificate) for the signing certificate. • Issuer (intermediate certificate) for the issuer of the signing certificate • Signing certificate • OCSP responder certificate for root OCSP endpoint • OCSP responder certificate for issuer OCSP endpoint • Timestamping server certificate
CRL	N/A. Only OCSP responses are included in the signature.
OCSP	The following OCSP responses shall be included • OCSP response for the signing certificate • OCSP response for the intermediate certificate • OCSP response for the root certificate • OCSP response for the Timestamping server

2.5 Document Time-Stamp Dictionary

The Document Time-Stamp extends the Signature Dictionary and forms a PAdES-LTA by adding a Time-Stamp Token. This Dictionary is similar with a Signature Dictionary but has the following changes:

Field	Description
Type	DocTimeStamp
SubFilter	ETSI.RFC3161
Contents	Hex encoding of DER encoded Time Stamp Token

ByteRange	The value of the messageImprint within the Time Stamp Token shall be hash of the bytes of the document indicated by ByteRange. The ByteRange shall cover the entire document, including the Document Time-Stamp Dictionary but excluding the Time Stamp Token itself, the entry with key Contents.

3 XAdES

This section profiles the elements from [XADES], table 2 to describe the XAdES format produced by the NemLog-in3 signature service.

A XAdES contains the same semantic information as a PAdES.

With XML signatures, the data to be signed (DTBS) and the signature can be placed relative to each other in the following ways, seen from the signature:

- Enveloped. The signature is included in the DTBS
- Enveloping. The signature contains the DTBS
- Detached. The DTBS and signature are two separate files.

The XML signatures produced by the NemLog-in3 signature service are enveloped.

Elements/Qualifying properties/Services	Description
Signature	
.SignedInfo	One element with SignerInfo
.SignatureValue	Base64 encoding of the raw signature value
.KeyInfo	Includes X509Data
.Object	The following object is included: • QualifyingProperties
SignedInfo	
.CanocalizationMethod	Canonical without comments: http://www.w3.org/2001/10/xml-exc-c14n#
.SignatureMethod	Algorithm: "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256"

.Reference	The following references are included:
	• Object with DTBS. It must include an identifier which is later on referenced from DataObjectFormat.
	  ○ Transform:
	  http://www.w3.org/2001/10/xml-exc-c14n#
	  ○ DigestMethod:
	  http://www.w3.org/2001/04/xmlenc#sha256
	• SignedProperties
	  ○ Transform:
	  http://www.w3.org/2001/10/xml-exc-c14n#
	  ○ DigestMethod:
	  http://www.w3.org/2001/04/xmlenc#sha256

X509Data	One element of X509Certificate shall be present and shall include signing certificate. • The signing certificate is included pr. standard requirement.
QualifyingProperties	The following QualifyingProperties will be included: • SignedProperties

	• UnsignedProperties

SignedProperties	The following SignedProperties will be included:
	• SignedSignatureProperties containing
	  ○ SigningTime
	  ○ SigningCertificateV2
	• SignedDataProperties
	  ○ DataObjectFormat

UnsignedProperties	The following UnsignedProperties will be included: • UnsignedSignatureProperties
UnsignedSignatureProperties	The following UnsignedSignatureProperties will be included • SignatureTimeStamp • CertificateValues • RevocationValues • ArchiveTimeStamp
SigningTime	Claimed time in UTC e.g.: 2019-11-21T09:41:41Z
SigningCertificateV2	A SigningCertificateV2 includes one Cert. The Cert includes • CertDigest ○ Digest method is SHA-256 • IssuerSerialV2 containing base64 encoding of ASN.1 DER encoding of a Sequence of issuer common name and subject serial number.
SignatureTimeStamp	Contains • CanonicalizationMethod with algorithm: http://www.w3.org/2001/10/xml-exc-c14n# • EncapsulatedTimeStamp containing a base64 encoded DER encoded TimeStampToken
DataObjectFormat	The DataObjectFormat contains: • ObjectReference with a reference identifier to the SignerInfo->Reference for the object to be signed. • MimeType with value text/xml
CertificateValues	Includes the following certificates: • Trust anchor (root certificate) for the path used to sign the XML. • Issuer (intermediate certificate) for the issuer of the signing certificate • Signing certificate • OCSP responder certificate for root OCSP endpoint • OCSP responder certificate for issuer OCSP endpoint • Timestamping server certificate
RevocationValues	The RevocationValues include two OCSPValues which as EncapsulatedOCSPValue have OCSP responses for • OCSP response for the signing certificate • OCSP response for the intermediate certificate • OCSP response for the root certificate • OCSP response for the Timestamping server
ArchiveTimeStamp	Contains

	• CanonicalizationMethod with algorithm: http://www.w3.org/2001/10/xml-exc-c14n# • EncapsulatedTimeStamp containing a base64 encoded DER encoded TimeStampToken
DTBS	The input to be signed.

4 TimeStampToken

Elements/Qualifying properties/Services	Description
CMS ContentInfo	
.ContentType	Contains one SignedData (1.2.840.113549.1.7.2)
.content	SignedData
SignedData	
.version	Version is 3
.digestAlgorithms	Set with one AlgorithmIdentifier which is SHA512 (2.16.840.1.101.3.4.2.3)
.encapContentInfo	EncapsulatedContentInfo
.certificates	Set of certificates containing the TSA certificate
.crls	N/A
.signerInfos	Set with one SignerInfo
EncapsulatedContentInfo	
.eContentType	ObjectIdentifier with TSTInfo (1.2.840.113549.1.9.16.1.4)
.eContent	OctetString containing the TSTInfo
TSTInfo	
.version	Version is 1
.policy	ObjectIdentifier with value 0.4.0.2023.1.1 (itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) poli-cyidentifiers(1) best-practices-ts-policy (1))
.messageImprint	MessageImprint
.serialNumber	Integer value, unique for the time stamp
.genTime	UTC time of generation
.accuracy	Accuracy

.ordering	N/A – default false to indicate that ordering of time stamps from this authority can only be done if the difference in time of their generation is larger than the accuracy.
.nonce	Integer with same value is in the request
.tsa	GeneralName with the following entries: • commonName: Kvalificeret tidsstemplingsenhed 1 • serialNumber: UI:DK-XXXXXXXX • organizationIdentifier: NTRDK-34051178 • organizationName: Digitaliseringsstyrelsen • countryName: DK
.extensions	Contains one extension with of type: qcStatements (1.3.6.1.5.5.7.1.3) with value esi4-qtst- Statement-1 (0.4.0.19422.1.1)
MessageImprint	
.hashAlgorithm	AlgorithmIdentifier with SHA512 (2.16.840.1.101.3.4.2.3)
.hashedMessage	Digest value of the message. Shall be 512/8 = 64 bytes.
Accuracy	
.seconds	N/A
.millis	Integer with value 500
.micros	N/A
SignerInfo	
.version	Version is 1
.sid	SignerIdentifier conducted by serial number and name
.digestAlgorithm	AlgorithmIdentifier with SHA512 (2.16.840.1.101.3.4.2.3)
.signedAttributes	Set of Attributes: • ContentType (1.2.840.113549.1.9.3) with value tstInfo (1.2.840.113549.1.9.16.1.4) • MessageDigest identified by 1.2.840.113549.1.9.4 • SigningCertificateV2 identified by OID 1.2.840.113549.1.9.16.2.47. The value is a Set Of with value SigningCertificateV2.

.signatureAlgorithm	`RSASSA-PSS-params ::= SEQUENCE {`
	`hashAlgorithm [0] HashAlgorithm DEFAULT sha1Identifier,`
	`maskGenAlgorithm [1] MaskGenAlgorithm DEFAULT mgf1SHA1Identifier,`
	`saltLength [2] INTEGER DEFAULT 20,`
	`trailerField [3] INTEGER DEFAULT 1 }`

	hashAlgorithm shall be SHA-512 maskGenAlgorithm shall be mgf1SHA-512Identifier saltLength is 64 and trailerField is default value.
.signature	Signature value
.unsignedAttributes	N/A