Telecommunications And Digital Government Regulatory Authority

TSP Framework

Digital signature standard manual

Issue date: 24/January/2024

Revision history

Version	Date	Description
1.0	24 January 2024	First version release

References

Reference	Title
[Law (3) 2003]	Federal Law by Decree No. 3 of 2003 Regarding the Organization of Telecommunications Sector
[Law (46) 2021]	Federal Decree by Law No. 46 of 2021 on Electronic Transactions and Trust Services Version 20.09.2021 https://u.ae/en/about-the-uae/digital-uae/electronic-transactions-and-trust-services-law
[Bylaw (28) 2023]	Cabinet Resolution No. 28 of 2023 regarding the executive regulations of the Electronic Transactions and Trust Services Law
[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 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
[SOG-IS Crypto WG]	SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms (https://www.sogis.eu/uk/supporting_doc_en.html)
[EN 319 122-1]	ETSI EN 319 122-1 V1.3.1 (2023-06): Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: "Building blocks and CAdES baseline signatures"
[EN 319 122-2]	ETSI EN 319 122-2 V1.2.1 (2022-02) : Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: "Extended CAdES Signatures"
[EN 319 132-1]	ETSI EN 319 132-1 V1.2.1 (2022-02): Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures
[EN 319 132-2]	ETSI EN 319 132-2 V1.1.1 (2016-04) : Electronic Signatures and Infrastructures (ESI); XAdES digital signatures ; Part 2 : Extended XAdES signatures
[EN 319 142-1]	ETSI EN 319 142-1 V1.1.1 (2016-04): Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures
[EN 319 142-2]	ETSI EN 319 142-2 V1.1.1 (2016-04): Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles
[TS 119 182-1]	ETSI TS 119 182-1 V1.1.1 (2021-03): Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures
[EN 319 162-1]	ETSI TS 319 162-1 V1.1.1 (2016-04): Electronic Signatures and Infrastructures (ESI); ASiC Associated Signature Containers; Part 1: Building blocks and ASiC baseline containers

[EN 319 102-1]	ETSI EN 319 102-1 V1.3.1(2021-11): Electronic Signatures and Infrastructures (ESI); Procedures for creation and validation of AdES Digital Signatures; Part1: Creation and Validation
[TS 119 615]	ETSI TS 119 615 V1.2.1(2023-06): Electronic Signatures and Infrastructures (ESI); Trusted lists; Procedures for using and interpreting European Union; Member States national trusted lists
[TS 119 172-4]	ETSI TS 119 172-4 V1.1.1(2021-05): Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists
[TS 119 312]	ETSI TS 119 312 V1.4.3(2023-08): Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[TR 119 100]	ETSI TR 119 100 V1.1.1(2016-03): Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation
[CID2015-1506]	Commission Implementing Decision (EU) 2015/1506

Abbreviations

AdES	Advanced Electronic Signature
ASiC	Associated Signature Containers
ASiC-S	Simple ASiC
ASiC-E	Extended ASiC
ASN.1	Abstract Syntax Notation One
CA	Certificate Authority
CAdES	CMS Advanced Electronic Signature
CMS	Cryptographic Message Syntax
EU	European Union
ETSI	European Telecommunications Standards Institute
PAdES	PDF Advanced Electronic Signature
PDF	Portable Document Format
TDRA	Telecommunications and Digital Government Regulatory Authority
TSA	Time-Stamp Authority
TSP	Trust service provider
UAE	United Arab Emirates
XAdES	XML Advanced Electronic Signature
XML	eXtensible Markup Language
JAdES	JSON Advanced Electronic Signature

Table of Contents

Revision history 2
References 2
Abbreviations 4
1. Introduction 6
1.1. Context 6
1.2. Objectives and Scope of this document 8
2. Overview of signature formats standards 8
2.1. Signature formats 9
2.1.1. CAdES 9
2.1.2. XAdES 9
2.1.3. PAdES 10
2.1.4. JAdES 10
2.1.5. ASiC container format 10
2.2. Signature baseline profiles 13
2.3. Signature packaging 16
3. Guidelines on signature creation and augmentation 18
3.1. Determine the AdES signature format 18
3.1.1. Signing a single document 18
3.1.2. Signing multiple documents 19
3.2. Determine the packaging 19
3.3. Determine the digest algorithm 20
4. Overview of signature validation standards 20

1. Introduction

1.1. Context

The European Telecommunications Standards Institute (ETSI) is in charge of the European framework for standardization on trust services and related or supporting building blocks related to electronic signatures, together with CEN/CENELEC. For international recognition purposes, it is proposed to adopt ETSI standards (profiled to the national context) as part of the United Arab Emirates (UAE) framework on trust services and electronic signatures.

As shown below, the standardization framework is rationalized and structured on different areas following a specific numbering scheme.

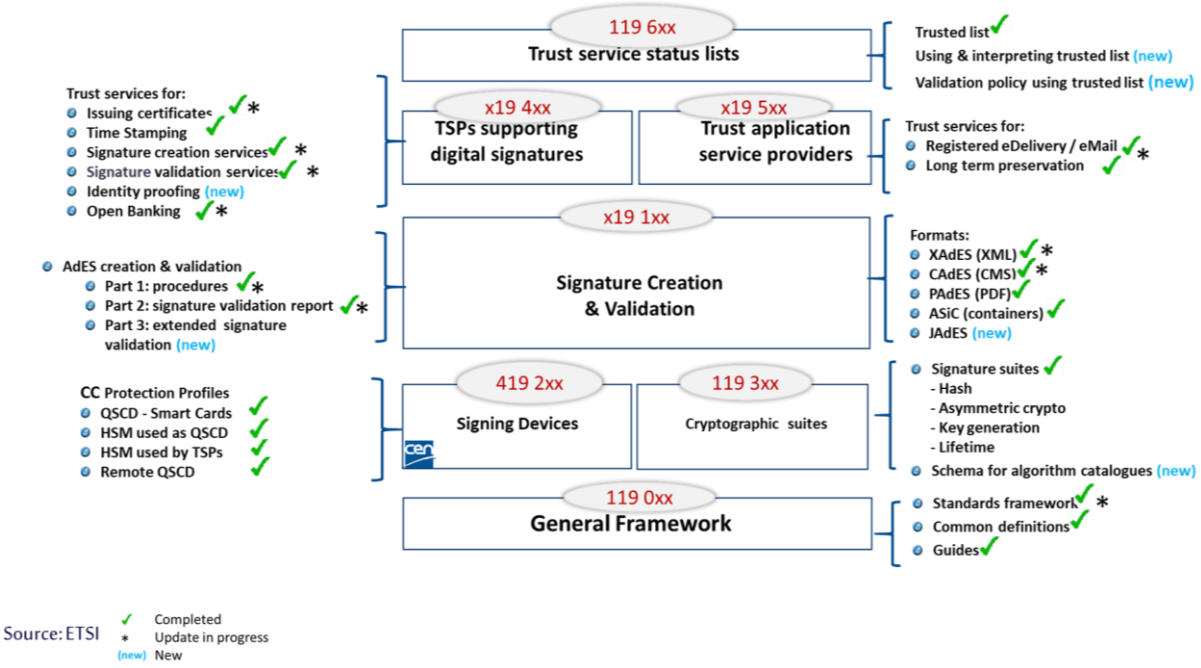


Figure 1: European standardization framework on trust services and ancillary building blocks

This numbering scheme is defined as follows (cf. ETSI [TR 119 000]): **ETSI DD L19 xxx-z**

Where:

- **DD** indicates the deliverable type in the standardization process, where:
  - TS is for Technical Specification (**L**=1), a document containing normative requirements;
  - TR is for Technical Report (**L**=1), a document containing informative elements;
  - EN is for European Standards (**L**=3), a document is intended to meet Europe regulation such as eIDAS.
- **19** indicates the document is related to eSignatures;
- **xxx** indicates the serial number;
- **-z** identifies multi-parts documents.

Four digital signature formats, i.e. CAdES, XAdES, PAdES, JAdES, and one signature container format, i.e. ASiC, are defined by ETSI standards[1]. CAdES, XAdES, PAdES and ASiCformats are made prescriptive in [eIDAS], via [CID2015-1506], for the public sector: EU Member States requiring an advanced electronic signature, or an advanced electronic signature based on a qualified certificate, shall recognize these digital signature formats.

Similarly to Europe, in order to foster interoperability among participants in electronic transactions in the UAE, to define a clear and regulated national trust services framework, and to support a future mutual recognition with Europe, the Telecommunications And Digital Government Regulatory Authority (TDRA) decided to make ETSI standards prescriptive in the UAE Regulation. In particular, TDRA decided to make prescriptive in the UAE Regulation the digital signature formats standards listed in Table 1 (known as the "baseline formats"[2]), enforcing their recognition by the public sector.

These digital signature formats shall apply to support the creation of both electronic signatures and electronic seals: Electronic signatures and electronic seals being similar from the technical point of view, the standards for formats of digital signatures apply to formats for digital seals.

AdES formats	Standard
CAdES	[ETSI EN 319 122-1]
XAdES	[ETSI EN 319 132-1]
PAdES	[ETSI EN 319 142-1]
JAdES	[ETSI TS 119 182-1]
Signature container format	
ASiC	[ETSI EN 319 162-1]

Table 1: Baseline signature formats standards

[2] The baseline formats are meant to minimize the number of options in the usage of AdES signatures and ASiC containers and maximize interoperability.

1.2. Objectives and Scope of this document

In line with the objectives of the existing UAE Trust Services Regulatory framework **[Law (46) 2021] and [Bylaw (28) 2023]**, and with the following goals in particular:

- Setting a clear legal framework for electronic trust services in a national and cross-border context.
- Being prescriptive enough to increase the certainty of implementations meeting the provisions laid down by the legal framework and securing investments while paying attention in providing a welcoming environment for trust service providers and not creating unnecessary barriers;
- Having a clear, attractive but regulated framework for electronic trust services;

the objective of this document is to define implementation aspects of digital signature formats. These technical requirements are then be made prescriptive through references from the legislation, providing a clear and attractive technical framework for both trust service providers and relying parties.

In line with the following goal:

- Positioning the UAE amongst the international scene as meeting the highest level of international standards and best practices;

an additional objective of this document is to rely as much as possible on existing international standards, profiling them to the national context of UAE where applicable or necessary.

This document is structured in the following three main sections:

Section 2 "Overview of signature formats standards" defines all signature[3] formats defined in ETSI standards and presents their related baseline profiles and packaging. These formats of signature provide basic features for a wide range of business and government use cases for electronic procedures and communications to be applicable to a wide range of communities, based on international interoperability best-practices.

Section 3 "Guidelines on signature creation and augmentation" offers a recommended step-by-guide guide to create digital signatures, depending on the format of the document to sign, the convenience of the signature formats, the digest algorithm, the packaging, and the level.

Section 4 "Overview of signature validation standards" gives an overview of the standards used as part of the validation of a signature regarding both its format and the linked certificate(s) (e.g. whether the certificate is qualified or non-qualified, whether the certificate is based on a QSCD).

2. Overview of signature formats standards

ETSI [TR 119 001] defines a digital signature as a "*data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient".* An AdES signature is defined as "*a digital signature*

[3] For the sake of simplicity, and in the absence of ambiguity between digital signature (the technical implementation) and electronic signature (the legal concept), "signature format" will be used instead of "digital signature format" in the present document.

that is either a CAdES signature, or a PAdES signature or a XAdES signature". These definitions will be reused as part of this document.

Advanced electronic signatures and advanced electronic seals being similar from the technical point of view, in the context of the UAE and similarly to Europe, formats of digital signatures apply for electronic seals.

The framework for standardization of signatures includes standards defining four digital signature formats, namely CAdES, XAdES, JAdES and PAdES (cf. Section 2.1) and one signature container format, namely ASiC (cf. Section 2.1.5).

These formats of signature are either composed by signed and unsigned attributes (for CAdES and PAdES) or signed and unsigned qualifying properties (for XAdES) or signed and unsigned header parameters (for JAdES) and fulfill certain common requirements regarding their baseline profiles (cf. Section 2.2).

Finally, three packagings are defined for these formats of signature, namely "enveloped", "enveloping" and "detached" (cf. Section 2.3).

Section 3 then proposes guidelines on signature creation and augmentation (e.g. what is the relevant format of signature depending on the format of the document to sign), based on the standards defined in this present section.

2.1. Signature formats

2.1.1. CAdES

CMS advanced electronic signature (CAdES) is a digital signature that satisfies the requirements specified in ETSI [EN 319 122-1] "Building blocks and CAdES baseline signatures" or [EN 319 122-2] "Extended CAdES signatures".

CAdES is built on Cryptographic Message Syntax (CMS), as defined in IETF RFC 5652, by incorporation of signed and unsigned attributes. In this regard, CAdES is a specific profile of CMS, a binary format of signature.

2.1.2. XAdES

XML advanced electronic signature (XAdES) is a digital signature that satisfies the requirements specified in ETSI [EN 319 132-1] "Building blocks and XAdES baseline signatures" or [EN 319 132-2] "Extended XAdES signatures".

XAdES is built on XMLDSIG by incorporation of signed and unsigned qualifying properties where:

- XMLDSIG is the XML-signature specified in *W3C Recommendation (11 April 2013): "XML Signature Syntax and Processing. Version 1.1"*;
- Qualifying properties are:
    - instance of XML types, as specified in *W3C Recommendation (26 November 2008): "Extensible Markup Language (XML) 1.0"*.

- using XML Schema syntax and structures defined in *W3C Recommendation Part 1 (28 October 2004): "XML Schema Part 1: Structures Second Edition"* and W*3C Recommendation Part 2 (28 October 2004): "XML Schema Part 2: Datatypes Second Edition"*.

In this regard, XAdES is a specific profile of XMLDSIG, an XML-based format of signature.

2.1.3. PAdES

PDF advanced electronic signatures (PAdES) is a digital signature that satisfies the requirements specified in ETSI [EN 319 142-1] “Building blocks and PAdES baseline signatures” or [EN 319 142-2] “Extended PAdES signatures”.

PAdES is built on PDF signatures, as specified in ISO 32000-1 with an alternative signature encoding to support digital signature formats equivalent to the CAdES signature format.

This signature format is handled by many PDF viewers, including the ubiquitous Adobe Acrobat Reader.

2.1.4. JAdES

JSON Advanced Electronic Signatures is a digital signature that satisfies the requirements specified in ETSI [TS 119 182-1] “Building blocks and JAdES baseline signatures”.

JAdES is built on JSON WEB signatures, as specified in IETF RFC 7515 it represents content secured with digital signatures or Message Authentication Codes (MACs) using JSON-based data structures.

2.1.5. ASiC container format

As defined in [EN 319 162], a container is “*a file created according to ZIP holding as internal elements files with related manifest, metadata and associated signature(s), under a folder hierarchy”*.

Associated Signature Container (ASiC), as defined in ETSI EN 319 162 (i.e. [EN 319 162-1] "Building blocks and ASiC baseline containers" and [EN 319 162-2] "Additional ASiC containers"), is “*a data container holding a set of file objects and associated digital signatures and/or time assertions using the ZIP format*”, where:

- The supported digital signatures formats are CAdES and XAdES ;
- A time assertion is either:
  - A timestamp token (cf. IETF RFC 5816) or
  - An evidence record (cf. IETF RFC 4998 or IETF RFC 6283).

Structure

The internal structure of ASiC containers includes:

- a root folder, for all the container content possibly including folders reflecting the content structure; and
  - a "META-INF" folder, in the root folder, for files containing metadata about the content, including associated signature or time assertion files.

Container nesting is allowed (e.g. an ASiC contained in another ASiC). It means the signed file object may itself be a container, for example ZIP, OCF, ODF or another ASiC.

ASiC types

As further detailed in the next subsections, [EN 319 162-1] defines two types of ASiC:

1. The simple ASiC (Section 2.1.5.1 “ASiC-S”) and
2. The extended ASiC (Section 2.1.5.2 “ASiC-E”).

2.1.5.1. ASiC-S

ASiC-S associates:

- **Only one** data file with **one or more** signature(s) in CAdES format, referred to as “ASiC-S with CAdES";
- **Only one** data file with **one or more** signature(s) in XAdES format, referred to as “ASiC-S with XAdES”;
- **Only one** data file with a time assertion without signature, referred to as “ASiC-S with time assertions”.

The high-level structure of an ASiC-S with one data file is represented in Figure 2.

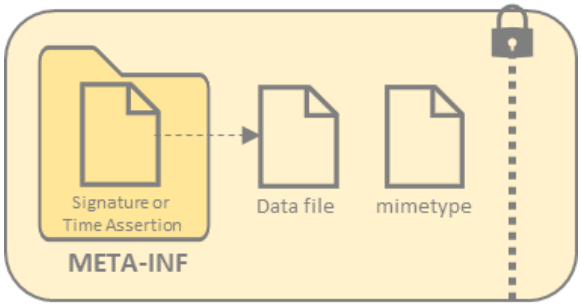


Figure 2: ASiC-S with one data file

As mentioned previously and as shown in Figure 3, the data file object may itself be a container (e.g. ZIP, OCF, ODF or another ASiC). It means that, when signing multiple data files using ASiC-S, these data files can be zipped, and the zip file will be associated to one or more signature(s).

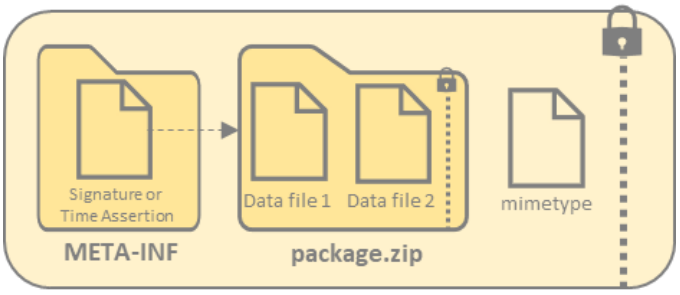


Figure 3: ASiC-S with two data files

2.1.5.2. ASiC-E

Compared to ASiC-S, ASiC-E can sign multiple data files (ASiC-S is only able to sign one single data file). Especially, ASiC-E associates:

- **One or more** data files with **one or more** signatures file(s) where each signature file contains one or more XAdES signature(s), referred as "ASiC-E with XAdES". An example where one signature (i.e. the XAdES signature in the signature.xml file) is used to sign two data files is illustrated in Figure 4. Another example, where a first signature (i.e. *signature1.xml*) is used to sign two data files and the second signature (i.e. *signature2.xml*) is used to sign one data file, is illustrated in Figure 5;

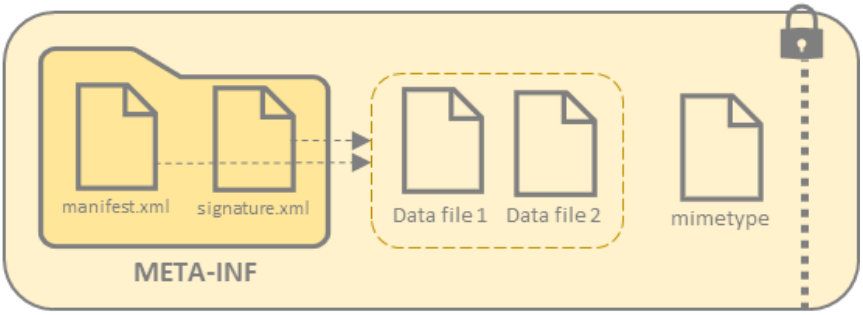


Figure 4: ASiC-E with XAdES with one signature and two data files

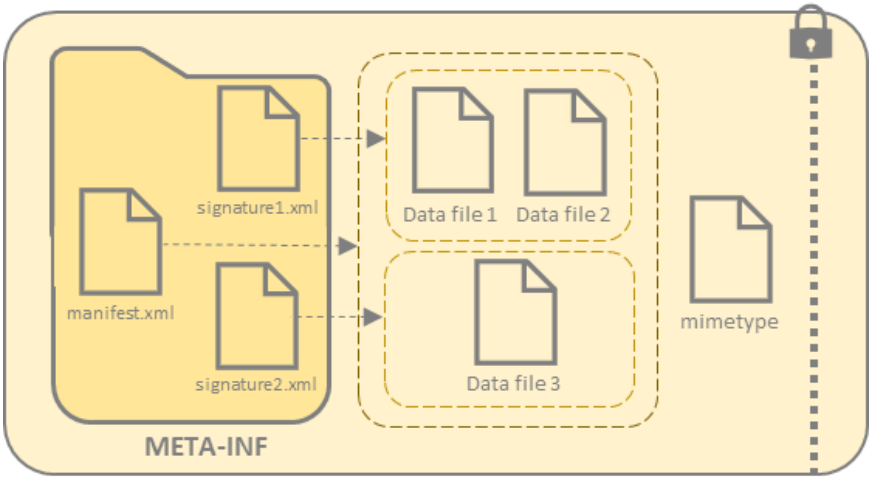


Figure 5: ASiC-E with XAdES with two signatures and three data files

- **One or more** data files with **one or more** signature file(s), each one containing a CAdES object, referred as "ASiC-E with CAdES". An example where one signature is used to sign two data files is illustrated in Figure 6. Another example, where a first signature (i.e. *signature1.p7s*) is used to sign two data files and the second signature (i.e. *signature2.p7s*) is used to sign one data file, is illustrated in Figure 5;

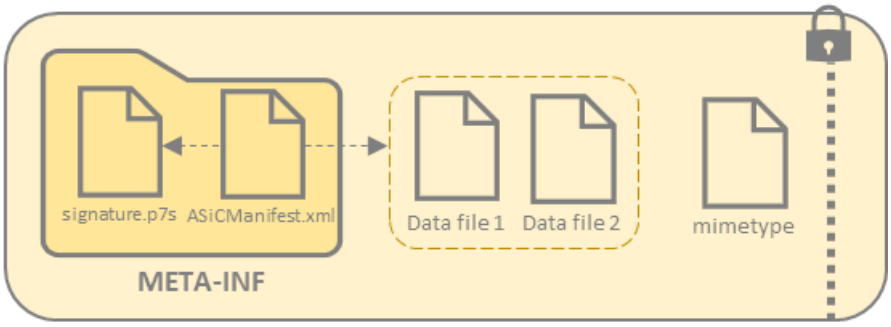


Figure 6: ASiC-E with CAdES with one signature and two data files

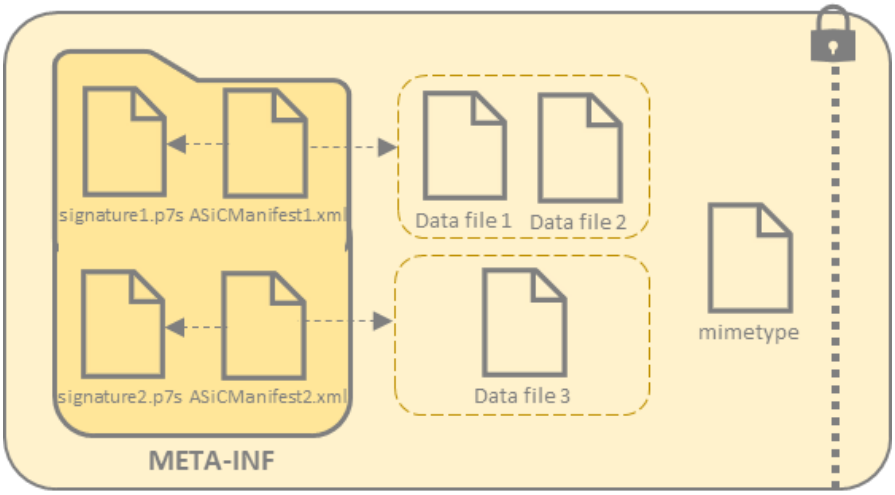


Figure 7: ASiC-E with CAdES with two signatures and three data files

- **One or more** data files with **one or more** time assertion file(s), each one containing time assertion, referred as "ASiC-E with time assertions".

2.2. Signature baseline profiles

Signature baseline profiles intend to facilitate interoperability by reducing the number of options when implementing formats, and yet to encompass the needs of the full life cycle of advanced electronic signatures.

These different needs are addressed by four levels of conformance: -B, -T, -LT, -LTA. The higher the level of conformance an AdES achieves, the longer the validity period of this AdES. In this respect, levels of conformance are used as part of the preservation process.

Preservation is important in order to maintain the validity of an AdES. An AdES, without preservation mechanisms, won't be verifiable anymore in a machine-processable way when:

- The certificate related to the private key which signed the document is expired or revoked;

- Validation material (e.g. revocation information) is not available anymore;
- Cryptographic algorithms are not trustworthy anymore (e.g. attacks on cryptographic libraries are discovered, related physical software or hardware becomes obsolete).

For this purpose, ETSI standards define four levels addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. These four levels are described here below. Independently of the signature format, further details and guidance on the four levels can be found in ETSI [TR 119 100] and [EN 319 102-1].

- **Basic (-B) level:** This level provides requirements for the incorporation of signed and some unsigned attributes when the signature is generated. This level is for short-term purposes (e.g. a few days to a few months) with no protection against the expiration or revocation of the signing certificate.

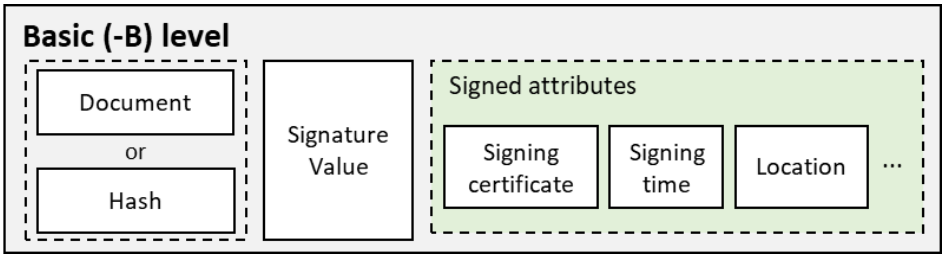


Figure 8: Basic signature

- **Time (-T) level:** This level is conformant with -B level. It provides requirements for the generation and inclusion of a timestamp for an existing signature. The timestamp shall be created before the signing certificate is revoked or expired, otherwise the validation of the signature may fail. This level aims to prove that a signature actually existed at (actually, before) a certain date and time and so provide an initial step towards the -LT level. This level is for mid-term purposes (e.g. a year).

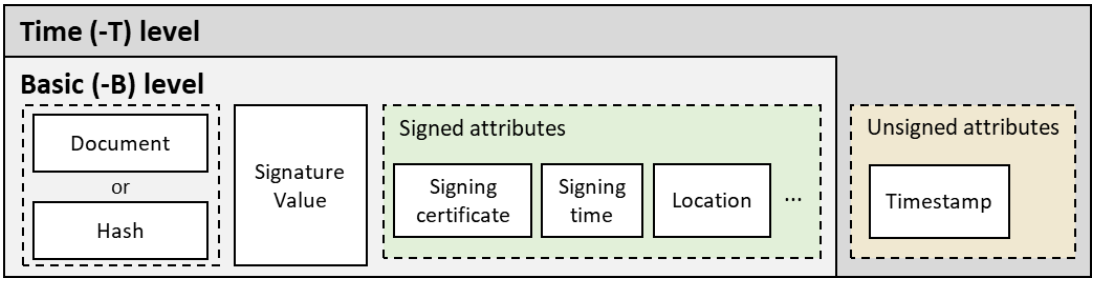


Figure 9: Signature with Time

The below levels (i.e. -LT and -LTA) are appropriate to ensure the validity of a signature when the related certificate expired or is revoked, when the validation material becomes unavailable, or when the related algorithm obsolescence is of concern.

The -LT and -LTA levels shall be achieved when the corresponding data are still valid[4]. For example, when applying the first -LT level with revocation data covering the signature and the timestamp, the signature and the timestamp shall be valid. When applying a second -LT level with revocation data on the archive timestamp, the archive timestamp shall be valid.

- **Long Term (-LT) level:** This level is conformant with -T level. It provides requirements for the incorporation of all the material required for validating the signature in the signature document (e.g. OCSP responses, CRL for each certificate in the validation chain except the trust anchor). This level aims to tackle the long-term availability of the validation material, even when the certificate is revoked/expired or when the CA or the Time Stamp Authority (TSA) is not available anymore. However, for long-term signatures, in practice it is instead suggested to use the below -LTA level as it offers proof of the existence of the revocation data at a given date. This level is for long-term purposes (e.g. a few years).

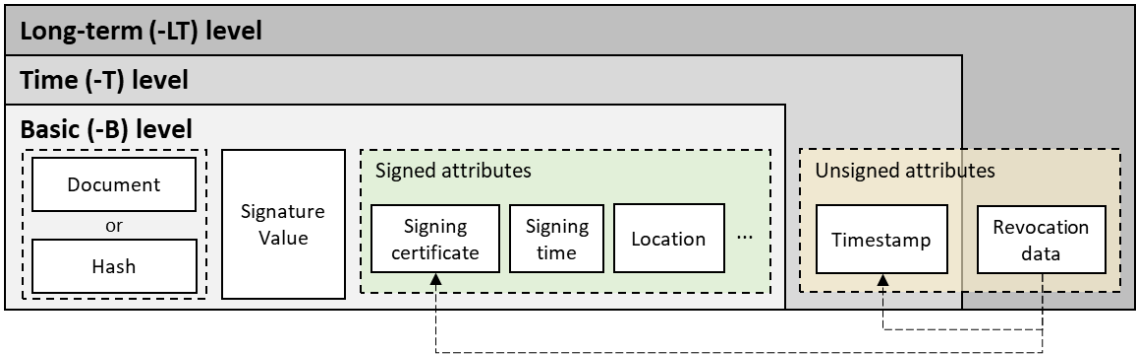
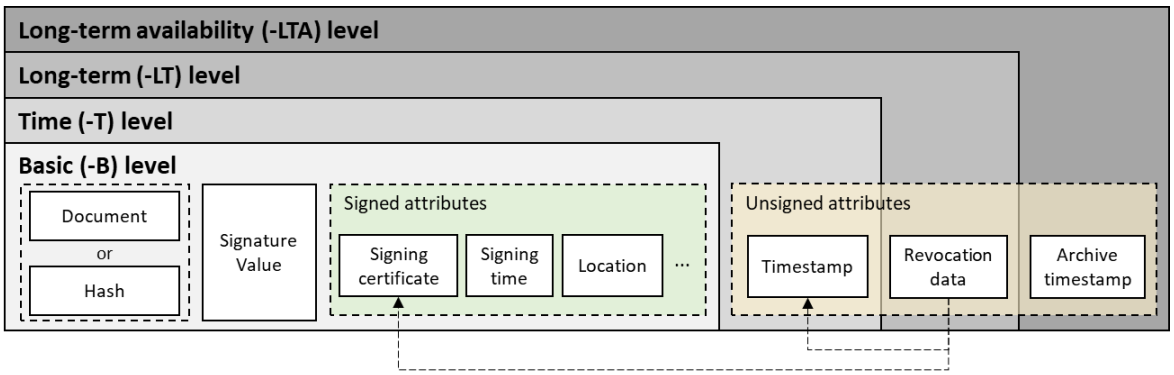


Figure 10: Signature with Long-Term Validation Material

- **Long Term Availability (-LTA) level:** This level is conformant with -LT level. It provides requirements for the incorporation of electronic timestamps that allow validation of the signature a long time after its generation. This level aims to tackle the long-term availability and integrity of the validation material by including an archive timestamp over all previous layers-related data and bringing proof of the existence of these data. This level is suggested for very long-term signatures (e.g. greater than 3 years).



[4] A validation algorithm is standardized in [EN 319 102-1].

Figure 11: Signature providing Long-Term Availability and Integrity of Validation Material

As a timestamp also has a limited validity period, this level requires repeated incorporations of timestamps, before the last timestamp expires or is revoked. When repeating the process, revocation data of the last timestamp shall be added together with the new timestamp. An example where two timestamps have been applied is illustrated in Figure 12.

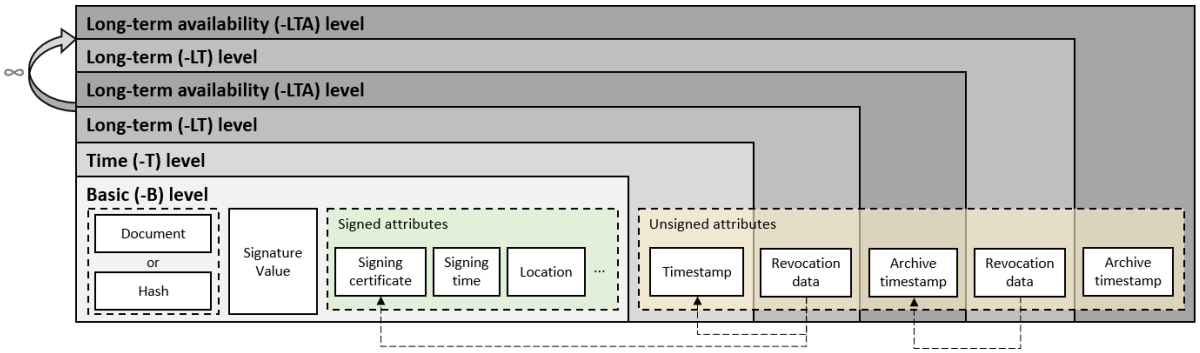


Figure 12: Signature providing Long Term Availability and Integrity of Validation Material after repetition

The archive timestamp can cover the signature (with the related properties) or the document together with the signature (and the related properties). It is important to note that, it is only when the archive timestamp covers the document that the obsolescence of the digest algorithm (cf. Section 3.3 “Determine the digest algorithm”) can be preserved. Applying the archive timestamp to cover both the signature and the document requires to have this original document at hand (this might not be the case for detached signatures).

2.3. Signature packaging

Packagings are combinations of the relative placements of signatures with regards to the signed data objects. The appropriate packaging will typically depend on the specific use case (e.g. the format of the document to sign), further detailed in Section 3.2.

Illustrated in Figure 13, there exist three types of packaging:

- **Enveloped:** The digital signature is embedded within the signed data object, so that the signature is part of the data object that is signed;
- **Enveloping:** The digital signature is embedding the signed data object;
- **Detached:** The digital signature that, with respect to the signed data object, is neither enveloping nor enveloped. As opposed to the other packagings, the signature and the signed content are separated, typically in separate files. In the particular case of “internally detached” XAdES though, these can be separate nodes under the same root in the same file.

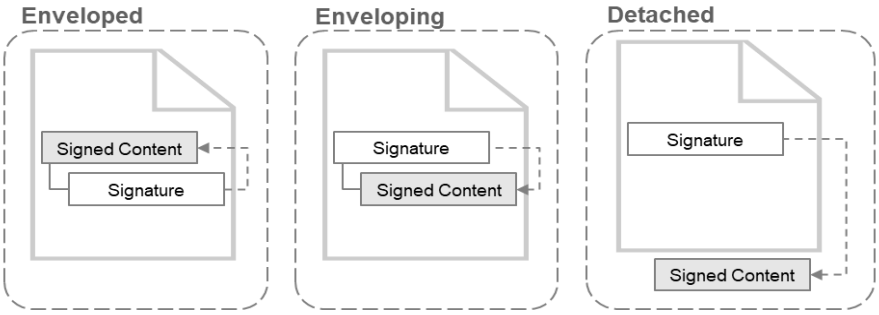


Figure 13: Signature packaging

3. Guidelines on signature creation and augmentation

This section offers guidelines and particular considerations regarding signature creation and augmentation. When signing a document, the typical steps are:

1. Determine the AdES signature format (Section 3.1);
2. Determine the packaging (Section 3.2);
3. Determine the digest algorithm (Section 3.3);
4. Sign the document at -B level;
5. If applicable, preserve the signature via augmentation to a higher level (-T, -LT, -LTA). These levels and their objectives are presented in Section 2.2.

Note: Complete guidance on the creation of digital signatures is provided in ETSI [TR 119 100] and [EN 319 102-1] specifies the procedures for creation and validation of AdES digital signatures.

3.1. Determine the AdES signature format

3.1.1. Signing a single document

This section contains guidelines for signing a single document, based on the format of the latter:

1. XML, PDF, JSON and ASN.1 formats

As laid down in [TR 119 100], when choosing which signature format is the most suitable for a given format of document, the suggested rule is: the closer the format of signature and format of document are, the better.

In this respect, when signing a single document, natural option for:

- XML document format is XAdES signature format ;
- PDF document format is PAdES signature format ;
- JSON document format is JAdES signature format ;
- Data objects whose structure is defined in ASN.1 is CAdES signature format.

2. Binary files

Binary files can be signed using both CAdES and XAdES with enveloping packaging (cf. Section 3.2). However, XAdES being based on XML format, this option is preferred over CAdES as XML offers plenty of benefits, including flexibility, ubiquity, human-readability and easier machine-processability.

3. Other document formats

Mixing formats is not recommended as the resulting file will be a newer format that can't be interpreted as the original format. For example, when signing a JSON file, it is not recommended to use XAdES enveloping signature format as it would mix XML and JSON formats, it is not recommended either to use CAdES enveloping signature format as it would mix ASN.1 and JSON formats.

In this respect, it is suggested to use either:

- XAdES (or CAdES) detached signature (cf. Section 3.2);
- ASiC container, further detailed in Section 3.1.2.

3.1.2. Signing multiple documents

When signing multiple documents, it is suggested to use “ASiC-E”, as this container can include several data objects and several signatures, detached from the aforementioned data objects, each signature selectively signing some of them.

Especially, it is recommended to use “ASiC-E with XAdES” format, as the mechanism for referencing all the documents signed by XML signatures is native (i.e. the usage of `ds:Reference` element). The XAdES signatures themselves appear within one or more files whose names follow the pattern "*signatures*.xml". When using “ASiC-E with CAdES”, the mechanism is less native as it requires the ASiC-E container to incorporate one additional XML file (ASiCManifest file) for each signature embedded within the container.

3.2. Determine the packaging

Following the decision taken in the previous section, one shall determine the related packaging. As illustrated in Table 2, not all packagings are compatible with each signature format.

When using a detached packaging, a separate file only containing the signature of the document’s digest is generated. When validating the signature, both the original document and the signature file are needed. Practically speaking, this means that in document workflows (emails, …) both files shall be circulated, which may be seen as either cumbersome or error-prone for the general public.

Only XAdES supports all packaging, as this signature format inherits from the XML signature mechanisms for explicitly referencing any signed data object (and in consequence, a standardized way of retrieving such data objects via the `ds:Reference` element). In XAdES, both enveloping and enveloped are suggested for signing XML files, while the enveloping packaging is suggested when signing other types of files (the file will be Base64-encoded and encapsulated within a `ds:Object` element).

	Enveloped	Enveloping	Detached
CAdES		**X**	**X**
XAdES	**X**	**X**	**X**
PAdES	**X**		
JAdES		**X**	**X**
ASiC			**X**

Table 2: Compatibility of the packaging with the AdES formats

3.3. Determine the digest algorithm

In the absence of an UAE national policy for the selection of these suites, algorithms proposed in [TS 119 312] and agreed by SOG-IS in the "Agreed Cryptographic Mechanisms [SOG-IS Crypto WG]" document[5] are suggested as a reference. These documents are regularly updated in order to sustain an appropriate level of security, taking into account a.o. an increasingly available computing power. Especially, [TS 119 312] proposes the recommended signature suites (i.e. digest algorithms and key lengths) for generating and augmenting digital signatures for a specific period of time.

In line with the above documents, and in the context of UAE, as digest algorithm, it is suggested to favor SHA-2 or SHA-3 family digest algorithms, in order to (as of today) properly preserve the integrity of the signed data. As mentioned in these same documents, algorithms that have been unanimously admitted as broken or weak (e.g. MD5, SHA-1), shall not be used as a digest algorithm.

4. Overview of signature validation standards

This section provides an overview of the signature validation standards. Because the UAE framework on trust services and electronic signatures is based on ETSI standards as explained above, the ETSI standards for signature validation can be reused as well, profiled when applicable to the national context.

ETSI standards relevant for signature validation are:

- ETSI [EN 319 102-1] which defines the procedures for validation of AdES digital signatures. This algorithm verifies the format, the revocation freshness, the X.509 certificate, the cryptographic validity of the signature then validates the signature according to its level (typically its baseline profile level). This standard is targeting the international community and is not specific to the EU context. It can be reused as is in the UAE context.
- ETSI [TS 119 615] which defines the procedures for using and interpreting European Union Member States national trusted lists. In particular, this standard defines the procedure for confirming the qualified status of a certificate, a timestamp, a validation service or a preservation service. As the UAE trusted list is based on the ETSI standard [TS 119 612], this standard is used as a basis for UAE Trusted List, adapted for the UAE context.
- ETSI [TS 119 172-4] defines the signature applicability rules for European qualified electronic signatures/seals using trusted lists. As the UAE trusted list and the UAE qualified electronic signatures/seal are similar to the European trusted lists and European qualified electronic signatures/seals, this standard can be applied to the UAE context. It is used as a basis for UAE Trusted List, adapted for the UAE context. Note: Complete guidance on validation of digital signatures is provided in ETSI [TR 119 100] standard.

[5] Available at https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.1.pdf