SLOVENSKI STANDARD
SIST-TS ETSI/TS 119 182-1 V1.1.1:2021

01-september-2021

Elektronski podpisi in infrastruktura (ESI) - Digitalni podpisi JAdES - 1. del: Gradniki in izhodiščni podpisi JAdES

Electronic Signatures and Infrastructures (ESI) - JAdES digital signatures - Part 1: Building blocks and JAdES baseline signatures

Ta slovenski standard je istoveten z: ETSI TS 119 182-1 V1.1.1 (2021-03)

ICS:

35.040.01	Kodiranje informacij na splošno	Information coding in general

SIST-TS ETSI/TS 119 182-1 V1.1.1:2021 en

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

Reference
DTS/ESI-0019182-1

Keywords
electronic signature, JSON

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://ipr.etsi.org/).

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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

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

The present document is part 1 of a multi-part deliverable covering JAdES digital signatures, as identified below:

Part 1: "Building blocks and JAdES baseline signatures";

Part 2: "Extended JAdES signatures".

One JSON schema file, whose location is detailed in clause B.1 and which contain JSON Schema definitions complements the present document.

The present document has taken as starting point the paper [i.18] "Bringing JSON signatures to ETSI AdES framework: meet JAdES signatures", by Juan Carlos Cruellas, in Computer Standards and Interfaces, Volume 71, August 2020.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Electronic commerce has emerged as a frequent way of doing business between companies across local, wide area and global networks. Trust in this way of doing business is essential for the success and continued development of electronic commerce. It is therefore important that companies using this electronic means of doing business have suitable security controls and mechanisms in place to protect their transactions and to ensure trust and confidence with their business partners. In this respect digital signatures are an important security component that can be used to protect information and provide trust in electronic business.

The present document is intended to cover digital signatures supported by PKI and public key certificates, and aims to meet the general requirements of the international community to provide trust and confidence in electronic transactions, including, amongst other, applicable requirements from Regulation (EU) No 910/2014 [i.1].

The present document can be used for any transaction between an individual and a company, between two companies, between an individual and a governmental body, etc. The present document is independent of any environment. It can be applied to any environment e.g. smart cards, SIM cards, special programs for electronic signatures, etc.

The present document is part of a rationalized framework of standards (see ETSI TR 119 000 [i.4]).

1 Scope

The present document:

1) Specifies a JSON [1] format for AdES signatures (JAdES signatures hereinafter) built on JSON Web Signatures (JWS hereinafter) as specified in IETF RFC 7515 [2]. For this, the present document:

   - Extends the JSON Web Signatures specified in IETF RFC 7515 [2] by defining an additional set of JSON header parameters that can be incorporated in the JOSE Header (either in its JWS Protected Header or its JWS Unprotected Header parts). Many of these new header parameters have the same semantics as the attributes/properties defined in CAdES [i.2] and XAdES [4] digital signatures. Other header parameters are defined to meet specific requirements that current JSON Web Signatures cannot meet (e.g. for explicitly referencing detached JWS Payload). These new header parameters and their corresponding types are defined in a JSON schema.

   - Specifies the mechanisms for incorporating the aforementioned JSON components in JSON Web Signatures [2] to build JAdES signatures, offering the same features as CAdES and XAdES in JSON syntax, and therefore fulfilling the same requirements (such as the long-term validity of digital signatures).

2) Defines four levels of JAdES baseline signatures addressing incremental requirements to maintain the validity of the signatures over the long term. Each level requires the presence of certain JAdES header parameters, suitably profiled for reducing the optionality as much as possible. The aforementioned levels provide the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications to be applicable to a wide range of communities when there is a clear need for interoperability of digital signatures used in electronic documents.

EXAMPLE: An example of requirements raised in specific domains is signing HTTP messages exchanged by parties in certain environments, which require signing both the HTTP body and some specific http headers. The format specified in IETF RFC 7515 [2] does not provide any native mechanism for individually identifying a detached JWS Payload. Clause 5.2.8 of the present document defines `sigD`, a new JSON header parameter that allows to identify one or more detached data objects which, suitably processed and concatenated, form the detached JWS Payload.

Procedures for creation, augmentation, and validation of JAdES digital signatures are out of scope.

NOTE 1: ETSI EN 319 102-1 [i.3] specifies procedures for creation, augmentation and validation of other types of AdES digital signatures.

The present multi-part deliverable aims at supporting electronic signatures independent of any specific regulatory framework.

NOTE 2: Specifically, but not exclusively, it is the aim that JAdES digital signatures specified in the present multi-part deliverable can be used to meet the requirements of electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as defined in Regulation (EU) No 910/2014 [i.1].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://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.

The following referenced documents are necessary for the application of the present document.

[1] IETF RFC 8259 (December 2017): "The JavaScript Object Notation (JSON) Data Interchange Format".

[2] IETF RFC 7515 (May 2015): "JSON Web Signature (JWS)".

[3] IETF RFC 3061 (February 2001): "A URN Namespace of Object Identifiers".

[4] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

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

[6] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[7] IETF RFC 3161 (August 2001): "Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)".

[8] IETF RFC 5280 (May 2008): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[9] IETF RFC 6960 (June 2013): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[10] IETF RFC 5816 (April 2010): "ESSCertIDv2 Update for RFC 3161".

[11] IETF RFC 3494 (March 2003): "Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status".

[12] IETF RFC 4648 (October 2006): "The Base16, Base32, and Base64 Data Encodings".

[13] IETF RFC 3230 (January 2002): "Instance Digests in HTTP".

[14] IETF RFC 7797 (February 2016): "JSON Web Signature (JWS) Unencoded Payload Option".

[15] IETF RFC 3339 (July 2002): "Date and Time on the Internet: Timestamps".

[16] IETF RFC 7518 (May 2015): "JSON Web Algorithms (JWA)".

[17] IETF RFC 3986 (January 2005): "Uniform Resource Identifier (URI): Generic Syntax".

[18] IETF RFC 2616 (June 1999): "Hypertext Transfer Protocol - HTTP/1.1".

[19] draft-handrews-json-schema-01 (March 2018): "JSON Schema: A Media Type for Describing JSON Documents".

[20] draft-handrews-json-schema-validation-01 (March 2018): "JSON Schema Validation: A Vocabulary for Structural Validation of JSON".

[21] ETSI TS 119 312 (V1.3.1): "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[22] FIPS Publication 180-4 (August 2015): "Secure Hash Standard (SHS)", National Institute of Standards and Technology.

[23] FIPS Publication 202 (August 2015): "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions", National Institute of Standards and Technology.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.08.2014, p. 73-114.

[i.2] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.3] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.4] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview".

[i.5] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.6] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation".

[i.7] ETSI TS 119 172-1: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents".

[i.8] OASIS Standard: "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0".

[i.9] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".

[i.10] IETF RFC 4998: "Evidence Record Syntax (ERS)".

[i.11] W3C Recommendation (19 November 2019): "Verifiable Credentials Data Model 1.0".

[i.12] draft-cavage-http-signatures-10 (May 2018): "Signing HTTP Messages".

[i.13] JSON Schema Specification in json-schema.org website.

NOTE: Available at https://json-schema.org/specification.html.

[i.14] draft-handrews-json-schema-02 (September 2019): "JSON Schema: A Media Type for Describing JSON Documents".

[i.15] draft-handrews-json-schema-validation-02 (September 2019): "JSON Schema Validation: A Vocabulary for Structural Validation of JSON".

[i.16] IETF RFC 7517 (May 2015): "JSON Web Key (JWK)".

[i.17] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions -- Part 1: Country code".

[i.18] Juan Carlos Cruellas: "Bringing JSON signatures to ETSI AdES framework: meet JAdES signatures". Computer Standards and Interfaces, Volume 71, August 2020.

3 Definition of terms, symbols, abbreviations and terminology

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.5], IETF RFC 7515 [2] and the following apply:

JAdES signature: JSON Web Signature

NOTE: As specified in IETF RFC 7515 [2], or other parts of this multi-part deliverable.

JWS Signature Value: digital signature cryptographic value calculated over a sequence of octets derived from the JWS Protected Header and data to be signed

NOTE 1: IETF RFC 7515 [2] uses the term JWS Signature for this concept. The present document does not use this term, but the JWS Signature Value, for the sake of terminological coherence of other AdES specifications.

NOTE 2: The present document uses the term **JSON Web Signature**, as defined by IETF RFC 7515 [2], i.e. for denoting the JSON data structure for representing a digitally signed message.

3.2 Symbols

Void.

3.3 Abbreviations

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

ASCII	American Standard Code For Information Interchange
ASN.1	Abstract Syntax Notation 1
CA	Certification Authority
CRL	Certificate Revocation List
FIPS	Federal Information Processing Standards
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
JOSE	JSON Object Signing and Encryption
JSON	JavaScript Object Notation
JWS	JSON Web Signature
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PKI	Public Key Infrastructure
RFC	Request For Comments
SAML	Security Assertion Markup Language

SHA	Secure Hash Algorithm
SIM	Subscriber Identification Module
SPO	Service Provision Option
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UTC	Coordinated Universal Time

3.4 Terminology

The present document adopts, wherever it is possible the same terminology as the terminology used in IETF RFC 7515 [2] and in IETF RFC 8259 [1].

Therefore, within the present document, the term "JSON Web Signature" shall denote the JSON structure specified in IETF RFC 7515 [2].

The present document uses the term "JSON value" for denoting JSON objects, or JSON arrays, or JSON numbers, or JSON strings, i.e. a subset of the potential meanings of "JSON value" listed in clause 3 of IETF RFC 8259 [1].

The present document uses the term "header parameter" for denoting a JSON object, JSON array, JSON number, or JSON string, which is member either of the JWS Protected Header or the JWS Unprotected Header specified in IETF RFC 8259 [1].

The present document uses the term "member" for denoting a JSON object's member, as specified in clause 4 of IETF RFC 8259 [1].

The present document uses the term "element" or "element of the array" for denoting the contents of a position within a JSON array (specified in clause 5 of IETF RFC 8259 [1]).

NOTE: These last terms will be used for denoting each of the JSON values that will be added to the `etsiU` JSON array (specified in clause 5.3.1 of the present document), which will be incorporated in the JWS Unprotected header as a header parameter. Therefore, these JSON values will play, within the present document, an equivalent role to the role played by the unsigned attributes in CAdES and the unsigned qualifying properties in XAdES.

The present document uses the term "JAdES component" or "component" for denoting any JAdES signature constituent, regardless it is a header parameter, a member of a JSON Object, an element of a JSON array, or any other JSON Value.

The present document uses this special `font` for denoting tags of JAdES components.

As for the names of the header parameters and elements of the `etsiU` JSON array, the following criteria and conventions have been used:

1) The names have been selected to have a maxim length of 8 characters; most of the names are shorter.

2) The names of header parameters qualifying the signature itself use to start with "sig".

3) The names of header parameters qualifying the signer use to start with "sr".

4) The names of header parameters qualifying the data to be signed use to start with "sd".

5) The names of header parameters dealing with time-stamp tokens use to finalize with "tst".

6) The names of header parameters dealing with certificates use to start or contain "x" (following the convention of IETF RFC 7515 [2], which defines the header parameters `x5u`, `x5c`, `x5t`, and `x5t#S256`).

7) The names of header parameters dealing with revocation values (CRLs or OCSP responses) use to start or contain "r".

8) The names of header parameters dealing with attribute certificates or the corresponding revocation values use to start "a".

9) The names of header parameters dealing with values (of certificates or revocation values) use to contain "Vals".

10) The names of header parameters dealing with references (to certificates or revocation values) use to contain "Refs" (except `x5t`, and `x5t#S256`, which have been defined in IETF RFC 7515 [2], contain references to certificates, and do not include it).

4 General Requirements

The JAdES components defined in the present document shall be carried within the JOSE header as specified in IETF RFC 7515 [2].

All the JAdES signed header parameters specified in clause 5.2 of the present document, as well as: `cty`, `kid`, `crit`, and `x5u` header parameters specified in IETF RFC 7515 [2] and further profiled in clause 5.1 of the present document, if required to be present, shall be incorporated as header parameters of the JWS Protected Header of the JSON Web Signature, specified in IETF RFC 7515 [2].

JAdES signatures may be serialized using either JWS Compact Serialization or JWS JSON Serialization as specified in clause 3 of IETF RFC 7515 [2].

JWS Unprotected Header in JAdES signatures shall contain only one header parameter, namely the `etsiU` header parameter (specified in clause 5.3 of the present document), which is defined as a JSON array.

NOTE 1: The rationale for this is that the JWS Unprotected Header is a JSON object, and no order may be inferred in its different members. This is the reason why the present document defines `etsiU` header parameter as a JSON array.

NOTE 2: The elements of this JSON array will contain JSON values that play for JAdES signatures the same role as the role played by the unsigned attributes for CAdES signatures, and the role played by the unsigned qualifying properties for XAdES signatures.

NOTE 3: An immediate consequence is that a time-stamp token present within the `arcTst` object specified in clause 5.3.6.2 of the present document, protects the JWS Payload, the JWS Protected Header, the JAdES Signature Value, and the `etsiU` header parameter within the JWS Unprotected Header.

Header parameters defined by IETF RFC 7515 [2] and IETF RFC 7797 [14] not further profiled within the present document may be added as header parameters within the JAdES signature, following the requirements specified in the present document.

In JAdES signatures, the JWS Payload may be attached or detached.

Detached JWS Payload may either be one detached object, or result from the concatenation of more than one detached data objects. See the specification of `sigD` signed header parameter in clause 5.2.8 of the present document.

NOTE 4: At the moment of producing the present document, JSON Schema was under development. The working draft being used at the present document was the one specified by draft-handrews-json-schema-01 [19], and draft-handrews-json-schema-validation-01 [20]. These documents, though, do not correspond to the latest version (draft-handrews-json-schema-02 [i.14], and draft-handrews-json-schema-validation-02 [i.15]) due to the fact that tools checking correctness of JSON schema files have not been yet completed. The drafts of JSON schema specifications may be accessed at JSON Schema Specification in json-schema.org website [i.13].

NOTE 5: Although at the moment of producing the present document there exist several proposals for JSON canonicalization algorithms, none have been formally adopted by any standardisation organization. Nevertheless, the present document uses placeholders for identifiers of canonicalization algorithms in a number of components that could use them if such algorithms are standardized in the future.

5 Header parameters semantics and syntax

5.1 Use of header parameters defined in IETF RFC 7515 and IETF RFC 7797

5.1.1 Introduction

This clause defines additional requirements for the use of some of header parameters specified in IETF RFC 7515 [2].

JAdES signatures may incorporate any of the header parameters specified in IETF RFC 7515 [2] and IETF RFC 7797 [14].

NOTE: Clause 6.3 also specifies requirements (mainly of presence and cardinality), for the use of some of the header parameters specified in IETF RFC 7515 [2] for JAdES baseline signatures.

5.1.2 The `alg` (X.509 URL) header parameter

Semantics

The `alg` header parameter shall be a signed header parameter that qualifies the signature.

The `alg` header parameter shall have the semantics specified in IETF RFC 7515 [2], clause 4.1.1.

Syntax

The `alg` header parameter shall have the syntax specified in IETF RFC 7515 [2], clause 4.1.1.

Its value should be one of the algorithms for digital signatures recommended by in ETSI TS 119 312 [21].

5.1.3 The `cty` (content type) header parameter

Semantics

The `cty` header parameter shall be a signed header parameter that qualifies the JWS Payload.

The `cty` header parameter shall have the semantics specified in IETF RFC 7515 [2], clause 4.1.10.

The `cty` header parameter should not be present if the `sigD` header parameter, specified in clause 5.2.8 of the present document, is present within the JAdES signature.

The `cty` header parameter should not be present if the content type is implied by the JWS Payload.

The `cty` header parameter shall not be present if the JWS Payload is a (counter-signed) signature.

NOTE: The `sigD` header parameter has one member that contains information of the format and type of the constituents of the JWS Payload.

Syntax

The `cty` header parameter shall have the syntax specified in IETF RFC 7515 [2], clause 4.1.10.

5.1.4 The `kid` (key identifier) header parameter

Semantics

The `kid` header parameter shall be a signed header parameter that qualifies the signature.

The `kid` header parameter shall have the semantics specified in IETF RFC 7515 [2], clause 4.1.4.