Profile X.509 Certificate Status for OASIS Digital Signature Services Version 2.0

Working Draft 01

DD Month YYYY

Technical Committee:

[OASIS Digital Signature Services eXtended (DSS-X) TC](https://www.oasis-open.org/committees/dss-x/)

Chairs:

Stefan Hagen (stefan@hagen.link), Individual

Editor:

Andreas Kuehne (kuehne@trustable.de), Individual

Stefan Hagen (stefan@hagen.link), Individual

Additional artifacts:

This prose specification is one component of a Work Product that also includes:

* JSON and XML schemas: <http://docs.oasis-open.org/dss-x/dss-core/v2.0/csd01/schemas/>

Related work:

This specification is related to:

* RFC 5280 Internet X.509 Public Key Infrastructure Certificate
* and Certificate Revocation List (CRL) Profile: <https://tools.ietf.org/html/rfc5280>

Declared XML namespaces:

* http://docs.oasis-open.org/dss/ns/X.509

Abstract:

This document defines a protocol and processing profile of the DSS Signing and Verifying Protocol specified in **[DSSCore]**, which allows to create JSON Web Signatures and to return verification outcome for each signature in a verification request.

Status:

This [Working Draft](https://www.oasis-open.org/policies-guidelines/tc-process) (WD) has been produced by one or more TC Members; it has not yet been voted on by the TC or [approved](https://www.oasis-open.org/policies-guidelines/tc-process) as a Committee Draft (Committee Specification Draft or a Committee Note Draft). The OASIS document [Approval Process](https://www.oasis-open.org/policies-guidelines/tc-process) begins officially with a TC vote to approve a WD as a Committee Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Draft.

Any machine-readable content ([Computer Language Definitions](https://www.oasis-open.org/policies-guidelines/tc-process)) declared Normative for this Work Product must also be provided in separate plain text files. In the event of a discrepancy between such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

URI patterns:

Initial publication URI:
<http://docs.oasis-open.org/dss-x/>???

Permanent “Latest version” URI:
http://docs.oasis-open.org/dss-x/???

(Managed by OASIS TC Administration; please don’t modify.)

Copyright © OASIS Open 2017. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full [Policy](https://www.oasis-open.org/policies-guidelines/ipr) may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Table of Contents

[1 Introduction 4](#_Toc511147236)

[1.1 Organization of DSS Core Protocols, Elements, and Bindings 4](#_Toc511147237)

[1.2 Terminology 4](#_Toc511147238)

[1.2.1 Terms and Definitions 4](#_Toc511147239)

[1.2.2 Abbreviated Terms 4](#_Toc511147240)

[1.3 Normative References 4](#_Toc511147241)

[1.4 Non-Normative References 5](#_Toc511147242)

[1.5 Typographical Conventions 5](#_Toc511147243)

[2 Design Considerations 7](#_Toc511147244)

[2.1 Construction Principles 7](#_Toc511147245)

[2.2 Domain Models 7](#_Toc511147246)

[2.2.1 Date and Time Model 7](#_Toc511147247)

[2.3 Schema Organization and Namespaces 7](#_Toc511147248)

[2.4 DSS Overview (Non-normative) 8](#_Toc511147249)

[2.5 Syntax variants 8](#_Toc511147250)

[3 Structure Models 9](#_Toc511147251)

[3.1 Structure Models defined in this document 9](#_Toc511147252)

[3.1.1 Component SerializationSyntax 9](#_Toc511147253)

[3.1.1.1 Semantics 9](#_Toc511147254)

[3.1.1.2 XML Syntax 9](#_Toc511147255)

[3.1.1.3 JSON Syntax 9](#_Toc511147256)

[3.1.2 Component OptionalInputSign 10](#_Toc511147257)

[3.1.2.1 Semantics 10](#_Toc511147258)

[3.1.2.2 XML Syntax 11](#_Toc511147259)

[3.1.2.3 JSON Syntax 12](#_Toc511147260)

[3.1.3 Component OptionalInputVerify 13](#_Toc511147261)

[3.1.3.1 Semantics 13](#_Toc511147262)

[3.1.3.2 XML Syntax 13](#_Toc511147263)

[3.1.3.3 JSON Syntax 13](#_Toc511147264)

[4 Conformance 15](#_Toc511147265)

[4.1 Level 1 – “Basic” 15](#_Toc511147266)

[4.2 Level 2 – “Comprehensive” 15](#_Toc511147267)

[Appendix A. Index 16](#_Toc511147268)

[Appendix B. Revision History 17](#_Toc511147269)

# Introduction

## Organization of DSS Core Protocols, Elements, and Bindings

This document defines a protocol and processing profile of the DSS Signing and Verifying Protocol specified in **[DSSCore]**, which allows to support the creation and verification of JSON Web Signatures.

The following sections describe how to understand the rest of this document.

## Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

### Terms and Definitions

For the purposes of this document, the following applies:

**Term** — meaning and maybe ref

### Abbreviated Terms

**Acronym** — Spelled out

## Normative References

[RFC2119] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.

**[RFC 2396]** T. Berners-Lee et al. *Uniform Resource Identifiers (URI): Generic Syntax.* IETF RFC 2396, August 1998.
<http://www.ietf.org/rfc/rfc2396.txt>.

[DSS2XSD] S. Hagen,. *DSS 2.0 Core Schema*. OASIS, ToDo.

[DSS2BASEXSD] S. Hagen,. *DSS 2.0 Base Schema*. OASIS, ToDo.

**[DSSJWS-XSD]** A. Kuehne, et. al.: “*DSS JSON Web Signatures Schema”*, , ToDo.

**[RFC 2440]** J. Callas, L. Donnerhacke, H. Finney, R. Thayer. *OpenPGP Message Format*. IETF RFC 2440, November 1998.
<http://www.ietf.org/rfc/rfc2440.txt>.

**[RFC 2616]** R. Fielding et al. *Hypertext Transfer Protocol – HTTP/1.1*. IETF RFC 2616, June 1999.
[http://www.ietf.org/rfc/rfc2616.txt](http://www.ietf.org/rfc/rfc2440.txt).

**[RFC 2648]** R. Moats. *A URN Namespace for IETF Documents*. IETF RFC 2648, August 1999.
<http://www.ietf.org/rfc/rfc2648.txt>.

**[RFC 2822]** P. Resnick. *Internet Message Format*. IETF RFC 2822, April 2001. <http://www.ietf.org/rfc/rfc2822.txt>

**[RFC 3161]** C. Adams, P. Cain, D. Pinkas, R. Zuccherato. *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*. IETF RFC 3161, August 2001.
[http://www.ietf.org/rfc/rfc3161.txt](http://www.ietf.org/rfc/rfc3075.txt).

**[RFC 5280]** D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. IETF RFC 5280, May 2008.
<http://www.ietf.org/rfc/rfc5280.txt>.

**[RFC 5652]** R. Housley. *Cryptographic Message Syntax*. IETF RFC 5652, September 2009.
<http://www.ietf.org/rfc/rfc5652.txt>.
(Remark: As used in DSS, all implementations based upon RFC 5652 and previous releases of CMS will suffice. For the sake of simplicity the "urn:ietf:rfc:3369" is used throughout the document to indicate a CMS message as specified in RFC 5652 or RFC 3369 or any version (including PKCS #7).

**[****RFC7159]** T. Bray, Ed., Google, Inc., The JavaScript Object Notation (JSON) Data Interchange Format, ISSN: 2070-1721, March 2014.
<https://tools.ietf.org/html/rfc7159>.

**[RFC7515]** M. Jones, Microsoft, JSON Web Signature (JWS), ISSN: 2070-1721, May 2015.
<https://tools.ietf.org/html/rfc7515>.

[XML] Extensible Markup Language (XML) 1.0 (Fifth Edition), T. Bray, J. Paoli, M. Sperberg-McQueen, E. Maler, F. Yergeau, Editors, W3C Recommendation, November 26, 2008, <http://www.w3.org/TR/2008/REC-xml-20081126/>.
Latest version available at <http://www.w3.org/TR/xml>.

[XML-Schema-1] W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures, S. Gao, M. Sperberg-McQueen, H. Thompson, N. Mendelsohn, D. Beech, M. Maloney, Editors, W3C Recommendation, April 5, 2012,
<http://www.w3.org/TR/2012/REC-xmlschema11-1-20120405/>.
Latest version available at <http://www.w3.org/TR/xmlschema11-1/>.

[XML-Schema-2] W3C XML Schema Definition Language (XSD) 1.1 Part 2: DatatypesW3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes, D. Peterson, S. Gao, A. Malhotra, M. Sperberg-McQueen, H. Thompson, Paul V. Biron, Editors, W3C Recommendation, April 5, 2012,
<http://www.w3.org/TR/2012/REC-xmlschema11-2-20120405/>.
Latest version available at <http://www.w3.org/TR/xmlschema11-2/>.

**[XPATH]** XML Path Language (XPath) Version 1.0. W3C Recommendation 16 November 1999 <http://www.w3.org/TR/xpath>

## Non-Normative References

[ISO8601] Data elements and interchange formats — Information interchange — Representation of dates and times, International Standard, ISO 8601:2004(E), December 1, 2004, <https://www.iso.org/standard/40874.html>.

## Typographical Conventions

Keywords defined by this specification use this monospaced font.

Normative source code uses this paragraph style.

Text following the special symbol («) – an opening Guillemet (or French quotation mark) – within this specification identifies conformance statements. Every conformance statement is separated from the following text with the special end symbol (») – a closing Guillemet, and has been assigned a reference that follows that end symbol in the format [dSS-section#-local#].

Some sections of this specification are illustrated with non-normative examples.

Example 1: text describing an example uses this paragraph style

Non-normative examples use this paragraph style.

All examples in this document are non-normative and informative only.

Representation-specific text is indented and marked with vertical lines.

Representation-Specific Headline

Normative representation-specific text

All other text is normative unless otherwise labeled e.g. like:

Non-normative Comment:

This is a pure informative comment that may be present, because the information conveyed is deemed useful advice or common pitfalls learned from implementer or operator experience and often given including the rationale.

# X.509 Certificate Status Profile

## Overview

This profile supports the computation of the status of an X.509 certificate [[RFC5280]](#refRFC5280) without the presence of a signature. This functionality is usually implemented in a DSS-X compliant validation server. With this profile, the computation of the status of an X.509 certificate can be used separately.

It is assumed that the client has a basic understanding of X.509 certificates and is able to interpret the Certificate Extensions (e.g. ‘Usage’). The DSS server focusses on the certificate status (by checking CRL or OCSP), the construction of the certificate chain and the path to the trust anchor.

The details regarding the outcome of the certificate’s status will be transported within the Result component. The status will be represented by the ResultMinor element:

|  |  |
| --- | --- |
| Certificate Status | ResultMinor |
| valid | urn:oasis:names:tc:dss:1.0:resultminor:valid:signature:OnAllDocuments |
| chain problem | urn:oasis:names:tc:dss:1.0:resultminor:CertificateChainNotComplete |
| revoked | urn:oasis:names:tc:dss:1.0:resultminor:certificate:revoked |
| expired | urn:oasis:names:tc:dss:1.0:resultminor:certificate:expired |
| not valid yet | urn:oasis:names:tc:dss:1.0:resultminor:certificate:notValidYet |
| on hold | urn:oasis:names:tc:dss:1.0:resultminor:certificate:onHold |

For the computation of the status of an X.509 certificate the following operations apply:

* VerifyRequest: This structure supports requests for:
	+ Computing the status of an existing X.509 certificate [[RFC5280]](#refRFC5280).
* VerifyResponse: This structure supports delivery of:
	+ Computed status.

## Profile Features

### Scope

This document profiles the DSS verifying protocols defined in [DSSCore].

### Relationship to Other Profiles

The profile in this document is based on the [DSSCore].

## Profile of Verifying Protocol

### Component VerifyRequest

This clause specifies the profile for the contents of the VerifyRequest when used for requesting the status of an X.509 certificate.

#### Component SignatureObject

This component MUST contain the X.509 certificate to be processed in the Base64Signature element. The type of element, specified by the MimeType element of the Base64DataType component, MUST be “application/pkix-cert”.

#### Component InputDocument

The SignatureObject holds the X.509 certificate. The X.509 certificate encapsulates the signed content. So the InputDocument element MUST NOT be used.

#### Component OptionalInputs

There are no restrictions on the optional inputs in component OptionalInputs, specified in the **[DSS Core].**

#### Component OptionalInputsBase

The elements of component OptionalInputsBase, specified in the **[DSS Core]** MUST NOT be used conjunction with this profile**.**

#### Component OptionalInputVerify

Only a few of the optional inputs specified in the **[DSS Core]** are usable in this profile. See the list of optional inputs below.

##### AdditionalKeyInfo

The absence of a signature makes it more likely that additional certificates are required for the construction of the certificate chain. The X509Certificate element of the AdditionalKeyInfo component may transport these certificates.

##### ReturnSignerIdentity

The OptionalInputVerify element ReturnSignerIdentity may be used to request the name of the certificate issuer.

##### UseVerificationTime, ReturnVerificationTimeInfo

The OptionalInputVerify elements UseVerificationTime, ReturnVerificationTimeInfo may be used in conjunction with this profile.

### Component VerifyResponse

This clause profiles the dss:VerifyResponse component.

#### Component OptionalOutputs

There are no restrictions on the elements in component OptionalInputs, specified in the **[DSS Core].**

#### Component OptionalOutputsBase

The elements of component OptionalOutputsBase, specified in the **[DSS Core]** MUST NOT be used conjunction with this profile**.**

#### Component OptionalOutputVerify

Only a few of the optional outputs specified in the **[DSS Core]** are usable in this profile. See the list of optional inputs below.

##### VerificationTimeInfo

The optional VerificationTimeInfo component MAY contain an VerificationTime element. It MUST NOT contain any AdditionalTimeInfo elements.

##### SignerIdentity

The optional SignerIdentity component MAY contain name of the certificate issuer.

# Structure Models

This profile does not define additional components.

# Identifiers defined in this specification

## Result Identifiers

This profile defines the <ResultMinor> values listed below:

urn:oasis:names:tc:dss:1.0:resultminor:valid:signature:OnAllDocuments

urn:oasis:names:tc:dss:1.0:resultminor:certificate:revoked

urn:oasis:names:tc:dss:1.0:resultminor:certificate:expired

urn:oasis:names:tc:dss:1.0:resultminor:certificate:onHold

1. Acknowledgements

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

1. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Editor** | **Changes Made** |
|  |  |  |  |