Digital Signature Service Core Protocols, Elements, and Bindings 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:

Juan Carlos Cruellas ([cruellas@ac.upc.edu](mailto:cruellas@ac.upc.edu)), [Univ Politecnica de Cataluna](http://www.ac.upc.edu/)

Stefan Hagen ([stefan@hagen.link](mailto:stefan@hagen.link)), Individual

Editor:

Stefan Hagen ([stefan@hagen.link](mailto: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 replaces or supersedes:

* Stefan Drees et al., Digital Signature Service Core Protocols, Elements, and Bindings, Version 1.0, OASIS Standard, 11 April 2007,  
  <http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf>

This specification is related to:

* Related specifications (hyperlink, if available)

Declared XML namespaces:

* <http://docs.oasis-open.org/dss-x/ns/dss-core/v2.0/dss>

Abstract:

This document defines JSON and XML based request/response protocols for signing and verifying documents and other data. It also defines a timestamp format, and a signature property for use with these protocols. Finally, it defines transport and security bindings for the protocols.

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/dss-core/v2.0/csd01/dss-core-v2.0-csd01.docx

Permanent “Latest version” URI:  
http://docs.oasis-open.org/dss-x/dss-core/v2.0/dss-core-v2.0.docx

(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 9](#_Toc482893695)

[1.1 Organization of DSS Core Protocols, Elements, and Bindings 9](#_Toc482893696)

[1.2 Terminology 9](#_Toc482893697)

[1.2.1 Terms and Definitions 9](#_Toc482893698)

[1.2.2 Abbreviated Terms 9](#_Toc482893699)

[1.3 Normative References 9](#_Toc482893700)

[1.4 Non-Normative References 11](#_Toc482893701)

[1.5 Typographical Conventions 11](#_Toc482893702)

[2 Design Considerations 12](#_Toc482893703)

[2.1 Construction Principles 12](#_Toc482893704)

[2.2 Domain Models 12](#_Toc482893705)

[2.2.1 Date and Time Model 12](#_Toc482893706)

[2.3 Schema Organization and Namespaces 12](#_Toc482893707)

[2.4 DSS Overview (Non-normative) 13](#_Toc482893708)

[2.5 Version 2.0 motivation [non-normative] 14](#_Toc482893709)

[2.6 Syntax variants 14](#_Toc482893710)

[3 Structure Models 15](#_Toc482893711)

[3.1 Type Base64DataType 15](#_Toc482893712)

[3.2 Type AnyType 16](#_Toc482893713)

[3.3 Type InternationalStringType 16](#_Toc482893714)

[3.4 Type KeyInfoType 17](#_Toc482893715)

[3.5 Element InputDocuments 18](#_Toc482893716)

[3.5.1 Type DocumentBaseType 19](#_Toc482893717)

[3.5.2 Type DocumentType 19](#_Toc482893718)

[3.5.2.1 XML Syntax 19](#_Toc482893719)

[3.5.2.2 JSON Syntax 20](#_Toc482893720)

[3.5.3 Type TransformedDataType 20](#_Toc482893721)

[3.5.3.1 XML Syntax 21](#_Toc482893722)

[3.5.3.2 JSON Syntax 21](#_Toc482893723)

[3.5.4 Type DocumentHashType 21](#_Toc482893724)

[3.5.4.1 XML Syntax 22](#_Toc482893725)

[3.5.4.2 JSON Syntax 22](#_Toc482893726)

[3.6 Element SignatureObject 22](#_Toc482893727)

[3.6.1 XML Syntax 23](#_Toc482893728)

[3.6.2 JSON Syntax 24](#_Toc482893729)

[3.7 Element Result 24](#_Toc482893730)

[3.7.1 XML Syntax 26](#_Toc482893731)

[3.7.2 JSON Syntax 26](#_Toc482893732)

[3.8 Common Optional Inputs 27](#_Toc482893733)

[3.8.1 Optional Input ServicePolicy 27](#_Toc482893734)

[3.8.1.1 XML Syntax 27](#_Toc482893735)

[3.8.1.2 JSON Syntax 27](#_Toc482893736)

[3.8.2 Optional Input ClaimedIdentity 27](#_Toc482893737)

[3.8.2.1 XML Syntax 28](#_Toc482893738)

[3.8.2.2 JSON Syntax 28](#_Toc482893739)

[3.8.3 Optional Input Language 28](#_Toc482893740)

[3.8.3.1 XML Syntax 28](#_Toc482893741)

[3.8.3.2 JSON Syntax 28](#_Toc482893742)

[3.8.4 Optional Input Profile 29](#_Toc482893743)

[3.8.4.1 XML Syntax 29](#_Toc482893744)

[3.8.4.2 JSON Syntax 29](#_Toc482893745)

[3.8.5 Optional Input Schemas 29](#_Toc482893746)

[3.8.5.1 XML Syntax 30](#_Toc482893747)

[3.8.5.2 JSON Syntax 30](#_Toc482893748)

[3.8.6 Type Optional Input ReturnTransformedDocument and Output TransformedDocument 30](#_Toc482893749)

[3.8.6.1 XML Syntax 31](#_Toc482893750)

[3.8.6.2 JSON Syntax 31](#_Toc482893751)

[3.9 OptionalInputsBaseType 31](#_Toc482893752)

[3.9.1.1 XML Syntax 32](#_Toc482893753)

[3.9.1.2 JSON Syntax 32](#_Toc482893754)

[3.10 Common Optional Outputs 33](#_Toc482893755)

[3.10.1 Optional Output Schemas 33](#_Toc482893756)

[3.11 OptionalOutputsBaseType 33](#_Toc482893757)

[3.11.1.1 XML Syntax 33](#_Toc482893758)

[3.11.1.2 JSON Syntax 34](#_Toc482893759)

[3.12 Type RequestBaseType 34](#_Toc482893760)

[3.12.1 XML Syntax 35](#_Toc482893761)

[3.12.2 JSON Syntax 35](#_Toc482893762)

[3.13 Type ResponseBaseType 35](#_Toc482893763)

[3.13.1 XML Syntax 35](#_Toc482893764)

[3.13.2 JSON Syntax 35](#_Toc482893765)

[4 The DSS Signing Protocol 37](#_Toc482893766)

[4.1 Element SignRequest 37](#_Toc482893767)

[4.1.1 XML Syntax 37](#_Toc482893768)

[4.1.2 JSON Syntax 37](#_Toc482893769)

[4.2 Element SignResponse 37](#_Toc482893770)

[4.2.1 XML Syntax 38](#_Toc482893771)

[4.2.2 JSON Syntax 38](#_Toc482893772)

[4.3 Processing for XML Signatures 39](#_Toc482893773)

[4.3.1 Basic Process for XML 39](#_Toc482893774)

[4.3.2 Process Variant for TransformedData 40](#_Toc482893775)

[4.3.3 Process Variant for DocumentHash 40](#_Toc482893776)

[4.4 Basic Processing for CMS Signatures 41](#_Toc482893777)

[4.4.1 Process Variant for DocumentHash 41](#_Toc482893778)

[4.5 Optional Inputs and Outputs 41](#_Toc482893779)

[4.5.1 Optional Input SignatureType 42](#_Toc482893780)

[4.5.1.1 XML Syntax 42](#_Toc482893781)

[4.5.1.2 JSON Syntax 42](#_Toc482893782)

[4.5.2 Optional Input AddTimestamp 42](#_Toc482893783)

[4.5.2.1 XML Syntax 42](#_Toc482893784)

[4.5.2.2 JSON Syntax 42](#_Toc482893785)

[4.5.2.3 Processing of signatures time-stamping 43](#_Toc482893786)

[4.5.2.3.1 Processing for CMS signatures time-stamping 43](#_Toc482893787)

[4.5.2.3.2 Processing for XML Timestamps on XML signatures 43](#_Toc482893788)

[4.5.2.4 Processing for RFC 3161 Timestamps on XML signatures 44](#_Toc482893789)

[4.5.3 Optional Input IntendedAudience 44](#_Toc482893790)

[4.5.3.1 XML Syntax 44](#_Toc482893791)

[4.5.3.2 JSON Syntax 44](#_Toc482893792)

[4.5.4 Optional Input KeySelector 45](#_Toc482893793)

[4.5.4.1 XML Syntax 45](#_Toc482893794)

[4.5.4.2 JSON Syntax 45](#_Toc482893795)

[4.5.5 Optional Input Properties 45](#_Toc482893796)

[4.5.5.1 XML Syntax 45](#_Toc482893797)

[4.5.5.2 JSON Syntax 46](#_Toc482893798)

[4.5.6 Optional Input IncludeObject 46](#_Toc482893799)

[4.5.6.1 XML Syntax 47](#_Toc482893800)

[4.5.6.2 JSON Syntax 47](#_Toc482893801)

[4.5.6.3 XML Signatures Variant Optional Input IncludeObject 47](#_Toc482893802)

[4.5.7 Optional Input IncludeEContent 48](#_Toc482893803)

[4.5.8 Enveloped Signatures, Optional Input SignaturePlacement and Output DocumentWithSignature 49](#_Toc482893804)

[4.5.8.1 XML Syntax 50](#_Toc482893805)

[4.5.8.2 JSON Syntax 51](#_Toc482893806)

[4.5.9 Optional Input SignedReferences 51](#_Toc482893807)

[4.5.9.1 XML Syntax 53](#_Toc482893808)

[4.5.9.2 JSON Syntax 53](#_Toc482893809)

[4.6 OptionalInputsSignType 53](#_Toc482893810)

[4.6.1.1 XML Syntax 54](#_Toc482893811)

[4.6.1.2 JSON Syntax 54](#_Toc482893812)

[4.7 OptionalOutputsSignType 55](#_Toc482893813)

[4.7.1.1 XML Syntax 55](#_Toc482893814)

[4.7.1.2 JSON Syntax 55](#_Toc482893815)

[5 The DSS Verifying Protocol 57](#_Toc482893816)

[5.1 Element VerifyRequest 57](#_Toc482893817)

[5.1.1 XML Syntax 57](#_Toc482893818)

[5.1.2 JSON Syntax 57](#_Toc482893819)

[5.2 Element VerifyResponse 58](#_Toc482893820)

[5.2.1 JSON Syntax 58](#_Toc482893821)

[5.3 Basic Processing for XML Signatures 58](#_Toc482893822)

[5.3.1 Multi-Signature Verification 59](#_Toc482893823)

[5.3.2 Signature Timestamp verification procedure 60](#_Toc482893824)

[5.3.2.1 Processing for RFC 3161 Timestamp tokens on CMS Signatures. 60](#_Toc482893825)

[5.3.2.2 Processing for XML timestamp tokens on XML signatures 60](#_Toc482893826)

[5.3.2.3 Processing for RFC 3161 timestamp tokens on XML Signatures 61](#_Toc482893827)

[5.4 Basic Processing for CMS Signatures 62](#_Toc482893828)

[5.5 Optional Inputs and Outputs 62](#_Toc482893829)

[5.5.1 Optional Input VerifyManifests and Output VerifyManifestResults 62](#_Toc482893830)

[5.5.1.1 XML Syntax 62](#_Toc482893831)

[5.5.1.2 JSON Syntax 63](#_Toc482893832)

[5.5.2 Optional Input UseVerificationTime 63](#_Toc482893833)

[5.5.2.1 XML Syntax 63](#_Toc482893834)

[5.5.2.2 JSON Syntax 64](#_Toc482893835)

[5.5.3 Optional Input/Output ReturnVerificationTimeInfo / VerificationTimeInfo 64](#_Toc482893836)

[5.5.3.1 XML Syntax 65](#_Toc482893837)

[5.5.3.2 JSON Syntax 65](#_Toc482893838)

[5.5.4 Optional Input AdditionalKeyInfo 66](#_Toc482893839)

[5.5.4.1 XML Syntax 66](#_Toc482893840)

[5.5.4.2 JSON Syntax 66](#_Toc482893841)

[5.5.5 Optional Input ReturnProcessingDetails and Output ProcessingDetails 66](#_Toc482893842)

[5.5.5.1 XML Syntax 67](#_Toc482893843)

[5.5.5.2 JSON Syntax 68](#_Toc482893844)

[5.5.6 Optional Input ReturnSigningTimeInfo and Output SigningTimeInfo 68](#_Toc482893845)

[5.5.6.1 XML Syntax 69](#_Toc482893846)

[5.5.6.2 JSON Syntax 69](#_Toc482893847)

[5.5.7 Optional Input ReturnSignerIdentity and Output SignerIdentity 70](#_Toc482893848)

[5.5.7.1 XML Syntax 70](#_Toc482893849)

[5.5.7.2 JSON Syntax 70](#_Toc482893850)

[5.5.8 Optional Input ReturnUpdatedSignature and Outputs DocumentWithSignature, UpdatedSignature 70](#_Toc482893851)

[5.5.8.1 XML Syntax 71](#_Toc482893852)

[5.5.8.2 JSON Syntax 72](#_Toc482893853)

[5.5.9 Optional Input ReturnTransformedDocument and Output TransformedDocument 72](#_Toc482893854)

[5.5.9.1 XML Syntax 72](#_Toc482893855)

[5.5.9.2 JSON Syntax 73](#_Toc482893856)

[5.5.10 Optional Input ReturnTimestampedSignature and Outputs DocumentWithSignature, TimestampedSignature 73](#_Toc482893857)

[5.5.10.1 XML Syntax 74](#_Toc482893858)

[5.5.10.2 JSON Syntax 74](#_Toc482893859)

[5.6 OptionalInputsVerifyType 74](#_Toc482893860)

[5.6.1.1 XML Syntax 75](#_Toc482893861)

[5.6.1.2 JSON Syntax 75](#_Toc482893862)

[5.7 OptionalOutputsVerifyType 76](#_Toc482893863)

[5.7.1.1 XML Syntax 77](#_Toc482893864)

[5.7.1.2 JSON Syntax 77](#_Toc482893865)

[6 DSS Core Elements 78](#_Toc482893866)

[6.1 Element Timestamp 78](#_Toc482893867)

[6.1.1 XML Timestamp Token 78](#_Toc482893868)

[6.1.2 Element TstInfo 79](#_Toc482893869)

[6.1.2.1 XML Syntax 79](#_Toc482893870)

[6.1.2.2 JSON Syntax 79](#_Toc482893871)

[6.2 Element RequesterIdentity 80](#_Toc482893872)

[6.2.1.1 XML Syntax 80](#_Toc482893873)

[6.2.1.2 JSON Syntax 80](#_Toc482893874)

[7 DSS Core Bindings 81](#_Toc482893875)

[7.1 HTTP POST Transport Binding 81](#_Toc482893876)

[7.2 SOAP 1.2 Transport Binding 81](#_Toc482893877)

[7.2.1 SOAP Attachment Feature and Element <AttachmentReference> 82](#_Toc482893878)

[7.2.1.1 Signing Protocol, Processing for XML Signatures, Process Variant for <AttachmentReference> 82](#_Toc482893879)

[7.2.1.2 Verifying Protocol, Processing for XML Signatures, Process Variant for <AttachmentReference> 83](#_Toc482893880)

[7.2.1.3 Signing Protocol, Basic Processing for CMS Signatures, Process Variant for <AttachmentReference> 83](#_Toc482893881)

[7.2.1.4 Verifying Protocol, Basic Processing for CMS Signatures, Process Variant for <AttachmentReference> 83](#_Toc482893882)

[8 Processing Model 84](#_Toc482893883)

[9 JSON Format 85](#_Toc482893884)

[9.1 JSON – Type Base64DataType 85](#_Toc482893885)

[9.2 JSON – Type AnyType 85](#_Toc482893886)

[9.3 JSON – Type InternationalStringType 86](#_Toc482893887)

[9.4 JSON – Type KeyInfoType 86](#_Toc482893888)

[9.5 JSON – Element InputDocuments 87](#_Toc482893889)

[9.5.1 JSON – Type DocumentBaseType 87](#_Toc482893890)

[10 XML Format 89](#_Toc482893891)

[10.1 XML – Type Base64DataType 89](#_Toc482893892)

[10.2 XML – Type AnyType 89](#_Toc482893893)

[10.3 XML – Type InternationalStringType 90](#_Toc482893894)

[10.4 XML – Type KeyInfoType 90](#_Toc482893895)

[10.5 XML – Element InputDocuments 91](#_Toc482893896)

[10.5.1 XML – Type DocumentBaseType 92](#_Toc482893897)

[10.6 AnElement – REMOVE\_ME\_AFTER\_FIRST\_PASS 93](#_Toc482893898)

[11 DSS-Defined Identifiers 95](#_Toc482893899)

[11.1 Signature Type Identifiers 95](#_Toc482893900)

[11.1.1 XML Signature 95](#_Toc482893901)

[11.1.2 XML TimeStampToken 95](#_Toc482893902)

[11.1.3 RFC 3161 TimeStampToken 95](#_Toc482893903)

[11.1.4 CMS Signature 95](#_Toc482893904)

[11.1.5 PGP Signature 95](#_Toc482893905)

[12 Conformance 96](#_Toc482893906)

[12.1 Conformance as a DSS version 2.0 document 96](#_Toc482893907)

[12.1.1 Conformance for XML format 96](#_Toc482893908)

[12.1.2 Conformance for JSON format 96](#_Toc482893909)

[Appendix A. Acknowledgments 97](#_Toc482893910)

[Appendix B. 98](#_Toc482893911)

[B.1 Use of Exclusive Canonicalization 98](#_Toc482893912)

[B.2 More Complex Response Example 98](#_Toc482893913)

[Appendix C. 99](#_Toc482893914)

[C.1 Element InputDocuments 99](#_Toc482893915)

[C.1.1 XML Syntax 100](#_Toc482893916)

[C.1.2 JSON Syntax 100](#_Toc482893917)

[C.1.3 Type TransformedDataType 101](#_Toc482893918)

[Appendix D. Table of Types, Elements and Attributes 103](#_Toc482893919)

[Appendix E. List of Figures 105](#_Toc482893920)

[Appendix F. Index 106](#_Toc482893921)

[Appendix G. JSON Helpers 107](#_Toc482893922)

[Appendix H. Revision History 108](#_Toc482893923)

# Introduction

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

The specification is split into twelve chapters.

## 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 Schema*. OASIS, 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>.

**[SAMLCore1.1]** E. Maler et al. Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V 1.1. OASIS, November 2002.   
<http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf>

**[SOAP]** M. Gudgin et al. *SOAP Version 1.2 Part 1: Messaging Framework.* W3C Recommendation, June 2003.   
<http://www.w3.org/TR/xmlschema-1/>

**[SOAPAtt]** H. F. Nielsen, H. Ruellan *SOAP 1.2 Attachment Feature,* W3C Working Group Note, 8 June 2004  
<http://www.w3.org/TR/soap12-af/>

**[WS-I-Att]** Ch. Ferris, A. Karmarkar, C. K. Liu *Attachments Profile Version 1.0,* The Web Services-Interoperability Organization (WS-I)*,* 20 April 2006  
<http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html>

**[XML-C14N]** J. Boyer. *Canonical XML Version 1.0*. W3C Recommendation, March 2001.   
<http://www.w3.org/TR/xml-c14n>

**[XML-xcl-c14n]** Exclusive XML Canonicalization Version 1.0. W3C Recommendation 18 July 2002 <http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/>

**[xml:id]** xml:id, Version 1.0, W3C Recommendation, 9 September 2005, http://www.w3.org/TR/xml-id/

**[XML-ns]** T. Bray, D. Hollander, A. Layman. *Namespaces in XML.* W3C Recommendation, January 1999.   
[http://www.w3.org/TR/1999/REC-xml-names-19990114](http://www.w3.org/TR/1999/REC-xml-names-19990114/)

**[XML-NT-Document]** [http://www.w3.org/TR/2004/REC-xml-20040204/#NT-document](http://www.w3.org/TR/2004/REC-xml-20040204/)

**[XML-PROLOG]** Tim Bray, Jean Paoli, C. M. Sperberg-McQueen, et al. *Prolog and Document Type Declaration* in *Extensible Markup Language (XML) 1.0 (Third Edition)*, W3C Recommendation, 04 February 2004, <http://www.w3.org/TR/REC-xml/#sec-prolog-dtd>

**[XMLDSIG]** *D. Eastlake et al. XML-Signature Syntax and Processing. W3C Recommendation, February 2002.*<http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/>

[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.

# Design Considerations

Blurb

## Construction Principles

## Domain Models

### Date and Time Model

The specific concept of date and time used in this document is defined in this section and noted in subsequent usage as**:**

DateTime

« All date time values inside a DSS document MUST adhere to the ISO 8601 [[ISO8601](#refISO8601)] basic or extended Format (as given there in section 4.3.2 “Complete representations” and with the addition of decimal fractions for seconds, similar to ibid. section 4.2.2.4 “Representations with decimal fraction” but with the full stop (.) being the preferred separator for DSS). » [DSS-2.2.1-1].

## Schema Organization and Namespaces

The structures described in this specification are contained in the schema file **[Core2.0-XSD]**. All schema listings in the current document are excerpts from the schema file. In the case of a disagreement between the schema file and this document, the schema file takes precedence.

This schema is associated with the following XML namespace:

urn:oasis:names:tc:dss:2.0:core:schema

If a future version of this specification is needed, it will use a different namespace.

Conventional XML namespace prefixes are used in the schema:

* The prefix dss2: stands for the DSS core namespace **[DSS2XSD]**.
* The prefix ds: stands for the W3C XML Signature namespace **[XMLDSIG]**.
* The prefix xs: stands for the W3C XML Schema namespace **[Schema1]**.
* The prefix saml: stands for the OASIS SAML Schema namespace **[SAMLCore1.1]**.

Applications MAY use different namespace prefixes, and MAY use whatever namespace defaulting/scoping conventions they desire, as long as they are compliant with the Namespaces in XML specification **[XML-ns]**.

The following schema fragment defines the XML namespaces and other header information for the DSS core schema:

<xs:schema xmlns:dss2="urn:oasis:names:tc:dss:2.0:core:schema"

xmlns:ds="http://www.w3.org/2000/09/xmldsig#"

xmlns:xs="http://www.w3.org/2001/XMLSchema"

xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"

targetNamespace="urn:oasis:names:tc:dss:2.0:core:schema"

elementFormDefault="qualified"

attributeFormDefault="unqualified">

<xs:annotation>

<xs:documentation xml:lang="en">This Schema defines the Digital Signature Service Core Protocols, Elements, and Bindings Committee Draft 1 for Public Review</xs:documentation>

</xs:annotation>

<xs:import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>

<xs:import namespace="urn:oasis:names:tc:SAML:1.0:assertion" schemaLocation="http://www.oasis-open.org/committees/download.php/3408/oasis-sstc-saml-schema-protocol-1.1.xsd"/>

<xs:import namespace="http://www.w3.org/XML/1998/namespace" schemaLocation="http://www.w3.org/2001/xml.xsd"/>

## DSS Overview (Non-normative)

This specification describes two request/response protocols:

1. a signing protocol and
2. a verifying protocol.

Through these protocols a client can send documents (or document hashes) to a server and receive back a signature on the documents; or send documents (or document hashes) and a signature to a server, and receive back an answer on whether the signature verifies the documents.

The elements in which the protocols are formulated are provided in a format agnostic language and also in JSON and XML format. Provided are additional mappings from the generic to the specific entities.

These protocol operations could be useful in a variety of contexts – for example, they could allow clients to access a single corporate key for signing press releases, with centralized access control, auditing, and archiving of signature requests. They could also allow clients to create and verify signatures without needing complex client software and configuration.

The signing and verifying protocols are chiefly designed to support the creation and verification of XML signatures **[XMLDSIG]**, XML timestamps (see section 6.1), binary timestamps **[RFC 3161]** and CMS signatures **[RFC 3852]**. These protocols may also be extensible to other types of signatures and timestamps, such as PGP signatures **[RFC 2440]**.

It is expected that the signing and verifying protocols will be *profiled* to meet many different application scenarios. In anticipation of this, these protocols have only a minimal set of required elements, which deal with transferring “input documents” and signatures back and forth between client and server. The input documents to be signed or verified can be transferred in their entirety or the client can hash the documents themselves and only send the hash values to save bandwidth and protect the confidentiality of the document content.

All functionality besides transferring input documents and signatures is relegated to a framework of “optional inputs” and “optional outputs”. This document defines a number of optional inputs and outputs. Profiles of these protocols can pick and choose which optional inputs and outputs to support and can introduce their own optional inputs and outputs when they need functionality not anticipated by this specification.

Examples of optional inputs to the signing protocol include: what type of signature to produce, which key to sign with, who the signature is intended for, and what signed and unsigned properties to place in the signature. Examples of optional inputs to the verifying protocol include: the time for which the client would like to know the signature’s validity status, additional validation data necessary to verify the signature (such as certificates and CRLs), and requests for the server to return information such as the signer’s name or the signing time.

The signing and verifying protocol messages must be transferred over some underlying protocol(s) which provide message transport and security. A *binding* specifies how to use the signing and verifying protocols with some underlying protocol such as HTTP POST or TLS. Section 6 provides an initial set of bindings.

In addition to defining the signing and verifying protocols, this specification defines two elements that are related to these protocols. First, an XML timestamp element is defined in section 5.1. The signing and verifying protocols can be used to create and verify both XML and binary timestamps; a profile for doing so is defined in **[XML-TSP]**. Second, a RequesterIdentity element is defined in section 5.2. This element can be used as a signature property in an XML signature, to give the name of the end-user who requested the signature.

## Version 2.0 motivation [non-normative]

The main changes of this version of the DSS/X core document compared to version 1.0 are:

1. include requirements that became known only after publication of version 1.0
2. simplify the core schema, e.g. by dropping elements seldom used.
3. support other transport formats than SOAP.

To guide the implementation and to ease the use of the protocol with common frameworks the following list of requirements was compiled:

* Focus on Base64 as the most versatile way to transport documents and signatures
* Avoid the use of XML specifics (like e.g. mixed content)
* Avoid xs:any by replacing it with an enumeration of possible types, and if that is not feasible, use base64 blobs as a fallback.
* Define cardinality of OptionalInputs and OptionalOutputs child elements explicitly
* Rearrange sequences and choices to produce a strongly typed object model
* The set of comments and bug reports arrived since version DSS 1.0 became standard were respected.

## Syntax variants

This version of the DSS/X core document handles the representation of requests and response elements according to the JSON and XML syntax. The general semantics of the elements is discussed in the element’s main section. Details of the JSON or XML formats are discussed in specific subsections

* JSON syntax
* XML syntax

# Structure Models

## Structure Models defined in this document

### Component Any

**Semantics**

This element MAY hold a set of base64 encoded arbitrary data. To help the processing of the data it may be qualified by the mime type element.

Below follows a list of the sub-components that MAY be present within this component:

* The Content element MUST occur 1 or more times containing sub-components. [sub component Content details]
* The Base64Content element MUST contain one instance of base64 encoded binary data. [sub component Base64Content details]
* The optional MimeType element MUST contain one instance of a string. This element is denoting the type of the arbitrary data.

Non-normative Comment:

[component Any non normative details]

#### XML Syntax

The XML type AnyType SHALL implement the requirements defined in the Any component.

The AnyType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="AnyType">

<xs:sequence>

<xs:element maxOccurs="unbounded" minOccurs="1" name="Content">

<xs:complexType>

<xs:sequence>

<xs:element name="Base64Content" type="xs:base64Binary"/>

<xs:any maxOccurs="unbounded" minOccurs="0" processContents="lax"/>

</xs:sequence>

<xs:attribute name="MimeType" type="xs:string" use="optional"/>

</xs:complexType>

</xs:element>

</xs:sequence>

</xs:complexType>

Each child element of AnyType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

To provide backward compatibility and convenient processing of XML components the XML schema includes an xs:any element. This XML-specific mechanism should be used with caution as it is not compatible with the data-format-neutral approach of this specification.

#### JSON Syntax

The AnyType JSON object SHALL implement in JSON syntax the requirements defined in the Any component.

The AnyType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-AnyType": {

"type": "object",

"properties": {

"content": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-AnyType:Content"

}

}

},

"required": ["content"]

}

"dss-AnyType:Content": {

"type": "object",

"properties": {

"b64Content": {

"type": "string"

},

"mimeType": {

"type": "string"

}

},

"required": ["b64Content"]

}

Properties in the JSON schema above SHALL implement sub-component of Any component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| Content | content | [] |
| Base64Content | b64Content | [] |
| MimeType | mimeType | [] |

[component Any JSON schema details]

### Component InternationalString

**Semantics**

This element attaches an element to a human-readable string to specify the string’s language.

Below follows a list of the sub-components that MAY be present within this component:

* The value element MUST contain one instance of a string. The human readable string. In non-XML representations the value element contains the textual content.
* The lang element MUST contain one instance of an ISO language descriptor. This element identifies the language of the value element.

Non-normative Comment:

[component InternationalString non normative details]

#### XML Syntax

The XML type InternationalStringType SHALL implement the requirements defined in the InternationalString component.

The InternationalStringType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="InternationalStringType">

<xs:simpleContent>

<xs:extension base="xs:string">

<xs:attribute ref="xml:lang" use="required"/>

</xs:extension>

</xs:simpleContent>

</xs:complexType>

Each child element of InternationalStringType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name. The element 'value' is represented by the component's XML tag text content.

[component InternationalString XML schema details]

#### JSON Syntax

The InternationalStringType JSON object SHALL implement in JSON syntax the requirements defined in the InternationalString component.

The InternationalStringType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-InternationalStringType": {

"type": "object",

"properties": {

"value": {

"type": "string"

},

"lang": {

"type": "string"

}

},

"required": ["lang"]

}

Properties in the JSON schema above SHALL implement sub-component of InternationalString component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| value | value | [] |
| lang | lang | [] |

[component InternationalString JSON schema details]

### Component InputDocuments

**Semantics**

This element is used to send input documents to a DSS server, whether for signing or verifying. An input document can be any piece of data that can be used as input to a signature or timestamp calculation. An input document can even *be* a signature or timestamp (for example, a pre-existing signature can be counter-signed or timestamped). An input document could also be a <ds:Manifest>, allowing the client to handle manifest creation while using the server to create the rest of the signature. Manifest validation is supported by an optional input / output.

Below follows a list of the sub-components that MAY be present within this component:

* The Document element MAY occur zero or more times containing a sub-component. If present each instance MUST satisfy the requirements specified in this document in section Document. [sub component Document details]
* The TransformedData element MAY occur zero or more times containing a sub-component. If present each instance MUST satisfy the requirements specified in this document in section TransformedData. It contains the binary output of a chain of transforms applied by a client.
* The DocumentHash element MAY occur zero or more times containing a sub-component. If present each instance MUST satisfy the requirements specified in this document in section DocumentHash. It contains a set of digest algorithm and the corresponding hashes. Required transformation steps

Non-normative Comment:

[component InputDocuments non normative details]

#### XML Syntax

The XML type InputDocumentsType SHALL implement the requirements defined in the InputDocuments component.

The InputDocumentsType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="InputDocumentsType">

<xs:choice>

<xs:sequence maxOccurs="unbounded">

<xs:element name="Document" type="dss:DocumentType"/>

</xs:sequence>

<xs:sequence maxOccurs="unbounded">

<xs:element name="TransformedData" type="dss:TransformedDataType"/>

</xs:sequence>

<xs:sequence maxOccurs="unbounded">

<xs:element name="DocumentHash" type="dss:DocumentHashType"/>

</xs:sequence>

</xs:choice>

</xs:complexType>

Each child element of InputDocumentsType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component InputDocuments XML schema details]

#### JSON Syntax

The InputDocumentsType JSON object SHALL implement in JSON syntax the requirements defined in the InputDocuments component.

The InputDocumentsType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-InputDocumentsType": {

"type": "object",

"properties": {

"doc": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-DocumentType"

}

},

"transformed": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-TransformedDataType"

}

},

"docHash": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-DocumentHashType"

}

}

}

}

Properties in the JSON schema above SHALL implement sub-component of InputDocuments component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| Document | doc | [] |
| TransformedData | transformed | [] |
| DocumentHash | docHash | [] |

[component InputDocuments JSON schema details]

### Component DocumentBase

**Semantics**

The DocumentBaseType inherits its elements to the components DocumentType, TransformedDataType and DocumentHashType. The DocumentBaseType contains the basic information shared by the inheriting components and remaining persistent during the process from input document retrieval until digest calculation for the relevant document.

Below follows a list of the sub-components that MAY be present within this component:

* The optional ID element MUST contain one instance of a unique identifier. This identifier gives the input document a unique label within a particular request message. Through this identifier, an optional input can refer to a single input document. Using this identifier and the IDREF element it is possible to avoid redundant content.
* The optional RefURI element MUST contain one instance of an URI. This specifies the value for a <ds:Reference> element’s URI attribute when referring to this input document. The RefURI element SHOULD be specified. Not more than one RefURI element may be omitted in a single signing request.
* The optional RefType element MUST contain one instance of an URI. This specifies the value for a <ds:Reference> element’s Type attribute when referring to this input document.
* The optional SchemaRefs element MUST contain one instance of a unique identifier reference. The identified schemas are to be used to process the ID attributes during parsing and for XPath evaluation. If anything else but Schema are referred to, the server MUST report an error. If a referred to Schema is not used by the XML document instance this MAY be ignored or reported to the client in the Result subcomponent ResultMessage (for the definition of Schema subcomponent see the specification in section 3.1.20). The Document is assumed to be valid against the first Schema referred to by SchemaRefs. If a Schemas element is referred to first by SchemaRefs the document is assumed to be valid against the first Schema inside SchemaRefs. In both cases, the remaining schemas may occur in any order and are used either directly or indirectly by the first schema. If present, the server MUST use the schemas to identify the ID attributes and MAY also perform complete validation against the schemas.

Non-normative Comment:

It is recommended to use xml:id as defined in [xml:id] as id in the payload being referenced by a <ds:Reference>, because the schema then does not have to be supplied for identifying the ID attributes.

#### XML Syntax

The XML type DocumentBaseType SHALL implement the requirements defined in the DocumentBase component.

The DocumentBaseType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType abstract="true" name="DocumentBaseType">

<xs:attribute name="ID" type="xs:ID" use="optional"/>

<xs:attribute name="RefURI" type="xs:anyURI" use="optional"/>

<xs:attribute name="RefType" type="xs:anyURI" use="optional"/>

<xs:attribute name="SchemaRefs" type="xs:IDREFS" use="optional"/>

</xs:complexType>

Each child element of DocumentBaseType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component DocumentBase XML schema details]

#### JSON Syntax

The DocumentBaseType JSON object SHALL implement in JSON syntax the requirements defined in the DocumentBase component.

The DocumentBaseType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-DocumentBaseType": {

"type": "object",

"properties": {

"ID": {

"type": "string"

},

"refURI": {

"type": "string"

},

"refType": {

"type": "string"

},

"schemaRefs": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-DocumentType"

}

}

}

}

Properties in the JSON schema above SHALL implement sub-component of DocumentBase component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| ID | ID | [] |
| RefURI | refURI | [] |
| RefType | refType | [] |
| SchemaRefs | schemaRefs | [] |

[component DocumentBase JSON schema details]

### Component Document

**Semantics**

[component Document normative details]

Below follows a list of the sub-components that MAY be present within this component:

* The Base64Data element MUST contain one instance of a sub-component. This element MUST satisfy the requirements specified in this document in section Base64Data. [sub component Base64Data details]

A set of sub-components is inherited from component DocumentBase and is not repeated here.

Non-normative Comment:

[component Document non normative details]

#### XML Syntax

The XML type DocumentType SHALL implement the requirements defined in the Document component.

The DocumentType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="DocumentType">

<xs:complexContent>

<xs:extension base="dss:DocumentBaseType">

<xs:choice>

<xs:element name="Base64Data" type="dss:Base64DataType"/>

</xs:choice>

</xs:extension>

</xs:complexContent>

</xs:complexType>

Each child element of DocumentType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component Document XML schema details]

#### JSON Syntax

The DocumentType JSON object SHALL implement in JSON syntax the requirements defined in the Document component.

The DocumentType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-DocumentType": {

"type": "object",

"properties": {

"ID": {

"type": "string"

},

"refURI": {

"type": "string"

},

"refType": {

"type": "string"

},

"schemaRefs": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-DocumentType"

}

},

"b64Data": {

"type": "object",

"$ref": "#/definitions/dss-Base64DataType"

}

}

}

Properties in the JSON schema above SHALL implement sub-component of Document component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| ID | ID | [] |
| RefURI | refURI | [] |
| RefType | refType | [] |
| SchemaRefs | schemaRefs | [] |
| Base64Data | b64Data | [] |

[component Document JSON schema details]

### Component Base64Data

**Semantics**

The Base64Data component is a generic holder for arbitrary data. In addition to the data itself it also contains additional elements to qualify the MimeType of the data. It also offers a Id / Reference pair to implement a deduplication strategy, useful especially for bigger data blobs. The value element or the XML tag’s content MAY be empty. If it is empty, the AttRefURI element MAY point to the components content transferred in an attachment

Below follows a list of the sub-components that MAY be present within this component:

* The value element MUST contain one instance of base64 encoded binary data. In non-XML representations the value element contains the actual content.
* The optional MimeType element MUST contain one instance of a string. This element is denoting the type of the arbitrary data in the value element or the referenced attachment.
* The optional AttRefURI element MUST contain one instance of an URI. In the case of attachment identified by the AttRefURI element the server retrieves the MIME type from the MimeType element (if present) otherwise from the content-type MIME header of the attachment referred by AttRefURI. If the MimeType element diverges from the attachment's MIME header content-type, an implementation MAY either ignore the MIME header's content-type or issue a RequesterError qualified by a GeneralError and an appropriate message containing the AttRefURI.
* The optional ID element MUST contain one instance of a unique identifier. This identifier gives the binary data a unique label within a particular message. Using this identifier and the IDREF element it is possible to avoid redundant content.
* The optional IDREF element MUST contain one instance of a unique identifier reference. This element identifies another binary data element within a particular message.

Non-normative Comment:

There are different standards defined for handling and referencing an attachment. Maybe there will be more to come. Therefore the attachment reference mechanism is somehow generic here.

#### XML Syntax

The XML type Base64DataType SHALL implement the requirements defined in the Base64Data component.

The Base64DataType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="Base64DataType">

<xs:simpleContent>

<xs:extension base="xs:base64Binary">

<xs:attribute name="MimeType" type="xs:string" use="optional"/>

<xs:attribute name="AttRefURI" type="xs:anyURI" use="optional"/>

<xs:attribute name="ID" type="xs:ID" use="optional"/>

<xs:attribute name="IDREF" type="xs:IDREF" use="optional"/>

</xs:extension>

</xs:simpleContent>

</xs:complexType>

Each child element of Base64DataType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name. The element 'value' holding the base64 content is represented by the component's XML tag text content.

[component Base64Data XML schema details]

#### JSON Syntax

The Base64DataType JSON object SHALL implement in JSON syntax the requirements defined in the Base64Data component.

The Base64DataType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-Base64DataType": {

"type": "object",

"properties": {

"ID": {

"type": "string"

},

"value": {

"type": "string"

},

"mimeType": {

"type": "string"

},

"attRef": {

"type": "string"

},

"IDREF": {

"type": "string"

}

}

}

Properties in the JSON schema above SHALL implement sub-component of Base64Data component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| value | value | [] |
| MimeType | mimeType | [] |
| AttRefURI | attRef | [] |
| ID | ID | [] |
| IDREF | IDREF | [] |

[component Base64Data JSON schema details]

### Component TransformedData

**Semantics**

[component TransformedData normative details]

Below follows a list of the sub-components that MAY be present within this component:

* The optional Transforms element MUST contain a sub-component. A given element MUST satisfy the requirements specified in section Transforms. This is the sequence of transforms applied by the client. It specifies the value for a <ds:Reference> element’s <ds:Transforms> child element. In other words, this specifies transforms that the client has already applied to the input document before the server will hash it. This component is required on a SignRequest, optional on a VerifyRequest.
* The Base64Data element MUST contain one instance of a sub-component. This element MUST satisfy the requirements specified in this document in section Base64Data. This element gives the binary output of a sequence of transforms to be hashed at the server side.
* The optional WhichReference element MUST contain one instance of an integer. As there may be multiple TransformedDataType / DocumentHashType components of the same document having the same URI [RFC 2396] and RefType on a SignRequest or VerifyRequest - their correspondance to an already existing <ds:Reference> however needs to be established on a VerifyRequest only. There is a need to disambiguate such cases. This element hence offers a way to clearly identify the <ds:Reference> when URI and RefType match multiple components. The corresponding <ds:Reference> is indicated by this zero-based WhichReference element (0 means the first <ds:Reference> in the signature, 1 means the second, and so on).As there may be multiple TransformedDataType / DocumentHashType components of the same document having the same URI [RFC 2396] and RefType on a SignRequest or VerifyRequest - their correspondance to an already existing <ds:Reference> however needs to be established on a VerifyRequest only. There is a need to disambiguate such cases. This element hence offers a way to clearly identify the <ds:Reference> when URI and RefType match multiple components. The corresponding <ds:Reference> is indicated by this zero-based WhichReference element (0 means the first <ds:Reference> in the signature, 1 means the second, and so on).As there may be multiple TransformedDataType / DocumentHashType components of the same document having the same URI [RFC 2396] and RefType on a SignRequest or VerifyRequest - their correspondance to an already existing <ds:Reference> however needs to be established on a VerifyRequest only. There is a need to disambiguate such cases. This element hence offers a way to clearly identify the <ds:Reference> when URI and RefType match multiple components. The corresponding <ds:Reference> is indicated by this zero-based WhichReference element (0 means the first <ds:Reference> in the signature, 1 means the second, and so on).As there may be multiple TransformedDataType / DocumentHashType components of the same document having the same URI [RFC 2396] and RefType on a SignRequest or VerifyRequest - their correspondance to an already existing <ds:Reference> however needs to be established on a VerifyRequest only. There is a need to disambiguate such cases. This element hence offers a way to clearly identify the <ds:Reference> when URI and RefType match multiple components. The corresponding <ds:Reference> is indicated by this zero-based WhichReference element (0 means the first <ds:Reference> in the signature, 1 means the second, and so on). This component is ignored on a SignRequest, optional on a VerifyRequest.

A set of sub-components is inherited from component DocumentBase and is not repeated here.

Non-normative Comment:

It may be possible to establish the <ds:References> / TransformedDataType / DocumentHashType correspondence by comparing the optionally supplied chain of transforms to those of the <ds:References> having the same URI and RefType in the supplied <ds:Signature> if this chain of transform has been supplied. This can be quite expensive and even outnumber the advantages of TransformedDataType / DocumentHashType.

#### XML Syntax

The XML type TransformedDataType SHALL implement the requirements defined in the TransformedData component.

The TransformedDataType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="TransformedDataType">

<xs:complexContent>

<xs:extension base="dss:DocumentBaseType">

<xs:sequence>

<xs:element minOccurs="0" name="Transforms" type="ds:TransformsType"/>

<xs:element name="Base64Data" type="dss:Base64DataType"/>

</xs:sequence>

<xs:attribute name="WhichReference" type="xs:integer" use="optional"/>

</xs:extension>

</xs:complexContent>

</xs:complexType>

Each child element of TransformedDataType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component TransformedData XML schema details]

#### JSON Syntax

The TransformedDataType JSON object SHALL implement in JSON syntax the requirements defined in the TransformedData component.

The TransformedDataType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-TransformedDataType": {

"type": "object",

"properties": {

"ID": {

"type": "string"

},

"refURI": {

"type": "string"

},

"refType": {

"type": "string"

},

"schemaRefs": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-DocumentType"

}

},

"transforms": {

"type": "object",

"$ref": "#/definitions/dsig-TransformsType"

},

"b64Data": {

"type": "object",

"$ref": "#/definitions/dss-Base64DataType"

},

"whichRef": {

"type": "integer"

}

},

"required": ["b64Data"]

}

Properties in the JSON schema above SHALL implement sub-component of TransformedData component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| ID | ID | [] |
| RefURI | refURI | [] |
| RefType | refType | [] |
| SchemaRefs | schemaRefs | [] |
| Transforms | transforms | [] |
| Base64Data | b64Data | [] |
| WhichReference | whichRef | [] |

[component TransformedData JSON schema details]

### Component DocumentHash

**Semantics**

[component DocumentHash normative details]

Below follows a list of the sub-components that MAY be present within this component:

* The optional Transforms element MUST contain a sub-component. A given element MUST satisfy the requirements specified in section Transforms. It specifies the value for a <ds:Reference> element’s <ds:Transforms> child element when referring to this document hash. In other words, this specifies transforms that the client has already applied to the input document before hashing it. This component is required on a SignRequest, optional on a VerifyRequest. This component is required on a SignRequest, optional on a VerifyRequest.
* The DigestInfos element MUST occur 1 or more times containing a sub-component. Each instance MUST satisfy the requirements specified in this document in section DigestInfo. This element MAY contain more than one DigestInfo sub-component to represent the digest values calculated with different digest algorithms. This may be useful when a requestor doesn’t know upfront which digest algorithms are supported / accepted by the server for signing. In the case of a verification request the client may not be able to parse the signature and instead calculate the digest for a comprehensive set of digest algorithms.
* The optional WhichReference element MUST contain one instance of an integer. As there may be multiple TransformedDataType / DocumentHashType components of the same document having the same URI [RFC 2396] and RefType on a SignRequest or VerifyRequest - their correspondence to an already existing <ds:Reference> however needs to be established on a VerifyRequest only. There is a need to disambiguate such cases. This element hence offers a way to clearly identify the <ds:Reference> when URI and RefType match multiple components. The corresponding <ds:Reference> is indicated by this zero-based WhichReference element (0 means the first <ds:Reference> in the signature, 1 means the second, and so on).

A set of sub-components is inherited from component DocumentBase and is not repeated here.

Non-normative Comment:

[component DocumentHash non normative details]

#### XML Syntax

The XML type DocumentHashType SHALL implement the requirements defined in the DocumentHash component.

The DocumentHashType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="DocumentHashType">

<xs:complexContent>

<xs:extension base="dss:DocumentBaseType">

<xs:sequence>

<xs:element minOccurs="0" name="Transforms" type="ds:TransformsType"/>

<xs:element maxOccurs="unbounded" minOccurs="1" name="DigestInfos" type="dss:DigestInfoType"/>

</xs:sequence>

<xs:attribute name="WhichReference" type="xs:integer" use="optional"/>

</xs:extension>

</xs:complexContent>

</xs:complexType>

Each child element of DocumentHashType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component DocumentHash XML schema details]

#### JSON Syntax

The DocumentHashType JSON object SHALL implement in JSON syntax the requirements defined in the DocumentHash component.

The DocumentHashType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-DocumentHashType": {

"type": "object",

"properties": {

"ID": {

"type": "string"

},

"refURI": {

"type": "string"

},

"refType": {

"type": "string"

},

"schemaRefs": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-DocumentType"

}

},

"transforms": {

"type": "object",

"$ref": "#/definitions/dsig-TransformsType"

},

"di": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-DigestInfoType"

}

},

"whichRef": {

"type": "integer"

}

},

"required": ["di"]

}

Properties in the JSON schema above SHALL implement sub-component of DocumentHash component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| ID | ID | [] |
| RefURI | refURI | [] |
| RefType | refType | [] |
| SchemaRefs | schemaRefs | [] |
| Transforms | transforms | [] |
| DigestInfos | di | [] |
| WhichReference | whichRef | [] |

[component DocumentHash JSON schema details]

### Component DigestInfo

**Semantics**

The DigestInfo component holds a digest value and an identification of the used digest algorithm. The DigestMethod isn’t strongly typed intentionally to support a broad variety of identifiers.

Below follows a list of the sub-components that MAY be present within this component:

* The DigestMethod element MUST contain one instance of a string. The string describes the digest algorithm in an appropriate way for the server side processing. Depending on the signature format this may be an OID (e.g. ‘2.16.840.1.101.3.4.2.1’), an URI (e.g. ‘http://www.w3.org/2001/04/xmlenc#sha256’) or a descriptive string (‘SHA-256’).
* The DigestValue element MUST contain one instance of base64 encoded binary data. [sub component DigestValue details]

Non-normative Comment:

[component DigestInfo non normative details]

#### XML Syntax

The XML type DigestInfoType SHALL implement the requirements defined in the DigestInfo component.

The DigestInfoType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="DigestInfoType">

<xs:sequence>

<xs:element name="DigestMethod" type="xs:string"/>

<xs:element name="DigestValue" type="xs:base64Binary"/>

</xs:sequence>

</xs:complexType>

Each child element of DigestInfoType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component DigestInfo XML schema details]

#### JSON Syntax

The DigestInfoType JSON object SHALL implement in JSON syntax the requirements defined in the DigestInfo component.

The DigestInfoType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-DigestInfoType": {

"type": "object",

"properties": {

"alg": {

"type": "string"

},

"value": {

"type": "string"

}

},

"required": ["alg", "value"]

}

Properties in the JSON schema above SHALL implement sub-component of DigestInfo component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| DigestMethod | alg | [] |
| DigestValue | value | [] |

[component DigestInfo JSON schema details]

### Component SignatureObject

**Semantics**

The SignatureObject component contains a signature or timestamp of some sort. This element is returned in a sign response message, and sent in a verify request message.

Below follows a list of the sub-components that MAY be present within this component:

* The Base64Signature element MUST contain one instance of a sub-component. This element MUST satisfy the requirements specified in this document in section Base64Data. A base64 encoding of some arbitrary signature, such as a XML signature [XMLDSIG], PGP [RFC 2440] or CMS [RFC 3852] signature. The type of signature is specified by the MimeType element of the Base64DataType component.
* The SignaturePtr element MUST contain one instance of a sub-component. This element MUST satisfy the requirements specified in this document in section SignaturePtr. This element is used to point to an XML signature in an input (for a verify request) or output (for a sign response) document in which a signature is enveloped.
* The optional SchemaRefs element MUST contain one instance of a unique identifier reference. The identified schemas are to be used to process the ID attributes during parsing and for XPath evaluation. If anything else but <Schema> are referred to, the server MUST report an error. If a referred to <Schema> is not used by the XML document instance this MAY be ignored or reported to the client in the 3.1.12 subcomponent ResultMessage (for the definition of Schema subcomponent see the specification of 3.1.20)

Non-normative Comment:

[component SignatureObject non normative details]

#### XML Syntax

The XML type SignatureObjectType SHALL implement the requirements defined in the SignatureObject component.

The SignatureObjectType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="SignatureObjectType">

<xs:sequence>

<xs:choice>

<xs:element name="Base64Signature" type="dss:Base64DataType"/>

<xs:element name="SignaturePtr" type="dss:SignaturePtrType"/>

</xs:choice>

</xs:sequence>

<xs:attribute name="SchemaRefs" type="xs:IDREFS" use="optional"/>

</xs:complexType>

Each child element of SignatureObjectType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component SignatureObject XML schema details]

#### JSON Syntax

The SignatureObjectType JSON object SHALL implement in JSON syntax the requirements defined in the SignatureObject component.

The SignatureObjectType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-SignatureObjectType": {

"type": "object",

"properties": {

"b64Sig": {

"type": "object",

"$ref": "#/definitions/dss-Base64DataType"

},

"sigPtr": {

"type": "object",

"$ref": "#/definitions/dss-SignaturePtrType"

},

"schemaRefs": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-DocumentBaseType"

}

}

}

}

Properties in the JSON schema above SHALL implement sub-component of SignatureObject component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| Base64Signature | b64Sig | [] |
| SignaturePtr | sigPtr | [] |
| SchemaRefs | schemaRefs | [] |

[component SignatureObject JSON schema details]

### Component SignaturePtr

**Semantics**

[component SignaturePtr normative details]

Below follows a list of the sub-components that MAY be present within this component:

* The optional NsURIMapping element MAY occur zero or more times containing a sub-component. If present each instance MUST satisfy the requirements specified in section NsURIMapping. The NsURIMapping element allows the definition of additional namespace prefix to URI mappings required for the evaluation of the XPath expressions.
* The WhichDocument element MUST contain one instance of a unique identifier reference. This element identifies the input document being pointed at.
* The optional XPath element MUST contain one instance of a string. This element identifies the signature element being pointed at within the selected document. The XPath expression is evaluated from the root node (see section 5.1 of [XPATH]) of the document identified by WhichDocument. The context node for the XPath evaluation is the document’s DocumentElement (see section 2.1 Well-Formed XML Documents [XML]). Regarding namespace declarations for the expression necessary for evaluation see section 1 of [XPATH].

Non-normative Comment:

[component SignaturePtr non normative details]

#### XML Syntax

The XML type SignaturePtrType SHALL implement the requirements defined in the SignaturePtr component.

The SignaturePtrType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="SignaturePtrType">

<xs:sequence>

<xs:element maxOccurs="unbounded" minOccurs="0" name="NsURIMapping" type="ds:NsURIMappingType"/>

</xs:sequence>

<xs:attribute name="WhichDocument" type="xs:IDREF" use="required"/>

<xs:attribute name="XPath" type="xs:string" use="optional"/>

</xs:complexType>

Each child element of SignaturePtrType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component SignaturePtr XML schema details]

#### JSON Syntax

The SignaturePtrType JSON object SHALL implement in JSON syntax the requirements defined in the SignaturePtr component.

The SignaturePtrType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-SignaturePtrType": {

"type": "object",

"properties": {

"nsDecl": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dsig-NsURIMappingType"

}

},

"whichDoc": {

"type": "object",

"$ref": "#/definitions/dss-DocumentBaseType"

},

"xPath": {

"type": "string"

}

},

"required": ["whichDoc"]

}

Properties in the JSON schema above SHALL implement sub-component of SignaturePtr component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| NsURIMapping | nsDecl | . |
| WhichDocument | whichDoc | [] |
| XPath | xPath | [] |

[component SignaturePtr JSON schema details]

### Component Result

**Semantics**

The Result element is returned with every response message.

Below follows a list of the sub-components that MAY be present within this component:

* The ResultMajor element MUST contain one instance of an URI. Its value is limited to item of the following set:  
  urn:oasis:names:tc:dss:1.0:resultmajor:Success  
  urn:oasis:names:tc:dss:1.0:resultmajor:RequesterError  
  urn:oasis:names:tc:dss:1.0:resultmajor:ResponderError  
  urn:oasis:names:tc:dss:1.0:resultmajor:InsufficientInformation  
  The ResultMajor element describes the most significant component of the result code.
* The optional ResultMinor element MUST contain an URI.
* The optional ResultMessage element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section InternationalString. It represents a message which MAY be returned to an operator, logged, used for debugging, etc.

Non-normative Comment:

[component Result non normative details]

#### XML Syntax

The XML type ResultType SHALL implement the requirements defined in the Result component.

The ResultType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="ResultType">

<xs:sequence>

<xs:element name="ResultMajor">

<xs:simpleType>

<xs:restriction base="xs:anyURI">

<xs:enumeration value="urn:oasis:names:tc:dss:1.0:resultmajor:Success"/>

<xs:enumeration value="urn:oasis:names:tc:dss:1.0:resultmajor:RequesterError"/>

<xs:enumeration value="urn:oasis:names:tc:dss:1.0:resultmajor:ResponderError"/>

<xs:enumeration value="urn:oasis:names:tc:dss:1.0:resultmajor:InsufficientInformation"/>

</xs:restriction>

</xs:simpleType>

</xs:element>

<xs:element minOccurs="0" name="ResultMinor" type="xs:anyURI"/>

<xs:element minOccurs="0" name="ResultMessage" type="dss:InternationalStringType"/>

</xs:sequence>

</xs:complexType>

Each child element of ResultType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component Result XML schema details]

#### JSON Syntax

The ResultType JSON object SHALL implement in JSON syntax the requirements defined in the Result component.

The ResultType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-ResultType": {

"type": "object",

"properties": {

"maj": {

"type": "string",

"enum": ["urn:oasis:names:tc:dss:1.0:resultmajor:Success", "urn:oasis:names:tc:dss:1.0:resultmajor:RequesterError", "urn:oasis:names:tc:dss:1.0:resultmajor:ResponderError", "urn:oasis:names:tc:dss:1.0:resultmajor:InsufficientInformation"]

},

"min": {

"type": "string"

},

"msg": {

"type": "object",

"$ref": "#/definitions/dss-InternationalStringType"

}

},

"required": ["maj"]

}

Properties in the JSON schema above SHALL implement sub-component of Result component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| ResultMajor | maj | [] |
| ResultMinor | min | [] |
| ResultMessage | msg | [] |

[component Result JSON schema details]

### Component OptionalInputsBase

**Semantics**

The OptionalInputsBase contains a common set of additional inputs associated with the processing of the request. Profiles will specify the allowed optional inputs and their default values. If a server doesn’t recognize or can’t handle any optional input, it MUST reject the request with a ResultMajor code of RequesterError and a ResultMinor code of NotSupported.

Below follows a list of the sub-components that MAY be present within this component:

* The optional ServicePolicy element MAY occur zero or more times containing an URI. This element allows the client to define a set of policies under which the server MUST perform the requested operation. The policy may include information on the characteristics of the server that are not covered by the Profile element. The ServicePolicy element may be used to select a specific policy if a service supports multiple policies for a specific profile, or as a sanity-check to make sure the server implements the policy the client expects.
* The optional ClaimedIdentity element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section ClaimedIdentity. [sub component ClaimedIdentity details]
* The optional Language element MUST contain an ISO language descriptor. The Language element indicates which language the client would like to receive InternationalString values in. The server should return appropriately localized strings, if possible.
* The optional Schemas element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section Schemas. The Schemas element provides a mechanism for transporting XML schemas required for validating an XML document along with the request message.
* The optional AddTimestamp element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section UpdateSignatureInstruction. The AddTimestamp element indicates that the client wishes the server to embed a timestamp token as a property or attribute of the resultant or the supplied signature. The timestamp token will be applied to the signature value in the case of CMS/PKCS7 signatures or the <ds:SignatureValue> element in the case of XML signatures. Note: Procedures for handling other forms of timestamp may be defined in profiles of the Core. In particular, the DSS AdES profile **[DSS-AdES-P]** defines procedures for generating timestamps over the content which is about to be signed (sometimes called content timestamps), and the DSS Timestamp profile **[DSS-TS-P]** defines procedures for handling standalone timestamps.
* The optional Other element MAY occur zero or more times containing a sub-component. If present each instance MUST satisfy the requirements specified in this document in section Property. [sub component Other details]

Non-normative Comment:

[component OptionalInputsBase non normative details]

#### XML Syntax

The XML type OptionalInputsBaseType SHALL implement the requirements defined in the OptionalInputsBase component.

The OptionalInputsBaseType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType abstract="true" name="OptionalInputsBaseType">

<xs:sequence>

<xs:choice>

<xs:element maxOccurs="unbounded" minOccurs="0" name="ServicePolicy" type="xs:anyURI"/>

<xs:element maxOccurs="1" minOccurs="0" name="ClaimedIdentity" type="dss:ClaimedIdentityType"/>

<xs:element maxOccurs="1" minOccurs="0" name="Language" type="xs:language"/>

<xs:element maxOccurs="1" minOccurs="0" name="Schemas" type="dss:SchemasType"/>

<xs:element maxOccurs="1" minOccurs="0" name="AddTimestamp" type="dss:UpdateSignatureInstructionType"/>

<xs:element maxOccurs="unbounded" minOccurs="0" name="Other" type="dss:PropertyType"/>

</xs:choice>

</xs:sequence>

</xs:complexType>

Each child element of OptionalInputsBaseType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component OptionalInputsBase XML schema details]

#### JSON Syntax

The component OptionalInputsBase is abstract and therefore has no JSON definition.

[component OptionalInputsBase JSON schema details]

### Component OptionalInputsSign

**Semantics**

The OptionalInputsSign component defines a set of additional inputs associated with the processing of a signing request.

Below follows a list of the sub-components that MAY be present within this component:

* The optional SignatureType element MUST contain an URI. The SignatureType element indicates the type of signature or timestamp to produce (such as a XML signature, a XML timestamp, a RFC 3161 timestamp, a CMS signature, etc.). See section 7.1 for some URI references that MAY be used as the value of this element.
* The optional IntendedAudience element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section IntendedAudience. [sub component IntendedAudience details]
* The optional KeySelector element MAY occur zero or more times containing a sub-component. If present each instance MUST satisfy the requirements specified in this document in section KeySelector. The KeySelector provides details which key or sets of keys the client is expecting to be used.
* The optional Properties element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section PropertiesHolder. The Properties element is used to instruct the server to add certain signed or unsigned properties (aka “signature attributes”) into the signature. The client MAY send the server a particular value to use for each property, or leave the value up to the server to determine. The server MAY add additional properties, even if these aren’t requested by the client.
* The optional IncludeObject element MAY occur zero or more times containing a sub-component. If present each instance MUST satisfy the requirements specified in this document in section IncludeObject. The IncludeObject element is used to request the creation of an XMLSig enveloping signature.
* The optional IncludeEContent element MUST contain a boolean. Its default value is 'false'. If the value of the IncludeEContent is ‘true’ a CMS signature includes enveloped (or ‘encapsulated’) content.
* The optional SignaturePlacement element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section SignaturePlacement. The SignaturePlacement element is used to request the creation of an XMLSig enveloped signature placed within a document. The resulting document with the enveloped signature is placed in the optional output DocumentWithSignature.
* The optional SignedReferences element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section SignedReferences. The SignedReferences element gives the client greater control over how the <ds:Reference> elements of a XMLSig signature are formed.
* The optional Nonce element MUST contain an integer. The Nonce element MAY be used to provide a large random number to enable the client correlate a timestamp request with the response.
* The optional SignatureAlgorithm element MUST contain a string. The SignatureAlgorithm element MAY be used to request a specific signing algorithm.
* The optional SignatureActivationData element MUST contain a string. The SignatureActivationData element is used by the client to supply activation data.

A set of sub-components is inherited from component OptionalInputsBase and is not repeated here.

Non-normative Comment:

[component OptionalInputsSign non normative details]

#### XML Syntax

The XML type OptionalInputsSignType SHALL implement the requirements defined in the OptionalInputsSign component.

The OptionalInputsSignType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="OptionalInputsSignType">

<xs:complexContent>

<xs:extension base="dss:OptionalInputsBaseType">

<xs:sequence>

<xs:choice>

<xs:element maxOccurs="1" minOccurs="0" name="SignatureType" type="xs:anyURI"/>

<xs:element maxOccurs="1" minOccurs="0" name="IntendedAudience" type="dss:IntendedAudienceType"/>

<xs:element maxOccurs="unbounded" minOccurs="0" name="KeySelector" type="dss:KeySelectorType"/>

<xs:element maxOccurs="1" minOccurs="0" name="Properties" type="dss:PropertiesHolderType"/>

<xs:element maxOccurs="unbounded" minOccurs="0" name="IncludeObject" type="dss:IncludeObjectType"/>

<xs:element default="false" maxOccurs="1" minOccurs="0" name="IncludeEContent" type="xs:boolean"/>

<xs:element maxOccurs="1" minOccurs="0" name="SignaturePlacement" type="dss:SignaturePlacementType"/>

<xs:element maxOccurs="1" minOccurs="0" name="SignedReferences" type="dss:SignedReferencesType"/>

<xs:element maxOccurs="1" minOccurs="0" name="Nonce" type="xs:integer"/>

<xs:element maxOccurs="1" minOccurs="0" name="SignatureAlgorithm" type="xs:string"/>

<xs:element maxOccurs="1" minOccurs="0" name="SignatureActivationData" type="xs:string"/>

</xs:choice>

</xs:sequence>

</xs:extension>

</xs:complexContent>

</xs:complexType>

Each child element of OptionalInputsSignType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component OptionalInputsSign XML schema details]

#### JSON Syntax

The OptionalInputsSignType JSON object SHALL implement in JSON syntax the requirements defined in the OptionalInputsSign component.

The OptionalInputsSignType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-OptionalInputsSignType": {

"type": "object",

"properties": {

"policy": {

"type": "array",

"items": {

"type": "string"

}

},

"claimedIdentity": {

"type": "object",

"$ref": "#/definitions/dss-ClaimedIdentityType"

},

"lang": {

"type": "string"

},

"schemas": {

"type": "object",

"$ref": "#/definitions/dss-SchemasType"

},

"addTimestamp": {

"type": "object",

"$ref": "#/definitions/dss-UpdateSignatureInstructionType"

},

"other": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-PropertyType"

}

},

"sigType": {

"type": "string"

},

"aud": {

"type": "object",

"$ref": "#/definitions/dss-IntendedAudienceType"

},

"keySel": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-KeySelectorType"

}

},

"props": {

"type": "object",

"$ref": "#/definitions/dss-PropertiesHolderType"

},

"incObj": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-IncludeObjectType"

}

},

"incContent": {

"type": "boolean",

"default": "false"

},

"sigPlacement": {

"type": "object",

"$ref": "#/definitions/dss-SignaturePlacementType"

},

"sigRefs": {

"type": "object",

"$ref": "#/definitions/dss-SignedReferencesType"

},

"nonce": {

"type": "integer"

},

"sigAlgo": {

"type": "string"

},

"sad": {

"type": "string"

}

}

}

Properties in the JSON schema above SHALL implement sub-component of OptionalInputsSign component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| ServicePolicy | policy | [] |
| ClaimedIdentity | claimedIdentity | [] |
| Language | lang | [] |
| Schemas | schemas | [] |
| AddTimestamp | addTimestamp | [] |
| Other | other | [] |
| SignatureType | sigType | [] |
| IntendedAudience | aud | [] |
| KeySelector | keySel | [] |
| Properties | props | [] |
| IncludeObject | incObj | [] |
| IncludeEContent | incContent | [] |
| SignaturePlacement | sigPlacement | [] |
| SignedReferences | sigRefs | [] |
| Nonce | nonce | [] |
| SignatureAlgorithm | sigAlgo | [] |
| SignatureActivationData | sad | [] |

[component OptionalInputsSign JSON schema details]

### Component OptionalInputsVerify

**Semantics**

The OptionalInputsVerify component defines a set of additional inputs associated with the processing of a verification request.

Below follows a list of the sub-components that MAY be present within this component:

* The optional UseVerificationTime element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section UseVerificationTime. The UseVerificationTime element instructs the server to attempt to determine the signature’s validity at the specified time, instead of a time determined by the server policy.
* The optional ReturnVerificationTimeInfo element MUST contain a boolean. Its default value is 'false'. This element cam be used by the client to obtain the time instant used by the server to validate the signature.
* The optional AdditionalKeyInfo element MAY occur zero or more times containing a sub-component. If present each instance MUST satisfy the requirements specified in this document in section AdditionalKeyInfo. This element provides the server with additional data (such as certificates and CRLs) which it can use to validate the signature.
* The optional ReturnProcessingDetails element MUST contain a boolean. Its default value is 'false'. The ReturnSigningTimeInfo element instructs the server to return a 3.1.45 element.
* The optional ReturnSigningTimeInfo element MUST contain a boolean. Its default value is 'false'. This element allows the client to instruct the server to return the time instant associated to the signature creation as a 3.1.47 element.
* The optional ReturnSignerIdentity element MUST contain a boolean. Its default value is 'false'.
* The optional ReturnUpdatedSignature element MUST contain a boolean. Its default value is 'false'. This element allows the client to instruct the server to return an 3.1.48 output, containing a new or updated signature
* The optional ReturnTransformedDocument element MAY occur zero or more times containing a sub-component. If present each instance MUST satisfy the requirements specified in this document in section ReturnTransformedDocument. The ReturnTransformedDocument element instructs the server to return an input document to which the XML signature transforms specified by a particular <ds:Reference> have been applied. The result of the transformations will be returned as a 3.1.50 element.
* The optional ReturnTimestampedSignature element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section UpdateSignatureInstruction. It indicates that the client wishes the server to update the signature after its verification by embedding a signature timestamp token as an unauthenticated attribute (see "unauthAttrs" in section 9.1 [RFC 3852]) or \*unsigned\* property (see section 6.2.5 "The UnsignedSignatureProperties element" and section 7.3 "The SignatureTimeStamp element" [XAdES]) of the supplied signature. The timestamp token will be on the signature value in the case of CMS/PKCS7signatures or the <ds:SignatureValue> element in the case of XML signatures.
* The optional VerifyManifests element MUST contain a boolean. Its default value is 'false'. [sub component VerifyManifests details]

A set of sub-components is inherited from component OptionalInputsBase and is not repeated here.

Non-normative Comment:

[component OptionalInputsVerify non normative details]

#### XML Syntax

The XML type OptionalInputsVerifyType SHALL implement the requirements defined in the OptionalInputsVerify component.

The OptionalInputsVerifyType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="OptionalInputsVerifyType">

<xs:complexContent>

<xs:extension base="dss:OptionalInputsBaseType">

<xs:sequence>

<xs:choice>

<xs:element maxOccurs="1" minOccurs="0" name="UseVerificationTime" type="dss:UseVerificationTimeType"/>

<xs:element default="false" maxOccurs="1" minOccurs="0" name="ReturnVerificationTimeInfo" type="xs:boolean"/>

<xs:element maxOccurs="unbounded" minOccurs="0" name="AdditionalKeyInfo" type="dss:AdditionalKeyInfoType"/>

<xs:element default="false" maxOccurs="1" minOccurs="0" name="ReturnProcessingDetails" type="xs:boolean"/>

<xs:element default="false" maxOccurs="1" minOccurs="0" name="ReturnSigningTimeInfo" type="xs:boolean"/>

<xs:element default="false" maxOccurs="1" minOccurs="0" name="ReturnSignerIdentity" type="xs:boolean"/>

<xs:element default="false" maxOccurs="1" minOccurs="0" name="ReturnUpdatedSignature" type="xs:boolean"/>

<xs:element maxOccurs="unbounded" minOccurs="0" name="ReturnTransformedDocument" type="dss:ReturnTransformedDocumentType"/>

<xs:element maxOccurs="1" minOccurs="0" name="ReturnTimestampedSignature" type="dss:UpdateSignatureInstructionType"/>

<xs:element default="false" maxOccurs="1" minOccurs="0" name="VerifyManifests" type="xs:boolean"/>

</xs:choice>

</xs:sequence>

</xs:extension>

</xs:complexContent>

</xs:complexType>

Each child element of OptionalInputsVerifyType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component OptionalInputsVerify XML schema details]

#### JSON Syntax

The OptionalInputsVerifyType JSON object SHALL implement in JSON syntax the requirements defined in the OptionalInputsVerify component.

The OptionalInputsVerifyType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-OptionalInputsVerifyType": {

"type": "object",

"properties": {

"policy": {

"type": "array",

"items": {

"type": "string"

}

},

"claimedIdentity": {

"type": "object",

"$ref": "#/definitions/dss-ClaimedIdentityType"

},

"lang": {

"type": "string"

},

"schemas": {

"type": "object",

"$ref": "#/definitions/dss-SchemasType"

},

"addTimestamp": {

"type": "object",

"$ref": "#/definitions/dss-UpdateSignatureInstructionType"

},

"other": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-PropertyType"

}

},

"useVerificationTime": {

"type": "object",

"$ref": "#/definitions/dss-UseVerificationTimeType"

},

"returnVerificationTime": {

"type": "boolean",

"default": "false"

},

"addKeyInfo": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-AdditionalKeyInfoType"

}

},

"returnProcDetails": {

"type": "boolean",

"default": "false"

},

"returnSigningTime": {

"type": "boolean",

"default": "false"

},

"returnSigner": {

"type": "boolean",

"default": "false"

},

"returnUpdated": {

"type": "boolean",

"default": "false"

},

"returnTransformed": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-ReturnTransformedDocumentType"

}

},

"returnTimestamped": {

"type": "object",

"$ref": "#/definitions/dss-UpdateSignatureInstructionType"

},

"verifyManifests": {

"type": "boolean",

"default": "false"

}

}

}

Properties in the JSON schema above SHALL implement sub-component of OptionalInputsVerify component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| ServicePolicy | policy | [] |
| ClaimedIdentity | claimedIdentity | [] |
| Language | lang | [] |
| Schemas | schemas | [] |
| AddTimestamp | addTimestamp | [] |
| Other | other | [] |
| UseVerificationTime | useVerificationTime | [] |
| ReturnVerificationTimeInfo | returnVerificationTime | [] |
| AdditionalKeyInfo | addKeyInfo | [] |
| ReturnProcessingDetails | returnProcDetails | [] |
| ReturnSigningTimeInfo | returnSigningTime | [] |
| ReturnSignerIdentity | returnSigner | [] |
| ReturnUpdatedSignature | returnUpdated | [] |
| ReturnTransformedDocument | returnTransformed | [] |
| ReturnTimestampedSignature | returnTimestamped | [] |
| VerifyManifests | verifyManifests | [] |

[component OptionalInputsVerify JSON schema details]

### Component OptionalOutputsBase

**Semantics**

The OptionalOutputsBase contains a common set of additional outputs associated with the processing of the request. The client MAY request the server to respond with certain optional outputs by sending certain optional inputs. The server MAY also respond with outputs the client didn’t request, depending on the server’s profile and policy. If a server doesn’t recognize or can’t handle any optional input, it MUST reject the request with a ResultMajor code of RequesterError and a ResultMinor code of NotSupported.

Below follows a list of the sub-components that MAY be present within this component:

* The optional AppliedPolicy element MAY occur zero or more times containing an URI. This element lists the set of DSS policies used by the server.
* The optional TransformedDocument element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section TransformedDocument. The TransformedDocument element contains a document corresponding to the specified <ds:Reference>, after all the transforms in the reference have been applied. In other words, the hash value of the returned document should equal the <ds:Reference> element’s <ds:DigestValue>.
* The optional Schemas element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section Schemas. The Schemas element is typically used as an optional input in a VerifyRequest. However, there are situations where it may be used as an optional output. For example, a service that makes use of the ReturnUpdatedSignature mechanism may, after verifying a signature over an input document, generate a signature over a document of a different schema than the input document. In this case the Schemas element MAY be used to communicate the XML schemas required for validating a returned XML document.
* The optional DocumentWithSignature element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section DocumentWithSignature. DocumentWithSignature element contains the input document with the signature inserted.
* The optional Other element MAY occur zero or more times containing a sub-component. If present each instance MUST satisfy the requirements specified in this document in section Property. [sub component Other details]

Non-normative Comment:

[component OptionalOutputsBase non normative details]

#### XML Syntax

The XML type OptionalOutputsBaseType SHALL implement the requirements defined in the OptionalOutputsBase component.

The OptionalOutputsBaseType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType abstract="true" name="OptionalOutputsBaseType">

<xs:sequence>

<xs:element maxOccurs="unbounded" minOccurs="0" name="AppliedPolicy" type="xs:anyURI"/>

<xs:element maxOccurs="1" minOccurs="0" name="TransformedDocument" type="dss:TransformedDocumentType"/>

<xs:element maxOccurs="1" minOccurs="0" name="Schemas" type="dss:SchemasType"/>

<xs:element maxOccurs="1" minOccurs="0" name="DocumentWithSignature" type="dss:DocumentWithSignatureType"/>

<xs:element maxOccurs="unbounded" minOccurs="0" name="Other" type="dss:PropertyType"/>

</xs:sequence>

</xs:complexType>

Each child element of OptionalOutputsBaseType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component OptionalOutputsBase XML schema details]

#### JSON Syntax

The component OptionalOutputsBase is abstract and therefore has no JSON definition.

[component OptionalOutputsBase JSON schema details]

### Component OptionalOutputsSign

**Semantics**

The OptionalOutputsSignType component defines a set of additional outputs associated with the processing of a signing request. This document does not define any additional outputs but profiles may extend the set of additional outputs.

Below follows a list of the sub-components that MAY be present within this component:

A set of sub-components is inherited from component OptionalOutputsBase and is not repeated here.

Non-normative Comment:

[component OptionalOutputsSign non normative details]

#### XML Syntax

The XML type OptionalOutputsSignType SHALL implement the requirements defined in the OptionalOutputsSign component.

The OptionalOutputsSignType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="OptionalOutputsSignType">

<xs:complexContent>

<xs:extension base="dss:OptionalOutputsBaseType"/>

</xs:complexContent>

</xs:complexType>

Each child element of OptionalOutputsSignType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component OptionalOutputsSign XML schema details]

#### JSON Syntax

The OptionalOutputsSignType JSON object SHALL implement in JSON syntax the requirements defined in the OptionalOutputsSign component.

The OptionalOutputsSignType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-OptionalOutputsSignType": {

"type": "object",

"properties": {

"policy": {

"type": "array",

"items": {

"type": "string"

}

},

"transformed": {

"type": "object",

"$ref": "#/definitions/dss-TransformedDocumentType"

},

"schemas": {

"type": "object",

"$ref": "#/definitions/dss-SchemasType"

},

"docWithSignature": {

"type": "object",

"$ref": "#/definitions/dss-DocumentWithSignatureType"

},

"other": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-PropertyType"

}

}

}

}

Properties in the JSON schema above SHALL implement sub-component of OptionalOutputsSign component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| AppliedPolicy | policy | [] |
| TransformedDocument | transformed | [] |
| Schemas | schemas | [] |
| DocumentWithSignature | docWithSignature | [] |
| Other | other | [] |

[component OptionalOutputsSign JSON schema details]

### Component OptionalOutputsVerify

**Semantics**

The OptionalOutputsVerify component defines a set of additional outputs associated with the processing of a verification request.

Below follows a list of the sub-components that MAY be present within this component:

* The optional VerifyManifestResults element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section VerifyManifestResults. [sub component VerifyManifestResults details]
* The optional SigningTimeInfo element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section SigningTimeInfo. The SigningTimeInfo element returns the signature’s creation date and time. When there's no way for the server to determine the signing time, the server MUST omit this element.
* The optional VerificationTimeInfo element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section VerificationTimeInfo. In addition to the verification time, the server MAY include in the VerificationTimeInfo element any other relevant time instants that may have been used when determining the verification time or that may be useful for its qualification.
* The optional ProcessingDetails element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section ProcessingDetails. The ProcessingDetails element elaborates on what signature verification steps succeeded or failed.
* The optional SignerIdentity element MUST contain a sub-component. A given element MUST satisfy the requirements specified in section NameID. The SignerIdentity element contains an indication of who performed the signature.
* The optional UpdatedSignature element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section UpdatedSignature. The UpdatedSignature element contains the returned signature.
* The optional TimestampedSignature element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section UpdatedSignature. The TimestampedSignature element contains the returned timestamped signature.

A set of sub-components is inherited from component OptionalOutputsBase and is not repeated here.

Non-normative Comment:

[component OptionalOutputsVerify non normative details]

#### XML Syntax

The XML type OptionalOutputsVerifyType SHALL implement the requirements defined in the OptionalOutputsVerify component.

The OptionalOutputsVerifyType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="OptionalOutputsVerifyType">

<xs:complexContent>

<xs:extension base="dss:OptionalOutputsBaseType">

<xs:sequence>

<xs:choice>

<xs:element maxOccurs="1" minOccurs="0" name="VerifyManifestResults" type="dss:VerifyManifestResultsType"/>

<xs:element maxOccurs="1" minOccurs="0" name="SigningTimeInfo" type="dss:SigningTimeInfoType"/>

<xs:element maxOccurs="1" minOccurs="0" name="VerificationTimeInfo" type="dss:VerificationTimeInfoType"/>

<xs:element maxOccurs="1" minOccurs="0" name="ProcessingDetails" type="dss:ProcessingDetailsType"/>

<xs:element maxOccurs="1" minOccurs="0" name="SignerIdentity" type="saml2:NameIDType"/>

<xs:element maxOccurs="1" minOccurs="0" name="UpdatedSignature" type="dss:UpdatedSignatureType"/>

<xs:element maxOccurs="1" minOccurs="0" name="TimestampedSignature" type="dss:UpdatedSignatureType"/>

</xs:choice>

</xs:sequence>

</xs:extension>

</xs:complexContent>

</xs:complexType>

Each child element of OptionalOutputsVerifyType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component OptionalOutputsVerify XML schema details]

#### JSON Syntax

The OptionalOutputsVerifyType JSON object SHALL implement in JSON syntax the requirements defined in the OptionalOutputsVerify component.

The OptionalOutputsVerifyType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-OptionalOutputsVerifyType": {

"type": "object",

"properties": {

"policy": {

"type": "array",

"items": {

"type": "string"

}

},

"transformed": {

"type": "object",

"$ref": "#/definitions/dss-TransformedDocumentType"

},

"schemas": {

"type": "object",

"$ref": "#/definitions/dss-SchemasType"

},

"docWithSignature": {

"type": "object",

"$ref": "#/definitions/dss-DocumentWithSignatureType"

},

"other": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-PropertyType"

}

},

"result": {

"type": "object",

"$ref": "#/definitions/dss-VerifyManifestResultsType"

},

"signingTimeInfo": {

"type": "object",

"$ref": "#/definitions/dss-SigningTimeInfoType"

},

"verificationTimeInfo": {

"type": "object",

"$ref": "#/definitions/dss-VerificationTimeInfoType"

},

"procDetails": {

"type": "object",

"$ref": "#/definitions/dss-ProcessingDetailsType"

},

"signerIdentity": {

"type": "object",

"$ref": "#/definitions/saml2-NameIDType"

},

"updSignature": {

"type": "object",

"$ref": "#/definitions/dss-UpdatedSignatureType"

},

"timestampedSignature": {

"type": "object",

"$ref": "#/definitions/dss-UpdatedSignatureType"

}

}

}

Properties in the JSON schema above SHALL implement sub-component of OptionalOutputsVerify component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| AppliedPolicy | policy | [] |
| TransformedDocument | transformed | [] |
| Schemas | schemas | [] |
| DocumentWithSignature | docWithSignature | [] |
| Other | other | [] |
| VerifyManifestResults | result | [] |
| SigningTimeInfo | signingTimeInfo | [] |
| VerificationTimeInfo | verificationTimeInfo | [] |
| ProcessingDetails | procDetails | [] |
| SignerIdentity | signerIdentity | [] |
| UpdatedSignature | updSignature | [] |
| TimestampedSignature | timestampedSignature | [] |

[component OptionalOutputsVerify JSON schema details]

### Component ClaimedIdentity

**Semantics**

[component ClaimedIdentity normative details]

Below follows a list of the sub-components that MAY be present within this component:

* The Name element MUST contain one instance of a sub-component. This element MUST satisfy the requirements specified in section NameID. The claimed identity may be authenticated using the security binding, according to section 6, or using authentication data provided in the SupportingInfo element. The server MUST check that the asserted Name is authenticated before relying upon the Name.
* The optional SupportingInfo element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section Any. The SupportingInfo element can be used by profiles to carry information related to the claimed identity. One possible use of SupportingInfo is to carry authentication data that authenticates the request as originating from the claimed identity (examples of authentication data include a password or SAML Assertion, a signature or MAC calculated over the request using a client key).

Non-normative Comment:

[component ClaimedIdentity non normative details]

#### XML Syntax

The XML type ClaimedIdentityType SHALL implement the requirements defined in the ClaimedIdentity component.

The ClaimedIdentityType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="ClaimedIdentityType">

<xs:sequence>

<xs:element name="Name" type="saml2:NameIDType"/>

<xs:element minOccurs="0" name="SupportingInfo" type="dss:AnyType"/>

</xs:sequence>

</xs:complexType>

Each child element of ClaimedIdentityType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component ClaimedIdentity XML schema details]

#### JSON Syntax

The ClaimedIdentityType JSON object SHALL implement in JSON syntax the requirements defined in the ClaimedIdentity component.

The ClaimedIdentityType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-ClaimedIdentityType": {

"type": "object",

"properties": {

"name": {

"type": "object",

"$ref": "#/definitions/saml2-NameIDType"

},

"suppInfo": {

"type": "object",

"$ref": "#/definitions/dss-AnyType"

}

},

"required": ["name"]

}

Properties in the JSON schema above SHALL implement sub-component of ClaimedIdentity component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| Name | name | [] |
| SupportingInfo | suppInfo | [] |

[component ClaimedIdentity JSON schema details]

### Component Schemas

**Semantics**

The Schemas component provides an in band mechanism for communicating XML schemas required for validating an XML document.

Below follows a list of the sub-components that MAY be present within this component:

* The Schema element MUST occur 1 or more times containing a sub-component. Each instance MUST satisfy the requirements specified in this document in section Document. The elements RefType and

Non-normative Comment:

Note: It is recommended to use xml:id as defined in [xml:id] as id in the payload being referenced by a <ds:Reference>, because the schema then does not have to be supplied for identifying the ID attributes.

#### XML Syntax

The XML type SchemasType SHALL implement the requirements defined in the Schemas component.

The SchemasType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="SchemasType">

<xs:sequence>

<xs:element maxOccurs="unbounded" name="Schema" type="dss:DocumentType"/>

</xs:sequence>

</xs:complexType>

Each child element of SchemasType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component Schemas XML schema details]

#### JSON Syntax

The SchemasType JSON object SHALL implement in JSON syntax the requirements defined in the Schemas component.

The SchemasType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-SchemasType": {

"type": "object",

"properties": {

"schema": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-DocumentType"

}

}

},

"required": ["schema"]

}

Properties in the JSON schema above SHALL implement sub-component of Schemas component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| Schema | schema | [] |

[component Schemas JSON schema details]

### Component RequestBase

**Semantics**

[component RequestBase normative details]

Below follows a list of the sub-components that MAY be present within this component:

* The optional InputDocuments element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section InputDocuments. The InputDocuments element contains the input documents which the processing will be applied to.
* The optional Profile element MAY occur zero or more times containing an URI. This element indicates a set of DSS profiles. It is used by the client to select profiles the server supports.
* The optional RequestID element MUST contain one instance of a string. The RequestID element is used to correlate requests with responses. When present in a request, the server MUST return it in the response.

Non-normative Comment:

[component RequestBase non normative details]

#### XML Syntax

The XML type RequestBaseType SHALL implement the requirements defined in the RequestBase component.

The RequestBaseType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType abstract="true" name="RequestBaseType">

<xs:sequence>

<xs:element minOccurs="0" name="InputDocuments" type="dss:InputDocumentsType"/>

<xs:element maxOccurs="unbounded" minOccurs="0" name="Profile" type="xs:anyURI"/>

</xs:sequence>

<xs:attribute name="RequestID" type="xs:string" use="optional"/>

</xs:complexType>

Each child element of RequestBaseType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component RequestBase XML schema details]

#### JSON Syntax

The component RequestBase is abstract and therefore has no JSON definition.

[component RequestBase JSON schema details]

### Component ResponseBase

**Semantics**

[component ResponseBase normative details]

Below follows a list of the sub-components that MAY be present within this component:

* The Result element MUST contain one instance of a sub-component. This element MUST satisfy the requirements specified in this document in section Result. The Result element represents the status of the request..
* The optional AppliedProfile element MAY occur zero or more times containing an URI. This element lists the set of DSS profile applied by the server. This set MAY include the set of profiles requested by the client. But the server MAY use more comprehensive set of profiles and add additional profiles not requested by the client.
* The optional RequestID element MUST contain one instance of a string. The RequestID element is used to correlate this response with its request.

Non-normative Comment:

[component ResponseBase non normative details]

#### XML Syntax

The XML type ResponseBaseType SHALL implement the requirements defined in the ResponseBase component.

The ResponseBaseType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType abstract="true" name="ResponseBaseType">

<xs:sequence>

<xs:element name="Result" type="dss:ResultType"/>

<xs:element maxOccurs="unbounded" minOccurs="0" name="AppliedProfile" type="xs:anyURI"/>

</xs:sequence>

<xs:attribute name="RequestID" type="xs:string" use="optional"/>

</xs:complexType>

Each child element of ResponseBaseType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component ResponseBase XML schema details]

#### JSON Syntax

The component ResponseBase is abstract and therefore has no JSON definition.

[component ResponseBase JSON schema details]

### Component SignRequest

**Semantics**

The SignRequest component is sent by the client to request a signature or timestamp on some input documents.

Below follows a list of the sub-components that MAY be present within this component:

* The optional OptionalInputs element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section OptionalInputsSign. It is intended to transport additional input elements of the signing request.

A set of sub-components is inherited from component RequestBase and is not repeated here.

Non-normative Comment:

[component SignRequest non normative details]

#### XML Syntax

The XML type SignRequestType SHALL implement the requirements defined in the SignRequest component.

The SignRequestType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="SignRequestType">

<xs:complexContent>

<xs:extension base="dss:RequestBaseType">

<xs:sequence>

<xs:element minOccurs="0" name="OptionalInputs" type="dss:OptionalInputsSignType"/>

</xs:sequence>

</xs:extension>

</xs:complexContent>

</xs:complexType>

Each child element of SignRequestType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component SignRequest XML schema details]

#### JSON Syntax

The SignRequestType JSON object SHALL implement in JSON syntax the requirements defined in the SignRequest component.

The SignRequestType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-SignRequestType": {

"type": "object",

"properties": {

"inDocs": {

"type": "object",

"$ref": "#/definitions/dss-InputDocumentsType"

},

"profile": {

"type": "array",

"items": {

"type": "string"

}

},

"reqID": {

"type": "string"

},

"optInp": {

"type": "object",

"$ref": "#/definitions/dss-OptionalInputsSignType"

}

}

}

Properties in the JSON schema above SHALL implement sub-component of SignRequest component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| InputDocuments | inDocs | [] |
| Profile | profile | [] |
| RequestID | reqID | [] |
| OptionalInputs | optInp | [] |

[component SignRequest JSON schema details]

### Component SignResponse

**Semantics**

The SignResponse component returns the requested signature or timestamp to the requestor.

Below follows a list of the sub-components that MAY be present within this component:

* The optional OptionalOutputs element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section OptionalOutputsSign. The OptionalOutputs element contains additional signing related outputs returned by the server.
* The optional SignatureObject element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section SignatureObject. [sub component SignatureObject details]

A set of sub-components is inherited from component ResponseBase and is not repeated here.

Non-normative Comment:

[component SignResponse non normative details]

#### XML Syntax

The XML type SignResponseType SHALL implement the requirements defined in the SignResponse component.

The SignResponseType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="SignResponseType">

<xs:complexContent>

<xs:extension base="dss:ResponseBaseType">

<xs:sequence>

<xs:element minOccurs="0" name="OptionalOutputs" type="dss:OptionalOutputsSignType"/>

<xs:element minOccurs="0" name="SignatureObject" type="dss:SignatureObjectType"/>

</xs:sequence>

</xs:extension>

</xs:complexContent>

</xs:complexType>

Each child element of SignResponseType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component SignResponse XML schema details]

#### JSON Syntax

The SignResponseType JSON object SHALL implement in JSON syntax the requirements defined in the SignResponse component.

The SignResponseType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-SignResponseType": {

"type": "object",

"properties": {

"result": {

"type": "object",

"$ref": "#/definitions/dss-ResultType"

},

"profile": {

"type": "array",

"items": {

"type": "string"

}

},

"reqID": {

"type": "string"

},

"optOutp": {

"type": "object",

"$ref": "#/definitions/dss-OptionalOutputsSignType"

},

"sigObj": {

"type": "object",

"$ref": "#/definitions/dss-SignatureObjectType"

}

}

}

Properties in the JSON schema above SHALL implement sub-component of SignResponse component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| Result | result | [] |
| AppliedProfile | profile | [] |
| RequestID | reqID | [] |
| OptionalOutputs | optOutp | [] |
| SignatureObject | sigObj | [] |

[component SignResponse JSON schema details]

### Component UpdateSignatureInstruction

**Semantics**

The UpdateSignatureInstruction component can be used an optional input for both signing and verification requests and defines the type timestamp that should to be applied.

Below follows a list of the sub-components that MAY be present within this component:

* The optional Type element MUST contain one instance of an URI. The Type element indicates what type of timestamp to apply. Profiles that use this optional input MUST define the allowed values, and the default value, for the Type element (unless only a single type of timestamp is supported, in which case the Type attribute can be omitted).

Non-normative Comment:

[component UpdateSignatureInstruction non normative details]

#### XML Syntax

The XML type UpdateSignatureInstructionType SHALL implement the requirements defined in the UpdateSignatureInstruction component.

The UpdateSignatureInstructionType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="UpdateSignatureInstructionType">

<xs:attribute name="Type" type="xs:anyURI" use="optional"/>

</xs:complexType>

Each child element of UpdateSignatureInstructionType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component UpdateSignatureInstruction XML schema details]

#### JSON Syntax

The UpdateSignatureInstructionType JSON object SHALL implement in JSON syntax the requirements defined in the UpdateSignatureInstruction component.

The UpdateSignatureInstructionType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-UpdateSignatureInstructionType": {

"type": "object",

"properties": {

"type": {

"type": "string",

"format": "uri"

}

}

}

Properties in the JSON schema above SHALL implement sub-component of UpdateSignatureInstruction component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| Type | type | [] |

[component UpdateSignatureInstruction JSON schema details]

### Component IntendedAudience

**Semantics**

The IntendedAudience element tells the server who the target audience of this signature is. The server MAY use this to parameterize any aspect of its processing (for example, the server MAY choose to sign with a key that it knows a particular recipient trusts).

Below follows a list of the sub-components that MAY be present within this component:

* The Recipient element MUST occur 1 or more times containing a sub-component. Each instance MUST satisfy the requirements specified in section NameID. [sub component Recipient details]

Non-normative Comment:

[component IntendedAudience non normative details]

#### XML Syntax

The XML type IntendedAudienceType SHALL implement the requirements defined in the IntendedAudience component.

The IntendedAudienceType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="IntendedAudienceType">

<xs:sequence>

<xs:element maxOccurs="unbounded" name="Recipient" type="saml2:NameIDType"/>

</xs:sequence>

</xs:complexType>

Each child element of IntendedAudienceType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component IntendedAudience XML schema details]

#### JSON Syntax

The IntendedAudienceType JSON object SHALL implement in JSON syntax the requirements defined in the IntendedAudience component.

The IntendedAudienceType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-IntendedAudienceType": {

"type": "object",

"properties": {

"recipient": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/saml2-NameIDType"

}

}

},

"required": ["recipient"]

}

Properties in the JSON schema above SHALL implement sub-component of IntendedAudience component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| Recipient | recipient | [] |

[component IntendedAudience JSON schema details]

### Component KeySelector

**Semantics**

The KeySelector component holds data that selects a specific key or certificate or group of certificates. Only one of its sub-components MUST be present. But a KeySelector component can occur multiple times as a sub-component in the OptionalInputsSign component

Below follows a list of the sub-components that MAY be present within this component:

* The X509Digest element MUST contain one instance of a sub-component. This element MUST satisfy the requirements specified in this document in section X509Digest. [sub component X509Digest details]
* The X509SubjectName element MUST contain one instance of a string. The X509SubjectName element contains an X.509 subject distinguished name that SHOULD be represented as a string that complies with section 3 of RFC4514 [LDAP-DN].
* The X509SKI element MUST contain one instance of base64 encoded binary data. The X509SKI element contains the base64 encoded plain (i.e. non-DER-encoded) value of a X509 V.3 SubjectKeyIdentifier extension.
* The X509Certificate element MUST contain one instance of base64 encoded binary data. The X509Certificate element contains a base64-encoded [X509V3] certificate.
* The KeyName element MUST contain one instance of a string. It selects a key to be used for signing in a generic way. Usually the client knows about the valid values for KeyName.

Non-normative Comment:

[component KeySelector non normative details]

#### XML Syntax

The XML type KeySelectorType SHALL implement the requirements defined in the KeySelector component.

The KeySelectorType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="KeySelectorType">

<xs:choice>

<xs:element name="X509Digest" type="dss:X509DigestType"/>

<xs:element name="X509SubjectName" type="xs:string"/>

<xs:element name="X509SKI" type="xs:base64Binary"/>

<xs:element name="X509Certificate" type="xs:base64Binary"/>

<xs:element name="KeyName" type="xs:string"/>

</xs:choice>

</xs:complexType>

Each child element of KeySelectorType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component KeySelector XML schema details]

#### JSON Syntax

The KeySelectorType JSON object SHALL implement in JSON syntax the requirements defined in the KeySelector component.

The KeySelectorType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-KeySelectorType": {

"type": "object",

"properties": {

"x509Digest": {

"type": "object",

"$ref": "#/definitions/dss-X509DigestType"

},

"subject": {

"type": "string"

},

"ski": {

"type": "string"

},

"cert": {

"type": "string"

},

"name": {

"type": "string"

}

},

"minProperties": 1,

"maxProperties": 1

}

Properties in the JSON schema above SHALL implement sub-component of KeySelector component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| X509Digest | x509Digest | [] |
| X509SubjectName | subject | [] |
| X509SKI | ski | [] |
| X509Certificate | cert | [] |
| KeyName | name | [] |

[component KeySelector JSON schema details]

### Component X509Digest

**Semantics**

The X509Digest component contains a base64-encoded digest of a certificate. The digest algorithm URI is identified with a required Algorithm element. The input to the digest MUST be the raw octets that would be base64-encoded of a X509Certificate.

Below follows a list of the sub-components that MAY be present within this component:

* The value element MUST contain one instance of base64 encoded binary data. .
* The Algorithm element MUST contain one instance of a string. The string describes the digest algorithm in an appropriate way for the server side processing. Depending on the signature format this may be an OID (e.g. ‘2.16.840.1.101.3.4.2.1’), an URI (e.g. ‘http://www.w3.org/2001/04/xmlenc#sha256’) or a descriptive string (‘SHA-256’).

Non-normative Comment:

[component X509Digest non normative details]

#### XML Syntax

The XML type X509DigestType SHALL implement the requirements defined in the X509Digest component.

The X509DigestType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="X509DigestType">

<xs:simpleContent>

<xs:extension base="xs:base64Binary">

<xs:attribute name="Algorithm" type="xs:string" use="required"/>

</xs:extension>

</xs:simpleContent>

</xs:complexType>

Each child element of X509DigestType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name. The element 'value' holding the base64 content is represented by the component's XML tag text content.

[component X509Digest XML schema details]

#### JSON Syntax

The X509DigestType JSON object SHALL implement in JSON syntax the requirements defined in the X509Digest component.

The X509DigestType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-X509DigestType": {

"type": "object",

"properties": {

"value": {

"type": "string"

},

"algo": {

"type": "string"

}

},

"required": ["algo"]

}

Properties in the JSON schema above SHALL implement sub-component of X509Digest component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| value | value | [] |
| Algorithm | algo | [] |

[component X509Digest JSON schema details]

### Component PropertiesHolder

**Semantics**

The PropertiesHolder component is used to request that the server add certain signed or unsigned properties (aka “signature attributes”) into the signature. The client can send the server a particular value to use for each property, or leave the value up to the server to determine. The server can add additional properties, even if these aren’t requested by the client.

Below follows a list of the sub-components that MAY be present within this component:

* The optional SignedProperties element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section Properties. These properties will be covered by the signature.
* The optional UnsignedProperties element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section Properties. These properties will **not** be covered by the signature.

Non-normative Comment:

[component PropertiesHolder non normative details]

#### XML Syntax

The XML type PropertiesHolderType SHALL implement the requirements defined in the PropertiesHolder component.

The PropertiesHolderType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="PropertiesHolderType">

<xs:sequence>

<xs:element minOccurs="0" name="SignedProperties" type="dss:PropertiesType"/>

<xs:element minOccurs="0" name="UnsignedProperties" type="dss:PropertiesType"/>

</xs:sequence>

</xs:complexType>

Each child element of PropertiesHolderType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component PropertiesHolder XML schema details]

#### JSON Syntax

The PropertiesHolderType JSON object SHALL implement in JSON syntax the requirements defined in the PropertiesHolder component.

The PropertiesHolderType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-PropertiesHolderType": {

"type": "object",

"properties": {

"signedProps": {

"type": "object",

"$ref": "#/definitions/dss-PropertiesType"

},

"unsignedProps": {

"type": "object",

"$ref": "#/definitions/dss-PropertiesType"

}

}

}

Properties in the JSON schema above SHALL implement sub-component of PropertiesHolder component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| SignedProperties | signedProps | [] |
| UnsignedProperties | unsignedProps | [] |

[component PropertiesHolder JSON schema details]

### Component Properties

**Semantics**

[component Properties normative details]

Below follows a list of the sub-components that MAY be present within this component:

* The Property element MUST occur 1 or more times containing a sub-component. Each instance MUST satisfy the requirements specified in this document in section Property. [sub component Property details]

Non-normative Comment:

[component Properties non normative details]

#### XML Syntax

The XML type PropertiesType SHALL implement the requirements defined in the Properties component.

The PropertiesType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="PropertiesType">

<xs:sequence>

<xs:element maxOccurs="unbounded" name="Property" type="dss:PropertyType"/>

</xs:sequence>

</xs:complexType>

Each child element of PropertiesType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component Properties XML schema details]

#### JSON Syntax

The PropertiesType JSON object SHALL implement in JSON syntax the requirements defined in the Properties component.

The PropertiesType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-PropertiesType": {

"type": "object",

"properties": {

"prop": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-PropertyType"

}

}

},

"required": ["prop"]

}

Properties in the JSON schema above SHALL implement sub-component of Properties component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| Property | prop | [] |

[component Properties JSON schema details]

### Component Property

**Semantics**

[component Property normative details]

Below follows a list of the sub-components that MAY be present within this component:

* The Identifier element MUST contain one instance of a string.
* The optional Value element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section Any. The Value element contains arbitrary content wrapped in an Element Any.

Non-normative Comment:

[component Property non normative details]

#### XML Syntax

The XML type PropertyType SHALL implement the requirements defined in the Property component.

The PropertyType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="PropertyType">

<xs:sequence>

<xs:element name="Identifier" type="xs:string"/>

<xs:element minOccurs="0" name="Value" type="dss:AnyType"/>

</xs:sequence>

</xs:complexType>

Each child element of PropertyType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

. Therefore it occurs in the XML schema, too.

#### JSON Syntax

The PropertyType JSON object SHALL implement in JSON syntax the requirements defined in the Property component.

The PropertyType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-PropertyType": {

"type": "object",

"properties": {

"id": {

"type": "string"

},

"value": {

"type": "object",

"$ref": "#/definitions/dss-AnyType"

}

},

"required": ["id"]

}

Properties in the JSON schema above SHALL implement sub-component of Property component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| Identifier | id | [] |
| Value | value | [] |

[component Property JSON schema details]

### Component IncludeObject

**Semantics**

The IncludeObject component is used to request the creation of an XMLSig enveloping signature.

Below follows a list of the sub-components that MAY be present within this component:

* The optional WhichDocument element MUST contain one instance of a unique identifier reference. This element identifies the input document which will be inserted into the returned signature.
* The optional hasObjectTagsAndAttributesSet element MUST contain one instance of a boolean. Its default value is 'false'. If ‘true’ this element indicates that the Document contains a <ds:Object> element which has been prepared ready for direct inclusion in the <ds:Signature>.
* The optional ObjId element MUST contain one instance of a string. It sets the Id attribute on the returned <ds:Object>.
* The optional createReference element MUST contain one instance of a boolean. Its default value is 'true'. If the createReference element is set to false inhibits the creation of the <ds:Reference> associated to the RefURI element of the input document referred by the WhichDocument element, effectively allowing clients to include <ds:Object> elements not covered/protected by the signature being created.

Non-normative Comment:

[component IncludeObject non normative details]

#### XML Syntax

The XML type IncludeObjectType SHALL implement the requirements defined in the IncludeObject component.

The IncludeObjectType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="IncludeObjectType">

<xs:attribute name="WhichDocument" type="xs:IDREF"/>

<xs:attribute default="false" name="hasObjectTagsAndAttributesSet" type="xs:boolean"/>

<xs:attribute name="ObjId" type="xs:string" use="optional"/>

<xs:attribute default="true" name="createReference" type="xs:boolean" use="optional"/>

</xs:complexType>

Each child element of IncludeObjectType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component IncludeObject XML schema details]

#### JSON Syntax

The IncludeObjectType JSON object SHALL implement in JSON syntax the requirements defined in the IncludeObject component.

The IncludeObjectType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-IncludeObjectType": {

"type": "object",

"properties": {

"whichDoc": {

"type": "object",

"$ref": "#/definitions/dss-DocumentBaseType"

},

"hasObjectTagsAndAttributesSet": {

"type": "boolean",

"default": "false"

},

"objId": {

"type": "string"

},

"createRef": {

"type": "boolean",

"default": "true"

}

}

}

Properties in the JSON schema above SHALL implement sub-component of IncludeObject component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| WhichDocument | whichDoc | [] |
| hasObjectTagsAndAttributesSet | hasObjectTagsAndAttributesSet | [] |
| ObjId | objId | [] |
| createReference | createRef | [] |

[component IncludeObject JSON schema details]

### Component SignaturePlacement

**Semantics**

[component SignaturePlacement normative details]

Below follows a list of the sub-components that MAY be present within this component:

* The XPathAfter element MUST contain one instance of a string. This elements holds an XPath expression which identifies an element, inside the XML input document, after which the signature will be inserted.
* The XPathFirstChildOf element MUST contain one instance of a string. This elements holds an XPath expression which identifies an element, in the XML input document, which the signature will be inserted as the first child of.
* The optional NsURIMapping element MAY occur zero or more times containing a sub-component. If present each instance MUST satisfy the requirements specified in section NsURIMapping. The NsURIMapping element allows the definition of additional namespace prefix to URI mappings required for the evaluation of the XPath expressions.
* The optional WhichDocument element MUST contain one instance of a unique identifier reference. The WhichDocument element identifies the input document which the signature will be inserted into.
* The optional CreateEnvelopedSignature element MUST contain one instance of a boolean. Its default value is 'true'. If the CreateEnvelopedSignature element is set to true a reference having an enveloped signature transform is created.

Non-normative Comment:

[component SignaturePlacement non normative details]

#### XML Syntax

The XML type SignaturePlacementType SHALL implement the requirements defined in the SignaturePlacement component.

The SignaturePlacementType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="SignaturePlacementType">

<xs:sequence>

<xs:choice>

<xs:element name="XPathAfter" type="xs:string"/>

<xs:element name="XPathFirstChildOf" type="xs:string"/>

</xs:choice>

<xs:element maxOccurs="unbounded" minOccurs="0" name="NsURIMapping" type="ds:NsURIMappingType"/>

</xs:sequence>

<xs:attribute name="WhichDocument" type="xs:IDREF"/>

<xs:attribute default="true" name="CreateEnvelopedSignature" type="xs:boolean"/>

</xs:complexType>

Each child element of SignaturePlacementType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component SignaturePlacement XML schema details]

#### JSON Syntax

The SignaturePlacementType JSON object SHALL implement in JSON syntax the requirements defined in the SignaturePlacement component.

The SignaturePlacementType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-SignaturePlacementType": {

"type": "object",

"properties": {

"xPathAfter": {

"type": "string"

},

"xPathFirstChildOf": {

"type": "string"

},

"nsDecl": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dsig-NsURIMappingType"

}

},

"whichDoc": {

"type": "object",

"$ref": "#/definitions/dss-DocumentBaseType"

},

"createEnvelopedSignature": {

"type": "boolean",

"default": "true"

}

}

}

Properties in the JSON schema above SHALL implement sub-component of SignaturePlacement component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| XPathAfter | xPathAfter | [] |
| XPathFirstChildOf | xPathFirstChildOf | [] |
| NsURIMapping | nsDecl | [] |
| WhichDocument | whichDoc | [] |
| CreateEnvelopedSignature | createEnvelopedSignature | [] |

[component SignaturePlacement JSON schema details]

### Component DocumentWithSignature

**Semantics**

The DocumentWithSignature component contains a Document with the signature inserted as requested with the SignaturePlacement component.

Below follows a list of the sub-components that MAY be present within this component:

* The Document element MUST contain one instance of a sub-component. This element MUST satisfy the requirements specified in this document in section Document. This contains the input document with a signature inserted in some fashion.

Non-normative Comment:

[component DocumentWithSignature non normative details]

#### XML Syntax

The XML type DocumentWithSignatureType SHALL implement the requirements defined in the DocumentWithSignature component.

The DocumentWithSignatureType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="DocumentWithSignatureType">

<xs:sequence>

<xs:element name="Document" type="dss:DocumentType"/>

</xs:sequence>

</xs:complexType>

Each child element of DocumentWithSignatureType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component DocumentWithSignature XML schema details]

#### JSON Syntax

The DocumentWithSignatureType JSON object SHALL implement in JSON syntax the requirements defined in the DocumentWithSignature component.

The DocumentWithSignatureType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-DocumentWithSignatureType": {

"type": "object",

"properties": {

"doc": {

"type": "object",

"$ref": "#/definitions/dss-DocumentType"

}

},

"required": ["doc"]

}

Properties in the JSON schema above SHALL implement sub-component of DocumentWithSignature component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| Document | doc | [] |

[component DocumentWithSignature JSON schema details]

### Component SignedReferences

**Semantics**

The SignedReferences component gives the client greater control over how the <ds:Reference> elements are formed.

Below follows a list of the sub-components that MAY be present within this component:

* The SignedReference element MUST occur 1 or more times containing a sub-component. Each instance MUST satisfy the requirements specified in this document in section SignedReference. [sub component SignedReference details]

Non-normative Comment:

[component SignedReferences non normative details]

#### XML Syntax

The XML type SignedReferencesType SHALL implement the requirements defined in the SignedReferences component.

The SignedReferencesType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="SignedReferencesType">

<xs:sequence>

<xs:element maxOccurs="unbounded" name="SignedReference" type="dss:SignedReferenceType"/>

</xs:sequence>

</xs:complexType>

Each child element of SignedReferencesType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component SignedReferences XML schema details]

#### JSON Syntax

The SignedReferencesType JSON object SHALL implement in JSON syntax the requirements defined in the SignedReferences component.

The SignedReferencesType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-SignedReferencesType": {

"type": "object",

"properties": {

"signedRef": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-SignedReferenceType"

}

}

},

"required": ["signedRef"]

}

Properties in the JSON schema above SHALL implement sub-component of SignedReferences component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| SignedReference | signedRef | [] |

[component SignedReferences JSON schema details]

### Component SignedReference

**Semantics**

Each SignedReference component refers to an input document and allows multiple <ds:Reference> elements to be based on a single input document. Furthermore, the client can request additional transforms to be applied to each <ds:Reference>, and can set each <ds:Reference> element’s Id or URI attribute. These aspects of the <ds:Reference> can only be set through the SignedReference component; they cannot be set through the input documents, since they are aspects of the reference to the input document, not the input document itself.

Below follows a list of the sub-components that MAY be present within this component:

* The optional Transforms element MUST contain a sub-component. A given element MUST satisfy the requirements specified in section Transforms. The Transforms element requests the server to perform additional transforms on this reference.
* The WhichDocument element MUST contain one instance of a unique identifier reference. This defines which input document this reference refers to.
* The optional RefURI element MUST contain one instance of an URI. If this element is present, the corresponding <ds:Reference> element’s URI attribute is set to its value. If it is not present, the URI attribute is omitted in the corresponding <ds:Reference>.
* The optional RefId element MUST contain one instance of a string. This element sets the Id attribute of the corresponding <ds:Reference>.

Non-normative Comment:

[component SignedReference non normative details]

#### XML Syntax

The XML type SignedReferenceType SHALL implement the requirements defined in the SignedReference component.

The SignedReferenceType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="SignedReferenceType">

<xs:sequence>

<xs:element minOccurs="0" name="Transforms" type="ds:TransformsType"/>

</xs:sequence>

<xs:attribute name="WhichDocument" type="xs:IDREF" use="required"/>

<xs:attribute name="RefURI" type="xs:anyURI" use="optional"/>

<xs:attribute name="RefId" type="xs:string" use="optional"/>

</xs:complexType>

Each child element of SignedReferenceType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component SignedReference XML schema details]

#### JSON Syntax

The SignedReferenceType JSON object SHALL implement in JSON syntax the requirements defined in the SignedReference component.

The SignedReferenceType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-SignedReferenceType": {

"type": "object",

"properties": {

"transforms": {

"type": "object",

"$ref": "#/definitions/dsig-TransformsType"

},

"whichDoc": {

"type": "object",

"$ref": "#/definitions/dss-DocumentBaseType"

},

"refURI": {

"type": "string"

},

"refId": {

"type": "string"

}

},

"required": ["whichDoc"]

}

Properties in the JSON schema above SHALL implement sub-component of SignedReference component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| Transforms | transforms | [] |
| WhichDocument | whichDoc | [] |
| RefURI | refURI | [] |
| RefId | refId | [] |

[component SignedReference JSON schema details]

### Component VerifyRequest

**Semantics**

The VerifyRequest component is sent by the client to verify a signature or timestamp on some input documents.

Below follows a list of the sub-components that MAY be present within this component:

* The optional OptionalInputs element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section OptionalInputsVerify. [sub component OptionalInputs details]
* The optional SignatureObject element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section SignatureObject. The SignatureObject element contains a signature or timestamp, or else contains a <SignaturePtr> that points to an XML signature in one of the input documents.

A set of sub-components is inherited from component RequestBase and is not repeated here.

Non-normative Comment:

[component VerifyRequest non normative details]

#### XML Syntax

The XML type VerifyRequestType SHALL implement the requirements defined in the VerifyRequest component.

The VerifyRequestType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="VerifyRequestType">

<xs:complexContent>

<xs:extension base="dss:RequestBaseType">

<xs:sequence>

<xs:element minOccurs="0" name="OptionalInputs" type="dss:OptionalInputsVerifyType"/>

<xs:element minOccurs="0" name="SignatureObject" type="dss:SignatureObjectType"/>

</xs:sequence>

</xs:extension>

</xs:complexContent>

</xs:complexType>

Each child element of VerifyRequestType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component VerifyRequest XML schema details]

#### JSON Syntax

The VerifyRequestType JSON object SHALL implement in JSON syntax the requirements defined in the VerifyRequest component.

The VerifyRequestType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-VerifyRequestType": {

"type": "object",

"properties": {

"inDocs": {

"type": "object",

"$ref": "#/definitions/dss-InputDocumentsType"

},

"profile": {

"type": "array",

"items": {

"type": "string"

}

},

"reqID": {

"type": "string"

},

"optInp": {

"type": "object",

"$ref": "#/definitions/dss-OptionalInputsVerifyType"

},

"sigObj": {

"type": "object",

"$ref": "#/definitions/dss-SignatureObjectType"

}

}

}

Properties in the JSON schema above SHALL implement sub-component of VerifyRequest component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| InputDocuments | inDocs | [] |
| Profile | profile | [] |
| RequestID | reqID | [] |
| OptionalInputs | optInp | [] |
| SignatureObject | sigObj | [] |

[component VerifyRequest JSON schema details]

### Component VerifyResponse

**Semantics**

The VerifyResponse component is returned by the server to provide the results of verification.

Below follows a list of the sub-components that MAY be present within this component:

* The optional OptionalOutputs element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section OptionalOutputsVerify. [sub component OptionalOutputs details]

A set of sub-components is inherited from component ResponseBase and is not repeated here.

Non-normative Comment:

[component VerifyResponse non normative details]

#### XML Syntax

The XML type VerifyResponseType SHALL implement the requirements defined in the VerifyResponse component.

The VerifyResponseType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="VerifyResponseType">

<xs:complexContent>

<xs:extension base="dss:ResponseBaseType">

<xs:sequence>

<xs:element minOccurs="0" name="OptionalOutputs" type="dss:OptionalOutputsVerifyType"/>

</xs:sequence>

</xs:extension>

</xs:complexContent>

</xs:complexType>

Each child element of VerifyResponseType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component VerifyResponse XML schema details]

#### JSON Syntax

The VerifyResponseType JSON object SHALL implement in JSON syntax the requirements defined in the VerifyResponse component.

The VerifyResponseType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-VerifyResponseType": {

"type": "object",

"properties": {

"result": {

"type": "object",

"$ref": "#/definitions/dss-ResultType"

},

"profile": {

"type": "array",

"items": {

"type": "string"

}

},

"reqID": {

"type": "string"

},

"optOutp": {

"type": "object",

"$ref": "#/definitions/dss-OptionalOutputsVerifyType"

}

}

}

Properties in the JSON schema above SHALL implement sub-component of VerifyResponse component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| Result | result | [] |
| AppliedProfile | profile | [] |
| RequestID | reqID | [] |
| OptionalOutputs | optOutp | [] |

[component VerifyResponse JSON schema details]

### Component VerifyManifestResults

**Semantics**

The results of verifying individual <ds:Reference>'s within a <ds:Manifest> are returned in the VerifyManifestResults component.

Below follows a list of the sub-components that MAY be present within this component:

* The ManifestResult element MUST occur 1 or more times containing a sub-component. Each instance MUST satisfy the requirements specified in this document in section ManifestResult. [sub component ManifestResult details]

Non-normative Comment:

[component VerifyManifestResults non normative details]

#### XML Syntax

The XML type VerifyManifestResultsType SHALL implement the requirements defined in the VerifyManifestResults component.

The VerifyManifestResultsType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="VerifyManifestResultsType">

<xs:sequence>

<xs:element maxOccurs="unbounded" name="ManifestResult" type="dss:ManifestResultType"/>

</xs:sequence>

</xs:complexType>

Each child element of VerifyManifestResultsType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component VerifyManifestResults XML schema details]

#### JSON Syntax

The VerifyManifestResultsType JSON object SHALL implement in JSON syntax the requirements defined in the VerifyManifestResults component.

The VerifyManifestResultsType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-VerifyManifestResultsType": {

"type": "object",

"properties": {

"signedRef": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-ManifestResultType"

}

}

},

"required": ["signedRef"]

}

Properties in the JSON schema above SHALL implement sub-component of VerifyManifestResults component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| ManifestResult | signedRef | [] |

[component VerifyManifestResults JSON schema details]

### Component ManifestResult

**Semantics**

The VerifyManifestResults component is comprised of one or more ManifestResult

Below follows a list of the sub-components that MAY be present within this component:

* The ReferenceXpath element MUST contain one instance of a string. This element identifies the manifest reference, in the XML signature, to which this result pertains.
* The Status element MUST contain one instance of an URI. Its value is limited to item of the following set:  
  urn:oasis:names:tc:dss:1.0:manifeststatus:Valid  
  urn:oasis:names:tc:dss:1.0:manifeststatus:Invalid  
  This element indicates the manifest validation result.
* The optional NsURIMapping element MAY occur zero or more times containing a sub-component. If present each instance MUST satisfy the requirements specified in section NsURIMapping. The NsURIMapping element allows the definition of additional namespace prefix to URI mappings required for the evaluation of the XPath expressions.

Non-normative Comment:

[component ManifestResult non normative details]

#### XML Syntax

The XML type ManifestResultType SHALL implement the requirements defined in the ManifestResult component.

The ManifestResultType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="ManifestResultType">

<xs:sequence>

<xs:element name="ReferenceXpath" type="xs:string"/>

<xs:element name="Status">

<xs:simpleType>

<xs:restriction base="xs:anyURI">

<xs:enumeration value="urn:oasis:names:tc:dss:1.0:manifeststatus:Valid"/>

<xs:enumeration value="urn:oasis:names:tc:dss:1.0:manifeststatus:Invalid"/>

</xs:restriction>

</xs:simpleType>

</xs:element>

<xs:element maxOccurs="unbounded" minOccurs="0" name="NsURIMapping" type="ds:NsURIMappingType"/>

</xs:sequence>

</xs:complexType>

Each child element of ManifestResultType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component ManifestResult XML schema details]

#### JSON Syntax

The ManifestResultType JSON object SHALL implement in JSON syntax the requirements defined in the ManifestResult component.

The ManifestResultType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-ManifestResultType": {

"type": "object",

"properties": {

"xPath": {

"type": "string"

},

"status": {

"type": "string",

"enum": ["urn:oasis:names:tc:dss:1.0:manifeststatus:Valid", "urn:oasis:names:tc:dss:1.0:manifeststatus:Invalid"]

},

"nsDecl": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dsig-NsURIMappingType"

}

}

},

"required": ["xPath", "status"]

}

Properties in the JSON schema above SHALL implement sub-component of ManifestResult component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| ReferenceXpath | xPath | [] |
| Status | status | [] |
| NsURIMapping | nsDecl | [] |

[component ManifestResult JSON schema details]

### Component UseVerificationTime

**Semantics**

This UseVerificationTime component instructs the server to attempt to determine the signature’s validity at the specified time, instead of a time determined by the server policy.

Below follows a list of the sub-components that MAY be present within this component:

* The CurrentTime element MUST contain one instance of a boolean. Its default value is 'false'. This element instructs the server to use its current time (normally the time associated with the server-side request processing).
* The SpecificTime element MUST contain one instance of a date/time value. The SpecificTime element allows the client to manage manually the time instant used in the verification process. It SHOULD be expressed as UTC time (Coordinated Universal Time) to reduce confusion with the local time zone use.
* The optional Base64Content element MUST contain base64 encoded binary data. The Base64Content element allows the provision of additional date/time data.

Non-normative Comment:

[component UseVerificationTime non normative details]

#### XML Syntax

The XML type UseVerificationTimeType SHALL implement the requirements defined in the UseVerificationTime component.

The UseVerificationTimeType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="UseVerificationTimeType">

<xs:choice>

<xs:element default="false" name="CurrentTime" type="xs:boolean"/>

<xs:element name="SpecificTime" type="xs:dateTime"/>

<xs:element maxOccurs="1" minOccurs="0" name="Base64Content" type="xs:base64Binary"/>

</xs:choice>

</xs:complexType>

Each child element of UseVerificationTimeType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component UseVerificationTime XML schema details]

#### JSON Syntax

The UseVerificationTimeType JSON object SHALL implement in JSON syntax the requirements defined in the UseVerificationTime component.

The UseVerificationTimeType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-UseVerificationTimeType": {

"type": "object",

"properties": {

"currTime": {

"type": "boolean",

"default": "false"

},

"specTime": {

"type": "integer",

"format": "utc-millisec"

},

"b64Content": {

"type": "string"

}

},

"minProperties": 1,

"maxProperties": 1

}

Properties in the JSON schema above SHALL implement sub-component of UseVerificationTime component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| CurrentTime | currTime | [] |
| SpecificTime | specTime | [] |
| Base64Content | b64Content | [] |

[component UseVerificationTime JSON schema details]

### Component AdditionalTimeInfo

**Semantics**

The AdditionalTimeInfo component contains other time instant(s) relevant in the context of the verification time determination.

Below follows a list of the sub-components that MAY be present within this component:

* The value element MUST contain one instance of a date/time value. [sub component value details]
* The Type element MUST contain one instance of an URI. Its value is limited to item of the following set:  
  urn:oasis:names:tc:dss:1.0:additionaltimeinfo:signatureTimestamp  
  urn:oasis:names:tc:dss:1.0:additionaltimeinfo:signatureTimemark  
  urn:oasis:names:tc:dss:1.0:additionaltimeinfo:signedObjectTimestamp  
  urn:oasis:names:tc:dss:1.0:additionaltimeinfo:claimedSigningTime  
  The Type attribute qualifies the kind of time information included in the response. This specification defines the listed types, whose values MUST satisfy the format defined as xs:dateTime and SHOULD be expressed as UTC time (Coordinated Universal Time). Profiles MAY include and define new values for the Type attribute.
* The optional Ref element MUST contain one instance of a string. It allows to establish references to the source of the time information, and SHOULD be used when there is a need to disambiguate several AdditionalTimeInfo components with the same Type attribute.

Non-normative Comment:

[component AdditionalTimeInfo non normative details]

#### XML Syntax

The XML type AdditionalTimeInfoType SHALL implement the requirements defined in the AdditionalTimeInfo component.

The AdditionalTimeInfoType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="AdditionalTimeInfoType">

<xs:simpleContent>

<xs:extension base="xs:dateTime">

<xs:attribute name="Type" use="required">

<xs:simpleType>

<xs:restriction base="xs:anyURI">

<xs:enumeration value="urn:oasis:names:tc:dss:1.0:additionaltimeinfo:signatureTimestamp"/>

<xs:enumeration value="urn:oasis:names:tc:dss:1.0:additionaltimeinfo:signatureTimemark"/>

<xs:enumeration value="urn:oasis:names:tc:dss:1.0:additionaltimeinfo:signedObjectTimestamp"/>

<xs:enumeration value="urn:oasis:names:tc:dss:1.0:additionaltimeinfo:claimedSigningTime"/>

</xs:restriction>

</xs:simpleType>

</xs:attribute>

<xs:attribute name="Ref" type="xs:string" use="optional"/>

</xs:extension>

</xs:simpleContent>

</xs:complexType>

Each child element of AdditionalTimeInfoType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name. The element 'value' holding a date/time is represented by the component's XML tag text content.

[component AdditionalTimeInfo XML schema details]

#### JSON Syntax

The AdditionalTimeInfoType JSON object SHALL implement in JSON syntax the requirements defined in the AdditionalTimeInfo component.

The AdditionalTimeInfoType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-AdditionalTimeInfoType": {

"type": "object",

"properties": {

"value": {

"type": "integer",

"format": "utc-millisec"

},

"type": {

"type": "string",

"format": "uri"

},

"ref": {

"type": "string"

}

},

"required": ["type"]

}

Properties in the JSON schema above SHALL implement sub-component of AdditionalTimeInfo component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| value | value | [] |
| Type | type | [] |
| Ref | ref | [] |

[component AdditionalTimeInfo JSON schema details]

### Component VerificationTimeInfo

**Semantics**

The VerificationTimeInfo component allows the client to obtain the time instant used by the server to validate the signature.

Below follows a list of the sub-components that MAY be present within this component:

* The VerificationTime element MUST contain one instance of a date/time value. This time instant used by the server when verifying the signature. It SHOULD be expressed as UTC time (Coordinated Universal Time) to reduce confusion with the local time zone use.
* The optional AdditionalTimeInfo element MAY occur zero or more times containing a sub-component. If present each instance MUST satisfy the requirements specified in this document in section AdditionalTimeInfo. The AdditionalTimeInfo element can contain any other time instant(s) relevant in the context of the verification time determination.

Non-normative Comment:

[component VerificationTimeInfo non normative details]

#### XML Syntax

The XML type VerificationTimeInfoType SHALL implement the requirements defined in the VerificationTimeInfo component.

The VerificationTimeInfoType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="VerificationTimeInfoType">

<xs:sequence>

<xs:element name="VerificationTime" type="xs:dateTime"/>

<xs:element maxOccurs="unbounded" minOccurs="0" name="AdditionalTimeInfo" type="dss:AdditionalTimeInfoType"/>

</xs:sequence>

</xs:complexType>

Each child element of VerificationTimeInfoType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component VerificationTimeInfo XML schema details]

#### JSON Syntax

The VerificationTimeInfoType JSON object SHALL implement in JSON syntax the requirements defined in the VerificationTimeInfo component.

The VerificationTimeInfoType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-VerificationTimeInfoType": {

"type": "object",

"properties": {

"verificationTime": {

"type": "integer",

"format": "utc-millisec"

},

"additionalTimeInfo": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-AdditionalTimeInfoType"

}

}

},

"required": ["verificationTime"]

}

Properties in the JSON schema above SHALL implement sub-component of VerificationTimeInfo component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| VerificationTime | verificationTime | [] |
| AdditionalTimeInfo | additionalTimeInfo | [] |

[component VerificationTimeInfo JSON schema details]

### Component AdditionalKeyInfo

**Semantics**

The AdditionalKeyInfo component provides the server with additional data (such as certificates and CRLs) which it can use to validate the signature.

Below follows a list of the sub-components that MAY be present within this component:

* The X509CRL element MUST contain one instance of base64 encoded binary data. In addition to the elements included in component KeySelector the X509CRL element holds a CRL.

A set of sub-components is inherited from component KeySelector and is not repeated here.

Non-normative Comment:

[component AdditionalKeyInfo non normative details]

#### XML Syntax

The XML type AdditionalKeyInfoType SHALL implement the requirements defined in the AdditionalKeyInfo component.

The AdditionalKeyInfoType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="AdditionalKeyInfoType">

<xs:complexContent>

<xs:extension base="dss:KeySelectorType">

<xs:choice>

<xs:element name="X509CRL" type="xs:base64Binary"/>

</xs:choice>

</xs:extension>

</xs:complexContent>

</xs:complexType>

Each child element of AdditionalKeyInfoType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component AdditionalKeyInfo XML schema details]

#### JSON Syntax

The AdditionalKeyInfoType JSON object SHALL implement in JSON syntax the requirements defined in the AdditionalKeyInfo component.

The AdditionalKeyInfoType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-AdditionalKeyInfoType": {

"type": "object",

"properties": {

"x509Digest": {

"type": "object",

"$ref": "#/definitions/dss-X509DigestType"

},

"subject": {

"type": "string"

},

"ski": {

"type": "string"

},

"cert": {

"type": "string"

},

"name": {

"type": "string"

},

"X509CRL": {

"type": "string"

}

}

}

Properties in the JSON schema above SHALL implement sub-component of AdditionalKeyInfo component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| X509Digest | x509Digest | [] |
| X509SubjectName | subject | [] |
| X509SKI | ski | [] |
| X509Certificate | cert | [] |
| KeyName | name | [] |
| X509CRL | X509CRL | [] |

[component AdditionalKeyInfo JSON schema details]

### Component ProcessingDetails

**Semantics**

The ProcessingDetails component elaborates on what signature verification steps succeeded or failed.

Below follows a list of the sub-components that MAY be present within this component:

* The optional ValidDetail element MAY occur zero or more times containing a sub-component. If present each instance MUST satisfy the requirements specified in this document in section Detail. The ValidDetail element holds verification details that were evaluated and found to be valid.
* The optional IndeterminateDetail element MAY occur zero or more times containing a sub-component. If present each instance MUST satisfy the requirements specified in this document in section Detail. The IndeterminateDetail element holds verification details that could not be evaluated or were evaluated and returned an indeterminate result.
* The optional InvalidDetail element MAY occur zero or more times containing a sub-component. If present each instance MUST satisfy the requirements specified in this document in section Detail. The optional InvalidDetail element holds verification details that were evaluated and found to be invalid.

Non-normative Comment:

[component ProcessingDetails non normative details]

#### XML Syntax

The XML type ProcessingDetailsType SHALL implement the requirements defined in the ProcessingDetails component.

The ProcessingDetailsType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="ProcessingDetailsType">

<xs:sequence>

<xs:element maxOccurs="unbounded" minOccurs="0" name="ValidDetail" type="dss:DetailType"/>

<xs:element maxOccurs="unbounded" minOccurs="0" name="IndeterminateDetail" type="dss:DetailType"/>

<xs:element maxOccurs="unbounded" minOccurs="0" name="InvalidDetail" type="dss:DetailType"/>

</xs:sequence>

</xs:complexType>

Each child element of ProcessingDetailsType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component ProcessingDetails XML schema details]

#### JSON Syntax

The ProcessingDetailsType JSON object SHALL implement in JSON syntax the requirements defined in the ProcessingDetails component.

The ProcessingDetailsType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-ProcessingDetailsType": {

"type": "object",

"properties": {

"valid": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-DetailType"

}

},

"indeterminate": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-DetailType"

}

},

"invalid": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dss-DetailType"

}

}

}

}

Properties in the JSON schema above SHALL implement sub-component of ProcessingDetails component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| ValidDetail | valid | [] |
| IndeterminateDetail | indeterminate | [] |
| InvalidDetail | invalid | [] |

[component ProcessingDetails JSON schema details]

### Component Detail

**Semantics**

[component Detail normative details]

Below follows a list of the sub-components that MAY be present within this component:

* The optional Code element MUST contain an URI. This URI which more precisely specifies why this detail is valid, invalid, or indeterminate. It must be a value defined by some other specification, since this specification defines no values for this element.
* The optional Message element MUST contain a sub-component. A given element MUST satisfy the requirements specified in this document in section InternationalString. This is a human-readable message which MAY be logged, used for debugging, etc.
* The optional Base64Content element MUST contain base64 encoded binary data.
* The Type element MUST contain one instance of an URI. The Type URI identifies the detail. It may be a value defined by this specification, or a value defined by some other specification. Multiple detail elements of the same Type may appear in a single ProcessingDetails component. For example, when a signature contains a certificate chain that certifies the signing key, there may be details of the same Type present for each certificate in the chain, describing how each certificate was processed.

Non-normative Comment:

[component Detail non normative details]

#### XML Syntax

The XML type DetailType SHALL implement the requirements defined in the Detail component.

The DetailType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="DetailType">

<xs:sequence>

<xs:element minOccurs="0" name="Code" type="xs:anyURI"/>

<xs:element minOccurs="0" name="Message" type="dss:InternationalStringType"/>

<xs:element maxOccurs="1" minOccurs="0" name="Base64Content" type="xs:base64Binary"/>

</xs:sequence>

<xs:attribute name="Type" type="xs:anyURI" use="required"/>

</xs:complexType>

Each child element of DetailType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component Detail XML schema details]

#### JSON Syntax

The DetailType JSON object SHALL implement in JSON syntax the requirements defined in the Detail component.

The DetailType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-DetailType": {

"type": "object",

"properties": {

"code": {

"type": "string"

},

"msg": {

"type": "object",

"$ref": "#/definitions/dss-InternationalStringType"

},

"b64Content": {

"type": "string"

},

"type": {

"type": "string",

"format": "uri"

}

},

"required": ["type"]

}

Properties in the JSON schema above SHALL implement sub-component of Detail component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| Code | code | [] |
| Message | msg | [] |
| Base64Content | b64Content | [] |
| Type | type | [] |

[component Detail JSON schema details]

### Component SigningTimeInfo

**Semantics**

This SigningTimeInfo component allows the client to obtain the time instant associated to the signature creation.

Below follows a list of the sub-components that MAY be present within this component:

* The SigningTime element MUST contain one instance of a date/time value. This element returns the time value considered by the server to be the signature creation time.
* The optional SigningTimeBoundaries element MUST contain sub-components. This element returns the trusted time values considered as lower and upper limits for the signing time.
* The optional LowerBoundary element MUST contain a date/time value. The SigningTimeBoundaries element MUST contain at least one of the LowerBoundary or UpperBoundary elements.
* The optional UpperBoundary element MUST contain a date/time value. The SigningTimeBoundaries element MUST contain at least one of the LowerBoundary or UpperBoundary elements

Non-normative Comment:

[component SigningTimeInfo non normative details]

#### XML Syntax

The XML type SigningTimeInfoType SHALL implement the requirements defined in the SigningTimeInfo component.

The SigningTimeInfoType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="SigningTimeInfoType">

<xs:sequence>

<xs:element name="SigningTime" type="xs:dateTime"/>

<xs:element minOccurs="0" name="SigningTimeBoundaries">

<xs:complexType>

<xs:sequence>

<xs:element minOccurs="0" name="LowerBoundary" type="xs:dateTime"/>

<xs:element minOccurs="0" name="UpperBoundary" type="xs:dateTime"/>

</xs:sequence>

</xs:complexType>

</xs:element>

</xs:sequence>

</xs:complexType>

Each child element of SigningTimeInfoType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component SigningTimeInfo XML schema details]

#### JSON Syntax

The SigningTimeInfoType JSON object SHALL implement in JSON syntax the requirements defined in the SigningTimeInfo component.

The SigningTimeInfoType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-SigningTimeInfoType": {

"type": "object",

"properties": {

"signingTime": {

"type": "integer",

"format": "utc-millisec"

},

"signingTimeBounds": {

"type": "object",

"$ref": "#/definitions/dss-SigningTimeInfoType:SigningTimeBoundaries"

}

},

"required": ["signingTime"]

}

"dss-SigningTimeInfoType:SigningTimeBoundaries": {

"type": "object",

"properties": {

"lowerBound": {

"type": "integer",

"format": "utc-millisec"

},

"upperBound": {

"type": "integer",

"format": "utc-millisec"

}

}

}

Properties in the JSON schema above SHALL implement sub-component of SigningTimeInfo component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| SigningTime | signingTime | [] |
| SigningTimeBoundaries | signingTimeBounds | [] |
| LowerBoundary | lowerBound | [] |
| UpperBoundary | upperBound | [] |

[component SigningTimeInfo JSON schema details]

### Component UpdatedSignature

**Semantics**

The UpdatedSignature component contains the resulting updated signature or timestamp or, in the case of a signature being enveloped in an output document, a pointer to the signature.

Below follows a list of the sub-components that MAY be present within this component:

* The SignatureObject element MUST contain one instance of a sub-component. This element MUST satisfy the requirements specified in this document in section SignatureObject. This element contains an updated signature or timestamp.
* The optional Type element MUST contain one instance of an URI. [sub component Type details]

Non-normative Comment:

[component UpdatedSignature non normative details]

#### XML Syntax

The XML type UpdatedSignatureType SHALL implement the requirements defined in the UpdatedSignature component.

The UpdatedSignatureType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="UpdatedSignatureType">

<xs:sequence>

<xs:element name="SignatureObject" type="dss:SignatureObjectType"/>

</xs:sequence>

<xs:attribute name="Type" type="xs:anyURI" use="optional"/>

</xs:complexType>

Each child element of UpdatedSignatureType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component UpdatedSignature XML schema details]

#### JSON Syntax

The UpdatedSignatureType JSON object SHALL implement in JSON syntax the requirements defined in the UpdatedSignature component.

The UpdatedSignatureType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-UpdatedSignatureType": {

"type": "object",

"properties": {

"sigObj": {

"type": "object",

"$ref": "#/definitions/dss-SignatureObjectType"

},

"type": {

"type": "string",

"format": "uri"

}

},

"required": ["sigObj"]

}

Properties in the JSON schema above SHALL implement sub-component of UpdatedSignature component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| SignatureObject | sigObj | [] |
| Type | type | [] |

[component UpdatedSignature JSON schema details]

### Component ReturnTransformedDocument

**Semantics**

The ReturnTransformedDocument component instructs the server to return an input document to which the XML signature transforms specified by a particular <ds:Reference> have been applied. The <ds:Reference> is indicated by the zero-based WhichReference attribute (0 means the first <ds:Reference> in the signature, 1 means the second, and so on). Multiple occurrences of this optional input can be present in a single verify request message. Each occurrence will generate a corresponding optional output.

Below follows a list of the sub-components that MAY be present within this component:

* The WhichReference element MUST contain one instance of an integer. To match outputs to inputs, each TransformedDocument will contain a WhichReference attribute which matches the corresponding optional input.

Non-normative Comment:

[component ReturnTransformedDocument non normative details]

#### XML Syntax

The XML type ReturnTransformedDocumentType SHALL implement the requirements defined in the ReturnTransformedDocument component.

The ReturnTransformedDocumentType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="ReturnTransformedDocumentType">

<xs:attribute name="WhichReference" type="xs:integer" use="required"/>

</xs:complexType>

Each child element of ReturnTransformedDocumentType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component ReturnTransformedDocument XML schema details]

#### JSON Syntax

The ReturnTransformedDocumentType JSON object SHALL implement in JSON syntax the requirements defined in the ReturnTransformedDocument component.

The ReturnTransformedDocumentType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-ReturnTransformedDocumentType": {

"type": "object",

"properties": {

"whichRef": {

"type": "integer"

}

},

"required": ["whichRef"]

}

Properties in the JSON schema above SHALL implement sub-component of ReturnTransformedDocument component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| WhichReference | whichRef | [] |

[component ReturnTransformedDocument JSON schema details]

### Component TransformedDocument

**Semantics**

The TransformedDocument component contains a document corresponding to the specified <ds:Reference>, after all the transforms in the reference have been applied.

Below follows a list of the sub-components that MAY be present within this component:

* The Document element MUST contain one instance of a sub-component. This element MUST satisfy the requirements specified in this document in section Document. This element contains the transformed document.
* The WhichReference element MUST contain one instance of an integer. To match outputs to inputs, each TransformedDocument will contain a WhichReference element which matches the corresponding optional input.

Non-normative Comment:

[component TransformedDocument non normative details]

#### XML Syntax

The XML type TransformedDocumentType SHALL implement the requirements defined in the TransformedDocument component.

The TransformedDocumentType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="TransformedDocumentType">

<xs:sequence>

<xs:element name="Document" type="dss:DocumentType"/>

</xs:sequence>

<xs:attribute name="WhichReference" type="xs:integer" use="required"/>

</xs:complexType>

Each child element of TransformedDocumentType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component TransformedDocument XML schema details]

#### JSON Syntax

The TransformedDocumentType JSON object SHALL implement in JSON syntax the requirements defined in the TransformedDocument component.

The TransformedDocumentType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dss-TransformedDocumentType": {

"type": "object",

"properties": {

"doc": {

"type": "object",

"$ref": "#/definitions/dss-DocumentType"

},

"whichRef": {

"type": "integer"

}

},

"required": ["doc", "whichRef"]

}

Properties in the JSON schema above SHALL implement sub-component of TransformedDocument component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| Document | doc | [] |
| WhichReference | whichRef | [] |

[component TransformedDocument JSON schema details]

## Referenced Structure Models from other documents

### Component Transforms

**Semantics**

The XML element is defined in the XML namespace http://www.w3.org/2000/09/xmldsig# .

[component Transforms normative details]

Below follows a list of the sub-components that MAY be present within this component:

* The Transform element MUST occur 1 or more times containing sub-component. Each instance MUST satisfy the requirements specified in section Transform. [sub component Transform details]

Non-normative Comment:

[component Transforms non normative details]

#### XML Syntax

The XML type TransformsType SHALL implement the requirements defined in the Transforms component.

The TransformsType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<complexType name="TransformsType">

<sequence>

<xs:element maxOccurs="unbounded" ref="ds:Transform"/>

</sequence>

</complexType>

Each child element of TransformsType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component Transforms XML schema details]

#### JSON Syntax

The TransformsType JSON object SHALL implement in JSON syntax the requirements defined in the Transforms component.

The TransformsType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dsig-TransformsType": {

"type": "object",

"properties": {

"transform": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dsig-TransformType"

}

}

},

"required": ["transform"]

}

Properties in the JSON schema above SHALL implement sub-component of Transforms component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| Transform | transform | [] |

[component Transforms JSON schema details]

### Component Transform

**Semantics**

The XML element is defined in the XML namespace http://www.w3.org/2000/09/xmldsig# .

[component Transform normative details]

Below follows a list of the sub-components that MAY be present within this component:

* The optional value element MUST contain a string. [sub component value details]
* The optional Base64Content element MUST contain base64 encoded binary data.
* The optional XPath element MAY occur zero or more times containing a string. [sub component XPath details]
* The optional NsURIMapping element MAY occur zero or more times containing sub-component. If present each instance MUST satisfy the requirements specified in section NsURIMapping. [sub component NsURIMapping details]
* The Algorithm element MUST contain one instance of a string. [sub component Algorithm details]

Non-normative Comment:

[component Transform non normative details]

#### XML Syntax

The XML type TransformType SHALL implement the requirements defined in the Transform component.

The TransformType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="TransformType">

<xs:sequence>

<xs:element maxOccurs="1" minOccurs="0" name="value" type="string"/>

<xs:element maxOccurs="1" minOccurs="0" name="Base64Content" type="xs:base64Binary"/>

<xs:element maxOccurs="unbounded" minOccurs="0" name="XPath" type="string"/>

<xs:element maxOccurs="unbounded" minOccurs="0" name="NsURIMapping" type="ds:NsURIMappingType"/>

</xs:sequence>

<xs:attribute name="Algorithm" type="xs:string" use="required"/>

</xs:complexType>

Each child element of TransformType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component Transform XML schema details]

#### JSON Syntax

The TransformType JSON object SHALL implement in JSON syntax the requirements defined in the Transform component.

The TransformType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dsig-TransformType": {

"type": "object",

"properties": {

"value": {

"type": "string"

},

"b64Content": {

"type": "string"

},

"xpath": {

"type": "array",

"items": {

"type": "string"

}

},

"nsDecl": {

"type": "array",

"items": {

"type": "object",

"$ref": "#/definitions/dsig-NsURIMappingType"

}

},

"algo": {

"type": "string"

}

},

"required": ["algo"]

}

Properties in the JSON schema above SHALL implement sub-component of Transform component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| value | value | [] |
| Base64Content | b64Content | [] |
| XPath | xpath | [] |
| NsURIMapping | nsDecl | [] |
| Algorithm | algo | [] |

[component Transform JSON schema details]

### Component NsURIMapping

**Semantics**

The XML element is defined in the XML namespace http://www.w3.org/2000/09/xmldsig# .

The component allows to define additional namespace prefix to URI mappings. In non-XML environments (e.g. JSON) the mappings (e.g. for XPath evaluations) cannot be embedded seamlessly. This element is a new auxiliary structure within the XMLDSig namespace necessary to support the evaluation of XPath expressions while using Non-XML data formats.

Below follows a list of the sub-components that MAY be present within this component:

* The NamespacePrefix element MUST contain one instance of a string. This element defines the namespace prefix part of this component’s assignment.
* The NamespaceURI element MUST contain one instance of an URI. This element defines the namespace URI part of this component’s assignment.

Non-normative Comment:

[component NsURIMapping non normative details]

#### XML Syntax

The XML type NsURIMappingType SHALL implement the requirements defined in the NsURIMapping component.

The NsURIMappingType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:complexType name="NsURIMappingType">

<xs:sequence>

<xs:element name="NamespacePrefix" type="xs:string"/>

<xs:element name="NamespaceURI" type="xs:anyURI"/>

</xs:sequence>

</xs:complexType>

Each child element of NsURIMappingType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

[component NsURIMapping XML schema details]

#### JSON Syntax

The NsURIMappingType JSON object SHALL implement in JSON syntax the requirements defined in the NsURIMapping component.

The NsURIMappingType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"dsig-NsURIMappingType": {

"type": "object",

"properties": {

"ns": {

"type": "string"

},

"uri": {

"type": "string"

}

},

"required": ["ns", "uri"]

}

Properties in the JSON schema above SHALL implement sub-component of NsURIMapping component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| NamespacePrefix | ns | [] |
| NamespaceURI | uri | [] |

[component NsURIMapping JSON schema details]

### Component NameID

**Semantics**

The XML element is defined in the XML namespace urn:oasis:names:tc:SAML:2.0:assertion .

The NameID component is used when an element serves to represent an entity by a string-valued name.

Below follows a list of the sub-components that MAY be present within this component:

* The value element MUST contain one instance of a string. In non-XML representations the value element contains the actual identifier
* The optional Format element MUST contain one instance of an URI. The Format element represents the classification of string-based identifier information.
* The optional SPProvidedID element MUST contain one instance of a string. The SPProvidedID element defines the alternative identifier of the principal most recently set by the service provider or affiliation, if any
* The optional NameQualifier element MUST contain one instance of a string. The NameQualifier element contains the security or administrative domain that qualifies the name. This attribute provides a means to federate names from disparate user stores without collision.
* The optional SPNameQualifier element MUST contain one instance of a string. The SPNameQualifier element further qualifies a name with the name of a service provider or affiliation of providers. This attribute provides an additional means to federate names on the basis of the relying party or parties.

Non-normative Comment:

[component NameID non normative details]

#### XML Syntax

The XML type NameIDType SHALL implement the requirements defined in the NameID component.

The NameIDType XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<complexType name="NameIDType">

<simpleContent>

<extension base="string">

<attributeGroup ref="saml2:IDNameQualifiers"/>

<xs:attribute name="Format" type="anyURI" use="optional"/>

<xs:attribute name="SPProvidedID" type="string" use="optional"/>

</extension>

</simpleContent>

</complexType>

Each child element of NameIDType XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name. The element 'value' is represented by the component's XML tag text content.

[component NameID XML schema details]

#### JSON Syntax

The NameIDType JSON object SHALL implement in JSON syntax the requirements defined in the NameID component.

The NameIDType JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"saml2-NameIDType": {

"type": "object",

"properties": {

"value": {

"type": "string"

},

"format": {

"type": "string"

},

"provId": {

"type": "string"

},

"nameQual": {

"type": "string"

},

"spNameQual": {

"type": "string"

}

}

}

Properties in the JSON schema above SHALL implement sub-component of NameID component mapped by names as shown in the table below.

|  |  |  |
| --- | --- | --- |
| Element | Implementing JSON member name | Comments |
| value | value | [] |
| Format | format | [] |
| SPProvidedID | provId | [] |
| NameQualifier | nameQual | [] |
| SPNameQualifier | spNameQual | [] |

[component NameID JSON schema details]

Optional input SignaturePlacement is used to request the creation of an XMLSig enveloped signature placed within an input document. The resulting document with the enveloped signature is placed in the optional output DocumentWithSignature.

The server places the signature in the document identified using the WhichDocument attribute.

In the case of a non-XML input document then the server will return an error unless alternative procedures are defined by a profile or in the server policy for handling such a situation.

The DocumentHash component represents a document that will not be transported to the server but just the calculated digest of it. This may be useful to limit the amount of data transferred or to ensure privacy of the document.

The IncludeObject component is used to request the creation of an enveloping signature as follows. Multiple occurrences of this optional input can be present in a single SignRequest message. Each occurrence will cause the inclusion of an object inside the signature being created.

The SignaturePlacement component is used to request the creation of an XMLSig enveloped signature placed within an input document. The resulting document with the enveloped signature is placed in the optional output DocumentWithSignature element. The server places the signature in the document identified using the WhichDocument attribute.

In the case of a non-XML input document then the server will return an error unless alternative procedures are defined by a profile or in the server policy for handling such a situation.

All request messages can contain an OptionalInputSign or OptionalInputVerify element depending on the method called. The OptionalInputsBase component defines the elements that are common to all input inputs. Several optional inputs are defined in this document, and profiles can define additional ones.

The OptionalInputsSign component contains additional inputs associated with the processing of a signing request. Profiles MAY specify the allowed optional inputs and their default values. The definition of an optional input MAY include a default value, so that a client may omit the OptionalInputsSign yet still get service from any profile-compliant DSS server.

If a server doesn’t recognize or can’t handle any optional input, it MUST reject the request with a ResultMajor code of RequesterError and a ResultMinor code of NotSupported.

The OptionalInputsVerify component contains additional inputs associated with the processing of a verification request. Profiles MAY specify the allowed optional inputs and their default values. The definition of an optional input MAY include a default value, so that a client may omit the OptionalInputsVerify yet still get service from any profile-compliant DSS server.

If a server doesn’t recognize or can’t handle any optional input, it MUST reject the request with a ResultMajor code of RequesterError and a ResultMinor code of NotSupported.

This element indicates the identity of the client who is making a request. The server may use this to parameterize any aspect of its processing. Profiles that make use of this element MUST define its semantics.

All request messages can contain an OptionalInputSign or OptionalInputVerify element depending on the method called. The OptionalInputsBase component defines the elements that are common to all input inputs. Several optional inputs are defined in this document, and profiles can define additional ones.

The OptionalInputsSign component contains additional inputs associated with the processing of a signing request. Profiles MAY specify the allowed optional inputs and their default values. The definition of an optional input MAY include a default value, so that a client may omit the OptionalInputsSign yet still get service from any profile-compliant DSS server.

If a server doesn’t recognize or can’t handle any optional input, it MUST reject the request with a ResultMajor code of RequesterError and a ResultMinor code of NotSupported.

The OptionalInputsVerify component contains additional inputs associated with the processing of a signing request. Profiles MAY specify the allowed optional inputs and their default values. The definition of an optional input MAY include a default value, so that a client may omit the OptionalInputsVerify yet still get service from any profile-compliant DSS server.

If a server doesn’t recognize or can’t handle any optional input, it MUST reject the request with a ResultMajor code of RequesterError and a ResultMinor code of NotSupported.

# The Processing Model Signing

The following process diagram illustrates the major buildings blocks of the processing of a signing request. The sub processes are described in the next chapters.



Figure 1

The workflow splits into the sections for XMLDSig and CMS signature processing. The signature will be selected by the server considering a given SignatureType element of OptionalInputsSign (see section 3.1.14) and its configuration and policies.

If the element AddTimestamp of OptionalInputsSign is set to ‘true’ the sub-process ‘add Timestamp’ adds a timestamp to the signature.

The task of building the SignResponse (see section 3.1.24) is shared between all signature formats.

## Processing for XML Signatures

The first sub-process ‘process references’ of the XML signature creation is the processing of the references. The second sub-process handles the creation of the XML signature. These two sub-processes are described in detail below.

If the element CreateEnvelopedSignature of SignaturePlacement (see section 3.1.33) is set to true the signature will be inserted into the document and location selected by SignaturePlacement.

### Sub process ‘process references’

The following process diagram illustrates the processing steps for the assembly of references.



Figure 2

If the optional input SignedReferences is present (see section 3.1.35) each SignedReference element (see section 3.1.36) controls the creation of a corresponding <ds:Reference>. The task ‘collect references’ handles the SignedReferences.

Otherwise there will be a <ds:Reference> element for each given input documents. The set of transforms and their parameter will be selected by the server. The task ‘use default transforms’ select this set of <ds:Reference>.

Note: Transforms can be applied as a server implementation MAY choose to increase robustness of the Signatures created. These Transforms may reflect idiosyncrasies of different parsers or solve encoding issues or the like. Servers MAY choose not to apply transforms in basic processing and extract the binary data for direct hashing or canonicalize the data directly if certain optional inputs are not to be implemented.

If the element CreateEnvelopedSignature of SignaturePlacement (see section 3.1.33) is set to true the list of transforms will be prepended with an EnvelopedSignatureTransform entry. The task ‘add EnvelopedSignatureTransform’ processes the corresponding <ds:Reference>.

The RefURI attribute of <ds:Reference> element MUST be set to include a “same-document” URI which references either:

* The whole Document containing the signature (by using a RefURI=””)
* The relevant parts of the Document to be covered/protected by the signature (by using a “same-document” RefURI attribute having a value starting with “#”, like RefURI=”#some-id”, RefURI=”#xpointer(/)”, RefURI=”#xpointer(/DocumentElement/ToBeSignedElement)” or the like).  
  If the result of evaluating the expression included in the RefURI attribute doesn’t fit in any of the options described above, the server MUST reject the request using a ResultMajor RequesterError which MAY be qualified by a ResultMinor urn:oasis:names:tc:dss:1.0:resultminor:InvalidRefURI.

This aligment will be performed by the task ‘align same-doc references’.

### Sub process ‘create XML signature’



Figure 3

The first task (‘calculate remaining transforms’) of this section applies the given set of transforms. If a TransformedData (see section 3.1.7) element is provided by the client these calculations MUST be respected and just the remaining set of transforms must be processed by the server. The case of a Document (see section3.1.5) as base for a reference processing all transform steps MUST be applied.

Note: As required in **[XMLDSIG]** if the end result is an XML node set, the server MUST attempt to convert the node set back into an octet stream using Canonical XML **[XML-C14N]**.

The ‘calculate / use given hash’ task computes the digest upon the transformation output. If a DocumentHash (see section 3.1.8) element is provided by the client the hash values are used as input for the following steps. The DocumentHash MAY contain digests of different algorithms. The server selects the appropriate hash algorithm.

Performing the task ‘build XMLDSig’ the server forms a set of <ds:Reference> with the elements and attributes set as follows:

* If the Document has a RefURI attribute, the <ds:Reference> element’s URI attribute is set to the value of the RefURI attribute, else this attribute is omitted.   
  A signature MUST NOT be created if more than one RefURI is omitted in the set of input documents and the server MUST report a RequesterError by setting ResultMajor RequesterError qualified by a ResultMinor.
* If the Document has a RefType attribute, the <ds:Reference> element’s Type attribute is set to the value of the RefType attribute, else this attribute is omitted.
* The <ds:DigestMethod> element is set to the hash method used.
* The <ds:DigestValue> element is set to the hash value that is to be calculated as per **[XMLDSIG]**.
* The <ds:Transforms> element is set to the sequence of transforms applied by the server in step b. This sequence MUST describe the effective transform as a reproducible procedure from parsing until hash.
* References resulting from processing of optional inputs MUST be included. In doing so, the server MAY reflect the ordering of the Document elements.

The server creates an XML signature using these <ds:Reference> elements according to the processing rules in **[XMLDSIG]**.

The last task ‘insert ds:Object’ handles the creation of an enveloping signature. If one or more optional input elements IncludeObject (see section 3.1.32) are present they will cause the inclusion of an object inside the signature being created.

## Processing for CMS Signatures

### Sub process ‘process digest’

The following process diagram illustrates the processing steps required to calculate the digest for a CMS signature.



Figure 4

The SignRequest component MUST contain either a single Document not having RefURI, RefType set or a single DocumentHash component not having RefURI, RefType, Transforms.

If the InputDocuments (see section 3.1.3) component contains a Document element, the server hashes the octet stream represented by the Document. This is performed by the task ‘calculate digest’ If the InputDocuments (see section 3.1.3) component contains a DocumentHash element (see section 3.1.8), the server uses the hash values as an input for the following steps. The DocumentHash MAY contain digests of different algorithms. The server selects the appropriate hash algorithm.

### Sub process ‘create CMS signature’

The following process diagram illustrates the processing steps to create a CMS signature.



Figure 5

If the InputDocuments (see section 3.1.3) component contains a Document element and the IncludeEContent element of the OptionalInputsSign component (see section 3.1.17) is set to true then the task ‘include content’ creates a CMS structure with the document enveloped within the signature. For CMS details in this context please refer to [RFC 3852] sections 5.1 “SignedData Type” and 5.2 “EncapsulatedContentInfo Type”.

Otherwise the resulting signature MUST be detached (aka. external or “without eContent”).

The following task ‘build CMS signature’ builds a SignedData structure containing the SignerInfo computed as follows:

The server forms a SignerInfo structure based on the input document. The components of the SignerInfo are set as follows:

* The digestAlgorithm field is set to the OID value for the hash method that was used in the previous processing step.
* The signedAttributes field’s message-digest attribute contains the hash value that was calculated / provided in previous processing step. Other signedAttributes MAY be added by the server, according to its profile or policy, or according to the Properties optional input (see section 3.1.29).
* The remaining fields (sid, signatureAlgorithm, and signature) are filled in as per a normal CMS signature.

## General processing

### Sub process ‘add Timestamp’

The following process diagram illustrates the processing steps to insert a RFC 3161 timestamp.



Figure 6

If the MimeType element of the Base64Data component (see section 3.1.6) is set to ‘application/pkcs7-signature’ a timestamp token is created and embedded into the existing signature, without verification, which is passed in the InputDocuments component of this SignRequest. Otherwise a timestamp token is created and embedded into the signature being created as part of the processing of this SignRequest.

In both scenarios, the timestamp token created by the server SHALL be created according to [RFC 3161]. The MessageImprint field within the TstInfo structure of the timestamp token will be derived from the signature value of the just-created or incoming signature depending on the scenario. The timestamp SHALL be embedded in the CMS signature as an unsigned attribute with the object identifier (see Appendix A of [RFC 3161]):

{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-aa(2) 14}

The signature and its embedded timestamp is returned in the SignatureObject element of the SignResponse component (see section 3.1.24).

The Type element of the AddTimestamp optional input SHALL be set to:

"urn:ietf:rfc:3161".

If the signature being timestamped is an XML signature then the XML signature MUST contain an RFC 3161, placed in a <xades:EncapsulatedTimeStamp> within a <xades:SignatureTimeStamp> as defined in [XAdES].

Note: The server SHOULD not verify the incoming signature before adding the timestamp. If a client wishes that its signatures be verified as a condition of time stamping, the client SHOULD use the AddTimestamp optional input of the Verify protocol.

# The DSS Verifying Protocol

## Basic Processing for XML Signatures

A DSS server that verifies XML signatures SHOULD perform the following steps, upon receiving a VerifyRequest. These steps may be changed or overridden by the optional inputs, or by the profile or policy the server is operating under. For more details on multi-signature verification, see section 5.3.1.

1. The server retrieves one or more <ds:Signature> objects, as follows: If the SignatureObject is present, the server retrieves either the <ds:Signature> that is a child element of the SignatureObject (see: Note at the end of this section), or those <ds:Signature> objects which are pointed to by the SignaturePtr in the SignatureObject.
   1. If the SignaturePtr points to an input document but not a specific element in that document, the pointed-to input document must be a Document element containing XML.   
      If the SignatureObject is omitted, there MUST be only a single Document element. This case is handled as if a SignaturePtr pointing to the single Document was present: the server will search and find every <ds:Signature> element in this input document, and verify each <ds:Signature> according to the steps below.
2. For each <ds:Reference> in the <ds:Signature>, the server finds the input document with matching RefURI and RefType values (omitted attributes match omitted attributes). If the <ds:Reference> uses a same-document URI, the XPointer should be evaluated against the input document the <ds:Signature> is contained within, or against the <ds:Signature> itself if it is contained within the SignatureObject element. The SchemaRef element or optional input Schema of the input document or SignatureObject will be used, if present, to identify ID attributes when evaluating the XPointer expression. If the <ds:Reference> uses an external URI and the corresponding input document is not present, the server will skip the <ds:Reference>, and later return a result code such as ReferencedDocumentNotPresent to indicate this. The RefURI MAY be omitted in at most one of the set of Input documents.
   1. If the input document is a Document, the server extracts and decodes as described in 4.3.1 Step 1.0 (or equivalent step in variants of the basic process as defined in 4.3.2 onwards depending of the form of the input document).
   2. If the input document is a TransformedData, the server MAY check that the <ds:Transforms> (if supplied) match between the TransformedData and the <ds:Reference> and then hashes the resultant data object according to <ds:DigestMethod>, and MUST check that the result matches <ds:DigestValue>.
   3. If the input document is a DocumentHash, the server MAY check that the <ds:Transforms>, <ds:DigestMethod> (if supplied) and <ds:DigestValue> elements match between the DocumentHash and the <ds:Reference>.
   4. If the combination of RefURI and RefType matches more than one input document all of them MUST be either a TransformedData or a DocumentHash otherwise a RequesterError is issued qualified by result minor of ReferencedDocumentNotPresent.  
      Only one of them is allowed to have a WhichReference value that matches the order of the <ds:Reference> within the <ds:SignedInfo> in question otherwise a RequesterError is issued qualified by result minor of ReferencedDocumentNotPresent. Using this input document either variant b. or c. is applied respectively before continuing with step 3.
3. The server shall verify the validity of the signature at a particular time (i.e. current time, assumed signing time or other time), depending on the server policy. This behavior MAY be altered by using the optional input UseVerificationTime (see section 5.5.2).
4. If the signature validates correctly, the server returns one of the first three ResultMinor codes listed in section 5.4, depending on the relationship of the signature to the input documents (not including the relationship of the signature to those XML elements that were resolved through XPointer evaluation; the client will have to inspect those relationships manually). If the signature fails to validate correctly, the server returns some other code; either one defined in section 5.4 of this specification, or one defined by some profile of this specification.

### Multi-Signature Verification

If a client requests verification of an entire input document, either using a SignaturePtr without an XPath or a missing SignaturePtr (see section 5.3 step 1), then the server MUST determine whether the input document contains zero, one, or more than one <ds:Signature> elements. If zero, the server should return a ResultMajor code of RequesterError.

If more than one <ds:Signature> elements are present, the server MUST either reject the request with a ResultMajor code of RequesterError and a ResultMinor code of NotSupported, or accept the request and try to verify all of the signatures.

If the server accepts the request in the multi-signature case (or if only a single signature is present) and one of the signatures fails to verify, the server should return one of the error codes in section 5.4, reflecting the first error encountered.

If all of the signatures verify correctly, the server should return the Success ResultMajor code and the following ResultMinor code:

urn:oasis:names:tc:dss:1.0:resultminor:ValidMultiSignatures

Note: These procedures only define procedures for handling of multiple signatures on one input document. The procedures for handling multiple signatures on multiple documents are not defined in this core specification, but however such procedures, along with any optional elements that may be required, may be defined in profiles of this specification.

Only certain optional inputs and outputs are allowed when performing multi-signature verification. See section 5.5 for details.

### Signature Timestamp verification procedure

The following sub-sections will describe the processing rules for verifying:

- RFC 3161 timestamp tokens on CMS Signatures

- XML timestamp tokens on XML Signatures

- RFC 3161 timestamp tokens on XML Signatures

This section describes signature timestamp processing when the timestamp is embedded in the incoming signature.

Note: procedures for handling other forms of timestamp may be defined in profiles of the Core. In particular, the DSS AdES profile **[DSS-AdES-P]** defines procedures for handling timestamps against the document being signed, and the DSS Timestamp profile defines procedures for handling standalone timestamps.

For a definition of the Timestamp element see section 6.1 Details of the XML timestamp token can be found in subsection 6.1.1.

#### Processing for RFC 3161 Timestamp tokens on CMS Signatures.

The present section describes the processing rules for verifying a CMS RFC3161 timestamp token passed in on a Verify call within the SignatureObject of the VerifyRequest element. In the CMS case, since the "signature timestamp" is embedded in the signature as an unsigned attribute, only the time stamped signature is required for verification processing. As such, no additional input is required.

The processing by the server is broken down into the following steps:

1. The signature timestamp is embedded in the incoming signature as an unsigned attribute whose object identifier is 1.2.840.11359.1.9.16.2.14. Extract and verify the timestamp token.
2. Verify that the token's public verification certificate is authorized for time stamping by examining the Extended Key Usage field for the presence of the time stamping OID "1.3.6.1.5.5.7.3.8".
3. Validate that the TstInfo structure has a valid layout as defined in **[RFC 3161]**.
4. Extract the MessageImprint hash value and associated algorithm from the TstInfo structure which will be compared against the hash value derived in the next step.
5. Recalculate the hash of the signature value field of the signature in which the timestamp is embedded.
6. Compare the hash values from the two previous steps, and if they are equivalent, then this timestamp is valid for the signature that was time stamped.
7. Verify that the public verification certificate conforms to all relevant aspects of the relying-party's policy including algorithm usage, policy OIDs, time accuracy tolerances, and the Nonce value.
8. Set the Result element as defined in this specification. Minor Error   
   urn:oasis:names:tc:dss:1.0:resultminor:valid:signature:InvalidSignatureTimestamp MAY be used to indicate that the signature is valid but the timestamp against that signature is invalid.

#### Processing for XML timestamp tokens on XML signatures

The present section describes the processing rules for verifying and XML Signature timestamp token embedded within an XML signature using the incorporation mechanisms specified in XAdES (i.e., in the <xades:XMLTimeStamp> <xades:SignatureTimeStamp> element's child). This XML signature may be passed in on a Verify call within the SignatureObject or embedded within a Document’s child.

The server shall verify the timestamp token performing the steps detailed below. If any one of them results in failure, then the timestamp token SHOULD be rejected.

1. Extract the timestamp token embedded in the incoming signature as defined in 4.5.2.3.
2. Verify that the verification key and algorithms used conforms to all relevant aspects of the applicable policy. Should this key come within a public certificate, verify that the certificate conforms to all relevant aspects of the applicable policy including algorithm usage, policy OIDs, and time accuracy tolerances.
3. Verify that the aforementioned verification key is consistent with the ds:SignedInfo/SignatureMethod/@Algorithm attribute value.
4. Verify the timestamp token signature in accordance with the rules defined in **[XMLDSIG]**.
5. Verify that the <ds:SignedInfo> element contains at least two <ds:Reference> elements.
6. Verify that one of the <ds:Reference> elements has its Type attribute set to “urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken”. Take this one and proceed as indicated below:
   1. Retrieve the referenced data object. Verify that it references a <ds:Object> element, which in turn envelopes a <TSTInfo> element.
   2. Verify that the <TSTInfo> element has a valid layout as per the present specification.
   3. Extract the digest value and associated algorithm from its <ds:DigestValue> and <ds:DigestMethod> elements respectively.
   4. Recalculate the digest of the retrieved data object as specified by **[XMLDSIG]** with the digest algorithm indicated in <ds:DigestMethod>, and compare this result with the contents of <ds:DigestValue>.
7. Take each of the other <ds:Reference> elements and for each validate the hash as specified in **[XMLDSIG]**.
8. Check that for one of the <ds:Reference> elements the retrieved data object is actually the <ds:SignatureValue> element and that it contains its digest after canonicalization.
9. Set the Result element as appropriate. Minor Error   
   urn:oasis:names:tc:dss:1.0:resultminor:valid:signature:InvalidSignatureTimestamp MAY be used to indicate that the signature is valid but the timestamp against that signature is invalid.

#### Processing for RFC 3161 timestamp tokens on XML Signatures

The present section describes the processing rules for verifying an RFC 3161 timestamp token embedded within an XML signature as an unsigned property. This XML signature may be passed in on a Verify call within the SignatureObject or embedded within a Document’s child.

The server shall verify the timestamp token performing the steps detailed below. If any one of them results in failure, then the timestamp token SHOULD be rejected.

1. Extract the timestamp token embedded in the incoming signature as defined in 4.5.2.4.
2. Verify that the token's public verification certificate is authorized for time stamping by examining the Extended Key Usage field for the presence of the time stamping OID "1.3.6.1.5.5.7.3.8".
3. Process the signature timestamp as defined in **[XAdES]** Annex G.2.2.16.1.3.
4. Verify that the public verification certificate conforms to all relevant aspects of the relying-party's policy including algorithm usage, policy OIDs, time accuracy tolerances, and the Nonce value.
5. Set the Result element as appropriate.   
   urn:oasis:names:tc:dss:1.0:resultminor:valid:signature:InvalidSignatureTimestamp MAY be used to indicate that the signature is valid but the timestamp against that signature is invalid.

## Basic Processing for CMS Signatures

A DSS server that verifies CMS signatures SHOULD perform the following steps, upon receiving a VerifyRequest. These steps may be changed or overridden by the optional inputs, or by the profile or policy the server is operating under.

1. The server retrieves the CMS signature by decoding the Base64Signature child of SignatureObject.
2. The server retrieves the input data. If the CMS signature is detached, there must be a single input document: i.e. a single Document or DocumentHash element. Otherwise, if the CMS signature is enveloping, it contains its own input data and there MUST NOT be any input documents present.
3. The CMS signature and input data are verified in the conventional way (see **[RFC 3852]** for details).
4. If the signature validates correctly, the server returns the first ResultMinor code listed in section 5.4. If the signature fails to validate correctly, the server returns some other code; either one defined in section 5.4 of this specification, or one defined by some profile of this specification.

## Optional Inputs and Outputs

This section defines some optional inputs and outputs that profiles of the DSS verifying protocol might find useful. Section 2.8 defines some common optional inputs that can also be used with the verifying protocol. Profiles of the verifying protocol can define their own optional inputs and outputs, as well. General handling of optional inputs and outputs is discussed in section 2.7.

### Optional Input VerifyManifests and Output VerifyManifestResults

The presence of this element instructs the server to validate manifests in an XML signature.

On encountering such a document in step 2 of basic processing, the server shall repeat step 2 for all the <ds:Reference> elements within the manifest. In accordance with **[XMLDSIG]** section 5.1, DSS Manifest validation does not affect a signature's core validation. The results of verifying individual <ds:Reference>'s within a <ds:Manifest> are returned in the VerifyManifestResults optional output.   
For example, a client supplies the optional input VerifyManifests, then the returned ResultMinor is urn:oasis:names:tc:dss:1.0:resultminor:valid:hasManifestResults if XMLSig core validation succeeds and the optional output VerifyManifestResults is returned indicating the status of the manifest reference verification. In case of a negative XMLSig core validation no attempt is made to verify manifests.

The VerifyManifests optional input is allowed in multi-signature verification. The VerifyManifestResults is comprised of one or more ManifestResults that contain the following:

ReferenceXpath [Required]

Identifies the manifest reference, in the XML signature, to which this result pertains.

Status [Required]

Indicates the manifest validation result. It takes one of the values urn:oasis:names:tc:dss:1.0:manifeststatus:Valid or urn:oasis:names:tc:dss:1.0:manifeststatus:Invalid.

#### XML Syntax

XML schema snippet defining VerifyManifestResults:

<xs:element name="VerifyManifestResults" type="dss:VerifyManifestResultsType"/>

<xs:complexType name="VerifyManifestResultsType">

<xs:sequence>

<xs:element ref="dss:ManifestResult" maxOccurs="unbounded"/>

</xs:sequence>

</xs:complexType>

<xs:element name="ManifestResult">

<xs:complexType>

<xs:sequence>

<xs:element name="ReferenceXpath" type="xs:string"/>

<xs:element name="Status" type="xs:anyURI"/>

</xs:sequence>

</xs:complexType>

</xs:element>

#### JSON Syntax

Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| ManifestResult | result |
| ReferenceXpath | refXpath |
| Status | status |

### Optional Input UseVerificationTime

This element instructs the server to attempt to determine the signature’s validity at the specified time, instead of a time determined by the server policy.

Note: In order to perform the verification of the signature at a certain time, the server MUST obtain the information necessary to carry out this verification (e.g. CA certificates, CRLs) applicable at that time.

CurrentTime [Optional]

Instructs the server to use its current time (normally the time associated with the server-side request processing).

SpecificTime [Optional]

Allows the client to manage manually the time instant used in the verification process. It SHOULD be expressed as UTC time (Coordinated Universal Time) to reduce confusion with the local time zone use.

Profiles MAY define new child elements associated to other different behaviors.

If the verification time is a significant period in the past the server MAY need to take specific steps for this, and MAY need to ensure that any cryptographic weaknesses over the period do not affect the validation.

This optional input is allowed in multi-signature verification.

#### XML Syntax

XML schema snippet defining VerifyManifestResults:

<xs:element name="UseVerificationTime"/>

<xs:complexType name="UseVerificationTimeType">

<xs:choice>

<xs:element name="CurrentTime"/>

<xs:element name="SpecificTime" type="xs:dateTime"/>

<xs:sequence>

<xs:element name="Base64Content" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>

</xs:sequence>

</xs:choice>

</xs:complexType>

</xs:element>

#### JSON Syntax

Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| CurrentTime | currTime |
| SpecificTime | specTime |
| Base64Content | b64Content |

### Optional Input/Output ReturnVerificationTimeInfo / VerificationTimeInfo

These elements allow the client to obtain the time instant used by the server to validate the signature.

Optionally, in addition to the verification time, the server MAY include in the VerificationTimeInfo response any other relevant time instants that may have been used when determining the verification time or that may be useful for its qualification.

VerificationTime [Required]

The time instant used by the server when verifying the signature. It SHOULD be expressed as UTC time (Coordinated Universal Time) to reduce confusion with the local time zone use.

AdditionalTimeInfo [Optional]

Any other time instant(s) relevant in the context of the verification time determination.

The Type attribute qualifies the kind of time information included in the response. The Ref attribute allows to establish references to the source of the time information, and SHOULD be used when there is a need to disambiguate several AdditionalTimeInfo elements with the same Type attribute.

This specification defines the following base types, whose values MUST be of type xs:dateTime and SHOULD be expressed as UTC time (Coordinated Universal Time). Profiles MAY include and define new values for the Type attribute.

urn:oasis:names:tc:dss:1.0:additionaltimeinfo:signatureTimestamp

The time carried inside a timestamp applied over the signature value.

urn:oasis:names:tc:dss:1.0:additionaltimeinfo:signatureTimemark

The time instant associated to the signature stored in a secure record in the server.

urn:oasis:names:tc:dss:1.0:additionaltimeinfo:signedObjectTimestamp

The time carried inside a timestamp applied over a signed object.

Note that XML Signatures can be produced over multiple objects (via multiple ds:Reference elements), and therefore it's possible to have multiple timestamps, each one applied over each object. In this case, the Ref attribute MUST include the value of the Id attribute of the ds:Reference element.

urn:oasis:names:tc:dss:1.0:additionaltimeinfo:claimedSigningTime

The time claimed by the signer to be the signature creation time.

In the case of multi-signature verification, it’s a matter of server policy as to whether this element is supported.

This optional input is not allowed in multi-signature verification.

#### XML Syntax

XML schema snippet defining VerificationTimeInfo and related structures:

<xs:element type="xs:boolean" name="ReturnVerificationTimeInfo" default="false"/>

<xs:element name="AdditionalTimeInfo" type="dss:AdditionalTimeInfoType"/>

<xs:complexType name="AdditionalTimeInfoType">

<xs:simpleContent>

<xs:extension base="xs:dateTime">

<xs:attribute name="Type" type="xs:anyURI" use="required"/>

<xs:attribute name="Ref" type="xs:string" use="optional"/>

</xs:extension>

</xs:simpleContent>

</xs:complexType>

<xs:element name="VerificationTimeInfo"

type="dss:VerificationTimeInfoType"/>

<xs:complexType name="VerificationTimeInfoType">

<xs:sequence>

<xs:element name="VerificationTime" type="xs:dateTime"/>

<xs:element ref="dss:AdditionalTimeInfo" minOccurs="0"

maxOccurs="unbounded"/>

</xs:sequence>

</xs:complexType>

#### JSON Syntax

Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| Type | type |
| Ref | Ref |
| VerificationTime | verificationTime |
| AdditionalTimeInfo | additionalTimeInfo |

### Optional Input AdditionalKeyInfo

This element provides the server with additional data (such as certificates and CRLs) which it can use to validate the signature.

This optional input is not allowed in multi-signature verification.

#### XML Syntax

XML schema snippet defining AdditionalKeyInfo and related structures:

<xs:element name="AdditionalKeyInfo">

<xs:complexType>

<xs:complexContent>

<xs:extension base="dss:KeyInfoType">

<xs:choice>

<xs:element name="X509CRL" type="xs:base64Binary"/>

</xs:choice>

</xs:extension>

</xs:complexContent>

</xs:complexType>

</xs:element>

#### JSON Syntax

Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| X509CRL | x509CRL |

### Optional Input ReturnProcessingDetails and Output ProcessingDetails

The presence of the ReturnProcessingDetails optional input instructs the server to return a ProcessingDetails output.

These options are not allowed in multi-signature verification.

The ProcessingDetails optional output elaborates on what signature verification steps succeeded or failed. It may contain the following child elements:

ValidDetail [Any Number]

A verification detail that was evaluated and found to be valid.

IndeterminateDetail [Any Number]

A verification detail that could not be evaluated or was evaluated and returned an indeterminate result.

InvalidDetail [Any Number]

A verification detail that was evaluated and found to be invalid.

Each detail element is of type DetailType. A DetailType contains the following child elements and attributes:

Type [Required]

A URI which identifies the detail. It may be a value defined by this specification, or a value defined by some other specification. For the values defined by this specification, see below.

Multiple detail elements of the same Type may appear in a single ProcessingDetails. For example, when a signature contains a certificate chain that certifies the signing key, there may be details of the same Type present for each certificate in the chain, describing how each certificate was processed.

Code [Optional]

A URI which more precisely specifies why this detail is valid, invalid, or indeterminate. It must be a value defined by some other specification, since this specification defines no values for this element.

Message [Optional]

A human-readable message which MAY be logged, used for debugging, etc.

The values for the Type attribute defined by this specification are the following:

urn:oasis:names:tc:dss:1.0:detail:IssuerTrust

Whether the issuer of trust information for the signing key (or one of the certifying keys) is considered to be trustworthy.

urn:oasis:names:tc:dss:1.0:detail:RevocationStatus

Whether the trust information for the signing key (or one of the certifying keys) is revoked.

urn:oasis:names:tc:dss:1.0:detail:ValidityInterval

Whether the trust information for the signing key (or one of the certifying keys) is within its validity interval.

urn:oasis:names:tc:dss:1.0:detail:Signature

Whether the document signature (or one of the certifying signatures) verifies correctly.

urn:oasis:names:tc:dss:1.0:detail:ManifestReference

Whether a manifest reference in the XML signature verified correctly.

#### XML Syntax

XML schema snippet defining ProcessingDetails and related structures:

<xs:element name="ReturnProcessingDetails" type="xs:boolean" default="false"/>

<xs:element name=”ProcessingDetails”>

<xs:complexType>

<xs:sequence>

<xs:element name=”ValidDetail” type=”dss:DetailType”

minOccurs=”0” maxOccurs=”unbounded”/>

<xs:element name=”IndeterminateDetail”

type=”dss:DetailType”

minOccurs=”0” maxOccurs=”unbounded”/>

<xs:element name=”InvalidDetail” type=”xs:dss:DetailType”

minOccurs=”0” maxOccurs=”unbounded”/>

</xs:sequence>

</xs:complexType>

</xs:element>

<xs:complexType name="DetailType">

<xs:sequence>

<xs:element name="Code" type="xs:anyURI" minOccurs="0"/>

<xs:element name="Message" type="dss:InternationalStringType" minOccurs="0"/>

<xs:sequence minOccurs="0" maxOccurs="unbounded">

<xs:element name="Base64Content" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>

</xs:sequence>

</xs:sequence>

<xs:attribute name="Type" type="xs:anyURI" use="required"/>

</xs:complexType>

#### JSON Syntax

Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| ValidDetail | valid |
| IndeterminateDetail | indeterminate |
| InvalidDetail | invalid |
| Code | code |
| Message | msg |
| Base64Content | b64Content |
| Type | type |

### Optional Input ReturnSigningTimeInfo and Output SigningTimeInfo

This element allows the client to obtain the time instant associated to the signature creation.

Note: The signing time may be derived, for example, from a claimed signing time signed signature attribute.

Sometimes, depending on the applicable server policy, this signing time needs to be qualified, in order to avoid unacceptable measurement errors or false claims, using time boundaries associated to trustworthy time values (based on timestamps or time-marks created using trusted time sources). In this case, the server MAY include these values in the LowerBoundary and UpperBoundary elements, respectively.

Criteria for determining when a time instant can be considered trustworthy and for determining the maximum acceptable delays between the signing time and their boundaries (if any) is outside the scope of this specification.

When there's no way for the server to determine the signing time, the server MUST omit the SigningTimeInfo output.

SigningTime [Required]

The time value considered by the server to be the signature creation time.

SigningTimeBoundaries [Optional]

The trusted time values considered as lower and upper limits for the signing time. If this element is present, at least one of the LowerBoundary and UpperBoundary elements MUST be present.

This optional input is not allowed in multi-signature verification.

#### XML Syntax

XML schema snippet defining ProcessingDetails and related structures:

<xs:element name="ReturnSigningTimeInfo" type="xs:boolean" default="false"/>

<xs:element name="SigningTimeInfo" type="dss:SigningTimeInfoType"/>

<xs:complexType name="SigningTimeInfoType">

<xs:sequence>

<xs:element name="SigningTime" type="xs:dateTime"/>

<xs:element name="SigningTimeBoundaries" minOccurs="0">

<xs:complexType>

<xs:sequence>

<xs:element name="LowerBoundary" minOccurs="0"

type="xs:dateTime"/>

<xs:element name="UpperBoundary" minOccurs="0"

type="xs:dateTime"/>

</xs:sequence>

</xs:complexType>

</xs:element>

</xs:sequence>

</xs:complexType>

#### JSON Syntax

Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| SigningTimeInfo | signingTimeInfo |
| SigningTime | signingTime |
| SigningTimeBoundaries | signingTimeBounds |
| LowerBoundary | lowerBound |
| UpperBoundary | upperBound |

### Optional Input ReturnSignerIdentity and Output SignerIdentity

The presence of the ReturnSignerIdentity optional input instructs the server to return a SignerIdentity output.

The SignerIdentity optional output contains an indication of who performed the signature.

This optional input and output are not allowed in multi-signature verification.

#### XML Syntax

XML schema snippet defining SignerIdentity and related structures:

<xs:element name=”ReturnSignerIdentity” type="xs:boolean" default="false"/>

<xs:element name=”SignerIdentity” type=”saml:NameIdentifierType”/>

#### JSON Syntax

Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| SignerIdentity | signerIdentity |

### Optional Input ReturnUpdatedSignature and Outputs DocumentWithSignature, UpdatedSignature

The presence of the ReturnUpdatedSignature optional input instructs the server to return an UpdatedSignature output, containing a new or updated signature.

The Type attribute on ReturnUpdatedSignature, if present, defines exactly what it means to “update” a signature. For example, the updated signature may be the original signature with some additional unsigned signature properties added to it (such as timestamps, counter-signatures, or additional information for use in verification), or the updated signature could be an entirely new signature calculated on the same input documents as the input signature. Profiles that use this optional input MUST define the allowed values and their semantics, and the default value, for the Type attribute (unless only a single type of updated signature is supported, in which case the Type attribute can be omitted).

Multiple occurrences of this optional input can be present in a single verify request message. If multiple occurrences are present, each occurrence MUST have a different Type attribute. Each occurrence will generate a corresponding optional output. These optional outputs SHALL be distinguishable based on their Type attribute, which will match each output with an input.

SignatureObject [Optional]

The resulting updated signature or timestamp or, in the case of a signature being enveloped in an output document, a pointer to the signature. This is used in steps 2. and 3. in the processing described below.

The UpdatedSignature optional output contains the returned signature.

The UpdatedSignatureType is as follows.

These options are not allowed in multi-signature verification.

A DSS server SHOULD perform the following steps, upon receiving a ReturnUpdatedSignature. These steps may be changed or overridden by a profile or policy the server is operating under. (e.g for PDF documents enveloping cms signatures)

1. If the signature to be verified and updated appears within a SignatureObject's <ds:Signature> (detached or enveloping) or Base64Signature then the UpdatedSignature optional output MUST contain the modified SignatureObject with the corresponding <ds:Signature> (detached or enveloping) or Base64Signature child containing the updated signature.
2. If the signature to be verified and updated is enveloped, and if the VerifyRequest contains a SignatureObject with a SignaturePtr pointing to an InputDocument enveloping the signature then the server MUST produce the following TWO optional outputs, first a DocumentWithSignature optional output containing the document that envelopes the updated signature, second an UpdatedSignature optional output containing a SignatureObject having a SignaturePtr element that MUST point to the former DocumentWithSignature.
3. If there is no SignatureObject at all in the request then the server MUST produce only a DocumentWithSignature optional output containing the document with the updated signature.  
   No UpdatedSignature element will be generated.

As DocumentWithSignature appear in steps 2. and 3. of the processing above it is explained here again:

The DocumentWithSignature optional output (for the schema refer to section 4.5.8) contains the input document with the given signature inserted.

It has one child element:

Document [Required]

This returns the given document with a signature inserted in some fashion.

The resulting document with the updated enveloped signature is placed in the optional output DocumentWithSignature. The server places the signature in the document identified using the SignatureObject/SignaturePtr's WhichDocument attribute.

This Document MUST include a same-document RefURI attribute which references the data updated (e.g of the form RefURI).

#### XML Syntax

XML schema snippet defining UpdatedSignature and related structures:

<xs:element name=”ReturnUpdatedSignature”>

<xs:complexType>

<xs:attribute name=”Type” type=”xs:anyURI” use=”optional”/>

</xs:complexType>

</xs:element>

<xs:element name=”UpdatedSignature” type=”dss:UpdatedSignatureType”/>

<xs:coplexType name=”UpdatedSignatureType”>

<xs:sequence>

<xs:element ref="dss:SignatureObject"/>

</xs:sequence>

<xs:attribute name=”Type” type=”xs:anyURI” use=”optional”/>

</xs:complexType>

#### JSON Syntax

Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| Type | type |
| SignatureObject | sigObj |

### Optional Input ReturnTransformedDocument and Output TransformedDocument

The ReturnTransformedDocument optional input instructs the server to return an input document to which the XML signature transforms specified by a particular <ds:Reference> have been applied. The <ds:Reference> is indicated by the zero-based WhichReference attribute (0 means the first <ds:Reference> in the signature, 1 means the second, and so on). Multiple occurrences of this optional input can be present in a single verify request message. Each occurrence will generate a corresponding optional output.

The TransformedDocument optional output contains a document corresponding to the specified <ds:Reference>, after all the transforms in the reference have been applied. In other words, the hash value of the returned document should equal the <ds:Reference> element’s <ds:DigestValue>. To match outputs to inputs, each TransformedDocument will contain a WhichReference attribute which matches the corresponding optional input.

These options are not allowed in multi-signature verification.

#### XML Syntax

XML schema snippet defining TransformedDocument and related structures:

<xs:element name=”ReturnTransformedDocument”>

<xs:complexType>

<xs:attribute name=”WhichReference” type=”xs:integer”

use=”required”/>

</xs:complexType>

</xs:element>

<xs:element name=”TransformedDocument”>

<xs:complexType>

<xs:sequence>

<xs:element ref=”dss:Document”>

</xs:sequence>

</xs:complexType>

<xs:attribute name=”WhichReference” type=”xs:integer”

use=”required”/>

</xs:element>

#### JSON Syntax

Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| WhichReference | whichRef |
| Document | doc |

### Optional Input ReturnTimestampedSignature and Outputs DocumentWithSignature, TimestampedSignature

The ReturnTimestampedSignature element within a VerifyRequest message indicates that the client wishes the server to update the signature after its verification by embedding a signature timestamp token as an unauthenticated attribute (see "unauthAttrs" in section 9.1 [RFC 3852]) or \*unsigned\* property (see section 6.2.5 "The UnsignedSignatureProperties element" and section 7.3 "The SignatureTimeStamp element" [XAdES]) of the supplied signature.

The timestamp token will be on the signature value in the case of CMS/PKCS7signatures or the <ds:SignatureValue> element in the case of XML signatures.

The Type attribute, if present, indicates what type of timestamp to apply. This document defines two values for it, namely:

a. urn:ietf:rfc:3161 for generating a RFC 3161 timestamp token on the signature

b. urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken, for generating a XML timestamp token as defined in section 5.6 of this document.

Profiles that use this optional input MUST define the allowed values, and the default value, for the Type attribute (unless only a single type of timestamp is supported, in which case the Type attribute can be omitted).

A DSS server SHOULD perform the steps 1. - 3. as indicated in 5.5.7.2 upon receiving a ReturnTimeStampedSignature replacing UpdatedSignature by  
TimestampedSignature.

Procedures for handling RFC 3161 and XML timestamps are as defined in section 4.5.2.3.

Note: Procedures for handling other forms of timestamp may be defined in profiles of the Core. In particular, the DSS XAdES profile **[DSS-XAdES-P]** defines procedures for handling timestamps against the document being signed, and the DSS Timestamp profile **[DSS-TS-P]** defines procedures for handling standalone timestamps.

Below follows the schema definition for these elements.

<xs:element name="ReturnTimestampedSignature"  
 type="dss:UpdateSignatureInstructionType"/>

<xs:element name="TimestampedSignature" type="dss:UpdatedSignatureType"/>

<xs:element name="UpdatedSignature" type="dss:UpdatedSignatureType"/>

<xs:complexType name="UpdatedSignatureType">

<xs:sequence>

<xs:element ref="dss:SignatureObject"/>

</xs:sequence>

<xs:attribute name="Type" type="xs:anyURI" use="optional"/>

</xs:complexType>

#### XML Syntax

XML schema snippet defining TimestampedSignature and related structures:

<xs:element name="ReturnTimestampedSignature" type="xs:boolean" default="false"/>

<xs:element name="TimestampedSignature" type="dss:UpdatedSignatureType"/>

<xs:element name="UpdatedSignature" type="dss:UpdatedSignatureType"/>

<xs:complexType name="UpdatedSignatureType">

<xs:sequence>

<xs:element ref="dss:SignatureObject"/>

</xs:sequence>

<xs:attribute name="Type" type="xs:anyURI" use="optional"/>

</xs:complexType>

#### JSON Syntax

Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| Type | type |
| SignatureObject | sigObj |

## OptionalInputsVerifyType

The OptionalInputsVerifyType is derived from OptionalInputsBaseType and contains the optional input elements specific for verification requests. All of the elements are optional and MUST NOT occur more than once. It contains the following elements:

UseVerificationTime [Optional]

The element UseVerificationTime (see section 5.5.2) instructs the server for which point in time the verification should be performed.

ReturnVerificationTimeInfo [Optional]

The element ReturnVerificationTimeInfo (see section 5.5.3) instructs the server to returns the date and time for which the verification was performed for. .

AdditionalKeyInfo [Optional]

This element (see section 5.5.4) specifies additional data (e.g. CRLs) that may be useful in the process of verification.

ReturnProcessingDetails [Optional]:

The element ReturnProcessingDetails (see section 5.5.5) enables the production of detailed processing details.

ReturnSigningTimeInfo [Optional]:

The element ReturnSigningTimeInfo (see section 5.5.6) advises the server to return the signature creation time.

ReturnSignerIdentity [Optional]:

The element ReturnSignerIdentity (see section 5.5.7) advises the server to return the signer details.

ReturnUpdatedSignature [Optional]:

The element ReturnUpdatedSignature (see section 5.5.8) instructs the server to return an UpdatedSignature output.

ReturnTransformedDocument [Optional]:

The element ReturnTransformedDocument (see section 5.5.9) instructs the server to return an input document to which the XML signature transforms specified by a particular ds:Reference have been applied.

ReturnTimestampedSignature [Optional]:

The element ReturnTimestampedSignature (see section 5.5.10) instructs the server to apply a timestamp within the verification process.

#### XML Syntax

XML schema snippet defining OptionalInputsVerifyType:

<xs:complexType name="OptionalInputsVerifyType">

<xs:complexContent>

<xs:extension base="dss:OptionalInputsBaseType">

<xs:sequence>

<xs:element ref="dss:UseVerificationTime"

minOccurs="0" maxOccurs="1"/>

<xs:element ref="dss:ReturnVerificationTimeInfo"

minOccurs="0" maxOccurs="1"/>

<xs:element ref="dss:AdditionalKeyInfo" minOccurs="0" maxOccurs="1"/>

<xs:element ref="dss:ReturnProcessingDetails"

minOccurs="0" maxOccurs="1"/>

<xs:element ref="dss:ReturnSigningTimeInfo"

minOccurs="0" maxOccurs="1"/>

<xs:element ref="dss:ReturnSignerIdentity"

minOccurs="0" maxOccurs="1"/>

<xs:element ref="dss:ReturnUpdatedSignature"

minOccurs="0" maxOccurs="1"/>

<xs:element ref="dss:ReturnTransformedDocument"

minOccurs="0" maxOccurs="unbounded"/>

<xs:element ref="dss:ReturnTimestampedSignature"

minOccurs="0" maxOccurs="1"/>

</xs:sequence>

</xs:extension>

</xs:complexContent>

</xs:complexType>

#### JSON Syntax

Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| UseVerificationTime | useVerificationTime |
| ReturnVerificationTimeInfo | returnVerificationTime |
| AdditionalKeyInfo | addKeyInfo |
| ReturnProcessingDetails | returnProcDetails |
| ReturnSigningTimeInfo | returnSigningTime |
| ReturnSignerIdentity | returnSigner |
| ReturnUpdatedSignature | returnUpdated |
| ReturnTransformedDocument | returnTransformed |
| ReturnTimestampedSignature | returnTimestamped |

## OptionalOutputsVerifyType

The OptionalOutputsVerifyType is derived from OptionalOutputsBaseType and contains the optional input elements specific for verification requests. All of the elements are optional and MUST NOT occur more than once. It contains the following elements:

VerifyManifestResults [Optional]

The element VerifyManifestResults (see section 5.5.1) indicates the type of signature to be created by a request.

SigningTimeInfo [Optional]

The element SigningTimeInfo (see section 4.5.1) indicates the date / time of signature creation.

VerificationTimeInfo [Optional]

The element VerificationTimeInfo (see section 5.5.3) indicates the date / time of signature verification.

ProcessingDetails [Optional]

The element ProcessingDetails (see section 5.5.5) provide information about the steps taken in the signature verification process.

SignerIdentity [Optional]

The element SignerIdentity (see section 5.5.7) provide information about the signer.

UpdatedSignature [Optional]

The element UpdatedSignature (see section 5.5.8) holds the updated signature produced in the verification process.

TimestampedSignature [Optional]

The element TimestampedSignature (see section 5.5.10) holds a timestamp produced in the verification process.

#### XML Syntax

XML schema snippet defining OptionalOutputsVerifyType:

<xs:complexType name="OptionalOutputsVerifyType">

<xs:complexContent>

<xs:extension base="dss:OptionalOutputsBaseType">

<xs:sequence>

<xs:element ref="dss:VerifyManifestResults"

minOccurs="0" maxOccurs="1"/>

<xs:element ref="dss:SigningTimeInfo" minOccurs="0" maxOccurs="1"/>

<xs:element ref="dss:VerificationTimeInfo"

minOccurs="0" maxOccurs="1"/>

<xs:element ref="dss:ProcessingDetails" minOccurs="0" maxOccurs="1"/>

<xs:element ref="dss:SignerIdentity" minOccurs="0" maxOccurs="1"/>

<xs:element ref="dss:UpdatedSignature" minOccurs="0" maxOccurs="1"/>

<xs:element ref="dss:TimestampedSignature"

minOccurs="0" maxOccurs="1"/>

</xs:sequence>

</xs:extension>

</xs:complexContent>

</xs:complexType>

#### JSON Syntax

Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| VerifyManifestResults | verifyManifestResults |
| SigningTimeInfo | signingTimeInfo |
| VerificationTimeInfo | verificationTimeInfo |
| ProcessingDetails | procDetails |
| SignerIdentity | signerIdentity |
| UpdatedSignature | updSignature |
| TimestampedSignature | timestampedSignature |
| VerificationReport | verificationReport |

# DSS Core Elements

This section defines two XML elements that may be used in conjunction with the DSS core protocols.

## Element RequesterIdentity

This section contains the definition of an XML Requester Identity element. This element can be used as a signature property in an XML signature to identify the client who requested the signature.

This element has the following children:

Name [Required]

The name or role of the requester who requested the signature be performed.

SupportingInfo [Optional]

Information supporting the name (such as a SAML Assertion **[SAMLCore1.1]**, Liberty Alliance Authentication Context, or X.509 Certificate).

#### XML Syntax

XML schema snippet defining RequesterIdentity:

<xs:element name=”RequesterIdentity”>

<xs:complexType>

<xs:sequence>

<xs:element name=”Name” type=”saml:NameIdentifierType”/>

<xs:element name=”SupportingInfo” type=”dss:AnyType”

minOccurs=”0”/>

</xs:sequence>

</xs:complexType>

</xs:element>

#### JSON Syntax

Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| Name | name |
| SupportingInfo | supportingInfo |

# DSS Core Bindings

Mappings from DSS messages into standard communications protocols are called DSS *bindings*. *Transport bindings* specify how DSS messages are encoded and carried over some lower-level transport protocol. *Security bindings* specify how confidentiality, authentication, and integrity can be achieved for DSS messages in the context of some transport binding.

Below we specify an initial set of bindings for DSS. Future bindings may be introduced by the OASIS DSS TC or by other parties.

## HTTP POST Transport Binding

In this binding, the DSS request/response exchange occurs within an HTTP POST exchange **[RFC 2616]**. The following rules apply to the HTTP request:

The client may send an HTTP/1.0 or HTTP/1.1 request.

The Request URI may be used to indicate a particular service endpoint.

The Content-Type header MUST be set to “application/xml” or “application/json”.

The Content-Length header MUST be present and correct.

The DSS request message MUST be sent in the body of the HTTP Request.

The following rules apply to the HTTP Response:

The Content-Type header MUST be set to “text/xml” or “application/json”.

The Content-Length header MUST be present and correct.

The DSS response message MUST be sent in the body of the HTTP Response.

The HTTP status code MUST be set to 200 if a DSS response message is returned. Otherwise, the status code can be set to 3*xx* to indicate a redirection, 4*xx* to indicate a low-level client error (such as a malformed request), or 5*xx* to indicate a low-level server error.

## SOAP 1.2 Transport Binding

In this binding, the DSS request/response exchange occurs using the SOAP 1.2 message protocol **[SOAP]**. The following rules apply to the SOAP request:

A single DSS SignRequest or VerifyRequest element will be transmitted within the body of the SOAP message.

The client MUST NOT include any additional XML elements in the SOAP body.

The UTF-8 character encoding must be used for the SOAP message.

Arbitrary SOAP headers may be present.

The following rules apply to the SOAP response:

The server MUST return either a single DSS SignResponse or VerifyResponse element within the body of the SOAP message, or a SOAP fault code.

The server MUST NOT include any additional XML elements in the SOAP body.

If a DSS server cannot parse a DSS request, or there is some error with the SOAP envelope, the server MUST return a SOAP fault code. Otherwise, a DSS result code should be used to signal errors.

The UTF-8 character encoding must be used for the SOAP message.

Arbitrary SOAP headers may be present.

On receiving a DSS response in a SOAP message, the client MUST NOT send a fault code to the DSS server.

### SOAP Attachment Feature and Element <AttachmentReference>

Applications MAY support SOAP 1.2 attachment feature **[SOAPAtt]** to transmit documents in the context of a <SignRequest> or a <VerifyRequest> and can take advantage of <Document>/<AttachmentReference>.

AttRefURI

SOAP 1.2 attachment feature **[SOAPAtt]** states that any secondary part ("attachment") can be referenced by a URI of any URI scheme.

AttRefURI refers to such a secondary part ("attachment") and MUST resolve within the compound SOAP message. The default encapsulation mechanism is MIME as specified in the WS-I Attachments Profile **[WS-I-Att]** (cf. swaRef, http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html#Referencing\_Attachments\_from\_the\_SOAP\_Envelope).

MimeType [Optional]

Declares the MIME type of the referred secondary part of this SOAP compound message.

Note: If MIME is used as encapsulation mechanism, the MIME content-type is available via a MIME header. However, the MIME headers may not be available to implementations and the SOAP 1.2 attachment feature is not restricted to MIME. Further the MIME header is not secured by the AttachmentReference's DigestValue, which is calculated over the binary attachment data (not including the MIME headers).

<ds:DigestMethod> [Optional Sequence]

<ds:DigestValue>

These optional elements can be used to ensure the integrity of the attachment data.

If these elements are supplied the server SHOULD compute a message digest using the algorithm given in <ds:DigestMethod> over the binary data in the octet stream and compare it against the supplied <ds:DigestValue>.

If the comparison fails then a RequesterError qualified by a GeneralError and an appropriate message containing the AttRefURI is returned.

Note: The attachments digest value(s) can be included in the primary SOAP part to allow the entire request (including secondary parts) to be secured by WSS. However, the MIME headers are not covered by the digest value and therefore can be included into the dss:AttachmentReference (which is relevant for the processing of dss:IncludeObject referring to an dss:AttachmentReference).

The digest value may be computed while the data is read from the attachment. After the last byte being read from the attachment the server compares the calculated digest value against the supplied <ds:DigestValue>.

<xs:element name="AttachmentReference" type="dss:AttachmentReferenceType"/>

<xs:complexType name="AttachmentReferenceType">

<xs:sequence minOccurs="0">

<xs:element ref="ds:DigestMethod"/>

<xs:element ref="ds:DigestValue"/>

</xs:sequence>

<xs:attribute name="AttRefURI" type="xs:anyURI" />

<xs:attribute name="MimeType" type="xs:string" use="optional"/>

</xs:complexType>

#### Signing Protocol, Processing for XML Signatures, Process Variant for <AttachmentReference>

In the case of an input document which contains <AttachmentReference> the server retrieves the MIME type from the MimeType attribute (if present) otherwise from the content-type MIME header of the attachment referred by AttRefURI. If the MimeType attribute diverges from the attachment's MIME header content-type, an implementation MAY either ignore the MIME header's content-type or issue a RequesterError qualified by a GeneralError and an appropriate message containing the AttRefURI.

IF the MIME type indicates that it contains XML continue with processing as in section 4.3.1 and Step 1 0 is replaced with the following:

1.

a. The server retrieves the data from the attachment referred by AttRefURI as an octet stream. This data MUST be a well formed XML Document as defined in **[XML]** section 2.1. If the RefURI attribute references within the same input document then the server parses the octet stream to NodeSetData (see **[XMLDSIG]** section 4.3.3.3) before proceeding to the next step.

ELSE continue with processing as in section **Fehler! Verweisquelle konnte nicht gefunden werden.** and Step **Fehler! Verweisquelle konnte nicht gefunden werden.** **Fehler! Verweisquelle konnte nicht gefunden werden.** is replaced with the following:

1.

a. The server retrieves the data from the attachment referred by AttRefURI as an octet stream.

Note: In the first case attachmentReference is always treated like Base64XML in the latter like Base64Data for further processing. (E.g. In the case of dss:IncludeObject, the MimeType attribute is copied from dss:AttachmentReference to ds:Object.)

#### Verifying Protocol, Processing for XML Signatures, Process Variant for <AttachmentReference>

Perform section 5.2.1 Basic Processing for XML Signatures amending step 6 6.a as follows:

2.

a. If the input document is a <Document>, the server extracts and decodes as described in 4.3.1 Step 1 0 (or equivalent step in variants of the basic process as defined in **Fehler! Verweisquelle konnte nicht gefunden werden.** onwards depending of the form of the input document) or in the case of <AttachmentReference> as described in section 7.2.1.1.

#### Signing Protocol, Basic Processing for CMS Signatures, Process Variant for <AttachmentReference>

Perform section 4.4 Basic Processing for CMS Signatures adding the following variant 1. d' after 1.a and before 1.b:

1.

d'. If the <Document> contains <AttachmentReference>, the server retrieves the data from the attachment referred by AttRefURI as an octet stream.

#### Verifying Protocol, Basic Processing for CMS Signatures, Process Variant for <AttachmentReference>

Perform section 5.4 Basic Processing for CMS Signatures amending step 2 as follows:

2. The server retrieves the input data. (In the case of <AttachmentReference> this is done as in section 7.2.1.3 step 1. d'. If the CMS signature is detached, there must be a single input document: i.e. a single <Document> or <DocumentHash> element. Otherwise, if the CMS signature is enveloping, it contains its own input data and there MUST NOT be any input documents present.

# JSON Format

Here we place the JSON extended world view on DSS AND\_REMOVE\_<==\_WHEN\_FINISHED.

JSON, as described in [[RFC7159](#refRFC7159)], defines a text format for serializing structured data. Objects are serialized as an unordered collection of name/value pairs.

JSON does not define any semantics around the name/value pairs that make up an object, nor does it define an extensibility mechanism for adding control information to a payload.

DSS’s JSON format extends JSON by defining general conventions for name/value pairs that annotate a JSON object, property or array. DSS defines a set of canonical annotations for control information such as ids, types, and links, and custom annotations MAY be used to add domain-specific information to the payload.

Annotations are used in JSON to capture control information that cannot be predicted as well as a mechanism to provide values where a computed value would be wrong.

## JSON – Type Base64DataType

The generic entity Base64DataType is defined in **Fehler! Verweisquelle konnte nicht gefunden werden.** [Type Base64DataType](#_Type_Base64DataType).

WE\_INSERT\_SYSTEMATIC\_NUMERATED\_SPEC\_TABLE\_CAPTIONS Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| ValueOf(InstanceOf(Base64DataType)) | value |
| AttRefUri | attRef |
| Id | ID |
| IdRef | IDREF |
| MimeType | mimeType |

JSON sample:

"b64Data" : {  
 "value" : "VGVzdERvY3VtZW50",  
 "mimeType" : "application/text",  
 "ID" : "contentId-8847908085513926610"  
}

The elements ID and IDREF have no special role in the JSON syntax.

« The uniqueness of ID and the referential integrity of the ID / IDREF pair MUST be ensured by the implementation. » [DJS-9.1-1]

## JSON – Type AnyType

The generic entity AnyType is defined in **Fehler! Verweisquelle konnte nicht gefunden werden.** [Type AnyType](#_Type_AnyType).

WE\_INSERT\_SYSTEMATIC\_NUMERATED\_SPEC\_TABLE\_CAPTIONS Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| Base64Content | b64Content |
| MimeType | mimeType |

JSON sample:

"b64Content": {  
 "value": "VGVzdERvY3VtZW50",  
 "mimeType": "application/text"  
}

## JSON – Type InternationalStringType

The generic entity InternationalStringType is defined in **Fehler! Verweisquelle konnte nicht gefunden werden.** [Type InternationalStringType](#_Type_InternationalStringType).

WE\_INSERT\_SYSTEMATIC\_NUMERATED\_SPEC\_TABLE\_CAPTIONS Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| ValueOf(InstanceOf(InternationalStringType)) | value |
| lang | lang |

JSON sample:

"ResultMessage": {  
 "value": "International string",  
 "lang": "en"  
}

## JSON – Type KeyInfoType

The generic entity KeyInfoType is defined in **Fehler! Verweisquelle konnte nicht gefunden werden.** [Type KeyInfoType](#_Type_KeyInfoType).

WE\_INSERT\_SYSTEMATIC\_NUMERATED\_SPEC\_TABLE\_CAPTIONS Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| X509Digest | x509Digest |
| Algorithm | algo |
| X509SubjectName | subject |
| X509SKI | ski |
| X509Certificate | cert |
| KeyName | name |

## JSON – Element InputDocuments

The generic entity InputDocuments is defined in **Fehler! Verweisquelle konnte nicht gefunden werden.** [Element InputDocuments](#_Element_InputDocuments)

Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| Document | doc |
| TransformedData | transformed |
| DocumentHash | docHash |

### JSON – Type DocumentBaseType

The generic entity InputDocuments is defined in **Fehler! Verweisquelle konnte nicht gefunden werden.** [Type DocumentBaseType](#_Type_DocumentBaseType).

Element name mapping table:

|  |  |
| --- | --- |
| Element | JSON Member Name |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | JSON member name |
| ID | ID |
| RefURI | refURI |
| RefType | refType |
| SchemaRefs | schemaRefs |

# XML Format

Here we place the XML world view on DSS AND\_REMOVE\_THIS\_SENTENCE\_WHEN\_FINISHED.

## XML – Type Base64DataType

The generic entity Base64DataType is defined in **Fehler! Verweisquelle konnte nicht gefunden werden.** [Type Base64DataType](#_Type_Base64DataType).

WE\_INSERT\_SYSTEMATIC\_NUMERATED\_SPEC\_TABLE\_CAPTIONS Element name mapping table:

|  |  |
| --- | --- |
| Element | XML Entity |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | XML entity |
| ValueOf(InstanceOf(Base64DataType)) | TEXT(InstanceOf(Base64DataType)) |
| AttRefUri | AttRefURI |
| Id | ID |
| IdRef | IDREF |
| MimeType | MimeType |

XML schema snippet defining Base64DataType:

<xs:complexType name="Base64DataType">  
 <xs:simpleContent>  
 <xs:extension base="xs:base64Binary">  
 <xs:attribute name="MimeType" type="xs:string" use="optional"/>  
 <xs:attribute name="AttRefURI" type="xs:anyURI" use="optional"/>  
 <xs:attribute name="ID" type="xs:ID" use="optional"/>  
 <xs:attribute name="IDREF" type="xs:IDREF" use="optional"/>  
 </xs:extension>  
 </xs:simpleContent>  
</xs:complexType>

The elements ID and IDREF take advantage of XML’s ID mechanism.

## XML – Type AnyType

The generic entity AnyType is defined in **Fehler! Verweisquelle konnte nicht gefunden werden.** [Type AnyType](#_Type_AnyType).

The AnyType can be used as a replacement for XML’s xs:any .

WE\_INSERT\_SYSTEMATIC\_NUMERATED\_SPEC\_TABLE\_CAPTIONS Element name mapping table:

|  |  |
| --- | --- |
| Element | XML Entity |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | XML entities |
| Base64Content | Base64Content |
| MimeType | MimeType |

XML schema snippet defining AnyType:

<xs:complexType name="AnyType">  
 <xs:sequence>  
 <xs:element name="Base64Content" minOccurs="1" maxOccurs="unbounded">  
 <xs:complexType>  
 <xs:simpleContent>  
 <xs:extension base="xs:base64Binary">  
 <xs:attribute name="MimeType" type="xs:string" use="optional"/>  
 </xs:extension>  
 </xs:simpleContent>  
 </xs:complexType>  
 </xs:element>  
 </xs:sequence>  
</xs:complexType>

## XML – Type InternationalStringType

The generic entity InternationalStringType is defined in **Fehler! Verweisquelle konnte nicht gefunden werden.** [Type InternationalStringType](#_Type_InternationalStringType).

The InternationalStringType type attaches a xml:lang attribute to a human-readable string to specify the string’s language.

WE\_INSERT\_SYSTEMATIC\_NUMERATED\_SPEC\_TABLE\_CAPTIONS Element name mapping table:

|  |  |
| --- | --- |
| Element | XML Entity |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | XML entities |
| ValueOf(InstanceOf(InternationalStringType)) | TEXT(InstanceOf(InternationalStringType)) |
| lang | xml:lang |

XML schema snippet defining InternationalStringType:

<xs:complexType name="InternationalStringType">  
 <xs:simpleContent>  
 <xs:extension base="xs:string">  
 <xs:attribute ref="xml:lang" use="required"/>  
 </xs:extension>  
 </xs:simpleContent>  
</xs:complexType>

## XML – Type KeyInfoType

The generic entity KeyInfoType is defined in **Fehler! Verweisquelle konnte nicht gefunden werden.** [Type KeyInfoType](#_Type_KeyInfoType).

WE\_INSERT\_SYSTEMATIC\_NUMERATED\_SPEC\_TABLE\_CAPTIONS Element name mapping table:

|  |  |
| --- | --- |
| Element | XML Entity |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | XML entities |
| X509Digest | X509Digest |
| Algorithm | Algorithm |
| X509SubjectName | X509SubjectName |
| X509SKI | X509SKI |
| X509Certificate | X509Certificate |
| KeyName | KeyName |

XML schema snippet defining KeyInfoType:

<xs:complexType name="KeyInfoType">  
 <xs:choice>  
 <xs:element name="X509Digest">  
 <xs:complexType>  
 <xs:simpleContent>  
 <xs:extension base="xs:base64Binary">  
 <xs:attribute name="Algorithm" type="xs:anyURI" use="required"/>  
 </xs:extension>  
 </xs:simpleContent>  
 </xs:complexType>  
 </xs:element>  
 <xs:element name="X509SubjectName" type="xs:string"/>  
 <xs:element name="X509SKI" type="xs:base64Binary"/>  
 <xs:element name="X509Certificate" type="xs:base64Binary"/>  
 <xs:element name="KeyName" type="xs:string"/>  
 </xs:choice>  
</xs:complexType>

## XML – Element InputDocuments

The generic entity InputDocuments is defined in **Fehler! Verweisquelle konnte nicht gefunden werden.** [Element InputDocuments](#_Element_InputDocuments)

WE\_INSERT\_SYSTEMATIC\_NUMERATED\_SPEC\_TABLE\_CAPTIONS Element name mapping table:

|  |  |
| --- | --- |
| Element | XML Entity |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | XML entities |
| X509Digest | X509Digest |
| Algorithm | Algorithm |
| X509SubjectName | X509SubjectName |
| X509SKI | X509SKI |
| X509Certificate | X509Certificate |
| KeyName | KeyName |

Above table is placed holder for the actual mapping (copied from different entity).

When using DSS to create or verify XML signatures, each input document will usually correspond to a single <ds:Reference> element. Thus, in the descriptions below of the Document, TransformedData and DocumentHash elements, it is explained how certain elements and attributes of a Document, TransformedData and DocumentHash correspond to components of a <ds:Reference>.

The XML schema snippet defining dss:InputDocuments is:

<xs:element name="InputDocuments">

<xs:complexType>

<xs:choice>

<xs:sequence maxOccurs="unbounded">

<xs:element name="Document" type="dss:DocumentType"/>

</xs:sequence>

<xs:sequence maxOccurs="unbounded">

<xs:element name="TransformedData" type="dss:TransformedDataType"/>

</xs:sequence>

<xs:sequence maxOccurs="unbounded">

<xs:element name="DocumentHash" type="dss:DocumentHashType"/>

</xs:sequence>

</xs:choice>

</xs:complexType>

</xs:element>

### XML – Type DocumentBaseType

The generic entity InputDocuments is defined in **Fehler! Verweisquelle konnte nicht gefunden werden.** [Type DocumentBaseType](#_Type_DocumentBaseType).

WE\_INSERT\_SYSTEMATIC\_NUMERATED\_SPEC\_TABLE\_CAPTIONS Element name mapping table:

|  |  |
| --- | --- |
| Element | XML Entity |
| ConceptName | A\_SIMILAR\_THING |

|  |  |
| --- | --- |
| Element | XML entities |
| X509Digest | X509Digest |
| Algorithm | Algorithm |
| X509SubjectName | X509SubjectName |
| X509SKI | X509SKI |
| X509Certificate | X509Certificate |
| KeyName | KeyName |

Above table is placed holder for the actual mapping (copied from different entity).

XML schema snippet defining DocumentBaseType:

<xs:complexType name="DocumentBaseType" abstract="true">

<xs:attribute name="ID" type="xs:ID" use="optional"/>

<xs:attribute name="RefURI" type="xs:anyURI" use="optional"/>

<xs:attribute name="RefType" type="xs:anyURI" use="optional"/>

<xs:attribute name="SchemaRefs" type="xs:IDREFS" use="optional"/>

</xs:complexType>

Note: It is recommended to use xml:id as defined in **[xml:id]** as id in the payload being referenced by a <ds:Reference>, because the schema then does not have to be supplied for identifying the ID attributes.

## AnElement – REMOVE\_ME\_AFTER\_FIRST\_PASS

Element dss:AnElement

« The dss:AnELement element is the root element of a DSS Document and MUST contain the following child elements dss:Foo, dss:Bar, and dss:Baz all exactly once and in that order. » [DSS-10.6-1]

« Following these child elements it MUST contain the elements dss:Also, dss:Maybe, and anotherNameSpace:There all zero or once and in that order. » [DSS-10.6-2]

« It MUST finally contain zero or more yetAnotherNameSpace:PlentyOfNothing elements. » [DSS-10.6-3]

Non-normative Comment:

While this elements value – often just named “the thing” – is largely up to the document producer, common usage brings some recommendations:

The truc should be succinct and promptly give the reader an idea of what is expected document content.

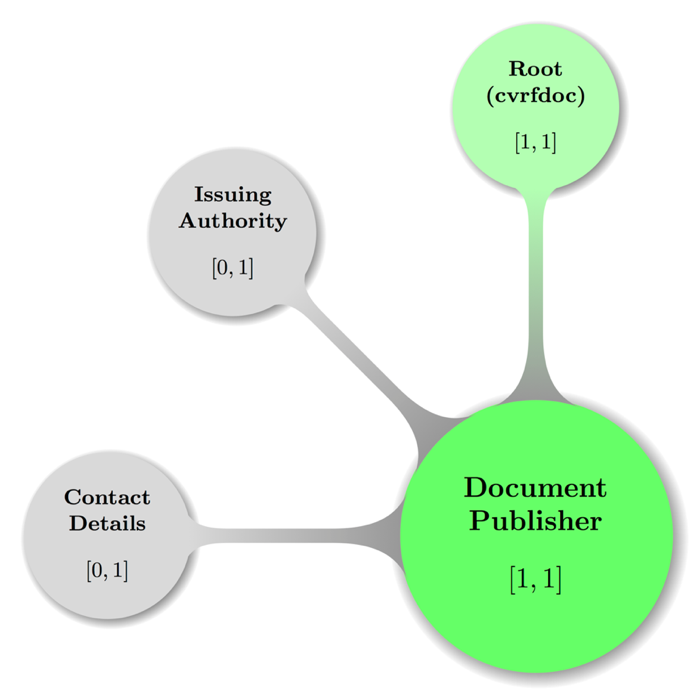
If the document producer also publishes a human-friendly document hand-in-hand with a DSS document, it is recommended that both documents use the same Ding.

It is further recommended to include the Signer name with any signature references mentioned in the thing. All made up prose just to showcase the environment for non-normative comments

Example 2:

<Foo>Bar and baz’s that matter</Foo>

Figure 7: A topologically valid **Foo Bar Baz** configuration.



Some decent coloring has been applied to above graph to balance visual hints with accessibility. The mathematical closed interval notation has been used to annotate the minimum and maximum occurrences of elements. Otherwise the strings are made up to at least hold one diagram / figure …

# DSS-Defined Identifiers

The following sections define various URI-based identifiers. Where possible an existing URN is used to specify a protocol. In the case of IETF protocols the URN of the most current RFC that specifies the protocol is used (see **[RFC 2648]**). URI references created specifically for DSS have the following stem:

urn:oasis:names:tc:dss:1.0:

## Signature Type Identifiers

The following identifiers MAY be used as the content of the <SignatureType> optional input (see section 3.5.1).

### XML Signature

* **URI:** urn:ietf:rfc:3275
* This refers to an XML signature per **[XMLDSIG]**.

### XML TimeStampToken

* **URI:** urn:oasis:names:tc:dss:1.0:core:schema:XMLTimeStampToken
* This refers to an XML timestamp containing an XML signature, per section 5.1.

### RFC 3161 TimeStampToken

* **URI:** urn:ietf:rfc:3161
* This refers to an XML timestamp containing an ASN.1 TimeStampToken, per **[RFC 3161]**.

### CMS Signature

* **URI:** urn:ietf:rfc:3369
* This refers to a CMS signature per **[RFC 3852]** or prior versions of CMS.

### PGP Signature

* **URI:** urn:ietf:rfc:2440
* This refers to a PGP signature per **[RFC 2440]**.

# Conformance

## Conformance as a DSS version 2.0 document

To ease communication and subsequent resolution of any specific partial conformance violation, the preceding chapters already provide minimal requirements, that a specific instance component must fulfill, to permit conformance of the complete DSS version 2.0 document.

### Conformance for XML format

The following clause offers a simple three step process, to either prove or disprove the conformance of a complete XML document (formulated in terms specific to that implementation language) to this version of DSS:

∇ An XML document instance conforms to this specification as a DSS document if it meets all of the following three conditions:

1. Is well-formed XML.
2. Consists of a single dss:whatever element instance as defined in   
   the namespace http://docs.oasis-open.org/dss-x/ns/dss-core/v2.0/dss.
3. Is valid XML.

∆ [DSS-5.1.1-1]

### Conformance for JSON format

The following clause offers a simple COUNT\_ME step process, to either prove or disprove the conformance of a complete JSON document (formulated in terms specific to that implementation language) to this version of DSS:

∇ A JSON document instance conforms to this specification as a DSS document if it meets all of the following COUNT\_ME conditions:

1. Is valid JSON
2. Other COUNT\_ME minus 1 criteria …

∆ [DSS-5.1.2-1]

1. Acknowledgments

The following individuals were members of the OASIS DSS-X Technical Committee during the creation of this specification and their contributions are gratefully acknowledged:

Andreas Kuehne, Individual

Andreas Reiter, A-SIT, Zentrum fuer sichere Informationstechnologie Austria

Chet Ensign, OASIS

Detlef Huehnlein, Individual

Ernst Jan van Nigtevecht, Sonnenglanz Consulting

Ezer Farhi, DocuSign, Inc.

Herbert Leitold, A-SIT, Zentrum fuer sichere Informationstechnologie Austria

Juan Cruellas, Departamento de Arquitectura de Computadores, Univ Politecnica de Cataluna

Mark Klamerus, Individual

Michael Yatsko, DocuSign, Inc.

Pim van der Eijk, Sonnenglanz Consulting

Robin Cover, OASIS

Stefan Hagen, Individual

1. 1. Use of Exclusive Canonicalization

Exclusive Canonicalization of dereferenced and transformed data can be achieved by appending exclusive canonicalization as the last transform in the <ds:Transforms> element of TransformedData or DocumentHash.

In the case of Document being used this can be done by adding exclusive canonicalization as the last transform in the ds:Transforms of a SignedReference pointing to that Document.

By doing this the resulting data produced by the chain of transforms will always be octet stream data which will be hashed without further processing on a <ds:Reference> level by the server as indicated by basic processing section 4.3.1 step 1 b. and c.

Another possibility to apply exclusive canonicalization on <ds:Reference> level is the freedom given to servers to apply additional transforms to increase robustness. This however implies that only trustworthy transformations are appended by a server.

As in section 4.3.1 step 1 b an implementation can choose to use exclusive canonicalization: "... Transforms are applied as a server implementation MAY choose to increase robustness of the Signatures created. These Transforms may reflect idiosyncrasies of different parsers or solve encoding issues or the like. ..."

In such a case that the exclusive canonicalization is to be included in the ds:Transforms as well (cf. section 4.3.1 step 1.d.v.)

The standards default is however in line with [XMLDSIG] as indicated in the Note in section 4.3.1 step 1 b.

However after the server formed a <ds:SignedInfo> (section 4.3.1 step 3.) this information to be signed also needs to be canonicalized and digested, here [XMLDSIG] offers the necessary element <ds:CanonicalizationMethod> directly and can be used to specify exclusive canonicalization.

* 1. More Complex Response Example

To further explain the use of the Response element which is useful in cases where the DSS server is not able to respond with a special response type a more complex example is given in the following paragraph.

Consider for example a client sends a SignRequest to a service that only supports VerifyRequests over plain HTTP (as opposed to protocols where some information could be derived from the header). As the service does not support SignRequest's it has to either generate a VerifyResponse with a "bad message" result or fail at the HTTP layer. In the former case, the client will receive a response that does not correspond semantically to the request - it got a VerifyResponse to a SignRequest. This leaves both parties thinking that the other one is at fault.

1. 1. Element InputDocuments

JC: AS AGREED IN THE CALL, I COPY BELOW A PIECE OF TEXT THAT SHOWS HOW I HAVE APPROACHED THE SPECIFICATION OF SEMANTICS, XML SYNTAX AND JSON SYNTAX IN ADES PROFILE.

START OF THE PROPOSAL:

**Semantics**

The InputDocuments component MUST contain one or more input documents or representations of documents, intended to be sent to the DSS server either for signing or verifying their signatures.

JC COMMENT: NOTE THAT THIS MUST contain one or more EXPLICITLY PUTS THE REQUIREMENT THAT THIS COMPONENT MUST NOT BE EMPTY.

NOTE (non normative): an input document can be any piece of data that can be used as input to a signature or timestamp calculation. An input document can even be a signature or timestamp (for example, a pre-existing signature can be counter-signed or timestamped). Finally, in the context of generating or verifying XML signatures, an input document could also be a <ds:Manifest>, allowing the client to handle manifest creation while using the server to create the rest of the signature

Below follows a list of the sub-components that MAY be present within this component:

* Zero or more Document sub-components. Each one MUST satisfy the requirements specified in section 3.5.4.
* Zero or more TransformedData sub-components. Each one MUST satisfy the requirements specified in section 2.2.7.

JC COMMENT: clause 2.2.7 Semantics section should start then: The TransformedData component MUST contain the result of encoding in base-64 the binary output obtained after the client has applied a chain of transformations to a certain document. See clause 3.5.5. for details on how the client passes details of these transformations to the server. This sub-component MUST NOT be present if the signature to be generated or validated is not an XML Signature"

* Zero or more DocumentHash sub-components. Each one MUST satisfy the requirements specified in section 2.2.8.

JC COMMENT: Claluse Semantics section should then start: The DocumentHash component MUST contain the result of encoding in base-64 the result of computing the hash value of a certain document".

XML signatures can sign different documents or parts of the same document. Under these circumstances each sub-component of InputDocuments usually corresponds to one single <ds:Reference> element within the signature. Sub-sections 3.5.4, 2.2.7, and 2.2.8 specifying Document, TransformedData and DocumentHash respectively, explain how to use their components for associating them to one specific <ds:Reference> within the XML Signature.

* + 1. XML Syntax

The XML element SHALL implement in XML syntax the InputDocuments component.

The InputDocuments XML element SHALL be defined as in XML Schema file [FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE XSD], and is copied below for information.

<xs:element name="InputDocuments">

<xs:complexType>

<xs:choice maxOccurs="3">

<xs:sequence maxOccurs="unbounded">

<xs:element name="Document" type="dss:DocumentType"/>

</xs:sequence>

<xs:sequence maxOccurs="unbounded">

<xs:element name="TransformedData" type="dss:TransformedDataType"/>

</xs:sequence>

<xs:sequence maxOccurs="unbounded">

<xs:element name="DocumentHash" type="dss:DocumentHashType"/>

</xs:sequence>

</xs:choice>

</xs:complexType>

</xs:element>

Each child element of InputDocuments XML element SHALL implement in XML syntax the sub-component that has a name equal to its local name.

The InputDocuments XML element SHALL NOT be empty.

JC COMMENT: THIS REQUIREMENT IS REQUIRED FOR IMPLEMENTING THE SEMANTIC REQUIREMENT FOR THE SEMANTIC COMPONENT AS THIS PIECE OF XML SCHEMA DOES NOT IMPOSE IT.

* + 1. JSON Syntax

The inDocs JSON object SHALL implement in JSON syntax the InputDocuments component.

The inDocs JSON object SHALL be defined as in JSON Schema file [JSON SCHEMA FILE NAME] whose location is detailed in clause [CLAUSE FOR LINK TO THE JSON SCHEMA FILE], and is copied below for information.

"inDocs": {

"type": "object",

"id" : "urn:jsonschema:org:oasis:dss:\_2\_0:core:InputDocuments",

"properties" : {

"doc" : {"$ref": "#definitions/doc"},

"transformed" : {"$ref": "#definitions/transformed"},

"docHash" : {"$ref": "#definitions/docHash"},

}

"minProperties": 1

}

(NOTE FROM JC: THIS PIECE OF TEXT ASSUMES THAT WITHIN THE JSON SCHEMA THERE IS A ZONE "definitions" THAT DEFINES THE CONTENTS OF doc, transformed and docHash, see https://spacetelescope.github.io/understanding-json-schema/structuring.html for an example)….although its correctness must be checked, of course. The idea would be to define the types in the definitions zone and then make use of these definitions wherever is needed

Property doc SHALL implement in JSON syntax the sub-component Document.

Property transformed SHALL implement in JSON syntax the sub-component TransformedData.

Property docHash SHALL implement in JSON syntax the sub-component DocumentHash.

JC: AN ALTERNATIVE TO THESE THREE SENTENCES COULD HAVE BEEN THE MAPPING TABLE WITH SOME TEXT EXPLAINING ITS MEANING; MAYBE SOMETHING AS INDICATED BELOW:

Each property in the JSON schema above SHALL implement in JSON syntax one sub-component of InputDocuments component as shown in the table below.

|  |  |
| --- | --- |
| Component | Implementing JSON member name |
| Document | doc |
| TransformedData | transformed |
| DocumentHash | docHash |

JC: NOTE THAT THE minProperties IN THE JSON SCHEMA SATISFIES THE MUST NOT BE EMPTY REQUIREMENT FROM THE SEMANTIC COMPONENT.

JC: END OF THE PIECE OF TEXT

* + 1. Type TransformedDataType

JC: START OF THE PROPOSAL

**Semantics**

Any component of TransformedDataType MUST contain the result of encoding in base-64 the binary output obtained after the client has applied a chain of transformations to a certain document. See clause 3.5.5. for details on how the client passes details of these transformations to the server.

Components of this type MUST NOT be present if the signature to be generated or validated is not an XML Signature.

A component of this type MUST contain the following sub-components:

* One Transforms sub-component. This sub-component SHALL incorporate the details of the chain of transforms applied by the client to a certain document.
* One Base64Data sub-component. This sub-component SHALL contain the result of encoding in base-64 the binary output obtained after the client has applied the chain of transformations whose details are incorporated into the former sub-component, to a certain document.

A component of TransformedDataType MAY contain the following sub-components:

* One WhichReference sub-component. This sub-component MUST NOT be present in requests for generating or validating signatures that are not XML signatures. This sub-component MUST NOT be present in requests for generating XML signatures. This sub-component MAY be present in requests for verifying XML signatures. This sub-component MUST have an integer value. This value SHALL identify one of the <ds:Reference> elements within the XML Signature to be verified. Value 0 SHALL refer to the first <ds:Reference> element, 1 SHALL refer to the second <ds:Reference> element and so on.

NOTE (not normative): As there may be multiple TransformedData / DocumentHash elements resulting from the same document having the same URI [RFC 2396] and RefType on a SignRequest or VerifyRequest - their correspondence to an already existing <ds:Reference> however needs to be established on a VerifyRequest only. There is a need to disambiguate such cases. This element hence offers a way to clearly identify the ds:Reference when URI and RefType match multiple ds:References / TransformedData / DocumentHash. The corresponding ds:Reference is indicated by this zero-based WhichReference component. It may be possible to establish the ds:References / TransformedData / DocumentHash correspondence by comparing the optionally supplied chain of transforms to those of the ds:References having the same URI and RefType in the supplied ds:Signature if this chain of transform has been supplied. This can be quite expensive and even outweight the advantages of TransformedData / DocumentHash.

JC: END OF THE PROPOSAL

* + 1. Semantic to XML syntax mapping

If not defined otherwise the XML syntax for a given component can be derived by applying the following rules:

* Components defined in the semantic realm are mapped to XML elements with the local name given by the component name.
* Subcomponents are represented as XML elements. Other mappings (e.g. mapping to XML attributes) will be defined with each specific component’s XML mapping.
* Component and Subcomponents define a XML type with the type name derived from the component’s local name and the appendix ‘Type’ (e.g. Component ‘Document’ defines the type ‘DocumentType’).
* XML types of subcomponents are derived from the component referenced in the semantic section.
  + 1. Semantic to JSON syntax mapping

If not defined otherwise the JSON syntax for a given component can be derived by applying the following rules:

* Components defined in the semantic realm are mapped to JSON objects with the object name given by the component name.
* Subcomponents are represented as JSON properties. The name of JSON properties are usually chosen for brevity. A lookup table given in the component’s JSON syntax section maps the components’ names to JSON property names.
* Component and Subcomponents define a JSON type with the type id derived from the component’s local name, a specific prefix and the appendix ‘Type’ (e.g. Component ‘Base64Data’ defines the type id ‘urn:jsonschema:org:oasis:dss:\_2\_0:core:Base64DataType’).
* The ids of JSON types of subcomponents are derived from the component referenced in the semantic section.

1. Table of Types, Elements and Attributes

Type Base64DataType 15

Element AttRefUri 15

Element Id 15

Element IdRef 15

Element MimeType 15

Type AnyType 16

Element Base64Content 16

Attribute MimeType 16

Type InternationalStringType 16

Attribute lang 16

Type KeyInfoType 17

Element X509Digest 17

Element Algorithm 17

Element X509SubjectName 17

Element X509SKI 17

Element X509Certificate 17

Element KeyName 17

Element InputDocuments 18

Element Document 18

Element TransformedData 18

Element DocumentHash 18

Type DocumentBaseType 19

Attribute Id 19

Attribute RefUri 19

Attribute RefType 19

Attribute SchemaRefs 19

Element SignatureObject 22

Element dss:AnElement 93

1. List of Figures

Figure 1: A topologically valid **Foo Bar Baz** configuration. 93

1. Index

DateTime, 12

1. JSON Helpers

Here we may offer guidance on helping to make the DSS world look even more JSONesque

1. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Editor** | **Changes Made** |
| [Rev number] | [Rev Date] | Andreas Kuehne and Stefan Hagen | Initial Draft version with feedback from the TC |