Securing DSS Version 2.0

Working Draft 01

20 March 2018

Technical Committee:

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

Chair:

Stefan Hagen (stefan@hagen.link), Individual

Editors:

Andreas Kuehne (kuehne@trustable.de), Individual

Stefan Hagen (stefan@hagen.link), Individual

Related work:

This document is related to:

* *Digital Signature Service Core Protocols, Elements, and Bindings Version 2.0*. Edited by Andreas Kuehne and Stefan Hagen. Work in progress. Latest version: http://docs.oasis-open.org/dss-x/dss-core/v2.0/dss-core-v2.0.html.

Abstract:

Securing DSS Version 2.0 serves as best effort information for implementers and users of Digital Signature Services (DSS) alike on where authentication issues, integrity problems and potential attack vectors typically occur.

Status:

This [Working Draft](https://www.oasis-open.org/policies-guidelines/tc-process#dWorkingDraft) (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#committeeDraft) as a Committee Note Draft. The OASIS document [Approval Process](https://www.oasis-open.org/policies-guidelines/tc-process#standApprovProcess) begins officially with a TC vote to approve a WD as a Committee Note Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Note Draft.

URI patterns:

Initial publication URI:
http://docs.oasis-open.org/dss-x/securing-dss/v2.0/cnd01/securing-dss-v2.0-cnd01.docx.

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

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

Copyright © OASIS Open 2018. All Rights Reserved.

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

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

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

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

Table of Contents

[1 Introduction 4](#_Toc509330980)

[1.1 References (non-normative) 4](#_Toc509330981)

[1.2 Section Level 2 4](#_Toc509330982)

[1.2.1 Section Level 3 4](#_Toc509330983)

[1.3 Section Level 2 4](#_Toc509330984)

[2 Heading 5](#_Toc509330985)

[Appendix A. Acknowledgments 6](#_Toc509330986)

[Appendix B. Some Appendix 7](#_Toc509330987)

[B.1 Subsidiary Appendix Section 7](#_Toc509330988)

[B.1.1 Sub-subsidiary Appendix Section 7](#_Toc509330989)

[Appendix C. Revision History 8](#_Toc509330990)

Introduction

Type introductory text here.

## References (non-normative)

**NOTE (remove this note and following examples before publication)**:

Recommended approach: Set up [Reference] label elements as "Bookmarks", then use hyperlinks to them within the document. (**Here’s how**: Insert hyperlink ->Place in this document -> scroll down to Bookmarks, select appropriate one.)

Use the "Ref" paragraph style to format references.

The proper format for citation of technical work produced by an OASIS TC (whether Standards Track or Non-Standards Track) is:

[Citation Label] Work Product [title](http://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html#workProductName) (italicized). Edited by Albert Alston, Bob Ballston, and Calvin Carlson. Approval date (DD Month YYYY). OASIS [Stage](http://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html#stage) Identifier and [Revision](http://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html#revision) Number (*e.g.*, OASIS Committee Specification Draft 01). Principal URI ([version-specific URI](http://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html#this-version), *e.g*., with stage component: somespec-v1.0-csd01.html). Latest version: ([latest version URI](http://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html#latest-version), without stage identifiers).

For example:

**[OpenDoc-1.2]** *Open Document Format for Office Applications (OpenDocument) Version 1.2*. Edited by Patrick Durusau and Michael Brauer. 19 January 2011. OASIS Committee Specification Draft 07. <http://docs.oasis-open.org/office/v1.2/csd07/OpenDocument-v1.2-csd07.html>. Latest version: <http://docs.oasis-open.org/office/v1.2/OpenDocument-v1.2.html>.

Reference sources:

For references to IETF RFCs, use the approved citation formats at:
<http://docs.oasis-open.org/templates/ietf-rfc-list/ietf-rfc-list.html>.

For references to W3C Recommendations, use the approved citation formats at: <http://docs.oasis-open.org/templates/w3c-recommendations-list/w3c-recommendations-list.html>.

## Section Level 2

### Section Level 3

## Section Level 2

Heading

Text.

1. Acknowledgments

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

Participants:

[Participant Name, Affiliation | Individual Member]

[Participant Name, Affiliation | Individual Member]

1. Some Appendix

Text.

* 1. Subsidiary Appendix Section

Text.

* + 1. Sub-subsidiary Appendix Section

text.

1. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Editor** | **Changes Made** |
| [Rev number] | [Rev Date] | [Modified By] | [Summary of Changes] |