SAM Threshold Sharing Schemes Version 1.0

Committee Specification Draft 01

20 November 2020

This version:

<https://docs.oasis-open.org/sam/sam-tss/v1.0/csd01/sam-tss-v1.0-csd01.docx> (Authoritative)

<https://docs.oasis-open.org/sam/sam-tss/v1.0/csd01/sam-tss-v1.0-csd01.html>

<https://docs.oasis-open.org/sam/sam-tss/v1.0/csd01/sam-tss-v1.0-csd01.pdf>

Previous version:

N/A

Latest version:

<https://docs.oasis-open.org/sam/sam-tss/v1.0/sam-tss-v1.0.docx> (Authoritative)

<https://docs.oasis-open.org/sam/sam-tss/v1.0/sam-tss-v1.0.html>

<https://docs.oasis-open.org/sam/sam-tss/v1.0/sam-tss-v1.0.pdf>

Technical Committee:

[OASIS Security Algorithms and Methods (SAM) TC](https://www.oasis-open.org/committees/sam/)

Chairs:

Tim Chevalier (Tim.Chevalier@netapp.com), [NetApp](http://www.netapp.com/)

Tony Cox (tony.cox@cryptsoft.com), [Cryptsoft Pty Ltd.](http://www.cryptsoft.com)

Editors:

Tim Chevalier (Tim.Chevalier@netapp.com), [NetApp](http://www.netapp.com/)

Tim Hudson (tjh@cryptsoft.com), [Cryptsoft Pty Ltd.](http://www.cryptsoft.com)

Additional artifacts:

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

* XML schemas: (list file names or directory name)
* Other parts (list titles and/or file names or directory name)
* (**Note:** Any normative computer language definitions that are part of the Work Product, such as XML instances, schemas and Java(TM) code, including fragments of such, must be (a) well formed and valid, (b) provided in separate plain text files, (c) referenced from the Work Product; and (d) where any definition in these separate files disagrees with the definition found in the document, the definition in the separate file prevails. Remove this note before submitting for publication.)

Related work:

This document replaces or supersedes:

* Documents replaced by this document (hyperlink, if available)

This document is related to:

* Related documents (hyperlink, if available) (remove "Related work" section or the "replaces" or "related" subsections if not used - instead of "N/A")

Abstract:

This document is intended for developers and architects who wish to design systems and applications that utilize threshold sharing schemes in an interoperable manner.

Status:

This document was last revised or approved by the OASIS Security Algorithms and Methods (SAM) TC on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at <https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=sam#technical>.

TC members should send comments on this document to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "[Send A Comment](https://www.oasis-open.org/committees/comments/index.php?wg_abbrev=sam)" button on the TC's web page at <https://www.oasis-open.org/committees/sam/>.

This document is provided under the [Non-Assertion](https://www.oasis-open.org/policies-guidelines/ipr#Non-Assertion-Mode) Mode of the [OASIS IPR Policy](https://www.oasis-open.org/policies-guidelines/ipr), the mode chosen when the Technical Committee was established. For information on whether any patents have been disclosed that may be essential to implementing this document, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (<https://www.oasis-open.org/committees/sam/ipr.php>).

Note that any machine-readable content ([Computer Language Definitions](https://www.oasis-open.org/policies-guidelines/tc-process#wpComponentsCompLang)) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any 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.

Key words:

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [[RFC2119](#RFC2119)] and [[RFC8174](#RFC8174)] when, and only when, they appear in all capitals, as shown here.

Citation format:

When referencing this document, the following citation format should be used:

[SAM-TSS-v1.0]

*SAM Threshold Sharing Schemes Version 1.0*. Edited by Tim Chevalier and Tim Hudson. 20 November 2020. OASIS Committee Specification Draft 01. <https://docs.oasis-open.org/sam/sam-tss/v1.0/csd01/sam-tss-v1.0-csd01.html>. Latest version: <https://docs.oasis-open.org/sam/sam-tss/v1.0/sam-tss-v1.0.html>.

Notices:

Copyright © OASIS Open 2020. All Rights Reserved.

Distributed under the terms of the OASIS IPR Policy, [<https://www.oasis-open.org/policies-guidelines/ipr>]. For complete copyright information please see the Notices section in the Appendix.

Table of Contents

[1 Introduction 4](#_Toc51166894)

[1.1 Changes from earlier versions 4](#_Toc51166895)

[1.2 Glossary 4](#_Toc51166896)

[1.2.1 Definitions of terms 4](#_Toc51166897)

[1.2.2 Acronyms and abbreviations 4](#_Toc51166898)

[1.2.3 Document conventions 4](#_Toc51166899)

[2 Section Title 5](#_Toc51166900)

[2.1 Level 2 section title 5](#_Toc51166901)

[2.1.1 Level 3 section title 5](#_Toc51166902)

[2.1.1.1 Level 4 section title 5](#_Toc51166903)

[2.1.1.1.1 Level 5 5](#_Toc51166904)

[2.1.1.1.1.1 Level 6 5](#_Toc51166905)

[3 Conformance 6](#_Toc51166906)

[Appendix A. References 7](#_Toc51166907)

[A.1 Normative References 7](#_Toc51166908)

[A.2 Informative References 8](#_Toc51166909)

[Appendix B. Security and Privacy Considerations 9](#_Toc51166910)

[Appendix C. Acknowledgments 10](#_Toc51166911)

[3.1 Special Thanks 10](#_Toc51166912)

[3.2 Participants 10](#_Toc51166913)

[Appendix D. Revision History 11](#_Toc51166914)

[Appendix E. Example Title 12](#_Toc51166915)

[E.1 Subsidiary section 12](#_Toc51166916)

[E.1.1 Sub-subsidiary section 12](#_Toc51166917)

[E.1.1.1 Sub-sub-subsidiary section 12](#_Toc51166918)

[E.1.1.1.1 Sub-sub-sub-subsidiary section 12](#_Toc51166919)

[Appendix F. Notices 13](#_Toc51166920)

# Introduction

[All text is normative unless otherwise labeled]

## Changes from earlier Versions

This section provides a description of significant differences from previously published, differently numbered Versions of this specification, if any. (Detailed revision history of this numbered Version should be tracked in an Appendix.)

## Glossary

### Definitions of terms

### Acronyms and abbreviations

### Document conventions

* Naming conventions
* Font colors and styles
* Typographical conventions

# Section Title

text

## Level 2 section title

text

### Level 3 section title

text

#### Level 4 section title

text

##### Level 5

Text

###### Level 6

Text

# Conformance

(**Note**: The [OASIS TC Process](https://www.oasis-open.org/policies-guidelines/tc-process#wpComponentsConfClause) requires that a specification approved by the TC for public review,l or for publication at the Committee Specification or OASIS Standard level must include a separate section, listing a set of numbered conformance clauses, to which any implementation of the specification must adhere in order to claim conformance to the specification (or any optional portion thereof). This is done by listing the conformance clauses here.

For the definition of "conformance clause," see [OASIS Defined Terms](https://www.oasis-open.org/policies-guidelines/oasis-defined-terms-2017-05-26#dConformanceClause).

See "Guidelines to Writing Conformance Clauses":
<https://docs.oasis-open.org/templates/TCHandbook/ConformanceGuidelines.html>.

Remove this note before submitting for publication.)

1. References

Note: Any normative work cited in the body of the text as needed to implement the work product must be listed in the Normative References section below. Each reference to a separate document or artifact in this work must be listed here and must be identified as either a Normative or an Informative Reference.

For all References – Normative and Informative:

Recommended approach: Set up **[Reference]** label elements as "Bookmarks", then create hyperlinks to them within the document.

The [Reference] label uses the style "Ref term".

The text of the reference uses the style "Ref". If there is a hyperlink, it should be visible and linked.

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 (italicized). Edited by Albert Alston, Bob Ballston, and Calvin Carlson. Approval date (DD Month YYYY). OASIS Stage Identifier and Revision Number (e.g., OASIS Committee Specification Draft 01). Principal URI (version-specific URI, e.g., with stage component: somespec-v1.0-csd01.html). Latest version: (static URI, 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. https://docs.oasis-open.org/office/v1.2/csd07/OpenDocument-v1.2-csd07.html. Latest version: https://docs.oasis-open.org/office/v1.2/OpenDocument-v1.2.html.

Reference sources:

For references to IETF RFCs, use the approved citation formats at:

https://docs.oasis-open.org/templates/ietf-rfc-list/ietf-rfc-list.html.

For references to W3C Recommendations, use the approved citation formats at:

https://docs.oasis-open.org/templates/w3c-recommendations-list/w3c-recommendations-list.html.

Remove this note before submitting for publication.

This appendix contains the normative and informative references that are used in this document. Normative references are specific (identified by date of publication and/or edition number or Version number) and Informative references are either specific or non-specific.

While any hyperlinks included in this appendix were valid at the time of publication, OASIS cannot guarantee their long term validity.

* 1. Normative References

The following documents are referenced in such a way that some or all of their content constitutes requirements of this document. This subsection is not used for Committee Notes.

[RFC2119]

Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.

[RFC8174]

Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<http://www.rfc-editor.org/info/rfc8174>>.

[ISO/IEC Directives] (Only used if ISO/IEC Key words are elected in front pages)

ISO/IEC Directives, Part 2 (Eighth edition) *Principles and rules for the structure and drafting of ISO and IEC documents*, International Organization for Standardization and International Electrotechnical Commission, 2018. <https://www.iso.org/sites/directives/current/part2/index.xhtml>.

[Reference]

[Full reference citation]

* 1. Informative References

The following referenced documents are not required for the application of this document but may assist the reader with regard to a particular subject area.

[RFC3552]

Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/info/rfc3552>.

[Reference]

[Full reference citation]

1. Security and Privacy Considerations

This section is not used for Committee Notes.

Note: OASIS strongly recommends that Technical Committees consider issues that might affect safety, security, privacy, and/or data protection in implementations of their work products and document these for implementers and adopters. For some purposes, you may find it required, e.g. if you apply for IANA registration.

While it may not be immediately obvious how your work product might make systems vulnerable to attack, most work products, because they involve communications between systems, message formats, or system settings, open potential channels for exploit. For example, IETF [[RFC3552](#RFC3552)] lists “eavesdropping, replay, message insertion, deletion, modification, and man-in-the-middle” as well as potential denial of service attacks as threats that must be considered and, if appropriate, addressed in IETF RFCs.

In addition to considering and describing foreseeable risks, this section should include guidance on how implementers and adopters can protect against these risks.

We encourage editors and TC members concerned with this subject to read Guidelines for Writing RFC Text on Security Considerations, IETF [[RFC3552](#RFC3552)], for more information.

1. Acknowledgments

Note: A Work Product approved by the TC must include a list of people who participated in the development of the Work Product. This is generally done by collecting the list of names in this appendix. This list shall be initially compiled by the Chair, and any Member of the TC may add or remove their names from the list by request. Remove this note before submitting for publication.

## Special Thanks

This is an optional subsection to call out contributions from TC members. If a TC wants to thank non-TC members then they should avoid using the term "contribution" and instead thank them for their "expertise" or "assistance".

Substantial contributions to this document from the following individuals are gratefully acknowledged:

[Participant Name, Affiliation | Individual Member]

## Participants

A TC can determine who they list here, however, Observers must not be listed. It is common practice for TCs to list everyone that was part of the TC during the creation of the document, but this is ultimately a TC decision on who they want to list and not list.

The following individuals were members of this Technical Committee during the creation of this document and their contributions are gratefully acknowledged:

[Participant Name, Affiliation | Individual Member]

1. Revision History

Revisions made since the initial stage of this numbered Version of this document may be tracked here.

Note: If revision tracking is handled in another system like github, provide a link to it instead of using this table, if desired. Remove this note before submitting for publication.

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

1. Example Title

Additional Appendixes may be added as needed:

* IANA Considerations
	1. Subsidiary section

text

* + 1. Sub-subsidiary section

Text

* + - 1. Sub-sub-subsidiary section

text

* + - * 1. Sub-sub-sub-subsidiary section

text

1. Notices

Copyright © OASIS Open 2020. 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: [<https://www.oasis-open.org/policies-guidelines/ipr>].

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. OASIS AND ITS MEMBERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THIS DOCUMENT OR ANY PART THEREOF.

As stated in the OASIS IPR Policy, the following three paragraphs in brackets apply to OASIS Standards Final Deliverable documents (Committee Specifications, OASIS Standards, or Approved Errata).

[OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Standards Final Deliverable, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this deliverable.]

[OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this OASIS Standards Final Deliverable by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this OASIS Standards Final Deliverable. OASIS may include such claims on its website, but disclaims any obligation to do so.]

[OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this OASIS Standards Final Deliverable or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Standards Final Deliverable, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.]

The name "OASIS" is a trademark of [OASIS](https://www.oasis-open.org/), the owner and developer of this document, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, documents, while reserving the right to enforce its marks against misleading uses. Please see <https://www.oasis-open.org/policies-guidelines/trademark> for above guidance.