Call for Participation: Security Algorithms and Methods (SAM) TC

Submitted by censign on Thu, 2020-05-21 14:15

Type:
Call for Participation

A new OASIS technical committee is being formed. The Security Algorithms and Methods (SAM) Technical Committee (TC) has been proposed by the members of OASIS listed in the charter below. The TC name, statement of purpose, scope, list of deliverables, audience, IPR mode and language specified in this proposal will constitute the TC's official charter.

Submissions of technology for consideration by the TC, and the beginning of technical discussions, may occur no sooner than the TC's first meeting.

The eligibility requirements for becoming a participant in the TC at the first meeting are:

(a) you must be an employee or designee of an OASIS member organization or an individual member of OASIS, and

(b) you must join the Technical Committee, which members may do by using the Roster "join group: link on the TC's web page at [a].

To be considered a voting member at the first meeting:

(a) you must join the Technical Committee at least 7 days prior to the first meeting (on or before 16 June 2020; and

(b) you must attend the first meeting of the TC, at the time and date fixed below (23 June 2020).

Participants also may join the TC at a later time. OASIS and the TC welcomes all interested parties.

Non-OASIS members who wish to participate may contact us about joining OASIS [b]. In addition, the public may access the information resources maintained for each TC: a mail list archive, document repository and public comments facility, which will be linked from the TC's public home page at [c].

Please feel free to forward this announcement to any other appropriate lists. OASIS is an open standards organization; we encourage your participation.
OASIS Security Algorithms and Methods (SAM) Technical Committee Charter

The charter for this TC is as follows.

Section 1: TC Charter

(1)(a) TC Name

Security Algorithms and Methods (SAM) TC

(1)(b) Statement of Purpose

The SAM Technical Committee will develop a set of documents to aid in the interoperability of implementations implementing cryptographic capabilities in support of OASIS and other standards and specifications. The TC's work products will allow for the earlier adoption of existing and emerging security algorithms and approaches and to provide other technical committees a path to adoption where those defining the algorithms, mechanisms and methods are themselves not focused on or interested in the formal standardisation process.

Business Benefits

Many organisations are unable to comply with a range of standards that deal with cryptographic algorithms or methods because there are a number of algorithms and methods that are not documented in a manner readily referenced by implementers. The SAM TC works to deliver the following business benefits:

- Enable referencing of existing and emerging algorithms and methods for utilisation in other standards work (including multiple OASIS TCs)
- Enable referencing of existing and emerging algorithms and methods, so that they can be used in an interoperable way
- Provide a faster path to the registration than existing methods such as NIST and the IETF

Note: SAM TC does not seek to replace the work of other standards bodies, merely to provide a fast path to referencing the information.
(1)(c) Scope

The primary goal of the SAM Technical Committee is to provide a standardised set of references of algorithms, mechanisms, and methods, including test-vectors, that can be used in other OASIS technical committees or where the standards are not yet defined by another recognised standards body.

Any analysis of the security properties of included cryptographic algorithms, methods, and objects contained in their specifications are out of scope.

(1)(d) Deliverables

The format of the SAM TC deliverables will be agreed upon by the SAM TC but will include sufficient documentation to:

- Capture target algorithms, mechanisms and methods in sufficient detail to enable implementers to use the work to reliably reproduce interoperable implementations;

- Test target algorithms, mechanisms and methods to ensure accurate implementations can be generated;

- Test target algorithms, mechanisms and methods to ensure implementations are interoperable; and

- Define references sufficiently, so that they can be used by OASIS and other standards in the production of other interoperable systems.

- Establish liaisons (as appropriate) with other organisations that perform similar work including those organisations noted in section 2a.

(1)(e) IPR Mode

The TC will operate under Non-Assertion mode.

(1)(f) Audience

SAM is intended for the following audiences:

Architects, designers, and implementers of providers and consumers of systems or services that need to utilise cryptographic algorithms, methods, or objects.

(1)(g) Language

Work group business and proceedings will be conducted in English.

(Optional References for Section 1)

N/A

Section 2: Additional Information

(2)(a) Identification of Similar Work

- Internet Engineering Task Force (IETF), Security Area (sec) - https://www.ietf.org/topics/areas/ [5]


(2)(b) First TC Meeting

June 23, 2020, 5pm US-EDT ? Conference Call

(2)(c) Ongoing Meeting Schedule

Cryptsoft will host online SAM TC meetings.

The Technical committee may organise face to face meetings as needed.

Meeting frequency will be determined by the committee members during quorate meetings.

Meeting times may be adjusted to suit the timezones of contributing committee members.

(2)(d) TC Proposers

- Tony Cox, tony.cox@cryptsoft.com [7], Cryptsoft

- Tim Hudson, tjh@cryptsoft.com [8], Cryptsoft

- Jason Thatcher, jason.thatcher@cryptsoft.com [9], Cryptsoft

- Tim Chevalier, Tim.Chevalier@netapp.com [10], NetApp

- Judy Furlong, Judith.Furlong@dell.com [11], Dell

(2)(e) Primary Representatives’ Support

- Tim Hudson, tjh@cryptsoft.com [8], as OASIS primary representative for Cryptsoft Pty Ltd, confirms our support for the proposed SAM TC charter and endorses our participants listed above.

- Judy Furlong, Judith.Furlong@dell.com [11] as OASIS primary representative for Dell, confirms our support for the proposed SAM TC charter and endorses our participants listed above.

- David Dale, ddale@netapp.com [12], as OASIS primary representative for NetApp Inc., confirms our support for the proposed SAM TC charter and endorses our participants listed above.

(2)(f) TC Convener

Tony Cox, tony.cox@cryptsoft.com [7], Cryptsoft

(2)(g) OASIS Member Section

ID Trust (http://www.oasis-idtrust.org/ [13])
(2)(h) Anticipated Contributions

N/A

(2)(i) FAQ Document

N/A

(2)(j) Work Product Titles and Acronyms

N/A

Associated TC:
Security Algorithms and Methods (SAM)

Associated MS:
IDtrust

Deadline:
Thu, 2020-05-21 - Tue, 2020-06-23

Links:
[5] https://www.ietf.org/topics/areas/
[7] mailto:tony.cox@cryptsoft.com
[8] mailto:tjh@cryptsoft.com
[9] mailto:jason.thatcher@cryptsoft.com
[10] mailto:Tim.Chevalier@netapp.com
[12] mailto:ddale@netapp.com