Published on *OASIS* (https://www.oasis-open.org)

Call for Participation: OASIS PKCS 11 TC

Submitted by censign on Fri, 2013-01-18 14:46
Type:
Call for Participation

A new OASIS technical committee is being formed. The OASIS PKCS 11 Technical Committee 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 the 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 25 February 2013); and?

(b) you must attend the first meeting of the TC, at the time and date fixed below (04 March 2013).

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.
----------?
[a] https://www.oasis-open.org/apps/org/workgroup/pkcs11/ [1]

[b] See http://www.oasis-open.org/join/?

[c] http://www.oasis-open.org/committees/pkcs11/ [2]

CALL FOR PARTICIPATION
The charter for this TC is as follows.

(1) TC Charter

(1)(a) Name of the TC

OASIS PKCS 11 Technical Committee

(1)(b) Statement of Purpose

The purpose of the PKCS 11 Technical Committee is the on-going enhancement and maintenance of the PKCS #11 standard, widely used across the industry as a core specification for cryptographic services. The PKCS #11 standard, originally developed under the leadership of RSA Laboratories, specifies an API, called Cryptoki, for devices which hold cryptographic information and perform cryptographic functions. The API follows a simple object-based approach, addressing the goals of technology independence (any kind of device) and resource sharing (multiple applications accessing multiple devices), presenting to applications a common, logical view of the device called a cryptographic token.

(1)(c) Scope of Work

The committee will address requirements for enhancements to and maintenance of the PKCS #11 standard as an API for devices that may hold cryptographic information and may perform cryptographic functions. These requirements include such areas as new mechanisms for instrumentation of the PKCS #11 application programming interface. Other areas of in-scope activity for the committee include the specification of new PKCS #11 functionality in support of integration with other standards, particularly OASIS Key Management Interoperability Protocol (KMIP). The committee will also engage in activities that support effective and interoperable implementation of PKCS #11, including such activities as developing guidance on the use of PKCS #11, supporting interoperability testing and coordination of reference implementations.

(1)(d) List of Deliverables

The initial goal of the OASIS PKCS 11 Technical Committee is to finalize the current draft work on V2.30 of the PKCS #11 Specification, based on the contributions listed in (2)(h)", within 12 to 18 months of the first meeting. Inclusion of additional mechanisms and other enhancements will also be considered for this release, to the extent that they can be accommodated within a reasonable time-frame. The deliverable for this initial work is the following:

- PKCS #11 Specification. This provides the normative expression of the application programming interface, including objects, attributes, operations, mechanisms and other elements. The specification may be created as a single document or (as is the case with the current draft) or in multiple parts to facilitate ease-of-use of the standard.

The PKCS #11 Specification will be the primary on-going deliverable of the TC. However, as part of its continuing work, the PKCS 11 TC will also support activities to encourage adoption of the PKCS #11 standard. These activities and related deliverables are anticipated to include:

- Development of PKCS #11 Test Cases documentation, describing test scenarios and implementation details for

purposes of validating PKCS #11 functionality and verifying interoperability across PKCS #11 implementations.

- Development of PKCS #11 Profiles documentation, containing profiles that enable PKCS #11 implementations to claim conformance to specific sets of PKCS #11 functionality.

- Development of PKCS #11 Usage Guide documentation, providing guidance on the use of PKCS #11 functionality

- Development of PKCS #11 Errata documentation, if and as needed.

- Definition of integration mechanism for use of PKCS #11 with other standards, such as OASIS KMIP.

- Coordination of functional testing validating PKCS #11 functionality

- Coordination of interoperability testing across PKCS #11 implementations as interoperability sessions to test effectiveness of the specification

- Coordination of efforts to develop reference implementations of PKCS #11

(1)(e) IPR Mode

The PKCS 11 TC is anticipated to operate under RF on RAND mode of the OASIS IPR Policy [https://www.oasis-open.org/policies-guidelines/ipr#s10.2.2].

(1)(f) Anticipated Audience or Users

PKCS #11 is intended for architects, designers and implementers of providers and consumers of cryptographic services.

(1)(g) Language

Work group business and proceedings will be conducted in English.

(2) Non-Normative Information Regarding TC

(2)(a) Similar or Applicable Work

PKCS #11 is one of the family of standards called Public-Key Cryptography Standards (PKCS), originally developed under the leadership of and published by RSA Laboratories. Minimal further development is anticipated at this time for the other standards within the PKCS family, some of which remain under RSA leadership and others of which have been transferred to IETF. The PKCS 11 Technical Committee will maintain TC Liaison relationships with both RSA and IETF with respect to the other standards in the PKCS family, to the extent that there is relevant activity in those organizations regarding these other standards.

Activity in support of cryptographic standardization is also going on in a number of other venues, including other OASIS committees such the Key Management Interoperability Protocol (KMIP) Technical Committee, other standards organizations such as IETF KeyProv, and under vendor sponsorship such as the Microsoft MS-CAPI standard. The PKCS 11 Technical Committee will seek to align its technical activities and deliverables with these other standardization initiatives in order to support harmonized vocabularies, avoid unnecessary duplication of effort, and promote interoperability and integration with respect to cryptographic objects and operations. Where deemed appropriate, the OASIS PKCS 11 Technical Committee will establish formal TC Liaison relationships with other organizations working on related standards.

(2)(b) Date, Time, and Location of First Meeting

The first meeting will be held in person on Monday, 4 March 2013, at 9:00 AM Pacific Standard Time. It will be hosted by EMC/RSA in the San Francisco area. Conference calling facilities will be provided for those who cannot attend in person.

(2)(c) Ongoing Meeting Plans and Sponsors

The TC expects to meet bi-weekly by conference call. Sponsorship is to be determined at the first meeting.

(2)(d) Proposers of the TC

1. Gil Abel, gil@athena-scs.com [3]. Athena.

2. Chris Zimman, czimman@bloomberg.com [4], Bloomberg

3. Tim Hudson, tjh@cryptsoft.com [5], Cryptsoft

4. Tony Cox, tjc@cryptsoft.com [6], Cryptsoft

5. Robert W. Griffin, robert.griffin@rsa.com [7], EMC.

6. Steve Wierenga, steve.wierenga@hp.com [8], HP

7. Valerie Fenwick, valerie.fenwick@oracle.com [9], Oracle.

8. Michael Stevens, ms@quintessencelabs.com [10], Quintessence Labs

9. Ajai Puri, ajai.puri@safenet-inc.com [11], SafeNet.

10. Mark Lambiase, mlambiase@gosecureauth.com [12], SecureAuth

11. Robert Lockhart, robert.lockhart@thales-esecurity.com [13], Thales.

12. Peter Gutmann, pgut001@cs.auckland.ac.nz [14], University of Auckland

(2)(e) Statements of Support

1. Gil Abel, gil@athena-scs.com [3]. Athena. ?As Athena's primary representative to OASIS, I approve the PKCS 11 TC charter and endorse all Athena proposers listed in (2)(d).?

2. Kevin Fleming, kpfleming@bloomberg.net [15], Bloomberg. ?As Bloomberg's primary representative to OASIS, I approve the PKCS 11 TC charter and endorse all Bloomberg proposers listed in (2)(d).?

3. Tim Hudson, tjh@cryptsoft.com [5], Cryptsoft. "As Cryptsoft?s primary representative to OASIS, I approve the PKCS 11 TC charter and endorse all Cryptsoft proposers listed in (2)(d)."

4. Robert Philpott, robert.philpott@rsa.com [16], EMC. "As EMC?s primary representative to OASIS, I approve the PKCS 11 TC charter and endorse all EMC proposers listed in (2)(d)."

5. Joel Fleck, joel.fleck@hp.com [17], HP. "As HP?s primary representative to OASIS, I approve the PKCS 11 TC charter and endorse all HP proposers listed in (2)(d)."

6. Martin Chapman, martin.chapman@oracle.com [18], Oracle. "As Oracle?s primary representative to OASIS, I approve the PKCS 11 TC charter and endorse all Oracle proposers listed in (2)(d)."

7. John Leiseboer, jl@quintessencelabs.com [19], Quintessence Labs. "As Quintessence Labs?s primary representative to OASIS, I approve the PKCS 11 TC charter and endorse all Quintessence Labs proposers listed in (2)(d)."

8. Bill Becker, bill.becker@safenet-inc.com [20], SafeNet. "As SafeNet?s primary representative to OASIS, I approve the PKCS 11 TC charter and endorse all SafeNet proposers listed in (2)(d)."

9. Mark Lambiase, mlambiase@gosecureauth.com [12], SecureAuth. "As SecureAuth?s primary representative to OASIS, I approve the PKCS 11 TC charter and endorse all SecureAuth proposers listed in (2)(d)."

10. Darren Learmonth, darren.learmonth@thales-esecurity.com [21], Thales. "As Thales? primary representative to OASIS, I approve the PKCS 11 TC charter and endorse all Thales proposers listed in (2)(d)."

(2)(f) TC Convener

Robert Griffin, robert.griffin@rsa.com [7], EMC will be the convener.

(2)(g) Member Section Affiliation

The PKCS 11 TC will request affiliation with the IDtrust Member Section.

(2)(h) Initial Contributions

EMC will contribute ?PKCS #11 Specification V2.30)" consisting of the following four documents:

- PKCS #11 V2.30 Specification Front Matter [1]
- PKCS #11 V2.30 Core Specification [2]
- PKCS #11 V2.30 Mechanisms Part 1 [3]
- PKCS #11 V2.30 Mechanisms Part 2 [4]

(2)(i) FAQ Document

An initial ?PKCS 11 TC FAQ? document is under development.

(2)(j) Work Product Titles

The PKCS 11 Technical Committee anticipates four primary work products with the following draft titles:

PKCS #11 Specification (this may consist of multiple documents, each comprising part of the complete specification)

PKCS #11 Test Cases

PKCS #11 Profiles

PKCS #11 Usage Guide

==========

References

==========

[1] PKCS #11 Version 2.30: Cryptographic Token Interface Standard: Front Matter (draft), April 2009.

ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-30/pkcs-11v2-30-d1.pdf [22]

[2] PKCS #11 Version 2.30: Cryptographic Token Interface Standard: Core Specification (draft), April 2009.

ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-30/pkcs-11v2-30b-d6.pdf [23]

[3] PKCS #11 Version 2.30: Cryptographic Token Interface Standard: Mechanisms Part 1 (draft), April 2009.

ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-30/pkcs-11v2-30m1-d7.pdf [24]

[4] PKCS #11 Version 2.30: Cryptographic Token Interface Standard: Mechanisms Part 2 (draft), April 2009.

ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-30/pkcs-11v2-30m2-d3.pdf [25]

Associated TC:
PKCS 11
Associated MS:
IDtrust
Deadline:
Fri, 2013-01-18 - Mon, 2013-03-04

Links:
[1] https://www.oasis-open.org/apps/org/workgroup/pkcs11/
[2] http://www.oasis-open.org/committees/pkcs11/
[3] mailto:gil@athena-scs.com
[4] mailto:czimman@bloomberg.com
[5] mailto:tjh@cryptsoft.com
[6] mailto:tjc@cryptsoft.com
[7] mailto:robert.griffin@rsa.com
[8] mailto:steve.wierenga@hp.com
[9] mailto:valerie.fenwick@oracle.com
[10] mailto:ms@quintessencelabs.com

[11] mailto:ajai.puri@safenet-inc.com
[12] mailto:mlambiase@gosecureauth.com
[13] mailto:robert.lockhart@thales-esecurity.com
[14] mailto:pgut001@cs.auckland.ac.nz
[15] mailto:kpfleming@bloomberg.net
[16] mailto:robert.philpott@rsa.com
[17] mailto:joel.fleck@hp.com
[18] mailto:martin.chapman@oracle.com
[19] mailto:jl@quintessencelabs.com
[20] mailto:bill.becker@safenet-inc.com
[21] mailto:darren.learmonth@thales-esecurity.com
[22] ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-30/pkcs-11v2-30-d1.pdf
[23] ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-30/pkcs-11v2-30b-d6.pdf
[24] ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-30/pkcs-11v2-30m1-d7.pdf
[25] ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-30/pkcs-11v2-30m2-d3.pdf