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

Call for Participation: OASIS Identity Based Attestation and Open Exchange Protocol Specification (IBOPS) TC

Submitted by censign on Fri, 2014-08-08 22:54
Type:
Call for Participation

A new OASIS technical committee is being formed. The OASIS Identity Based Attestation and Open Exchange Protocol Specification (IBOPS) 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 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 16 September 2014; and

(b) you must attend the first meeting of the TC, at the time and date fixed below (23 September 2014).

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/ibops/ [1]

[b] See http://www.oasis-open.org/join/ [2]

[c] http://www.oasis-open.org/committees/ibops/ [3]

?CALL FOR PARTICIPATION?
OASIS Identity Based Attestation and Open Exchange Protocol Specification (IBOPS) Technical Committee Charter

The charter for this TC is as follows:

--

Section 1: Charter

(1)(a) TC Name

OASIS Identity Based Attestation and Open Exchange Protocol Specification (IBOPS) TC

(1)(b) Statement of Purpose

One of our highest priorities in the information security field is the development of techniques to confirm that a person accessing online resources is who he claims to be. Simply stated, a person must be able to validate its identity before it is allowed to gain access to information, otherwise access to a resource should be denied.

Many recent enterprise level security breaches have been made by hackers with the aim to gain access to sensitive information. Such attacks have enhanced the awareness for the need for better authentication methods and means for protecting identity information to prevent crime and fraud at all levels.

There are five categories of authentication methods used by resource owners: 1) something you have, 2) something you know, 3) something you are, 4) something you do and 5) the context of your interaction. One of the most used authentication methods in today?s online systems belongs to the ?something we know? category and is generally based on user name and password. A more sophisticated method of authentication for example, can be based on ?something we have? category such as smart cards or tokens; these are not widely adopted due to cost and other factors.

In order to capitalize on strong authentication as a service types deployment, many countries are working towards establishing trust-based identity systems to enable the use of stronger authentication among relying parties across the identity landscape. Federation technologies, coupled with national and industry-specific trust frameworks, are emerging as a viable solution to capitalize on emerging stronger methods of authentication.

Until recently, the use of biometrics technology was resource intensive. However, the advent of smart phones, smart watches and mobile devices that include sensors (such as cameras, fingerprint scanners, and microphones, and GPS) has made it feasible and affordable to use biometrics for identification and authentication for online access. Biometrics Recognition systems can identify users based on either physiological or behavioral characteristics along with contextual information.

The demand for the ease and reliability offered by biometrics is growing. Individuals have password fatigue and tend to reuse passwords across many sites, which add to the risk of identity theft and fraud. At present, biometrics technology holds a great deal of promise as the solution the industry has been searching for.

Biometric technologies can potentially provide consumers with a long-awaited convenience to securely enter into the cyberspace using unique biological traits rather than user name and password combinations. The traits can be stored directly on the device or stored at the server. The Fast Identity Online (FIDO) Alliance is developing methods using universal authenticators that can support biometric methods that are local to a device and enable them to be used for strong authentication. There are other use cases, however, that require the enterprise or provider to store the biometric information on local servers either in addition to local clients or as an alternative to provide enhanced authentication solutions. These are the use cases that IBOPS is intended to address.

The goal of this Technical Committee is to develop the Identity-Based Attestation and Open Exchange Specification (IBOPS) with the aim to protect digital assets and digital identities on the client, server and the data exchange in-between. The TC will also develop a set of APIs that can be used by applications to interact with servers that store biometric information locally. IBOPS will define a standard API to be used by application developers to interact with such servers. The IBOPS communication architecture will run on any secure protocol such as Transport Layer Security (TLS) connections over the encryption mechanism to servers that hold identity data. IBOPS will not compete with other standards such as FIDO, since IBOPS is designed to address use cases that require the relying party to have access to biometric or other identity information.

The IBOPS standard will allow systems to meet security needs by using the IBOPS API coupled with the use of appropriate security concepts. In particular, IBOPS works with the assumption that security is accomplished by securing the identity data at the server, in transit, and on the device. The working assumption here is a hack of the central server will only compromise the data of one entity, thus a hacker would need to break the IBOPS system one user at a time before obtaining access to mass data.

The IBOPS functionality will offer developers the ability to use appropriate security to systems in development. IBOPS may be used as the sole security mechanism or it may be used in conjunction with other mechanisms, such as SAML.

IBOPS does not prevent the use of biometric or authentication work that is being developed or has been developed in other standardization bodies. In particular, IBOPS will adopt the authentication assurance concepts and principles as developed in ISO/IEC 29115, ITU-T X.1254 and OASIS Trust Elevation Specifications, and OASIS Biometric Identity Assurance Services (BIAS).

IBOPS will also reference best practices documents for Biometric-with-Mobile devices such ISO/IEC TR 30125, as the goal of IBOPS is to secure biometric data by eliminating the need for storing images on local devices or servers.

As such, IBOPS will not conflict or replace standards such as ISO/IEC 19794, (Biometric data interchange formats) or ISO/IEC 19785 (Common Biometric Exchange Formats Framework) or ISO/IEC 19795 (Biometric performance testing and reporting), ISO/IEC 24761:2009 (Authentication context for biometrics), ISO 19092:2008, (Financial services, Biometrics. Security framework)

IBOPS interoperability requires IBOPS to function through the IBOPS API, allowing pluggable components for Identity Assertion, Role Gathering, Access Control, Assurance, and Storage. Any tool using any implementation may ?plug? into any IBOPS-enabled server and continue conversational input for secure access.

(1)(c) Scope

The TC will develop the IBOPS specification to enable security systems to provide Identity Assertion, Role Gathering, Multi-Level Access Control, Assurance, and Auditing capabilities. IBOPS will define how software running on a client device can communicate with an IBOPS-enabled server. Methods for enabling security components to work with existing IBOPS components for integration into current operating environments will also be considered.

The TC will develop IBOPS specification with the aim of providing continuous protection of identity resources in a manner that enables defining of mechanisms that ensure security to a given service level guarantee of security.

IBOPS will allow systems to meet security needs by interacting with an API through a secure protocol and architecture that is RESTful and is language neutral. To facilitate maximum interoperability, all tools used and resulting IBOPS deliverables will adhere to open standards. Interoperability and conformance criteria will be clearly defined and developed in the TC Specifications.

The scope does not consider the ?how? of the standard. The specification shows the ?what? and is independent of implementation.

(1)(d) Deliverables

1. A use case and gap analysis document that depicts the problems that IBOPS is addressing.

2. An end-to-end specification describing the standards necessary to perform server-based enhanced biometric security. This solution will consider enrollment phase, maintenance, storage, and revocation. Version 1.0 of the specification should be completed within 18 to 24 months of the first meeting.

3. The TC might also develop interoperability profiles for OASIS Trust Elevation Protocol, FIDO, SAML, Open ID Connect and OAuth if deemed appropriate by the TC.

4. The TC may produce other deliverables as interoperability testing tools, tutorials, presentations, best practices, or non-normative definitions to be used for testing, as the TC may deem useful to implementers of the standard.

(1)(e) IPR Mode

This TC will operate under the Non-Assertion IPR mode as defined in the OASIS Intellectual Property Rights (IPR) Policy effective 21 June 2012.

(1)(f) Audience

Security evaluators, system underwriters, developers, and systems engineers will all benefit from IBOPS. For those wishing to underwrite an application, IBOPS will provide a mechanism that if adhered to, will ensure risk mitigation. Adhering to IBOPS removes the ?how to? for adjudicators, developers, administrators, and managers. Simply adopting IBOPS and adhering to its rules will mitigate security risk.

The audience for creating and considering IBOPS includes developers, system engineers, and adjudicators.

(1)(g) Language

English

Section 2: Additional Information

(2)(a) Identification of Similar Work

The TC will work closely and will coordinate with the IEEE Project P2410. , The TC will establish a Liaison relationship with IEEE, ISO JTC1 SC 37 and TC 68, ANSI, ITU-T SG 17 and other bodies (such as the Biometric Consortium).

(2)(b) First TC Meeting

The first meeting will be a face-to-face meeting to be held on September 23 in Geneva from 9:30 AM to 05: 30 PM local Geneva time at Place des Nations 1211 Geneva 20 Switzerland. The meeting will be face-to-face. Hoyos Labs will sponsor the first meeting. A teleconference bridge will be provided for TC members who are unable to attend in person.

(2)(c) Ongoing Meeting Schedule

The TC will meet biweekly by teleconference and hold face-to-face meetings as needed. Sponsorship of the meetings will rotate among the members.

(2)(d) TC Proposers

Scott Streit, scott@scottstreit.com [4], Villanova University
Abbie Barbir, abbie.barbir@bankofamerica.com [5], Bank of America
Liz Votaw, liz.votaw@bankofamerica.com [6], Bank of America
Eileen Bridges, eileen.bridges@innovate.bankofamerica.com [7], Bank of America
Gill, Davindar, davindar.gill@bankofamerica.com [8], Bank of America
Hector Hoyos, hhoyos@hoyoslabs.com [9], HOYOS Labs Corp
Anil Saldhana, anil.saldhana@redhat.com [10], Red Hat
Shahrokh Shahidzadeh, shahrokh.shahidzadeh@intel.com [11], Intel

(2)(e) Statements of support

Abbie Barbir, abbie.barbir@bankofamerica.com [5], Bank of America: As Bank of America?s Primary Representative, I approve the IBOPS TC Charter and support our proposers ?Abbie Barbir, Liz Votaw, Eileen Bridges, Gill, Davindar? as a named co-proposers.

Scott Streit, scott@scottstreit.com [4], Villanova University: As Villanova University?s Primary Representative, I approve the IBOPS TC Charter and agree to have my name as a named co-proposer.

Hector Hoyos, hhoyos@hoyoslabs.com [9], as HOYOS Labs Corp primary representative I approve the IBOPS TC Charter and agree to have my name as co-proposer.

I Mark Little, mlittle@redhat.com [12], Red Hat, ? As Red Hat?s" Primary Representative, I approve the IBOPS TC Charter and support our proposer ?Anil Saldhana? as a named co-proposers.?

I, Shahrokh Shahidzadeh, shahrokh.shahidzadeh@intel.com [11], Intel, ? As Intel?s" Primary Representative, I approve the IBOPS TC Charter, and agree to have my name as a named co-proposer.

(2)(f) Convener

Abbie Barbir of Bank of America will be the convener.

(2)(g) Member Section Affiliation

The TC intends to request affiliation with the IDtrust Member Section.

Associated TC:
etmf
Deadline:
Fri, 2014-08-08 - Tue, 2014-09-23

Links:
[1] https://www.oasis-open.org/apps/org/workgroup/ibops/
[2] http://www.oasis-open.org/join/
[3] http://www.oasis-open.org/committees/ibops/
[4] mailto:scott@scottstreit.com
[5] mailto:abbie.barbir@bankofamerica.com
[6] mailto:liz.votaw@bankofamerica.com
[7] mailto:eileen.bridges@innovate.bankofamerica.com
[8] mailto:davindar.gill@bankofamerica.com
[9] mailto:hhoyos@hoyoslabs.com
[10] mailto:anil.saldhana@redhat.com
[11] mailto:shahrokh.shahidzadeh@intel.com
[12] mailto:mlittle@redhat.com