Identity Based Attestation and Open Exchange Protocol Specification

(IBOPS)

Architecture and Security

Last Updated: Version 1.00, April 10, 2015

Specification URIs
This version:
Previous version:
Latest version:

Technical Committee:
Identity Based Attestation and Open Exchange Protocol Specification TC

Chairs:

Editors:

Related work:

Abstract:
This document is a specification that ...TBD
Table of Contents

Identity Background
   A Short History Of Identity
   Biometrics Overview

IBOPS Overview
   Introduction to BOPS
   Architecture Overview

IBOPS Identity Management
   Identity Genesis and User Enrollment
      Overview
      The Genesis/User Enrollment Process
      Secondary Devices and Backup
   Authentication/Identity Assertion
      Overview
      Client Software Authentication
      Post-genesis device/user authentication
      Server Authentication

Authenticated Session Management

Access Control

Intrusion Detection
   Overview
   Replay Prevention

Standards, Audit, and Quality Control
   Standards
   Audit Capabilities
   Implementation Quality

Data Protection
   Network Transmissions
   Data Protection Strategy
   Client-side data
   Server-side data
      IBOPS Server Data
      Host Data

IBOPS Server Resource Guide
1. Identity Background

   a. A Short History Of Identity

Identification of humans is a goal as ancient as humanity itself. As technology and services have developed in the modern world, human activities and transactions have proliferated in which rapid and reliable personal identification and authentication (asserting an identity) is required. Examples include passport control, computer login control, bank automatic teller machines and other transactions authorization, premises access control, and security systems generally. All such identification efforts share the common goals of speed, reliability, automation, and security of the identification process itself.

   b. Biometrics Overview

Biometrics is the science of measuring human beings based on unique biological features that are part of our bodies at birth: face, fingerprint, palm print, voice, vein patterns, retinal blood vessel patterns, DNA, retina, and iris.

The key to the power of biometrics to identify people is the amount of randomness and complexity that the biometric factor contains. This is what in biometrics is referred to as degrees of freedom or independent dimensions of variation. The more degrees of freedom the more biometrics information there is to identify you, and these vary across the different biometric factors.

Generally speaking, fingerprinting and iris scanning can be a far more accurate test than facial recognition; however, there is also a practical consideration of acquisition or usability due to convenience in the acquisition of a biometrics factor. There is also the spoofing issue of a biometrics factor.

IBOPS utilizes and considers multiple modalities/factors of biometrics, from fingerprint to face to iris. Regardless of the specific biometrics chosen, or if all are chosen in a multi-factor approach, our default biometrics-based solution consists of a client-server architecture.

2. IBOPS Overview

   a. Introduction to IBOPS
Biometric technologies provide consumers with long-awaited convenience to securely and reliably authenticate themselves to computer systems.

The Identity Biometric Open Protocol Standard (IBOPS) defines provides a guarantee that named users are who they claim to be. IBOPS identity assertion implies reliance on human biometrics, however IBOPS is an interoperable standard and can incorporate any number of identity asserters, be they biometrics-based or not, to allow retrofitting into existing identity assertion solutions.

The standard allows pluggable and interchangeable modules, including those that provide identity assertion, role gathering, assurance and auditing capabilities. IBOPS was designed to easily integrate into pre-existing identity management environments, where the pluggable components can replace the functionality of pre-existing components.

b. Architecture Overview

The IBOPS platform includes software running on client devices (eg mobile phones or desktop systems) and the back end IBOPS server.

The server infrastructure can easily be deployed within cloud or traditional on-premise environments as it integrated into web server systems as a web archive. The architecture is language-agnostic, allowing client-server and server-server communication via RESTful API’s and JSON.
The following diagram provides a high level overview of the IBOPS architecture, including data sets shared between the client and server, demonstrating the concept of a user’s Account, a device, and an authenticated session. This is described in detail in the following sections.

The example below shows one example configuration. The keystore works in conjunction with the SSL/TLS layer in providing data confidentiality. The reference to SSL/TLS refers to the latest version of TLS, which provides transport layer data confidentiality.

The keys in the keystore are the keychain necessary for the hostname defined in the base key, from a valid certifying authority. This key along with the root and intermediary keys comprise a full key chain for the given hostname. This keystore works in providing the https for web access. This is differentiated from the truststore.

The truststore provides, through the use of a custom Certifying Authority (CA) the identity a given can be, at any point in time. The truststore performs the handshaking between a certificate created by a CA and the given Web Server. The information in the certificate is present in every call to the server and is used with an authentication token to specify an authentication state.

The use of the keystore and truststore is one common mechanism for data confidentiality. This specification allow other key mechanisms as long as the confidentiality of a keystore is maintained and the identity from a truststore is also maintained.
GENESIS is an identity without a biometric. Devices have enrollments with initial biometrics. GENESIS is represented in storage as a singleton for each subject. Each subject may have many devices where each device has a biometric. The biometric per device may differ from device to device. For example, a phone may use a fingerprint as a biometric and a tablet may use an iris. For this example, the phone would have an initial enrollment of the fingerprint, and the tablet would have an initial enrollment of an iris.
3. IBOPS Identity Management

a. Identity and Genesis

Genesis is the initial creation of a subject. Genesis occurs once for each subject and is not bound to any particular device. A variety of options may occur to determine an identity for Genesis as the succeeding table shows.

Table 1 - Genesis Levels

<table>
<thead>
<tr>
<th>Genesis Level</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify SMS</td>
<td>Verify SMS</td>
<td>Verify SMS</td>
<td></td>
</tr>
<tr>
<td>Verify Email</td>
<td>Verify Email</td>
<td>Verify Email</td>
<td></td>
</tr>
<tr>
<td>Ask 3 Questions only know by Identity</td>
<td>Ask 3 Questions only know by Identity</td>
<td>Previous Identity Information</td>
<td></td>
</tr>
</tbody>
</table>

As table 1 shows, we have 3 Genesis Levels. The levels allow certain privileges to occur and IBOPS may be queried for the Genesis level of any subject. For Level 0, the users was confirmed by sending an SMS message and a confirming email. This is the lowest level of Genesis.

Level 1 uses the properties of Level 0 plus asking 3 questions that only the Subject should know. Proper answering of these questions places the Subject at Genesis Level 1.

Genesis Level 2 uses the properties of Level 1 plus using any other identity information an organization may have. This information was used prior to IBOPS to determine an identity.
During the Genesis process additional information comes to the IBOPS Server. Included in this information are two values (between 0 and 59) which are used as replay mitigation. Additionally, a certificate is given to the client which relates all subsequent application programming interface (API) calls to the subject. The diagram below illustrates the flow of a Genesis.

The following diagram provides a high level overview of the Enrollment process:

b. Identity and Enrollment
The enrolment process links a pre-existing digital identity (from a Genesis) with a single biometrically-identifiable user linked to a device. Other devices are linked to the Genesis phase through an Enrollment of a second, third or nth device.

 Depending upon implementation, the enrollment process may include verification of a pre-existing digital identity/account - for example, email address or phone number confirmation or validation utilizing a third party/pre-existing system. This can happen in several stages, and the order in which this happens depends on the specific product or solution. It is vendor dependent whether the certificate is tied to a Genesis, meaning the Subject has one and only one certificate, or alternately may use a separate certificate per enrollment and tie each enrollment to a Genesis in the IBOPS Server.
During enrollment the following steps take place.

1. **Obtain Client Certificate.**

A Client Certificate is generated on IBOPS Sever. This certificate is what represents a device/user pairing. The format of a certificate may vary from implementation to implementation. The following paragraph assumes an X.509 certificate, but it is the general concept which applies to the IBOPS standard. In summary, the certificate must be locked with a password or some referencing value, must be stored on the client device and must not store the password in plain text. The server must use the concept of a Certifying Authority and a truststore to create and validate the use of the client certificate.

For example, assume a Client Certificate is an X.509 certificate. This certificate contains a unique public key representing the device/user pair. This public key and the associated private key are generated on the server but not maintained or stored on the server.

The Client Certificate also contains an identifier known as a GUID (a part of a Distinguished Name in the certificate’s Subject field) that allows the server to refer to an individual user account. The GUID is unique to each client certificate/device.

The IBOPS server is also a Certificate Authority (CA), which signs a Client Certificate using the Server CA private key. The Server CA key pair and related certificate are referred as “Server CA keys” and “Server CA Certificate”. Those are stored by the IBOPS server’s host system.

A Server CA certificate, a Client Certificate, and an associated private key are incorporated into a PKCS #12 (p12) file, encrypted with a password\(^1\), and sent to the client via an API call over the pre-established TLS session.

\(^1\) More Details needed
The encrypted p12 with its embedded private key, Client Certificate, and Server CA Certificate are employed to establish subsequent TLS sessions.

The encrypted p12 is stored on a device².

---

² Refer to the section titled [Client-side data](#) for further information.
Client Certificate and associated private key example:

We are using RSA algorithm with 1024 key size. However, this is configurable in B0PS:
- **ALGORITHM_OID** / default value = 1.2.840.113549.1.1.5
- **KEY_LENGTH** / default value = 1024
- **KEY_CERTAINTY** / default value = 80

2. **Biometric enrollment.**

Biometric enrollment occurs as follows:

a. Acquire biometric factor data through the device (for example, face, fingerprint, iris etc).
b. Generate the biometric vector (hash).

c. Store biometric vector on the client for user authentication.

b. Authentication/Identity Assertion

i. Overview

Successful authentication of a user/device combination is required in order to allow access to requested resources. The IBOPS has multiple points of authentication to enable that:

- Initial client software is authenticated using embedded default certificates that are shared with the server within a standard TLS session handshake.

- After genesis/enrollment, users are authenticated using biometrics, matched locally on a mobile device.

- The pre-registered device authenticates to the server using a Client Certificate, shared over a standard TLS session handshake. The Client Certificate represents a pre-registered user/device pairing. A client certificate can't be submitted to a server until the certificate is decrypted with a password, which is obtained under a condition of a successful user authentication.

- Server authentication is also enabled using server certificates shared with the client during the TLS session handshake.

Each of these authentication points are described in detail in the following sections.

ii. Client Software Authentication

When installed, the client application comes pre-loaded with a default X.509 certificate that allows 2-way TLS-based authentication to be immediately enforced and active throughout the genesis/enrollment stages. This certificate allows establishment of an TLS session with a URI dedicated to allowing the initial stages of genesis alone, with a limited number of APIs available over that URI. After genesis/user enrollment, this default certificate is replaced with the Client Certificate.
iii. Post-enrolment device/user authentication

User Authentication:

A user is authenticated by matching biometric vectors and passing liveness tests. The user's biometrics, single factor or multi-factor, are acquired through the device (for example, face, fingerprint, iris etc). Biometric vector(s) are extracted from the acquired biometrics. The vector(s) are matched against saved biometric vector(s) obtained during genesis and enrollment.

IBOPS performs matching on the client side. After the client software validates the user via their biometrics, the biometrics authentication result is sent to the server regardless of the matching result.

In line with the IBOPS standard, all applications should include some form of liveness detection or an ability to ensure that the enrolled or authenticated user is an actual person and not an image or other representation of the user. For a face recognition system, it could be blink detection, for instance. Adjustable liveness detection levels are configurable on the Boriken server. Their adjustment affects false negative and false positive thresholds, timing, and usability. The choice of a liveness level is up to the organization using IBOPS and its particular needs.

Device authentication

IBOPS authenticates at two levels: within the underlying TLS session and within the server itself:

1. TLS-level authentication of the client device utilizes an X.509 certificate that was generated and signed by the Boriken server during user genesis/enrollment, linked to a stored user/device pairing, and then provided to the client. We refer to this as the Client Certificate. To authenticate a device, the client software unlocks the Client Certificate and submits it to the server as a part of the TLS session handshake. In line with the TLS handshake protocol the client then allows the Client Certificate to be verified by the server via the TLS “Certificate Verify” message. The Client Certificate is unlocked (decrypted) using a password obtained after successful authentication.

---

3 If enabled.
4 Because the TLS session is using a different client certificate to that used initially at genesis (which was the default certificate), the TLS session is established with a different URI endpoint.
2. After verification of the Client Certificate, the Boriken server login module extracts the client certificate’s device identifier (the GUID), looks up the appropriate account, checks for certificate revocation, determines roles associated with that account, and establishes an authenticated and authorized session.

iv. Server Authentication

Server authentication is achieved using the underlying TLS session. To meet the IBOPS requirements of two-way authentication between client and server, IBOPS requires TLS or TLS using client and server X.509 certificates.

The IBOPS server certificate used for TLS sessions is verified (signed) by a third party Certificate Authority, in this case GoDaddy, using their private key.

The client is able to verify the integrity of the IBOPS certificate by referring to the 3rd party CA (GoDaddy)’s public key, included as a certificate in the distribution of most common browsers and operating systems. This verification is completed as part of the standard SSL/TLS session handshake.

c. Authenticated Session Management

There are important characteristics of Session Management within IBOPS. First of all, the IBOPS protocol is stateless with respect to HTTP. This means that every call to a IBOPS-compliant server must have an identifier to the account, and the server must persist the current state. Through this mechanism IBOPS has session management. So iBOPS is HTTP stateless but stateful within its own context.

Sessions are tied to a specific user interacting with resources via the IBOPS server for a period of time. Each authorized user/device has its own unique Client Certificate, and that certificate contains a GUID which the server uses to identify the user. The identification of the User occurs by taking the GUID for the device and looking up the user for the device in the IBOPS server.

Initially the IBOPS server creates an opportunity for a session. This may be done in a variety of ways, but is most commonly done with a QR Code display. This call is a Session Opportunity meaning that the system displaying the QR Code may, after authentication, allow the establishment of a session. Or, alternately, the Session Opportunity may timeout or not authenticate.

In the case of successful user authentication and Session Opportunity, we have a Session.
Within the IBOPS server a persistent session is established specific to the account referenced via the Client Certificate.

Sessions may take in any kind of data as of tag/value pairs. This may be geospatial data, variable transaction amounts, or any other data we wish to store throughout the duration of the session. In the case of geo-fencing, which is wanting to control the physical location of a session, we add in latitude and longitude. In the case of an ATM, we add withdrawal amounts to the session.

At some point in time, the session completes. At session completion, all information about the session is written to a history/audit.

In the case of disallowing a device, user or account, the appropriate Client Certificates get revoked by removing the GUID from the IBOPS server. All future calls to the server will no longer result in successful communication.
d. Access Control

The Client Certificate is used to authenticate a user's identity and to manage access control.

In line with the IBOPS standard, the IBOPS server enforces a mandatory access control policy over all subjects and objects\(^5\) under its control. The mandatory access control policy guarantees all data is labelled and all users have roles.

Roles are attributes associated with a user, such as “Administrator” or “Guest”, which are either gathered and stored in the server or a pre-existing enterprise system such as Active Directory. The Boriken server may be the definitive role source, may delegate the role source, or may work in conjunction with a role source. For example, some implementations of an IBOPS server stores role information that deals with security levels such as liveness. Alternately, a IBOPS Server may be implemented as part of an AD integration for a large enterprise. Active Directory may be the role source for a given organization, but the same organization may use the IBOPSServer to dictate more refined liveness for certain other roles. In this case the combination of the Boriken server and Active Directory create the authoritative role source, available via an API call.

Data is labeled with characteristics that describe access or access patterns - for example data may be labeled as “All”, allowing all access. The server maintains these sensitivity labels.

A mapping between roles and sensitivity labels allows us to implement role-based adjudication. Boriken server administrators can specify and control sharing of objects with subjects and determine if a given subject may read, write or execute an object via an API within a particular session.

Roles are typically hierarchical in nature. A subject can write an object only if the hierarchical classification in the subject’s security level is less than or equal to the hierarchical classification in the object’s security level and all the non-hierarchical categories in the subject’s security level are included in the non-hierarchical categories in the object's security level.

To further illustrate, the IBOPS server receives a request. The request has a certificate which links the device to the user. The user has many roles so the roles (after the hierarchy is flattened) are stored in memory in something that the Java Authentication Services. The authenticated user is called a Principal. In subsequent processing, web pages may allow access for certain roles and data may have labels that correspond to the users roles. Data adjudication compares the data labels against the roles for the Principal. So access control is both on functionality and data.

\(^5\) A subject is an individual or group of named users, devices or programs. An object may be data, processes, files, segments, devices.
## LOGIN LEVELS

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SMS</td>
<td>SMS</td>
<td>Biometric</td>
<td>Biometric &amp; Liveness</td>
</tr>
</tbody>
</table>
4. Intrusion Detection

a. Overview

The IBOPS standard requires the implementation of intrusion detection capabilities. Depending on the specific implementation, these capabilities may provide active monitoring and blacklisting functionality to help address attacks, including credential spoofing via certificate impersonation, session replay, detection and prevention of account brute-forcing, session creation failures, and/or the detection of denial-of-service (distributed or single DOS) attacks. These functions should be governed by one or more intrusion detection systems which can take appropriate actions such as terminating session creation or blacklisting devices and/or IP addresses.

The IBOPS standard also requires specific intrusion detection capabilities implemented within a system on both server and client sides. Client-side intrusion detection must be capable of identifying patterns of trial and error in order to blacklist itself, or if the user fails to authenticate more than a configurable consecutive times. On a typical IBOPS implementation this could be around 4. Blacklisting may be enacted for a fixed period of time or indefinitely until the device can be properly assured that it is safe and valid. The IBOPS server can query the Intrusion Detection System (IDS) whether a device is blacklisted or not. If the device is blacklisted, all communication ceases. Depending on implementation, blacklisting may occur at the device level, the IP address level, the subnet level or beyond. A typical implementation may only blacklist on Device ID.

The following outlines an intrusion detection function for IBOPS.

b. Replay Prevention

One of the largest threats to network based systems is replay. Consider the scenario of an attacker modifying target software on a device and/or stealing session information from a valid session for replay, in an attempt to gain unauthorized access to a server.

Replay mitigation uses replay check values that are built into the communication to help prevent this type of attack.

From the server side perspective, the server has to recognize that the replay check values are not correct when under attack so the device can be blacklisted. The replay check values are requested by the client during Genesis and are one way encrypted by the IBOPS Server. The Boriken server looks up the one way encryption to find the values used for replay mitigation. Subsequent client calls use the check values placed by the client and expected by the server.
the values are as expected, communication continues. If the replay values are not expected the IDS receives a notification. Enough notifications and the client is blacklisted.

5. Standards, Audit, and Quality Control

a. Standards

IBOPS is designed to meet several minimum standards, including assessment against the Trusted Computer System Evaluation Criteria (TCSEC), which is a US Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system, the Director of the Central Intelligence Directive 6/3 protection levels 3, 4, and 5 (PL3, PL4, PL5), and the standards of Multiple Independent Levels of Security (MILS).

b. Audit Capabilities

Auditing ensures the appropriate artifacts for continued verification and validation of trusted access. All administrative actions (modification via the Admin dashboard) and authentication actions are captured and stored in a data repository. Account-specific authentication records can be audited by a user with Administrator privileges, via an administrator dashboard.
6. Data Protection

a. Network Transmissions

All network transmissions are required by the BOPS standard to run over Transport Layer Security (TLS) or its predecessor Secure Sockets Layer (SSL), with server and client-side X.509 certificates enforcing two-way authentication. Boriken servers (typically Apache Tomcat) are configured to use TLSv1.2.

Before a client and server can begin to exchange information protected by TLS, they must securely exchange keys and/or agree upon encryption keys and a cipher to use when encrypting data. These options are configurable and can also be negotiated on a per-session basis in line with client-side capabilities. For instance, if a client machine/application does not support TLSv1.2, then it may fallback to lower version.

Exact TLS configuration depends upon the IBOPS-compliant server configuration. Naturally, strong key generation and exchange algorithms are encouraged - similarly with encryption algorithms, in recognition of possible constraints such as compatibility or performance issues.

b. Data Protection Strategy

The general IBOPS standard philosophy is to prevent the centralized storage of sensitive data in one place. IBOPS does not create large server-side repositories of sensitive client data such as biometric images, for example.

Also as a general rule, encrypted data and the key to decrypt that data should not be in the same place. For example, in an IBOPS system, sensitive data such as the user's website credentials are stored encrypted on the mobile device, with the associated key stored in the IBOPS server repository, attached to the user's account. This helps prevent an attacker who has gained access to the mobile from reading the credentials, and vice-versa.

c. Client-side data

Sensitive data stored on the client side includes:

- the user's biometric vector (NOT the full biometric)
- the encrypted p12 file containing Client Certificate and private key
- (optional or implementation specific) encrypted user authentication data for third party identity systems

On IOS, all of this data is stored in the IOS KeyChain. This is an encrypted container that holds passwords for multiple applications and secure services.

On Android the p12 is stored in the app shared preferences:\n/data/data/com.your.package/shared_prefs/com.your.package_preferences.xml

The biometric vector is stored internal to the client side application.

It is important to note that except for a handful of unique situations, a full biometric data set cannot be derived from a biometric vector, and that the possession of a biometric vector alone is not sufficient in order to obtain authenticated access to the IBOPS server. Identity Assertion under the IBOPS standard relies on several stages of authentication, including biometric vector matching, liveness checking, and the submission of the Client Certificate. Should the biometric vector be replaced/replayed, a Client Certificate must also be present and liveness must succeed in order to impersonate a user. In addition, IBOPS has replay protection mechanisms built in (see the section titled Replay Prevention).

d. Server-side data

i. IBOPS Server Data

Sensitive data that may be stored within the Boriken server includes:

- Device identifiers
- Geospatial locations
- User identifiers such as email, phone number
- User roles
- Client Certificate password data
- Other possible attributes sent to the BOPS server during Genesis and/or session creation.

---

7 The sensitivity of the biometric vector is debatable, as a full biometric can usually not be extracted from the vector and in the event the vector is stolen we help address replay via the intrusion detection capabilities plus presence of the Client Certificate.
8 The user authentication data is stored in the same encrypted format that was returned from the Boriken server during genesis/enrollment. The data gets encrypted by the server using the Elliptic Curve Integrated Encryption Scheme (ECIES#) algorithm. The key used for this encryption (571 ECC) was generated and is stored on the server.
9 [http://developer.android.com/reference/android/content/SharedPreferences.html](http://developer.android.com/reference/android/content/SharedPreferences.html)
Depending on the IBOPS product or solution, session creation may add sensitive data. For example, the withdrawal of money from an ATM will add the account and amount as sensitive data.

Every session that is started and completed for and on behalf of a user or devices is also stored as an audit/history. This allows administrators or other privileged users to see usage patterns and other critical audit data.