IEEE STANDARDS ASSOCIATION

IEEE Standard for Biometric Open Protocol

IEEE Communications Society

Sponsored by the
Standards Development Board

and the

IEEE Technical Activities Board

Sponsored by the
Technical Committee on COM/SDB

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 2410™-2017
(Revision of
IEEE 2410-2015)

IEEE Std 2410™-2017
(Revision of
IEEE 2410-2015)

IEEE Standard for Biometric Open Protocol

Sponsor

Standards Development Board
of the
IEEE Communications Society

and the

Technical Committee on COM/SDB
of the
IEEE Technical Activities Board

Approved 28 September 2017

IEEE-SA Standards Board

Abstract: Identity assertion, role gathering, multilevel access control, assurance, and auditing are provided by the Biometric Open Protocol Standard (BOPS). The BOPS implementation includes software running on a client device, a trusted BOPS server, and an intrusion detection system. The BOPS implementation allows pluggable components to replace existing components' functionality, accepting integration into current operating environments in a short period of time. The BOPS implementation provides continuous protection to the resources and assurance of the placement and viability of adjudication and other key features. Accountability is the mechanism that proves a service-level guarantee of security. The BOPS implementation allows the systems to meet security needs by using the application programming interface. The BOPS implementation need not know whether the underlying system is a relational database management system or a search engine. The BOPS implementation functionality offers a "point-and-cut" mechanism to add the appropriate security to the production systems as well as to the systems in development. The architecture is language neutral, allowing Representational State Transfer (REST), JavaScript Object Notation (JSON), and Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to provide the communication interface. The architecture is built on the servlet specification, open SSLs, Java, JSON, REST, and an open persistent store. All tools adhere to open standards, allowing maximum interoperability.

Keywords: admin console, application, BOPS admin, BOPS cluster, BOPS IDS, BOPS server, client device IDS, IDS cluster, IEEE 2410™, Jena Rules, liveness, original site admin, site admin, trusted adjudicated data, user, user device

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-1-5044-4321-0 STD22773
Print: ISBN 978-0-5044-4322-7 STDPD22773

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents." They can also be obtained on request from IEEE or viewed at http://standards.ieee.org/IPR/disclaimers.html.

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association ("IEEE-SA") Standards Board. IEEE ("the Institute") develops its standards through a consensus development process, approved by the American National Standards Institute ("ANSI"), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Xplore at http://ieeexplore.ieee.org/ or contact IEEE at the address listed previously. For more information about the IEEE-SA or IEEE's standards development process, visit the IEEE-SA Website at http://standards.ieee.org.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: http://standards.ieee.org/findstds/errata/index.html. Users are encouraged to check this URL for errata periodically.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at http://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this IEEE standard was completed, the Biometrics Open Protocol Working Group had the following membership:

Scott Streit, *Chair*
Clayton Stewart, *Vice Chair*

Elizabeth Belousov	Bradley Boyer	Mark Thompson
	Stephen Suffian	

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Charles Barest	Marco Hernandez	Scott Streit
Sourav Dutta	Werner Hoelzl	Walter Struppler
Dan Friedman	Noriyuki Ikeuchi	Stephen Suffian
Fernando Garcia-Quismondo	Piotr Karocki	Mehmet Ulema
Randall Groves	Stuart Kerry	John Vergis
	Maximilian Riegel	Oren Yuen
	Clayton Stewart	

When the IEEE-SA Standards Board approved this standard on 28 September 2017, it had the following membership:

Jean-Phillipe Faure, *Chair*
Gary Hoffman, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Chuck Adams	Thomas Koshy	Robby Robson
Masayuki Ariyoshi	Joseph L. Koepfinger*	Dorothy Stanley
Ted Burse	Kevin Lu	Adrian Stephens
Stephen Dukes	Daleep Mohla	Mehmet Ulema
Doug Edwards	Damir Novosel	Phil Wennblom
J. Travis Griffith	Ronald C. Petersen	Howard Wolfman
Michael Janezic	Annette D. Reilly	Yu Yuan

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 2410™-2017, IEEE Standard for Biometric Open Protocol.

Biometrics encryption, enhanced intrusion detection system (IDS) analytics, and advanced identification process distinguish the architecture design of IEEE Std 2410™-2017 from its predecessor IEEE Std 2410™-2015. The reinforced architecture of the Biometric Open Protocol Standard (BOPS) is well suited for implementation into enterprise systems for secure authentication via biometric modalities.

The biometric enrollment information, i.e., representation of a fingerprint, voice, facial features, is cryptographically protected into two parts and stored, respectively, on a client device and a remote BOPS server. Visual cryptography (VC) and the Euclidian distance matching algorithms make it nearly impossible to recover or reverse engineer one part of biometrics if another part is compromised.

With the increasing need to secure user's access to their footprints of personally identifiable information (PII) in the Internet (financial and health records) and enterprise assets, the BOPS server is designed to control communication with its clients via two-way secure socket layer/transport layer security (SSL/TLS) and to monitor authentication logs and patterns with IDS analytics. Figure 1 describes the authentication cycle for the BOPS framework.

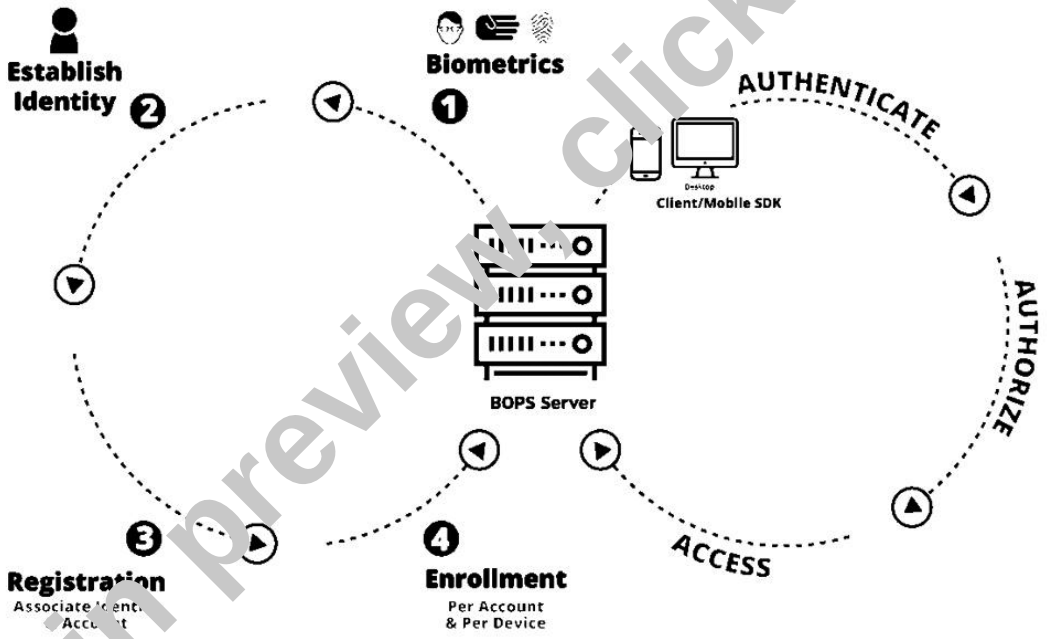

Figure 1—BOPS authentication cycle

Before users are being granted access via the BOPS platform, they shall authenticate their identity with an enterprise system that controls access to the resources and assets. If authentication is successful, the user is authorized to access the resource or asset (i.e., they are "granted access"). Otherwise, they are denied access. Identity is often established at some prior phase via registration of a username that identifies the user with an account in the system.

Biometrics have a long-held hope of replacing passwords by establishing a non-repudiated identity and providing authentication with convenience. Biometrics include a wide range of information taken from a person, e.g., fingerprints, face, voice, and iris pattern, and his/her behavioral properties, e.g., gait, date, time, and location. Recent increases in the processing power and sensor technologies allow digital signal processing (DSP) algorithms to run in the time needed for a real-time authentication (1–5 s similar to username and password login processing). Unlike passwords, biometrics cannot be script-injected; however, biometric data is considered highly sensitive due to its personal nature and unique association with users. Secure storage, transport, and processing of biometric data is paramount in the design and implementation of the BOPS system.

Where IEEE Std 2410-2015 signified a new approach in Identity and Access Management that enabled a password replacement and multi-factor authentication, the IEEE Std 2410-2017 brings a new level of consumer privacy assurance by keeping biometric data encrypted at rest and transit.

Contents

IEEE Standard for Biometric Open Protocol

1. Overview

1.1 Scope

The Biometric Open Protocol Standard (BOPS) provides identity assertion, role gathering, multilevel access control, assurance, and auditing. The BOPS implementation includes software running on a client (e.g., web or mobile), a trusted BOPS server, and an intrusion detection system (IDS). The BOPS implementation allows pluggable components to replace existing components' functionality, accepting integration into the current operating environments in a short period of time. The BOPS implementation adheres to the principle of continuous protection in adjudicating access to resources. Accountability is the mechanism that proves a service-level guarantee of security. The BOPS implementation allows the systems to meet security needs by using the application-programming interface (API). The BOPS implementation need not know whether the underlying system is a relational database management system (RDBMS) or a search engine. The BOPS implementation functionality offers a "point-and-cut" mechanism to add the appropriate security to the production systems as well as to the systems in development.

BOPS includes authentication with splitting of the initial biometric vector (IBV), sometimes called the initial template, optionally into one or two pieces. Irrespective of the number of pieces, the IBV is encrypted in a keyless fashion and the subsequent biometric match optionally occurs on the client or on the server, as denoted by an administration parameter.

1.2 Purpose

This standard provides a means to gather biometric data using a multi-level security protocol for authentication, identification, and access control and assurance.

1.3 Intended audience

The intended audience of this document includes security evaluators, system underwriters, developers, and systems engineers. The BOPS is subject to changes and updates.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.