IEEE SA
STANDARDS ASSOCIATION

IEEE Standard for Biometric Privacy

IEEE Communications Society

Developed by the
Edge, Fog, Cloud Communications with IOT and Big Data Standards Committee

IEEE Std 2410™-2021
(Revision of IEEE Std 2410-2019)

IEEE

STANDARDS

IEEE Std 2410™-2021
(Revision of IEEE Std 2410-2019)

IEEE Standard for Biometric Privacy

Developed by the

Edge, Fog, Cloud Communications with IOT and Big Data Standards Committe
of the
IEEE Communications Society

Approved 25 March 2021

IEEE SA Standards Board

Abstract: The Standard for Biometric Privacy (SBP) provides private identity assertion. SBP supersedes the prior IEEE Std 2410™-2019 by including a formal specification for privacy and biometrics such that a conforming SBP system does not incur GDPR, CCPA, BIPA or HIPAA privacy obligations. Homomorphic encryption ensures the biometric payload is always one-way encrypted with no need for key management and provides full privacy by ensuring plaintext biometrics are never received by the SBP server.The SBP implementation includes software running on a client device and on the SPB server. Pluggable components are used to replace legacy functionality to allow rapid integration into existing operating environments. The SBP implementation allows the systems to meet security needs by using the application programming interface, whether the underlying system is a relational database management system or a search engine. The SBP 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 Transport Layer Security (TLS) to provide the communication interface.This document describes the essential methodology to SBP.

Keywords: admin console, application, biometric-driven device, biometrics, privacy, client device IDS, IDS cluster, IEEE Std 2410™, Jena Rules, liveness, original site admin, SBP admin, SBP cluster, SBP IDS, SBP server, site admin, trusted adjudicated data, user

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

PDF: ISBN 978-1-5044-7500-6 STD24659
Print: ISBN 978-1-5044-7501-3 STDPD24659

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (https://standards.ieee.org/ipr/disclaimers.html), appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents."

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

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, 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 makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. 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: THE NEED TO PROCURE 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 is 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, nor 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 the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, 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 evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile and Interests area of the IEEE SA myProject system. An IEEE Account is needed to access the application.

Comments on standards should be submitted using the Contact Us form.

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 constitute 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.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

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 licensing fees, 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; https://www.copyright.com/. 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 IEEE Xplore or contact IEEE. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website. Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the IEEE SA Patent Policy.

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 https://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.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. 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.

Participants

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

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

Steve Bailey
Nathan Dent
Daniel Farinella
Suleyman Muhammad
Brian Streit
Stephen Suffian
Mark Thompson

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

Robert Aiello
Johann Amsenga
Danilo Antonelli
Juris Borzovs
Juan Carreon
Diego Chiozzi
Murphy Choy
Euclides Chuma
Scott Crawford
Nathan Dent
Dan Friedman
David Fuschi
Paulo Goncalves
Mark Heinrich
Mark Henley
Marco Hernandez
Eric Hibbard
Werner Hoelzl
Raj Jain
Richard Jessop
Ritesh Kalle
Piotr Karocki
Stuart Kerry
Yongbum Kim
Haobo Lai
Rajesh Murthy
Patty Polpattana
Venkatesha Prasad
Beth Pumo
R K Rannow
Annette Reilly
Maximilian Rieger
Pablo Rivas Perea
Benjamin Rolfe
Clayton Stewart
Brian Streit
Scott Streit
Walter Struppler
Stephen Suffian
David Tepen
Mark Thompson
Mark-Rene Uchida
John Vergis
Chun Yu Charles Wong
Forrest Wright
Hasan Yasar
Yu Yuan
Oren Yuen
Janusz Zalewski
Daidi Zhong

When the IEEE SA Standards Board approved this standard on 25 March 2021, it had the following membership:

Gary Hoffman, *Chair*
Jon Walter Rosdahl, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Edward A. Addy
Doug Edwards
Ramy Ahmed Fathy
J.Travis Griffith
Thomas Koshy
Joseph L. Koepfinger*
David J. Law
Howard Li
Daozhuang Lin
Kevin Lu
Daleep C. Mohla
Chenhui Niu
Damir Novosel
Annette Reilly
Dorothy Stanley
Mehmet Ulema
Lei Wang
F.Keith Waters
Karl Weber
Sha Wei
Howard Wolfman
Daidi Zhong

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 2410-2021, IEEE Standard for Biometric Privacy.

One-way fully homomorphic encryption, the inclusion of identification as well as authentication and a greatly simplified Application Programming Interface (API) distinguish the architecture design of IEEE Std 2410-2021 from legacy standard IEEE Std 2410-2017. The reinforced architecture of the Standard for Biometric Privacy (SBP) is well suited for implementation into enterprise systems for secure authentication via biometric modalities.

SBP represents significant progress toward the goal of replacing passwords with non-repudiable identity and providing authentication with convenience. Biometrics include a wide range of information taken from a person, e.g., fingerprints, face, voice, iris pattern, etc. 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 s to 5 s, or 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 of paramount importance in the design and implementation of the SBP system.

The SBP solution itself is simple and biometric agnostic. While the old standard considered matching in the plain text space, IEEE Std 2410-2021 brings a new level of consumer privacy assurance by keeping biometric data encrypted at rest, in transit and in use. Biometric enrollment information (i.e., representation of fingerprint, voice, facial, and other biometric features) is represented by distance-measurable feature vectors. These feature vectors allow all processing to occur in the encrypted space and ensure privacy by never processing, receiving, or holding the plaintext biometric. The result is full privacy, a complete specification without key management functions, and a simple standard implementation that consists of only three API endpoints.

With the increasing need to secure user access to their footprints of Personally Identifiable Information (PII) in the Internet (e.g., for financial and health records) and enterprise assets, the SBP server is designed to control communication with its clients via a two-way SSL/TLS homomorphic interface. Figure 1 below illustrates an SBP authentication cycle where users authenticate identity via the SBP platform before being granted access by an enterprise system that controls 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.

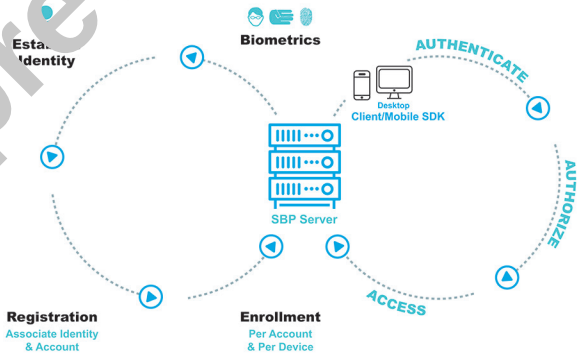

Figure 1—SBP authentication cycle

Contents

IEEE Standard for Biometric Privacy

1. Overview

1.1 Scope

The Standard for Biometric Privacy provides a biometric-agnostic security protocol for private authentication, identification, and liveness. The SBP implementation need not know whether the underlying system is a machine learning model, a relational database management system (RDBMS) or a search engine. The SBP 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.

SBP additionally includes the biometric identification which the industry frequently calls the 'one to many' case. In the past, biometric identification was not considered because this requires a lookup against previously stored biometrics and this lookup required indexing and storing the biometric in plain text biometric identification. This specification includes biometric identification by using biometric features vectors as input to the enroll endpoint, biometric feature vectors as input to the predict endpoint and either video or audio as input to the liveness endpoint.

1.2 Purpose

This standard provides a biometric-agnostic security protocol for authentication, identification, and liveness.

1.3 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).[1,2]

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

[1]The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.
[2]The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact.