International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Architecture and Standardization of Private Biometrics: IEEE P2410/BOPS

Iurii Gusev

Chief Technology Officer (CTO), Computer Science Innovations, LLC, Wroclaw, Poland
Email: *yury.gusev[at]ieee.org*

Abstract: ***This paper provides a comprehensive study of the Biometric Open Protocol Standard (BOPS) architecture, as defined in the Institute of Electrical and Electronics Engineers (IEEE) 2410 - 2018 specification, and demonstrates how it enables "private" processing of biometric data without decryption in accordance with the Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC) principles. The novelty of the work lies in analyzing the mechanisms of "point - and - cut" integration of BOPS into existing systems and considering the principle of "passive encryption, " which together ensure maximum security in the storage and transmission of biometric templates. The challenge of compliance with high standards of state and corporate certification, including TCSEC and Multiple Independent Levels of Security (MILS), when using fully homomorphic encryption (FHE), is addressed. A review of technical implementation scenarios, including interactions with database management systems (DBMS) and cloud services, is provided. This material will be of interest to the scientific community in the field of cybersecurity, as well as practitioners specializing in the implementation of biometric and cryptographic solutions in banks, medical institutions, and government agencies. The proposed approach enables the scalable deployment of private biometric services without compromising performance or recognition accuracy.***

Keywords: Biometric Open Protocol Standard, IEEE 2410 - 2018, homomorphic encryption, private biometrics, TCSEC, MILS, BOPS integration, passive encryption

1. Introduction

Global digitalization and the transition of numerous services (banking, governmental, etc.) to online formats impose increased requirements for secure authentication methods [1 - 3]. While password leaks can be mitigated relatively easily by changing the password, compromised biometric data cannot be revoked [4, 5]. Moreover, most existing solutions handle biometric data in plaintext, failing to comply with the principle of "continuous" (passive) protection, as described in the Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC), also known as the Orange Book [6]. In response to growing privacy breach threats, the Institute of Electrical and Electronics Engineers (IEEE) community developed the Biometric Open Protocol Standard (BOPS) within IEEE 2410 - 2018, ensuring secure biometric data processing at all stages—from capture on the client side to storage in the cloud [1, 2, 7].

Recent research in privacy - preserving biometrics based on homomorphic encryption indicates that working with encrypted biometric templates eliminates the need to store personal data in plaintext [8, 9]. Fully Homomorphic Encryption (FHE) approaches are already being implemented by several companies (e. g., Apple FaceID, Samsung, Google) for simplified (1: 1) biometric authentication [10, 11]. However, large - scale (1: many) authentication previously faced challenges such as high computational time (linear search) and the risk of template exposure [2, 12]. The IEEE 2410 - 2018 (BOPS III) standard legitimized the use of "one - way" FHE vectors on the server side, enabling matching without decryption [1, 7]. Additionally, BOPS incorporates Multiple Independent Levels of Security (MILS) architecture principles, ensuring security domain separation and compliance with TCSEC requirements [2, 6]. According to Apple Inc. [13], Samsung Research [14], and several academic studies [15, 16], integrating such protocols reduces the risk of data leaks, as biometric data remain inaccessible in plaintext even to cloud service providers.

Despite extensive coverage of cryptographic aspects [2, 4, 8], issues related to standardization, architectural implementation, and integration with DoD TCSEC/MILS often remain overlooked. Existing literature either focuses on purely cryptographic solutions (FHE, partially homomorphic schemes) or general approaches to biometric authentication without addressing governmental and industry standards. Consequently, there is a lack of comprehensive analysis of how BOPS (IEEE 2410 - 2018) fits into multi - layered security systems, adheres to MILS principles, and simultaneously meets the "passive encryption" requirements of TCSEC. Additionally, there is no systematic description of the precise mechanisms for integrating BOPS into existing infrastructures (Relational Database Management Systems (RDBMS), enterprise applications) and subsequent certification processes [1, 7].

The objective of this study is to conduct a comprehensive analysis of the BOPS architecture in relation to DoD TCSEC and MILS architecture requirements, as well as to develop recommendations for its practical integration into cloud and enterprise systems.

The scientific novelty lies in identifying and substantiating mechanisms that enable BOPS to simultaneously ensure homomorphic (privacy - preserving) biometrics and compliance with strict security standards (TCSEC, MILS). A generalized method for implementing BOPS in high - load environments (banking and government services) is proposed, taking into account "continuous protection" and "auditability" requirements without decrypting biometric templates.

The hypothesis of this study is that incorporating "privacy - preserving biometrics" in the form of FHE vectors (BOPS III)

into corporate system architecture will not only enhance confidentiality by eliminating all plaintext operations but also simplify compliance with TCSEC/MILS requirements by removing the "decryption window" risk.

The following approaches are applied in this study:

1) Theoretical analysis of standards and regulatory documents (IEEE 2410 - 2018, TCSEC, MILS, National Institute of Standards and Technology Special Publication 800 - 53 (NIST SP 800 - 53)) to identify key requirements for architecture and encryption mechanisms [6, 7, 16].
2) Review of scientific literature and patent solutions in the field of privacy - preserving biometrics (FHE, cancelable biometrics, BioHashing) to assess the current state of technology [3, 8, 15].
3) Development of a generalized BOPS integration model into existing systems (using typical CRUD (Create, Read, Update, Delete) applications and cloud services as examples), considering the specifics of MILS - based domain separation.
4) Expert evaluation (in the form of a comparative table) of the advantages and risks of implementing BOPS compared to traditional biometric solutions without homomorphic encryption.

2. Biometric Open Protocol (BOPS) in IEEE P2410

The BOPS protocol was initiated as a universal and biometrically neutral authentication mechanism, enabling organizations to implement secure solutions without being tied to a specific type of biometrics (e. g., face, iris, fingerprint) [1]. Its specification (IEEE 2410 - 2018) [7] clearly defines the following aspects:

1) Identity Assertion. The core of the protocol is the identity verification mechanism based on biometric data, which is immediately encrypted on the client side using a FHE method.
2) Role Gathering and Multi - Level Access Control. The protocol provides dynamic role assignment to users and policy - based access control, simplifying the configuration of a flexible permission model (e. g., different levels of access within a corporate network).
3) Logging and Auditing. BOPS adheres to the principle of accountability, where every authentication and access event is logged, with these records available for audit under internal and external regulatory requirements (General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), etc.).

The BOPS architecture includes the following key components:

- Client device (smartphone, computer, ATM), which captures biometric data (e. g., a facial image) and immediately converts it into a one - way feature vector encrypted with an FHE algorithm.
- BOPS server, functioning as a trusted node, receives the encrypted vector and performs verification (1: 1 or 1: many) against a database that also stores only homomorphically encrypted biometric templates. It is critical that the server does not require access to plaintext data— all matching operations are executed within the encrypted domain [2].
- Intrusion Detection System (IDS), continuously monitoring network transactions and operations within the BOPS server, detecting anomalies, and ensuring compliance with the "continuous protection" concept outlined in TCSEC [6].

The point - and - cut principle (sometimes referred to as "plug - and - play"), embedded in the standard, allows developers to integrate BOPS into existing applications (Customer Relationship Management (CRM) systems, search engines, RDBMS) using a standard Application Programming Interface (API) [1]. Additionally, modular replacement of specific components is permitted, such as employing different homomorphic encryption schemes—Brakerski - Gentry - Vaikuntanathan (BGV), Brakerski - Fan - Vercauteren (BFV), and Cheon - Kim - Kim - Song (CKKS) —while maintaining the overall protocol logic [8].

Table 1: Comparison of Traditional Biometric Approach and BOPS [1, 2, 3, 7, 8]

Criterion	Traditional Approach	BOPS Approach
Template Storage	The template is stored in the database in a (semi -) plaintext format or requires a password/key for decryption.	The template is stored as a one - way (fully homomorphically) encrypted vector with no possibility of decryption.
Key Management	Keys must be stored to decrypt and process biometrics.	No key storage for the raw template; the generated vector is irreversible. FHE keys are used only for computations.
Scalability 1: many	Computationally intensive for large databases (linear search, partial encryption).	Polynomial search algorithms are used in the encrypted space (vector ~4KB, FHE - supported).
"Passive Encryption" Requirement	Usually not met: templates are decrypted for computations.	Fully enforced: all operations (storage, verification) occur on encrypted data.
MILS Compliance	Not guaranteed, as plaintext biometrics are accessible within a single domain.	Domain separation is implemented: the client device processes biometrics, while the server only accesses encrypted vectors.

In the IEEE 2410 - 2018 version [7], drawing on commercial and academic research (Apple FaceID, Samsung, Google FaceNet, Private. id, etc.), the concept of "private biometrics" was introduced— a "one - way" FHE vector that ensures:

- No decryption keys for raw templates. Traditional biometric systems required secure key storage for decryption, as key leaks could allow attackers to reconstruct biometric data [4]. Under the BOPS scheme, a neural network - generated feature vector (e. g., 128 float components) cannot be reversed into the original image (one - way property) [3].
- Principle of "passive encryption. " Data remains encrypted both "at rest" (in storage) and "in transit" (during transmission). FHE enables operations on vectors without

decryption, which was previously considered unattainable under TCSEC [6].
- Simplified API and risk reduction. Since the biometric payload is one - way, the BOPS protocol eliminates complex key management schemes for storing raw templates. All operations— authentication (1: 1) or search (1: many) — are conducted directly on homomorphically encrypted templates [7].

Additionally, the BOPS protocol is compatible with MILS architecture (Multiple Independent Levels of Security), where each sensitive operation (biometric matching, database read/write) occurs within a strictly defined security domain. Notably, plaintext biometric data exists only for a few seconds in a trusted execution environment on the client side (TEE— Trusted Execution Environment or Secure Enclave), while the server only receives the homomorphically encrypted vector [1]. All other domains only access encrypted vectors and cannot decode the biometric template.

With the adoption of IEEE 2410 - 2018 (BOPS III) in organizational infrastructures (from banking to government sectors), critical vulnerabilities related to biometric storage and plaintext transmission are eliminated, increasing system trust through formal compliance with TCSEC/MILS principles. At the same time, the authentication process remains seamless and convenient for the end user, who simply interacts with their client device (e. g., taking a facial scan or fingerprint), while all encryption and key management complexities are handled automatically in the background.

3. Implementation features and compatibility with DoD TCSEC

In the United States, one of the key regulatory documents in the field of computer security has long been TCSEC, commonly known as the "Orange Book" [6]. Among other aspects, TCSEC places significant emphasis on the principle of "passive encryption, " which requires data to be encrypted not only during transmission but also during storage ("at rest"). However, in practice, implementing this approach encountered a critical issue: if data needed to be actively processed (e. g., for database searches), it had to be decrypted, thereby creating a plaintext "window. "
BOPS eliminates these challenges since biometric templates are neither stored nor transmitted in plaintext; all matching operations are performed on FHE vectors [1, 7]. Consequently:
1) No "window" (time window) where biometric data is available in plaintext. According to BOPS, the server only processes encrypted vectors, and all matching operations occur through homomorphic computation [8].
2) Simplified TCSEC certification at C2/B1 levels and above. The protocol ensures "continuous protection" since data remains encrypted even during computational processes [6].

As a result, BOPS allows organizations to meet the stringent requirements of the Orange Book more flexibly, without introducing cumbersome plaintext key management mechanisms.

Table 2: Comparison of TCSEC Requirements and BOPS Capabilities [1, 6, 7]

TCSEC Requirements	Brief Description	BOPS Implementation
Authentication & Identity	The system must reliably verify a subject's identity.	BOPS ensures authentication through "private biometrics" (FHE vectors).
Discretionary Access Control (DAC)	Access control is based on administrator - defined policies.	BOPS supports Role Gathering and Multi - Level Access Control based on biometric identification.
Security Audit	Security - relevant events must be logged and available for review.	BOPS includes Logging and Auditing mechanisms for every authentication event and role update.
Object Reuse Protection	Resources (memory, disk) must not expose data from previous users.	With one - way biometric encryption, object reuse does not pose a leakage risk.
Trusted Path/Continuous Protection	Users must interact with the system only through a trusted path, ensuring data protection "at rest. "	BOPS implements passive encryption, ensuring biometric data is never decrypted on the server.

One of the key advantages of BOPS (IEEE 2410 - 2018) is its capability for modular integration into existing infrastructures [2]. The following section outlines the key technical aspects of such integration.
1) Support for Popular Database Management Systems (DBMS). Most relational (MySQL, PostgreSQL) and NoSQL (MongoDB) systems are not initially designed for searching encrypted fields. However, BOPS provides an intermediary service or module (plugin) responsible for performing homomorphic operations on Biometric Feature Vectors. This module communicates with the DBMS through a standard API without exposing biometric data [1].
2) Utilization of Cloud Services. By adhering to BOPS and FHE principles, even a public cloud cannot access the original plaintext biometric template. The cloud server functions as a homomorphic computation operator, receiving only encrypted vectors and returning encrypted matching results [7].
3) Compliance with GDPR and HIPAA. Confidentiality is critical for banking and medical applications. BOPS eliminates the risk of mass biometric compromise by ensuring that no plaintext data exists on the server side. This aligns with the "Privacy by Design" principle outlined in GDPR (EU) and HIPAA (US) [1, 6].

Table 3: Technical Scenarios for BOPS Integration [1, 3, 7]

Scenario	Description	Key Components
Banking Application	1: many client search via biometric templates (credit transactions, AML checks).	Homomorphic search module (FHE Plugin), remote database storing encrypted vectors, automatic logging in BOPS - Audit.
Medical System	Secure physician access to electronic health records based on iris scans or fingerprints, ensuring HIPAA/GDPR compliance.	BOPS server (or cloud) receives only encrypted vectors. IDS monitors access and detects anomalous transactions.
E - Government Services	Citizen authentication for online document submission without exposing photos or biometric identifiers to government systems.	MILS role separation: Citizen (client) ↔ BOPS server ↔ Government DBMS. Optimized homomorphic matching algorithms for large - scale (1: many) databases.
Corporate Network with RDBMS	Internal employee authentication (system logins, access control).	BOPS plugin handling FHE vectors, integrated with Active Directory or LDAP.

Thus, BOPS serves as a universal standard that is compatible with both corporate solutions and large - scale public cloud infrastructures. Its implementation eliminates midway decryption risks and enables end - to - end data protection, meeting DoD TCSEC requirements while enhancing security through FHE methods.

4. Conclusion

This study has provided a detailed examination of the IEEE 2410 - 2018 (BOPS) standard, which governs the application of private biometrics and homomorphic encryption in authentication systems. The findings indicate that BOPS architecture not only meets DoD TCSEC requirements for passive encryption, but also supports modular integration into various IT infrastructures, ranging from relational DBMS to cloud platforms. The use of one - way encrypted biometric vectors completely eliminates the risk of template compromise, which is critical for GDPR and HIPAA compliance. Additionally, BOPS demonstrates compatibility with MILS architecture, enabling security domain separation and preventing the storage of unencrypted biometric data on the server. The results confirm that BOPS has the potential to become a universal standard for developing highly secure biometric systems, meeting the demands of both industry and government for global digital security.

References

[1] Hoyos Labs. (2015). Biometrics Open Protocol Standard P2410 Working Group. . [Electronic resource] - URL: https: //www.prnewswire. com/news - releases/hoyos - labs - biometrics - open - protocol - becomes - ieee - standard - 300141966. html
[2] Wikipedia. (2021). Private biometrics. [Electronic resource] - URL: https: //en. wikipedia. org/wiki/Private_biometrics#ex2
[3] Wikipedia. (2021). Homomorphic encryption. [Electronic resource] - URL: https: //en. wikipedia. org/wiki/Homomorphic_encryption
[4] Paillier, P. (1999, April). Public - key cryptosystems based on composite degree residuosity classes. In International conference on the theory and applications of cryptographic techniques (pp.223 - 238). Berlin, Heidelberg: Springer Berlin Heidelberg.
[5] Bolle, R. M., Connell, J. H., & Ratha, N. K. (2002). Biometric perils and patches. Pattern recognition, 35 (12), 2727 - 2738.
[6] US Department of Defense. (1983). Trusted Computer System Evaluation Criteria (TCSEC). DoD 5200.28 - STD. [Electronic resource] - URL: https: //csrc. nist. gov/files/pubs/conference/1998/10/08/proceedings - of - the - 21st - nissc - 1998/final/docs/early - cs - papers/dod85. pdf
[7] Biometrics Open Protocol (BOPS) III. IEEE 2410 - 2018, IEEE Standards Association.2018. [Electronic resource] - URL: https: //web. archive. org/web/20150415004908/http: //standards. ieee. org/develop/wg/BOP. html
[8] Gentry, Craig (2009). "Fully homomorphic encryption using ideal lattices. " Proceedings of the forty - first annual ACM symposium on Theories of computing. pp.169–178. doi: 10.1145/1536414.1536440.
[9] Streit, Scott; Streit, Brian; Suffian, Stephen (2017). "Privacy - Enabled Biometric Search". arXiv: 1708.04726
[10] Selleck, Evan. “Craig Federighi Says Apple is ‘Focusing Face ID on Single User Authentication. ’” Phone Hacks. [Electronic resource] - URL: http: //www.iphonehacks. com/2017/12/face - id - single - user - authentication. html
[11] Evans, Johnny. “iPhone X & Face ID: Everything you need to know. ” ComputerWorld.9/13/2017. [Electronic resource] - URL: https: //www.computerworld. com/article/3224569/apple - ios/iphone - x - and - face - id - everything - you - need - to - know. html
[12] FIDO Alliance. (2021). FIDO2: Moving the World Beyond Passwords. [Electronic resource] - URL: https: //fidoalliance. org
[13] Apple Inc. (2017). Face ID Security. [Electronic resource] - URL: https: //www.apple. com/business - docs/FaceID_Security_Guide. pdf
[14] Samsung Research. (2018). Using Biometrics for Authentication and Data Encryption. [Electronic resource] - URL: https: //insights. samsung. com/2018/01/18/using - biometrics - for - authentication - and - data - encryption/
[15] Cheon, Jung Hee; Kim, Andrey; Kim, Miran; Song, Yongsoo (2017). "Homomorphic encryption for arithmetic of approximate numbers". Takagi T., Peyrin T. (eds) Advances in Cryptology – ASIACRYPT 2017. ASIACRYPT 2017. Lecture Notes in Computer Science. Vol.10624. Springer, Cham. pp.409–437. doi: 10.1007/978 - 3 - 319 - 70694 - 8_15
[16] NIST. (2020). Security and Privacy Controls for Information Systems and Organizations (SP 800 - 53 Rev.5). Gaithersburg, MD: National Institute of Standards and Technology.