BANK OF THAILAND

Guideline for Biometric Technology Adoption in Financial Services

SEPTEMBER 2023

Payment Systems and Financial Technology Policy Department
& Technology Risk Supervision Department
Bank of Thailand
FinTechDept@bot.or.th

Unofficial Translation
This translation is for convenience of those unfamiliar with Thai Language
Please refer to the Thai official version

Table of Content

Topics **Page**

1. Rationale....3

2. Repealed Guideline....4

3. Scope....4

4. Definition....4

5. Overview of Biometric Technology 5

5.1 Operation of biometric technology 5

5.2 Important issues to be considered for managing risks related to biometric technology 6

6. Guiding Principle for Financial Service Providers 7

Principle 1: Policy framework and governance 7

Principle 2: Collecting biometric data....8

Principle 3: Processing biometric data....9

Principle 4: Protecting customer's biometric data....10

Principle 5: Consumer protection....12

Principle 6: Operational risk management....13

Appendix A. Minimum requirement 15

Guideline for Biometric Technology Adoption in Financial Services

1. Rationale

Biometric technology is the technology for identifying individuals' physical identities, such as face, fingerprints, or behaviors such as speaking and writing, which aims to identify and verify individuals.

Biometric Technology has been developed significantly in terms of accuracy in identifying individuals as well as ease of use. As a result, biometric technology has been widely adopted to increase efficiency of various services in the financial sector, particularly customer verification such as Know Your Customer (KYC) for opening accounts or applying for other services to reduce frauds and provide alternative online channel using reliable eKYC to further enhance customers' convenience.

However, adopting biometric technology in financial services involves the use of individuals' physical identities, which are considered sensitive personal information. Inappropriate and inadequate management of such information will affect customers' privacy and their trust in financial system. Therefore, priorities must be given on the issue in several dimensions, including the technology's capability in identifying, authenticating and verifying identities, security of personal data, consumer protection and education.

Financial service providers have adopted and tested biometric technology within limited scope under the Bank of Thailand's (BOT) regulatory sandbox program. The financial service providers have applied the biometric technology to elevate the security in verification process for opening saving accounts and e-Money accounts by comparing customers' faces and fingerprints with trusted sources, such as the photo on national ID cards and passports. BOT then assesses their testing results and monitors relevant risks closely to ensure that proper risk management and consumer protection measures are in place.

BOT encourages financial service providers to leverage new technologies to create financial innovation which brings about benefits to financial sector, and, at the same time, has appropriate risk mitigation. Therefore, BOT launches this guideline defining minimum requirements for financial service providers in applying biometric technology to provide safe and sound financial services and ensure that the financial service providers have adequate policies, secured processes, and appropriate managements in their biometric technology adoption. For example, the financial service providers completely must define

policies, procedures, and operation manuals for biometric adoption for the entire life cycle of biometric data including data collection, storage, process, and destruction.

This guideline conforms to international standards including International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST) Information System Audit and Control Association (ISACA) and FIDO Biometric Requirements. In addition, financial service providers must adhere to other laws and regulations related to biometrics such as BOT's Information Technology Risk and Cyber Hygiene Framework. This guideline will help improve financial inclusion, ensure financial stability and maintain consumers' trust in relevant financial services.

2. Repealed Guideline

Repeal the Guideline for Biometric Technology Adoption in Financial Services dated 22 July 2020.

3. Scope

This guideline is intended to encourage financial service providers regulated by BOT, including financial institutions and payment service providers, to apply guiding principles to biometric technology implementation for financial services.

4. Definition

In this guideline

Biometric technology means measurable biological or behavioral characteristics, which reliably distinguishes one person from another, used to recognize the identity, or verify the claimed identity of individuals.

Biometric data[1] means personal data extracted by using biometric techniques or technologies to identify physical traits, such as faces and fingerprints, or behavioral traits, such as speech or writing patterns, to identify, authenticate or verify person's identity.

Biometric reference means data representing the biometric measurement of individuals, extracted from ones' biometric sample, and stored to be used by a biometric system for comparison against subsequently submitted match templates.

Biometric sample means initial (raw) biometric data, which is captured and processed to be in an electronic form, but has not been transformed into a biometric template, such as facial capture to be used for facial comparison.

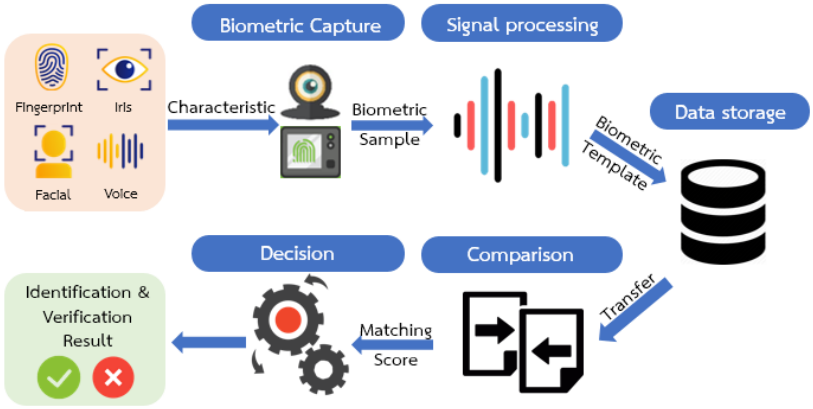
[1] Biometric data in this guideline refers to biometric in Personal Data Protection Act.

Biometric template means digital representation of individual's biometric features that are extracted and processed electronically to be in a format possible for biometric comparison and cannot be reversed to initial biometric data, such as data points representing key facial features of an individual.

5. Overview of Biometric Technology

There are five processes and related considerations as follows.

5.1 Operation of biometric technology consists of 5 processes.



(1) Biometric capture – collects data by using an input device or a sensor that captures the biometric information from a customer and converts it into compatible form for processing. For example, a camera captures a user's face for facial recognition, and a fingerprint reader collects a user's fingerprint.

(2) Signal processing – receives raw biometric data from biometric capture process and transforms the data electronically into a form or a template for matching process which is not reversable to raw biometric data. For example, facial recognition typically defines face landmarks (such as eyes, eyebrow tail, lips), or fingerprint recognition typically defines physical characteristic (such as minutiae), and the landmarks and characteristics will be extracted into a set of values for comparison.

(3) Data storage – maintains the template for the enrolled users in a database which links biometric template with personal information of users (such as name/surname, national identification number, address) for identity comparison.

(4) Comparison – matches biometric data from signal processing and biometric template from data storage or trusted source of information and presents the level of confidence (matching score) for the purpose of two functions:

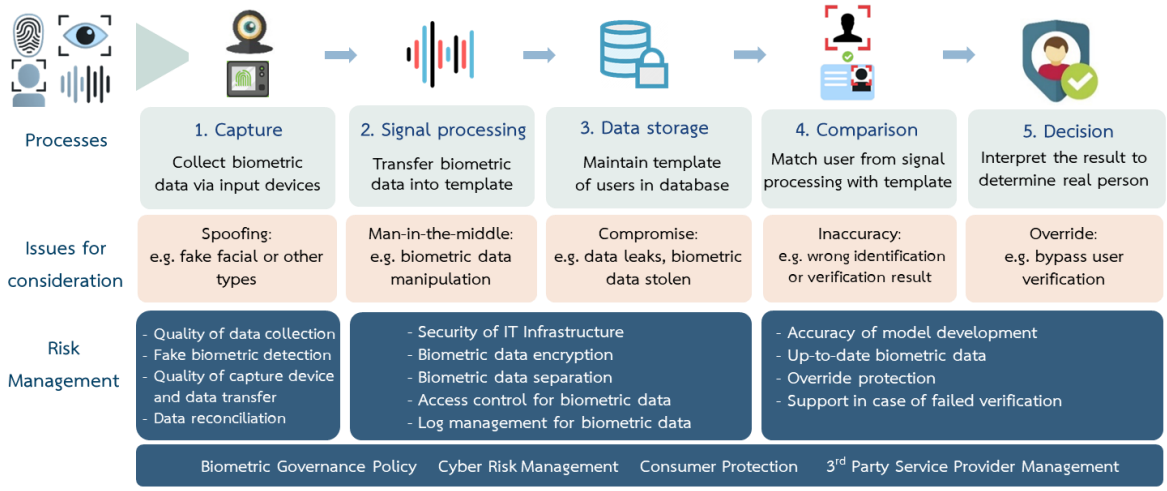
- **Identification** – is the process for recognizing an individual from the enrolled database. When a user presents the required biometric characteristics, and the system will compare the biometric data to a set of templates in the system database.

- **Verification and authentication** – are the processes of comparing between user's biometric data and claimed identity or trusted source of information in order to determine whether that user is the authentic owner of the claimed identity.

(5) Decision – is the process displaying the identification and verification results from a biometric system matching process. The system calculates the biometric matching score by comparing between system's threshold score and the biometric confidence score from the identification and verification process.

5.2 Important considerations for managing risks related to biometric technology

Adopting biometric technology is related to identification and verification of people which are considered as important personal information. Therefore, proper and adequate controls for all operational processes are required in order to protect biometric data, which can be summarized as below diagram:



(1) Spoofing means the use of different materials to create artificial physical or behavioral characteristics. For example, attackers may use 3D-mask, or use video to emulate person's liveness.

(2) Man-in-the-middle means the use of techniques or devices to capture biometric data during data-in-transit in processing system.

(3) Compromise means the attempts to copy, steal, manipulate, or destroy biometric data in database system.

(4) Inaccuracy means the system performing biometric verification or identification at the lower level than expected, which may be caused by insufficient model training.

(5) Override means attempts to manipulate or bypass decision of biometric verification, for example, threshold manipulation.

6. Guiding Principles for Financial Service Providers

consist of six topics which are minimum requirements for financial service providers as follows.

Principle 1: Policy Framework and Governance

> **Intended outcome:** Financial service providers realize benefits and associated risks before applying biometric technology to their businesses. By having policy framework and solid governance process, financial service providers will be able to apply biometric technology to products and services efficiently, securely, and suitably.

Recommended Practice

(1) Establish governance processes on adopting biometric technology to ensure that all related risks will be properly managed. Financial service providers can leverage existing or set up additional governance processes to oversee biometric adoption. Governance structure should cover all important processes, for instance, technology risk assessment, vendor risk, risk mitigation plan and should include technology and risk experts specializing in biometrics technology. Moreover, the established governance structure must adhere to related laws and regulations such as Personal Data Protection Act, IT Risk management guideline, and Cyber hygiene.

(2) Create or enhance existing policies to govern the use of biometric data such as IT risk management, data governance policy, and data classification policy. These policies must be embedded in the whole biometric life cycle from collecting to destroying biometric data.

(3) Assess all related factors for adopting biometric technology prior launching any services, including business benefit evaluation, type of suitable biometrics for each financial service, effect on personal data protection[2], risks from each type of biometrics, and risk mitigation methods for technology risk, operational risk, reputation risk, legal risk, consumer protection, and other related regulations.

[2] Data Protection Impact Assessment can be referred to regulations under personal data privacy.

Principle 2: Collecting Biometric Data

Intended Outcome: Financial service providers should have proper biometric data collection processes, which maintain good biometric data quality for identification, verification, and authentication. At the same time, the customers should be well communicated to maintain trust in biometric technology.

Recommended Practice

(1) Define proper and sufficient processes or procedures for collecting biometric data from customers to identify and verify customers accurately. Scope of procedures should incorporate guidelines and recommendations for users in collecting data, such as instructions on taking a selfie picture by mobile phone or taking picture at a photo kiosk and other related conditions assisting customers get good-quality biometric data for processing, for example, the brightness of environment, the accessories that must not be worn when taking pictures such as hat or sunglasses. In addition, there should be facial image quality assessment and exemption procedures when systems detecting poor quality biometric data such as unclear facial image on ID card, blur fingerprint.

The procedures to control quality of collecting biometric data may be varied based on type and channel of services. However, especially for facial recognition, financial service providers should consider other details in Appendix A, complying with ISO 19794-5 Biometric data interchange formats – Part 5 Face image data.

(2) Clearly notify customers about the objective of biometric data collection as well as benefits, customers' rights, and the consequences of not providing biometric data, adhering to relevant laws and regulations (e.g. Personal Data Protection Acts).

(3) Establish procedures on detecting biometric fraudulent to prevent imposter in biometric data collection process in both face-to-face and non-face-to-face registration. For example, trusted sources of information such as National ID card or passport are used to verify customer identity, and implement presentation attack detection or liveness detection technology, and other controls when possible.

(4) Define internal control and procedures to regularly check the trustworthiness of biometric data collection process to ensure the compliance of internal operational processes with all defined policies.

(5) Define procedures to maintain useability and security of biometric capture devices such as cameras or webcams at branches or ATMs, fingerprint readers at kiosks, and their readiness of data transmission channel. In addition, customers' biometric data must not be retained in biometric capture devices of financial service providers and in the systems of 3rd party service providers.

Principle 3: Processing Biometric Data

Intended Outcome: Financial service providers should accurately process, identify, and verify biometrics of customers at sufficient level for financial services and also be able to prevent identity manipulation in order to maintain the safety and trustworthiness of financial services.

Recommended Practice

(1) Define proper technology selection or development methodology for biometric comparison by considering various factors including accuracy of identity comparison, type of financial services, level of risk, adherence to international standard[3], and ability to detect biometric manipulation such as presentation attack detection[4].

For both in-house development or vendor technology adaptation, financial service providers should consider quality of test samples, amount of sample size, and variety of samples which are suitable for selected financial service. [5] In addition, accuracy of biometric comparison model should be aligned with international standards[6] and regularly re-validated to maintain defined accuracy.

(2) Define validation process to ensure the authenticity of biometric data and personal identity document for identification and verification. For example, the authenticity and latest status of ID card or passport as trusted sources for biometric comparison are validated. The appropriate methodology is used to collect the up-to-date biometric data such as setting specific times when customers are required to update facial data.

---

[3] Accuracy of biometric comparison based on international standards, (for example, verifing facial with trusted sources) should have False Acceptance Ratio (FAR) < 0.1% based on NIST Special Publication 800-63B Digital Identity Guideline: Authentication and Life Cycle management, and False Reject Ratio (FRR) < 3% based on FIDO Biometric Requirement. In addition, financial service provider should consider the effectiveness of vendor's algorithm under NIST FRVT 1:1 Verification (for example, False non-match Rate (FNMR) ranking is in top 50).

[4] Presentation Attack Detection (PAD) can be categorized as following

Low: Easy to obtain materials and identity information for creating fake biometrics, requiring little time and low skills to produce such as using face data from social media.

Medium: Use specific tools and some private identity information, requiring medium time and skills to produce such as using video of individuals to mimic liveness detection.

High: Use specific tools and sensitive identity information, requiring large amount of time and high skills to produce such as 3D mask.

Financial service providers should conduct presentation attack detection based on international standards such as NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management, ISO30107 – Biometric presentation attack detection and FIDO Biometric Requirements.

[5] Financial service providers should have at least 2,000 sample size of individual in order to use facial recognition for saving and e-Money account opening. However, financial service providers can use 1,000-sample size in case of using facial recognition technology from vendor who have been verified accuracy with international standards and comply with BOT assessment.

[6] Refer to ISO 19795 – Biometric Performance testing and reporting

(3) Define mechanism to detect and prevent biometric spoofing or manipulation in biometric comparison and verification processes such as setting attempt limit or transaction time-out[7].

(4) Define protocol in case of unsuccessful or failed biometric verification, which is relevant and suitable for specific type and risk of financial services. For example, alternative verification procedures are provided; alternative documents from trusted sources are acceptable for verification.

(5) Define procedures for securing biometric data in processing and verification process, especially in case of using 3rd party services where data must not be shared or retained in 3rd party's system.

Principle 4: Protecting Customer Biometric Data

> **Intended outcome**: Financial service providers should be able to store personal information, which is biometric data, in secure manner and aligned with international standards to ensure that customers' information is safely protected.

Recommended Practice

(1) Define IT-related policy and design IT infrastructure which incorporate security of biometric data and scalability that can accommodate increasing transaction volume in the future.

(2) Do not store customers' raw biometric data but store it in the form of biometric template for identity comparison purpose, which is not reversible to raw biometric data, except for facial biometric data or other biometric data that needs to be stored to comply with the laws and regulations. In addition, financial service providers must comply with related laws such as Personal Data Protection Act.

(3) Define secure processes to store, transfer, and link with biometric template as follows:

(3.1) Store and transfer biometric template that can prevent unauthorized usage and ability to identify its owners. For example, biometric template data encryption is required for data-in-transit, starting from biometric capture device, communication line; and

[7] Refer to NIST SP 800-63B Digital Identity Guidelines Authentication and Life Cycle Management and ETDA Recommendations on Digital Identity for Thailand, which defines failed authentication attempts less than 5 times for normal case and less than 10 times for presentation attack detection. In case of limit reached, should perform following steps:

- Delay 30 seconds before next authentication and increase delay time in exponential such as 30 sec, 1 minute, 2 minutes, 4 minutes, 8 minutes.
- Deny authentication and recommend using other method.

storing data (data-at-rest). The encryption is also required at file or data field level that complies with international standards including encryption algorithm, key length, and strong key management process.

(3.2) Store biometric template separately from customer personal information (such as name, surname, national ID number) at server or database level which can prevent biometric data leakage along with personal information. For example, facial database should be separated from customer information database. In addition, access control and encryption key of the two systems should be separated.

(3.3) Do not link biometric data template data with indirect reference, such as National ID number and customer information number, to refer customer identity. This is to prevent impact from attacks or data leakage.

(3.4) Define network zoning, biometrics data and related systems based on level of data classification. For example, biometric data and related systems should not be stored in Demilitarized zone (DMZ) to prevent attacks from external network.

(3.5) Use secured communication channels and procedures for transferring biometric data between internal systems and external parties.

(4) Define access control process for biometric data by granting the access right to the designated person only. The right to access should be reviewed regularly. In addition, integrity checking process should be put in place for biometric data to prevent unauthorized biometric data manipulation.

(5) Define vulnerability management process for IT system related to biometric data, in accordance with risk level, to identify, prevent, and control risks promptly. Financial service providers must perform vulnerability assessment on IT infrastructure, related to biometric data at least once a year or whenever there are any significant changes in IT system such as changing of technology vendors, and when there are any vulnerability alerts which could widely affect biometric data.

(6) Perform penetration testing by independent professional at least once a year or when there are any significant changes to identify, prevent, and control risks promptly when there is any risk gap.

(7) Define patch management process which covers IT systems that support biometric data storage and processing as well as hardware and software prompt support from vendor when vulnerabilities or bugs are found.

(8) Record log files which relate to biometric data including access log, activity log, transaction log, and security event log in secure manner and sufficiently for review, examination in case of suspicious events and to be used as evidence in law enforcement.

(9) Define strict policies and procedures to securely maintain biometric data when using cloud computing for customer data storage and biometric data processing. The scope of policies should incorporate strong access control, security assessment of cloud service providers such as international certification, security policy for customers, concentration risk assessment, terms and conditions, right to audit, and procedure to support the readiness in using the system and storage based in the country[8].

(10) Regularly perform security audit for biometric data of customers by either internal auditor or external auditor at least once a year. The scope of audit should cover IT service which using 3rd party service provider (in case).

Principle 5: Consumer Protection

> **Intended outcome:** Financial service providers should have sufficient and proper consumer protection processes to be able to provide the safe and sound services together with adhering to all related regulations such as consumer protection and persona data protection. The knowledge and information about biometric technology should be provided for customers.

Recommended Practice

(1) Define biometric data collection, use, and disclosure that comply with related laws such as PDPA. Financial service providers must obtain consent clearly from customers. In case that the consent is required, financial service providers must obtain consent before or during servicing (opt-in consent). In addition, biometric data collection should be performed only if necessary. Financial service providers must inform the objective of data collection to their customers before or at the time of collecting. For example, for making a contract or providing additional services, financial service providers must use biometric data based on objective of customers defined in consent or by laws. Furthermore, financial service providers must inform customers in detail about how the financial service providers will use their data to provide the services and the benefits.

(2) Financial service providers must request for consent from customers in paper or electronic form and must be separated clearly from other parts. The wording in the documents must be easy to understand and not lead to misunderstanding or misinterpreting but allow customers to have choices in giving consent. In addition, in case of using customers biometric data in a different way from initial objective (especially in changing of terms and

[8] Can refer to BOT 3rd Party Risk Management Guideline

conditions), financial service providers must request for another consent again to support the acknowledgement of latest information about using their biometric data.

(3) Notify the right of biometric data owner to customers, such as right to access their biometric data, right to change biometric data to be updated and completed, and conditions which relate to biometric data, such as effect on customer right and service received, in case customers do not allow biometric data collection.

(4) Define customer protection process for biometric data owner. For example, customers must be able to check consent given history and revoke consent. Channels for customers to complain or report problems from using services must be provided with clearly defined service level agreement. And define communication channel with customers and regulator in case of incident occurred that may affect customer biometric data. In addition, customer relief program should also be put in place.

(5) Provide knowledge about biometric technology to customers in terms of their benefits and rights.

(6) Define process for biometric data disclosure as specified by law in case of transferring biometric data to the 3rd party such as outsource companies. Financial service providers must obtain consent from customers and inform them that their data will be shared to 3rd party with limited use as defined or by law.

Principle 6: Operational Risk Management

> **Intended outcome**: Financial service providers can manage significant operational risks including business continuity plan, fraudulent transaction monitoring and third-party service management to ensure the safety and trust of customers.

Recommended Practice

(1) Define business continuity plan for financial services that use biometric technology, which include IT infrastructure disaster recovery plan and operation procedure in case of service disruption. In addition, financial service providers should have cybersecurity incident response plan which covers biometric data such as unauthorized access, biometric data leakage and regularly perform such plan.

(2) Define fraud analyzing and monitoring process, related to biometric-related transaction such as abnormal change of customer facial data in short period. In addition, financial service providers may define additional authentication or verification processes, if necessary, to increase confidence level, such as request for additional documents or another information from trusted sources to be submitted for in-depth investigation.

(3) Define 3rd party management process which is related to biometric data such as biometric data collection and processing via agent, biometric data storage on cloud computing. The process must cover risk analysis, define risk mitigation, and have a contract

defining roles and responsibility, right to audit by regulators, and conditions of service, especially safeguarding biometric data of customers. Also, it is vital to consider business continuity plan and managing risks from contract cancellation or termination. By such process, financial service providers can continually run the business and respond to the changing technology trend in the future.

Appendix A.

Minimum requirement and guiding principle for collecting facial data for biometric comparison.

1. **Rationale**

This guideline is aimed to encourage financial service providers to have minimum standards and guiding principle for collecting facial data of customers that have a certain level of quality for processing in order to accurately identify and verify user and adhere to international standards.

2. **Details**

Part 1 Minimum requirement for collecting facial data

Collecting facial data from both face-to-face and non-face-to-face should have details as following:

1.1 Picture resolution should be at least 1280 x 720 pixels or 1080 x 1080 pixels. However, picture height and width can be adjustable depending on technology development with the requirement to achieve baseline accuracy level.

1.2 Picture compression should be lossless data compression or lossly data compression and must ensure the quality of picture is compatible for operation.

1.3 Color image only

1.4 Customers must show full frontal face (not smiling and open lips)

1.5 Image is clear and in focus.

1.6 Image must show full head of users without any cover (except for religious or medical purposes)

1.7 Image must clearly show eyes of user and without red eyes.

1.8 Users can wear eyeglasses if there is no any shadow or no any reflect in image.

1.9 Users must not wear sunglasses during taking picture process.

1.10 Length of facial should be 60%-80% of height of picture.

1.11 There must be only one face of a user in the image, without any appearance of other's faces on any part of the image which might impact to facial comparison capability.

1.12 Image must be in an appropriate brightness.

Part 2 Guiding principle for collecting facial data

Financial service providers should have procedures to ensure good quality of data for processing as following:

2.1 User's face should not bend, perk, or tilt which may impact significantly to face comparison.

2.2 User's eye socket should not have shadow.

2.3 User's width (from left ear to right ear) should be 60%-75% of picture width.

2.4 Picture background should be light color and have no texture and shadow in order to clearly separate user's face and background.

2.5 Picture should not include face of the other person.

2.6 In case of taking picture at branches or service points, financial service providers should provide a proper environment with appropriate light setting. In case of user taking selfie picture with mobile phone, financial service providers should provide recommendation on taking picture with proper light setting. In addition, light on user's face should be consistent and have no hotspot.

2.7 Financial service providers should provide frame or gridline in screen which could facilitate picture adjustment.