

FAQs Biometric Authentication System

Q1. What are the various applications where biometric authentication system is useful?

Biometric authentication system is used in various applications like Financial Inclusion, Rural Banking, Microfinance, Micro Insurance, Remittances, Pension Disbursements, SHG schemes, Women Empowerment Programs, Public Distribution System, Transportation System, Government Identity Projects, Rural employment etc.

Q2. What are the various user processes involved in any biometrics authentication system?

There are two basic biometric user processes involved in the system, an enrollment process and a verification process.

Q3. How do we define an Enrollment Process?

Enrollment relates to the process of registering the fingerprints of a customer against their other demographic data as a record of their biometric identity. It is a one-time process in which a customer is asked to present their fingers on a scanner and the fingerprints are recorded and stored.

Q4. How many fingers are required to enroll?

This is based on the level of security and convenience to be offered to the end user. Typically 2/4 fingers are enrolled; however in certain applications all 10 fingers may be enrolled.

Q5. What kind of image format is used for fingerprints verification?

While the raw image acquired during enrollment will always be stored in a database, the raw image is not useful for verification. Verification requires an extraction of certain key features from the image into a template that can then be used for quick matching. There are various template formats, both proprietary and standards based. Innoviti uses the ISO 19794-2/ANSI/Proprietary standard template format.

Q6. What is the level of false acceptance and false rejection that is acceptable for the application?

The level of false acceptance and false rejection are dependent upon the application and are customizable.

Q7. What is the difference in offline and online biometric authentication system?

Biometric authentication mechanism are primarily of two kinds

- a) offline, in which the authentication is done against a fingerprint template stored in a smart card or POS and
- b) online, in which the authentication is done against a template extracted online from a database.

Q8. What all steps are involved in the enrolment process?

In an online biometric authenticated system, the verification is carried out by retrieving the customer's biometric template using their identity number and then matching that against a live fingerprint. The enrollment process involves recording the templates against an identity number. The typical steps in an enrollment process are:

- i) The customer is asked to enter a customer identity number (this could be a bank related number, a national ID or any other unique identity number).
- ii) The customer is then asked to present their fingers on a scanner that then captures the images.
- iii) The enrollment system may ask the customer to present the finger multiple times to ensure that the quality of image captured is good for verification.
- iv) An ISO 19794-2 template is derived from the captured images.
- v) The template along with the raw image is stored in the biometric server (trueServer) against the customer identity number for later retrieval and verification.

And in case of offline authentication system, the template is stored in the smart card without a need for any customer identity number for retrieval as in case of online system.

Q9. What is De-duplication?

In De-duplication a very high quality images are captured. These images are sent to AFIS (Automated Fingerprint Identification System) for de-duplication. AFIS is a large system designed to conduct 1:N matching between captured images and already stored enrollment images. This is an expensive system.

Q10. How do we define the verification process?

The verification process involves the customer verifying their identity through a live fingerprint to authenticate a payment. This process is carried out every time the customer is carrying out a transaction.

Q11. Is the system supposed to recognize any of the enrolled fingers or will the customer be prompted to present a specific finger or sequence of fingers? Are all enrolled fingers to be verified for completing verification or any one finger will be sufficient?

Typically the verification logic requires the customer to be prompted to present a specific finger, thereby reducing verification complexity and also improving user interface. Hence, only one finger is sufficient for completing the verification.

Q12. Is 360 degrees rotation to be allowed for verification?

Rotation is typically allowed for verification?

Q13. What is the extent of verification required? (strict, moderate, weak)

Verification is kept moderate to strict.

Q13. How the verification process works?

In verification process the customer enters their customer identity number or inserts his smart card into the verification system. The system then prompts the customer to present their live fingerprint on the scanner. The live fingerprint is then compared with the biometric template stored in the smart card or against the template customer identity number in the biometric server. In case the verification is successful the payment transaction is considered authenticated and the transaction sent to the bank for processing. In case of a failure the customer may be asked to present the finger again up to a certain maximum number of tries.

Q14. What all system elements are needed for implementing a biometric authenticated payment system?

Implementing a biometric authenticated payment system requires three primary system elements to be put in place by a bank, these are:

- a) **Enrollment system:** Used for enrolling customers on to the program and recording their fingerprint identity.
- b) **Verification system:** Used at point of transaction for verifying the live fingerprints with the stored fingerprints for authenticating payments or transactions.
- c) **Biometric server/ Smart cards:** Used for storing the fingerprints, extracting and verifying fingerprints during a payment process and providing an interface to banks for managing the customer data and reports.

Q15. What all devices are used for Enrollment system?

Enrollment systems are PC based systems with a fingerprint scanner and necessary application software that can be used to enroll a customer's fingerprints. Innoviti provides the PC-truеID scanner for this purpose that can be interfaced to the USB port of a PC. Innoviti also provides the enrollment application that allows for capture of standard demographic data of a customer against a customer identity and associating the fingerprint data with that identity. The application also takes care of securely communicating and storing the data onto the biometric server. The raw images of the fingerprints as well as the derived templates are stored on the biometric server or smart card.

Q16. What devices are needed for Verification system?

Innoviti provides the Vx610-truеID-GPRS verification system, designed using a Vx610 Point-of-Sale (PoS) machine of VeriFone. And recently introduced MagIC-3-truеID-GPRS, on Gemalto platform. These systems are portable, wireless, biometric devices that can be used at point of transaction for accepting live fingerprints for verifying the customer identity. The PoS platform is PCI compliant and EMV certified and can be used for typical payment applications. The products are designed with an optional high performance battery for portable applications. The case design uses UV resistant plastics that makes them a rugged platform for outdoor use, e.g. in rural programs.

Q17. How the verification process flows using these devices and transaction happen?

Typical verification process involves a customer entering their customer ID into the system through a numeric keypad. The device then connects to the biometric server over GPRS or dial-up (both options available) to retrieve the templates stored against that ID. Verification is then carried out and if verified, the system allows the payment to proceed to the acquirer. There are two methods possible to connect the biometric verification process to the payment process as follows;

a) First verification is carried out. The verification status is then sent from the PoS as a part of the payment packet (as a flag) to the acquirer for payment processing. The flag status is considered as verification status by the acquirer.

b) A payment packet is sent with the customer ID to the bank host, which in turn connects to the biometric server with the customer ID and PoS number and it to complete the verification. The biometric server connects to the PoS to complete the verification process between the live fingerprint and the template extracted using the customer ID. The verification status is then sent back by the server to the bank host for further processing.

Q18. What is the difference between the above two methods?

The primary difference between the approaches is in the network configuration. Option a) requires the PoS to be connected to the biometric server and the bank host independently but no connectivity is required between the server and the host. The verification status flag in the payment packet sent by the PoS is considered as being valid for payment processing. Option b) requires the bank host and the biometric server to be connected in addition to the connectivity between the PoS and the biometric server and the bank host. However communication of verification status happens only between the biometric server and the bank host and not with the PoS.

Q19. Are the above communications over the network are secure?

The template storage at the biometric server and the communication of templates between the PoS and the biometric server are encrypted, using 128/256-bit AES encryption.

Q20. What is Biometric Server and what all component applications does it includes?

Biometric Server (trueServer) is a biometric server application And the trueServer has the following component applications running in it:

a) ISO 8583 switch: An ISO 8583 switch that can take in 8583 packets from a POS system, parse them, forward the information to the business process engine using pre-defined formats and provide a response back to the PoS system.

b) Gateway: A converter that provides different input data interfaces and provides a common interface on the other end to the business process engine.

c) Business Process Engine: An application that runs the basic business process intelligence, including rules for verification, enrollment, database updation, presentation etc.

d) Database: A database for storing the enrollment data, including the fingerprint data in an encrypted format. The database can also optionally store the verification request transactions for reporting.

e) Web Portal: An application that provides a web interface to the database for viewing, editing and managing customer information for the acquiring administrator.

Q21. What are the different interfaces used for the biometric server?

There are two interfaces presented to the biometric server externally, as follows:

a) An interface for the POS device through an ISO 8583 switch. The switch then connects to the business process engine through a gateway and b) a direct interface to the gateway for an enrollment system through a static IP. In addition the web portal provides for a user-friendly web interface for the bank to manage the customer's biometric data.

Q22. What steps are involved in Integrating a Biometrics with any existing payment system?

The process of integrating the above biometric system elements into an existing system involve usually the following steps:

Step 1: Specification phase: In this phase the exact requirement for biometric verification has to be specified and the user processes captured. This would include defining how the enrollment will happen, the enrollment specifications, how verification will happen, data storage etc. Innoviti will provide consultation during this phase to ensure that there is an optimal mapping of the business processes carried out.

Step 2: Proof of Concept (POC) phase: In this phase the business processes specified in Step 1 above are implemented using the various system elements that Innoviti has. In case there are any customizations to the basic elements then that is also carried out. The aim of the POC phase is to implement the key business processes to check on certain basic performance parameters such as integration of the payment and biometric verification process, security considerations, database management, response time etc. During this phase all the system elements need to be implemented on a smaller scale and tested in a controlled environment.

Step 3: Pilot phase: The pilot phase involves setting up the system for end users to conduct live transactions, however in a controlled manner on a smaller scale. The main aim of this phase is to understand user issues and live transaction issues.

Step 4: Commercial phase: In this phase the system is taken commercial.