MANTRA
Innovation that counts

WHITE PAPER

L1 FINGERPRINT SENSORS

A Step towards Unbeatable Security

www.mantratec.com

Table of Contents:

Introduction

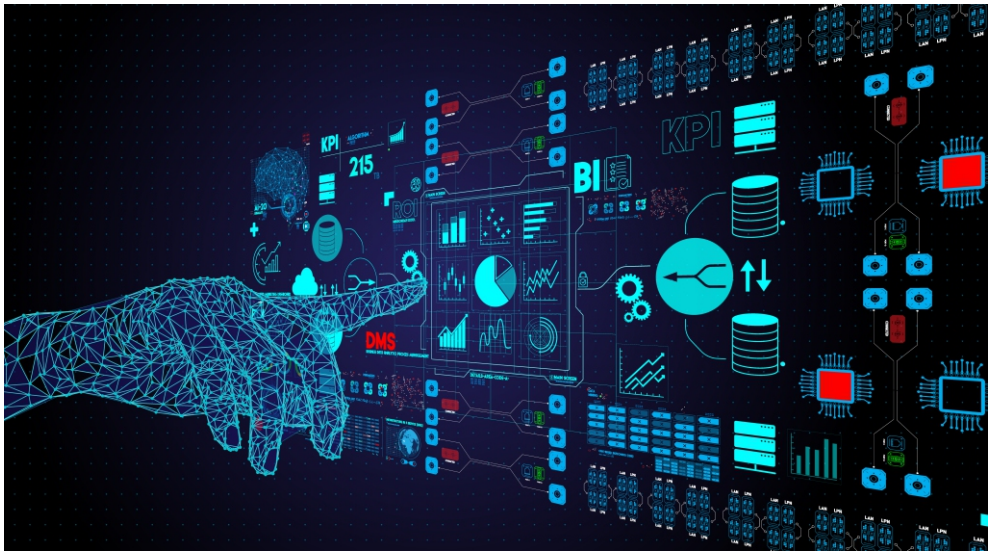
As the world becomes more digital, the necessity for strong security measures to protect personal and sensitive information rises. PIN codes and traditional password protection are no longer sufficient to address the constantly evolving security threats. It is one of the main factors influencing the widespread use of biometric authentication and security advancements. The current Registered level 0 fingerprint sensors need to be upgraded to match the increasing security and authentication criteria. L1 fingerprint sensors fill this need, offering a higher level of security in a more interconnected society.

L1 fingerprint sensors use powerful encryption technology in conjunction with the safe sharing of device identity methods to ensure that biometric data is secured and not shared with third-party platforms. In this white paper, we'll look at the advantages of L1 fingerprint sensors and how they can give you unbreakable security. We will delve into the L1 fingerprint sensors' technical aspects, including how they work and how they differ from more traditional security measures. The limitations of registered L0 devices will also be covered, along with how L1 fingerprint sensors might increase security.

The Need For More Secure Fingerprint Authentication

Biometrics is being used as a primary form of authentication in everything from consumer devices to wearable devices, as well as in enterprises, governments, businesses, and consumer devices. Simple logins to high-security applications for banking, healthcare, and citizen identification for government schemes are some of the applications. Passwords were replaced by biometrics because they are ineffective in the face of today's cyber threats for high-throughput applications. According to various studies submitted before the European Union parliament, password encryption is easy to crack for hackers since most people use predictable passwords and the same password for multiple platforms.

There are problems with the storage and transmission of biometric data as well as the verification of the source of biometric authentication, even with biometric authentication. This means that even if the biometric data is encrypted, it may still be possible to hack it from the biometric devices or while it is being transferred. Additionally, hackers can duplicate the biometric sensor device identity and biometric data for multi-platform authentication. People should therefore be extra cautious when selecting a biometric device for verification.

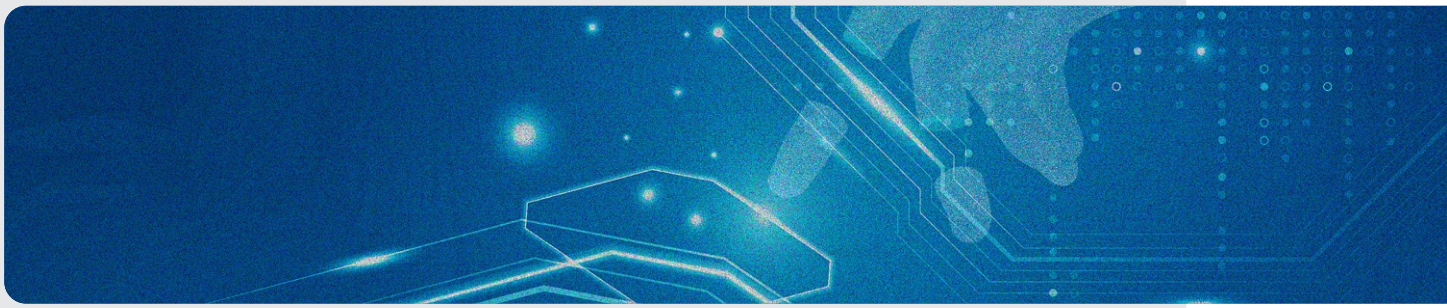


The importance of secured biometric authentication

Authentication is a crucial step in the process of verifying a user's identity. It aids in preventing unauthorized access to sensitive information, such as financial and personal data, in the online environment. This is crucial when it comes to internet banking because private financial information is transferred over third-party platforms. Biometric authentication is considered the most secure way to authenticate, and it is a blend of both convenience and security.

The biometric authentication method makes it unnecessary for users to carry physical tokens or memorize passwords, making it easier for them to access their devices or accounts. User adoption may rise as a result, and pain levels may drop. Biometric information is far more secure than typical passwords because it cannot be lost, forgotten, or stolen that easily. Because they rely on distinctive physical characteristics, biometric verification systems are more difficult to fake.

The Introduction of Registered Devices



Registered biometric devices were introduced to ensure the biometric sample submitted to an identity database for verification is from trusted encrypted devices. The pre-registered device identification and the biometric identity of a person will be shared by the registered devices, ensuring the validity of the sample provided. This process is very much essential for high throughput applications like government ones.

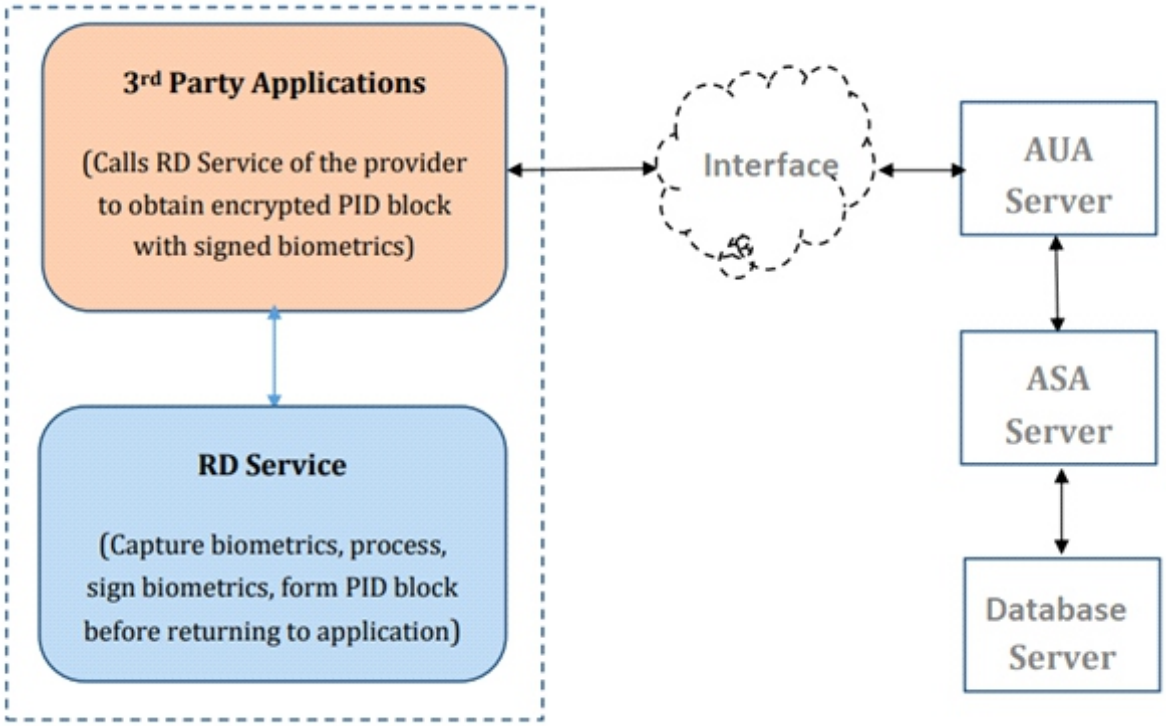


Fig1: Registered device data flow.

The registered devices will have an encrypted signature of device identity that is shared with the identity database while authenticating, allowing traceability, analytics, and fraud management. Additionally, registered devices never store biometric information; instead, the data is encrypted using the device key to confirm that it was recorded live and saved inside an encrypted PID block. Any host OS accessing the biometric data will be given the encrypted PID block to decrypt the key.

L0 and L1 devices were introduced as the different levels of registered devices. The L0 is the minimum requirement for registered biometric devices, and its makers must address: the security of the PID block, the fact that the biometric data is not shared with the host OS, and the encryption of the device ID.

L1 devices are the next level of registered devices and the most secure of their kind. We discuss more it in the upcoming sections.

The L1 Biometric Fingerprint Device

The L1 fingerprint device carries out the signing and encryption of biometric data and is transferred only through a Trusted Execution Environment (TEE) that completely isolates the host OS from obtaining the private key or injecting biometrics. The TEE executes the private key management and the biometric PID block for the transmission.

Hardware security, on the other hand, ensures that the chip identity is either guarded within the crypto block or wrapped with the instance-specific unique key (non-extractable and stored within the secure crypto block). It could reduce the risk of data leakage and the attack surface at the system level by employing techniques such as, but not limited to, hidden traces, protective meshing, encrypted communication, and so on.

Crypto block technology works by encrypting data using complex algorithms, making it nearly impossible for hackers or unauthorized users to access the data. When biometric data is stored in a TEE with crypto block technology, it is encrypted and protected from any unauthorized access or tampering. This helps ensure that biometric data remains confidential and secure, even if the data falls into the wrong hands.

TEE security

A secure environment that is separate from the primary operating system is called the Trusted Execution Environment (TEE), and it remains on the device. The TEE is designed to provide secured settings for processing and biometric data storage.

The TEE environment provides a secure location for storing and processing biometric data and it is designed to be impenetrable to alteration and unauthorized access. The biometric data is first gathered and then processed within the TEE when a biometric authentication method is initiated. The TEE then checks the stored data against the sample data for authentication, and if a match is confirmed, the TEE notifies the host operating system to grant access.

TEE in the L1 device manages three key processes.

- Biometric processing/extraction to create the bio element
- Signing the bio element.
- Encryption of the PID block

In the case of shared hardware, i.e., the processor used for purposes other than L1-registered device functionality, a global platform-certified TEE is required.

Crypto hardware attack protection

All L1 devices must have a certified crypto block or similar protection that can protect against hardware overflow attacks. The crypto block guards the chip identity and is strongly tied to the cryptoprocessor to prevent any possibility of hardware cloning.

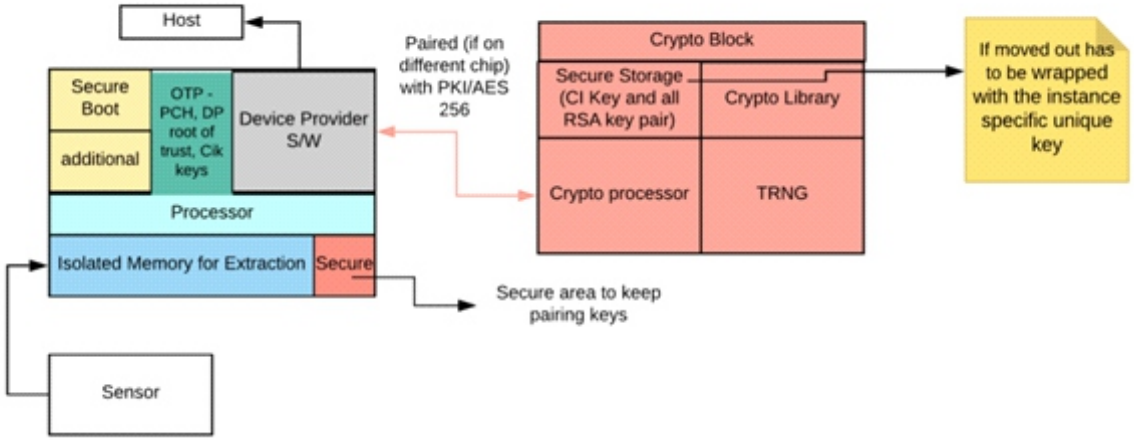


Fig 2: L1 Fingerprint Sensor Block Diagram with certified Crypto block

The identity is created by generating a key pair in the secure crypto block, and the public key is signed by the pre-certified hardware device. This signed public certificate should be permanent and written to One Time Programmable memory. That means the chip will have only one identity for the rest of its life. Memory for the execution of cryptographic operations is segregated to protect the crypto block from buffer overflow attacks.

In addition, the crypto block in L1 devices is designed to be tamper-resistant with software support that prevents physical, voltage, frequency, and temperature attacks on the crypto block. And it will make it impossible to employ any identity block on devices other than the precertified identity.

Advantages of using L1 biometric device

Encryption: Encrypting biometric data before storing it on the blockchain ensures that it is secure and cannot be accessible by unauthorized parties.

Hashing: Hashing is a technique that can store biometric data on the blockchain in a secure and tamper-proof manner. Instead of storing the raw data, this method includes turning the biometric data into a unique code stored on the blockchain.

Access controls: Access controls can be put in place to limit who can see or change the biometric data stored on the blockchain. Password protection, multi-factor authentication, and permission-based access are examples of this.

Auditing: Regular blockchain audits can aid in detecting illegal access to biometric data stored on it and preventing misuse.

Regulation: Compliance with relevant privacy laws and regulations can help to protect biometric data stored on the blockchain and ensure that it is used ethically and responsibly.

Conclusion

As our world becomes more digital, stronger security measures are becoming increasingly important. We explored the different benefits of L1 fingerprint sensors and the greater security they provide over traditional identifying techniques in this white paper. We've discussed how they function technically and how their power systems and sensors provide fast, accurate, and safe authentication.

The L1 fingerprint sensor is a significant step towards unbeatable security. L1 is a true game-changer in the security industry because of its cutting-edge TEE security and cryptographic encryption. The technology will enhance the usage of fingerprint authentication in numerous high-security applications.

+91-79-49068001 sales@mantratec.com www.mantratec.com

8. Versatility

Many companies offer embedded software for desktops with their multi-fingerprint scanners; the scanner will only work with this software. This is unacceptable in the case of security applications and citizen enrollment; they must be universally inter-portable.

Third-party software dependency poses a security risk to law enforcement and other government agencies. And so, multi fingerprint scanners should have universal portability as per the standards.

Conclusion

Choosing a multi-fingerprint scanner is as easy as it gets. When it comes to specs, one must select between FAP 40 and FAP 60 devices. Their specifications are mentioned above in this article. Their applications, where each kind is appropriate, are also outlined. As the security threats and throughput in each system are increasing, the need for multi-fingerprint scanners will also increase. Aside from public enrollment and security, the scanners will find use in the commercial and financial sectors. As a result, there will be additional advancements in device size, design, durability, connection, and capabilities.

+91-79-49068001 sales@mantratec.com www.mantratec.com