March 2025
Manilla, Philippines

MOSIP

Training:
Essential Integrations: ABIS, SDK & Biometrics

Name | Suraj S, MOSIP

Secure Biometric Interface

Secure Biometric Interface (SBI) Standard

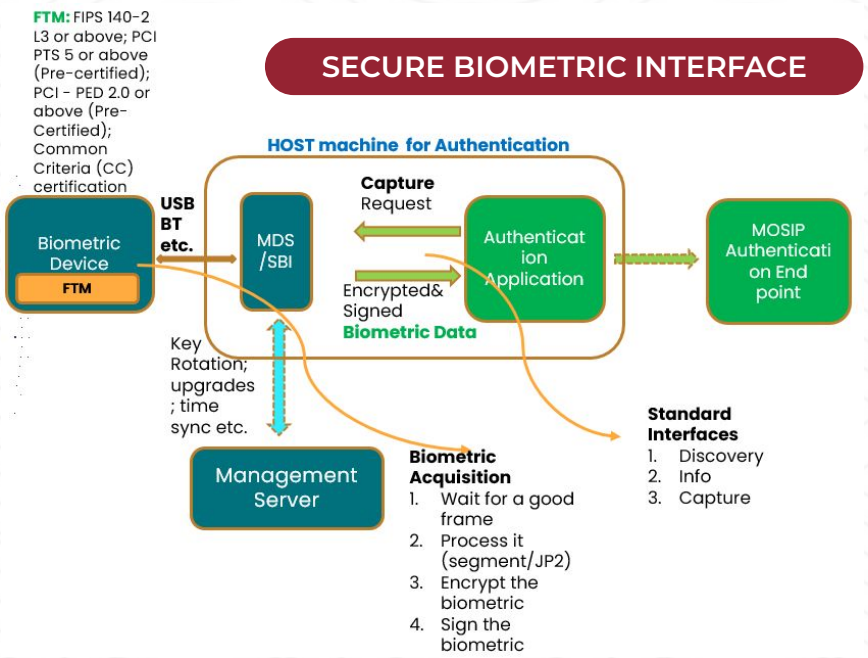
- Biometric Replay/Injection
- Cryptographic Traceability
- Standardised interfaces
- Purpose driven capture

SBI 1.0

- Host based security
- For controlled environments

SBI 2.0

- Hardware based (FTM) security
- For uncontrolled environments

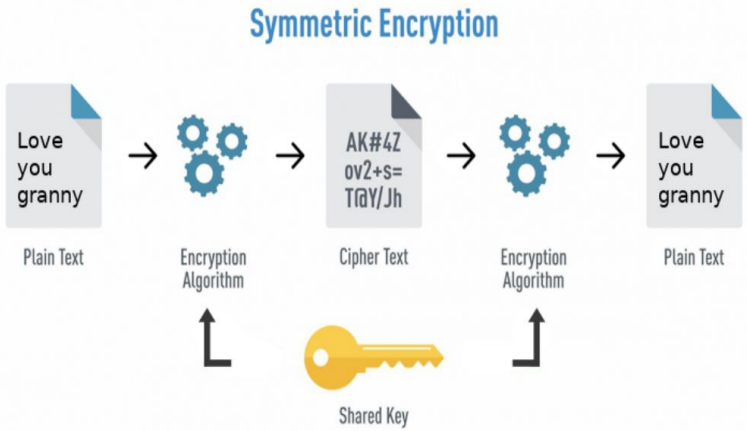


Managed Devices | Remote Upgrades | Secure Provisioning | Secure Boot

Time Sync | Key Rotations | Trusted Apps | Forward upgrades

Basic Concepts

Symmetric and Asymmetric Encryption



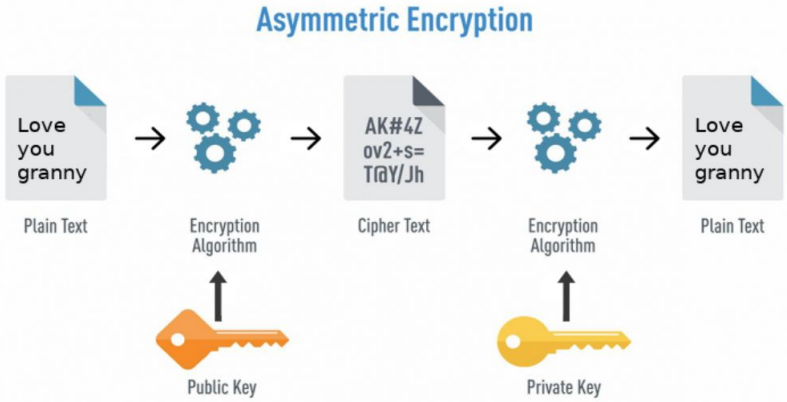
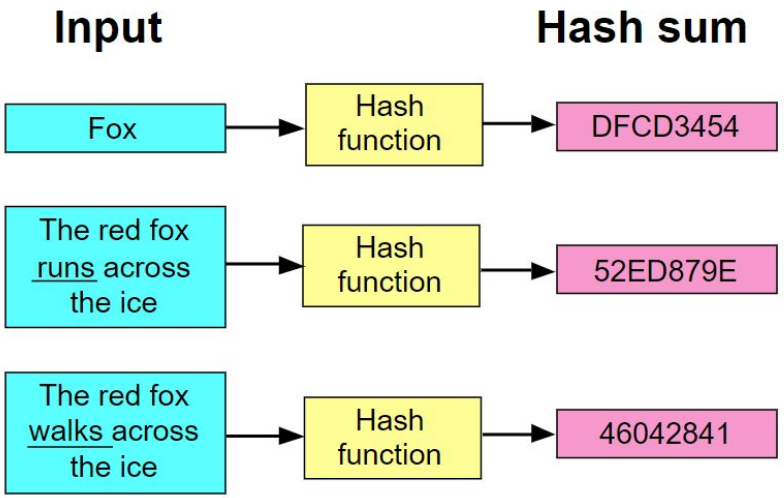


Image courtesy:
https://hackernoon.com/

Hashing & Digital Signature



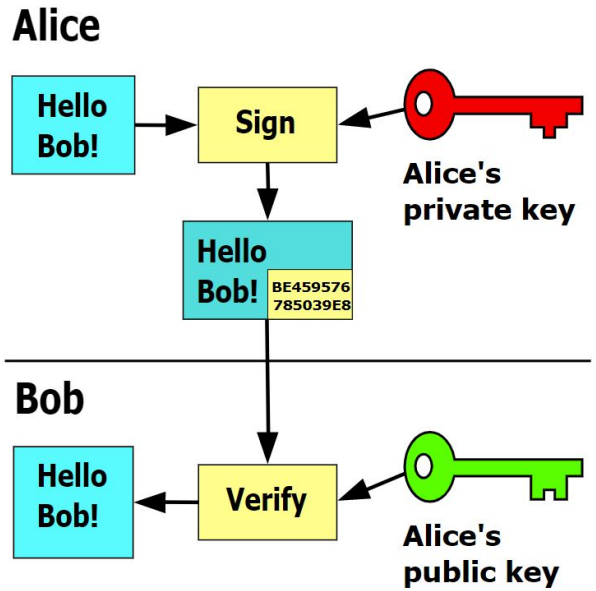
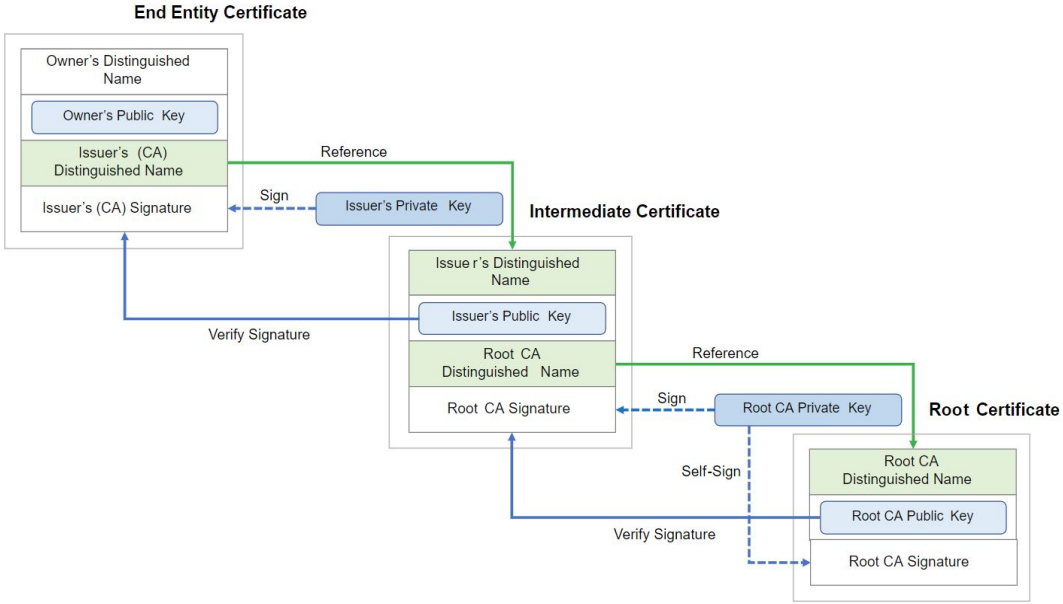
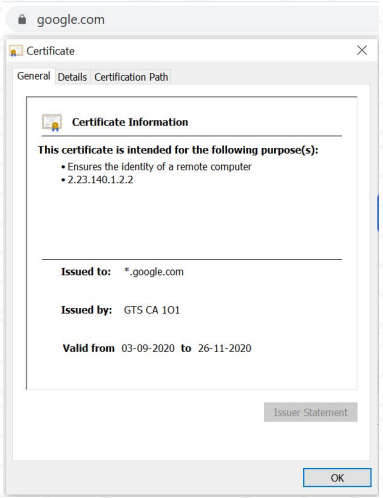


Image courtesy: wiki

Certificate Chain Validation





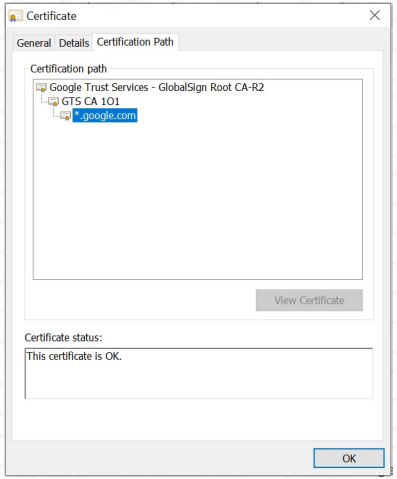


Image courtesy: wiki

Secure Biometric Interface

SBI 1.0 and SBI 2.0

- Signing is done on the host inside its device driver or the SBI service
- The trust is provided at the software level. No hardware level trust exist.

SBI 1.0 (Controlled Enviroment)

- Signing on the device inside its trusted zone.
- The trust is provided by a secure chip with secure execution environment

SBI 2.0 (Uncontrolled Environment)

Secure Biometric Interface

- No external Biometrics can be injected
- Should have a signing mechanism
- Signing Keys cannot be extracted
- Biometric Capture Processing, Signing and encryption

SBI Service

- Rotate the signing keys.
- Validate own devices and issue certificates
- Repo of devices, Device Provider Keys in HSM (FIPS 140-2 L3)
- Sync time with SBI; manage upgrades

Management Server

Secure Capture/Transfer of Biometrics

Sender

Hash, Encrypt,
Digitally Sign

Recipient

Encrypt Using
Random** Session Key - **1234

Decrypt Using Same
*Session Key - **1234***

Sender

Recipient

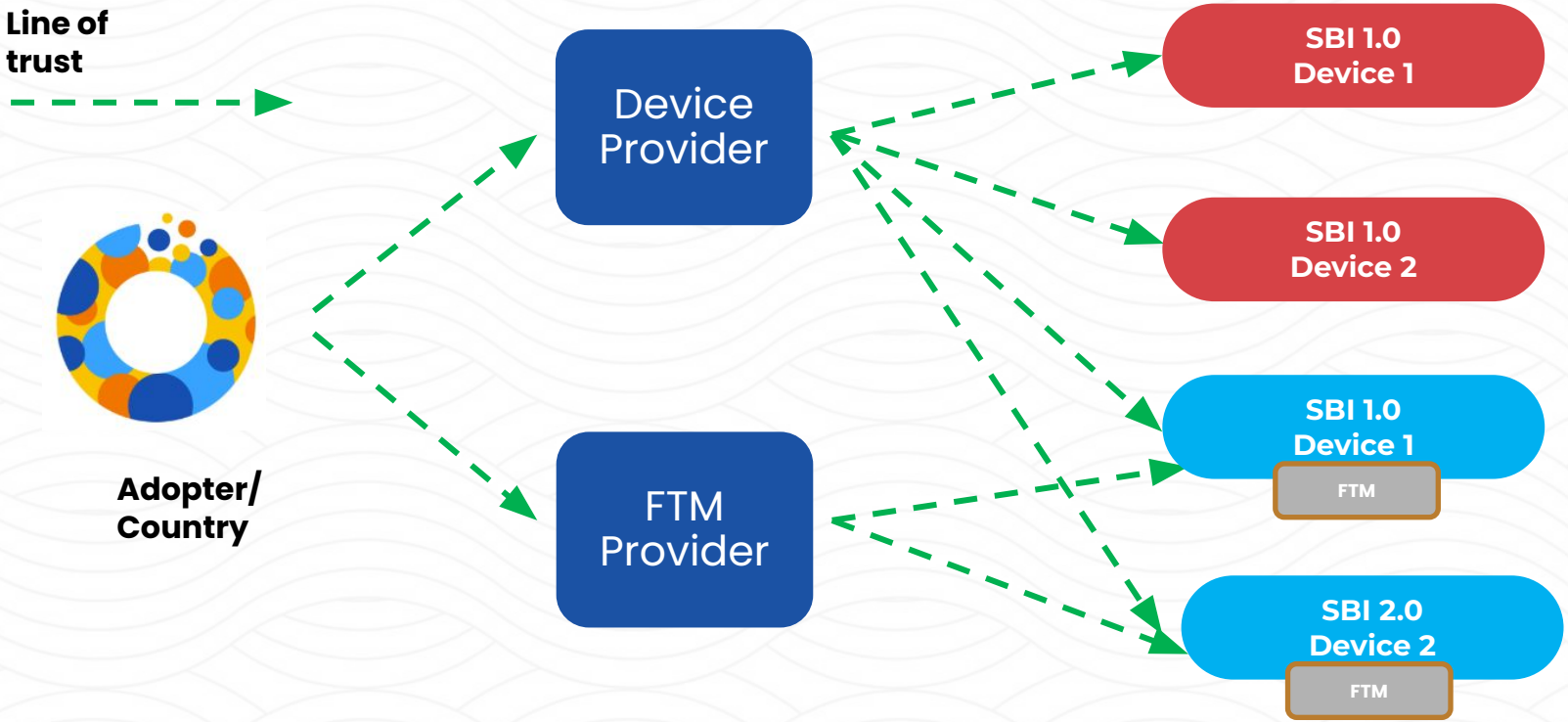
***Encrypt** using*
Recipient Public Key

***Decrypt** using*
Recipient Private Key

SBI Communication Interfaces

Device Discovery	*Device discovery would be used to identify MOSIP compliant devices in a system by the applications*
Device Info	*The device information API would be used to identify the MOSIP compliant devices and their status by the applications*
Capture	*Used to capture a biometric from MOSIP compliant devices by the applications. Response will provide the actual biometric data in encrypted and digitally signed form*
Device Stream	*Used only for the registration module compatible devices. Visible only for the devices that are registered for the purpose as "Registration".*
Registration Capture	*Used by Registration Client.* • *Response will provide the actual biometric data in a digitally signed non encrypted form.* • *The device to send the images as well as its extraction values.*

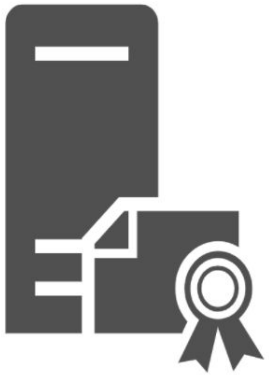
It's all about Trust !



On boarding/Trusting the Device Provider

1. "ABC Biometrics" obtains a CA signed certificate from a valid CA registered in the MOSIP ecosystem

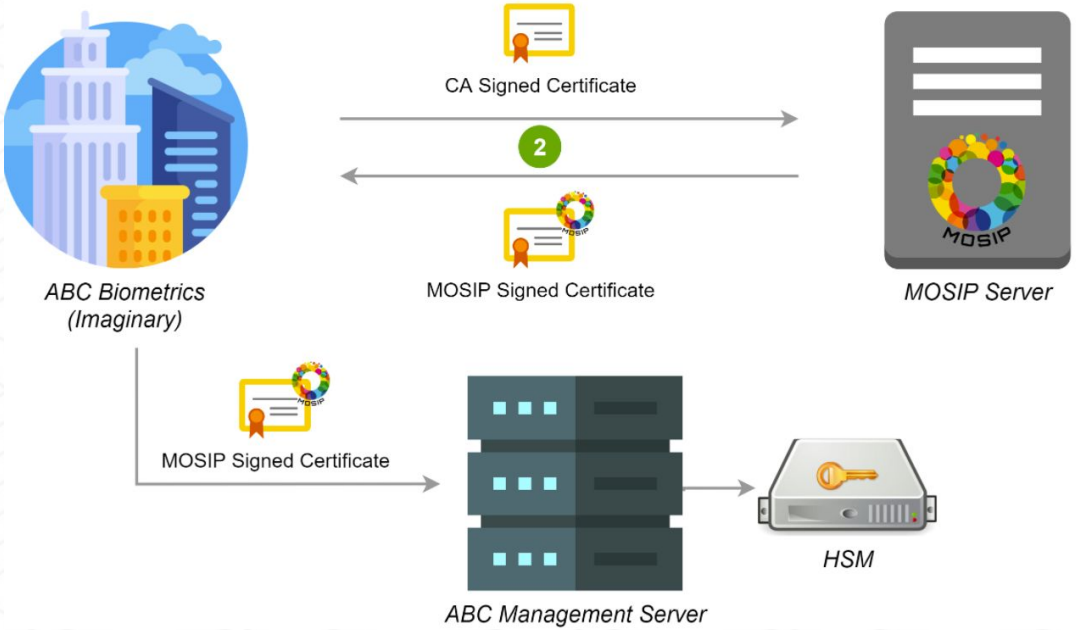
ABC Biometrics (Imaginary)



Country Approved Certificate Authority

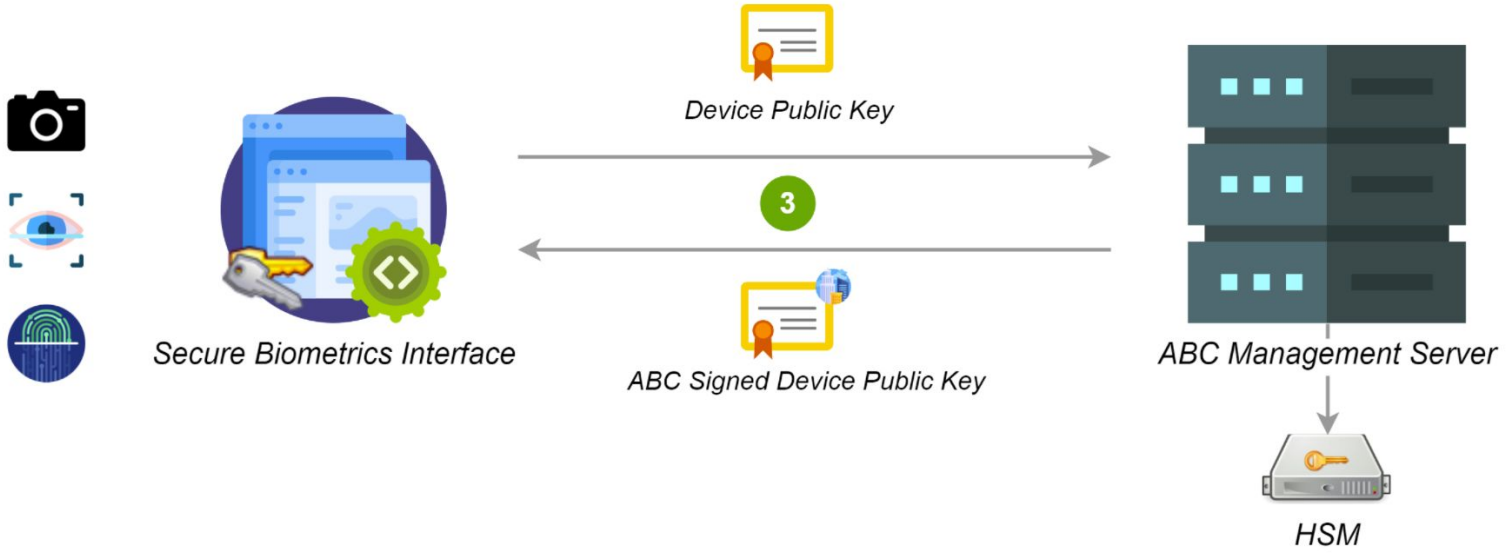
On boarding/Trusting the Device Provider

2. "ABC Biometrics" now uploads the CA signed certificate in MOSIP's partner management portal to get a MOSIP signed certificate which is later uploaded to the Management Server

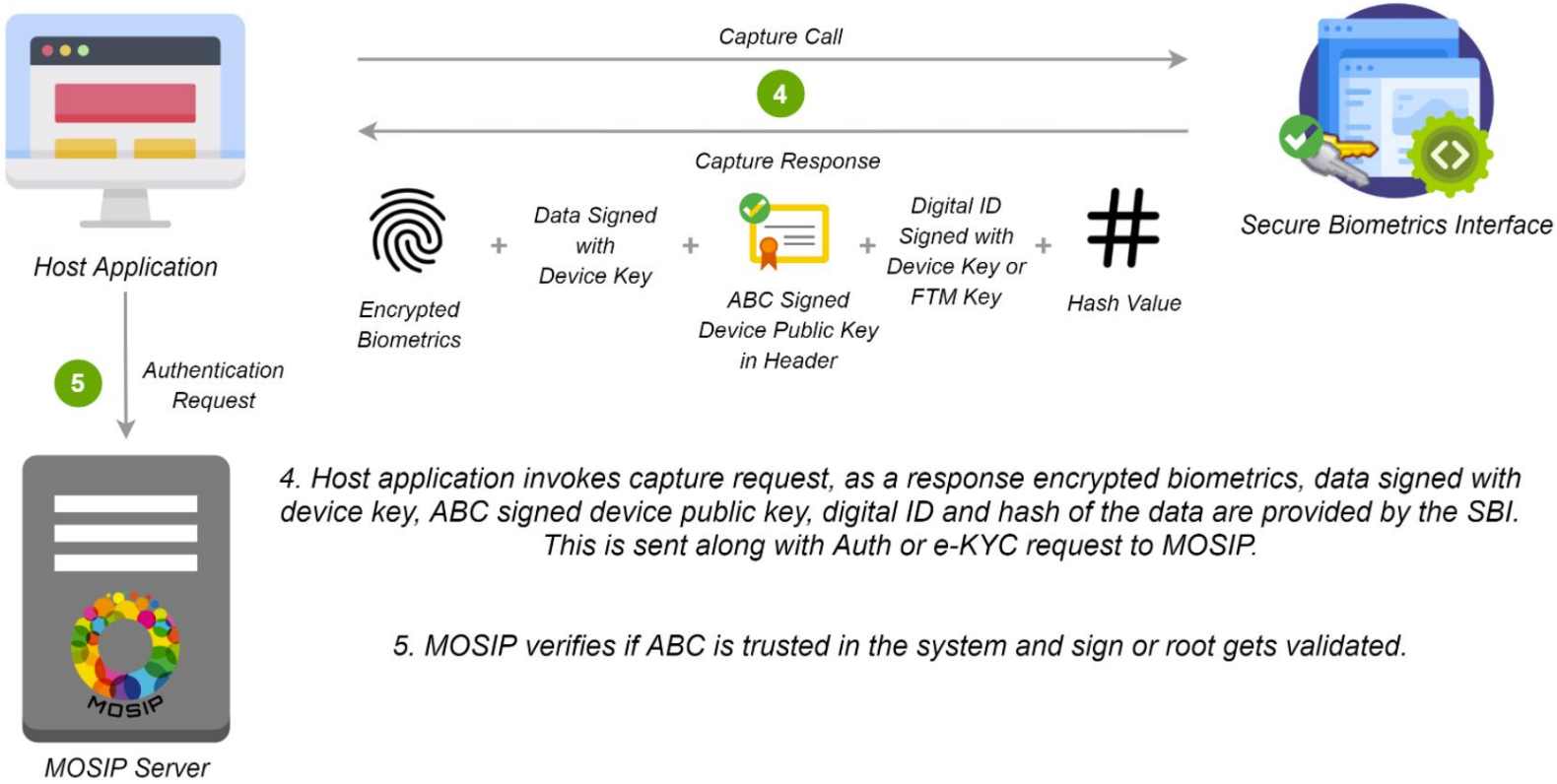


On boarding/Trusting the Device Provider

3. Each individual device or SBI creates its own key pair, and sends the public key to the Management Server gets back a "ABC Biometrics" signed public certificate



On boarding/Trusting the Device Provider



4. Host application invokes capture request, as a response encrypted biometrics, data signed with device key, ABC signed device public key, digital ID and hash of the data are provided by the SBI. This is sent along with Auth or e-KYC request to MOSIP.

5. MOSIP verifies if ABC is trusted in the system and sign or root gets validated.

Secure Biometric Interface (SBI) Standard

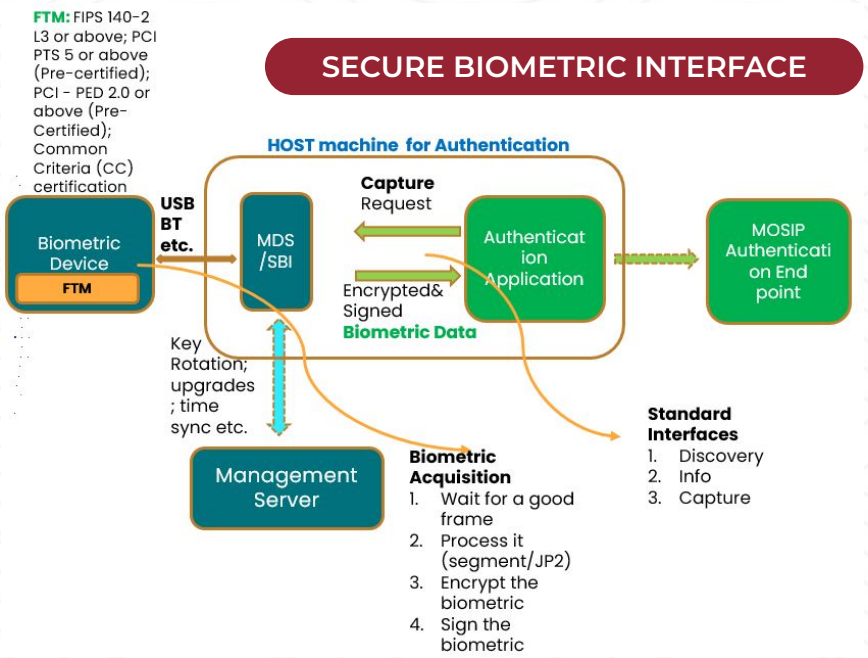
- Biometric Replay/Injection
- Cryptographic Traceability
- Standardised interfaces
- Purpose driven capture

SBI 1.0

- Host based security
- For controlled environments

SBI 2.0

- Hardware based (FTM) security
- For uncontrolled environments

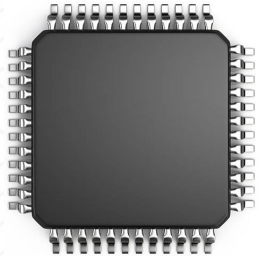


Managed Devices | Remote Upgrades | Secure Provisioning | Secure Boot

Time Sync | Key Rotations | Trusted Apps | Forward upgrades

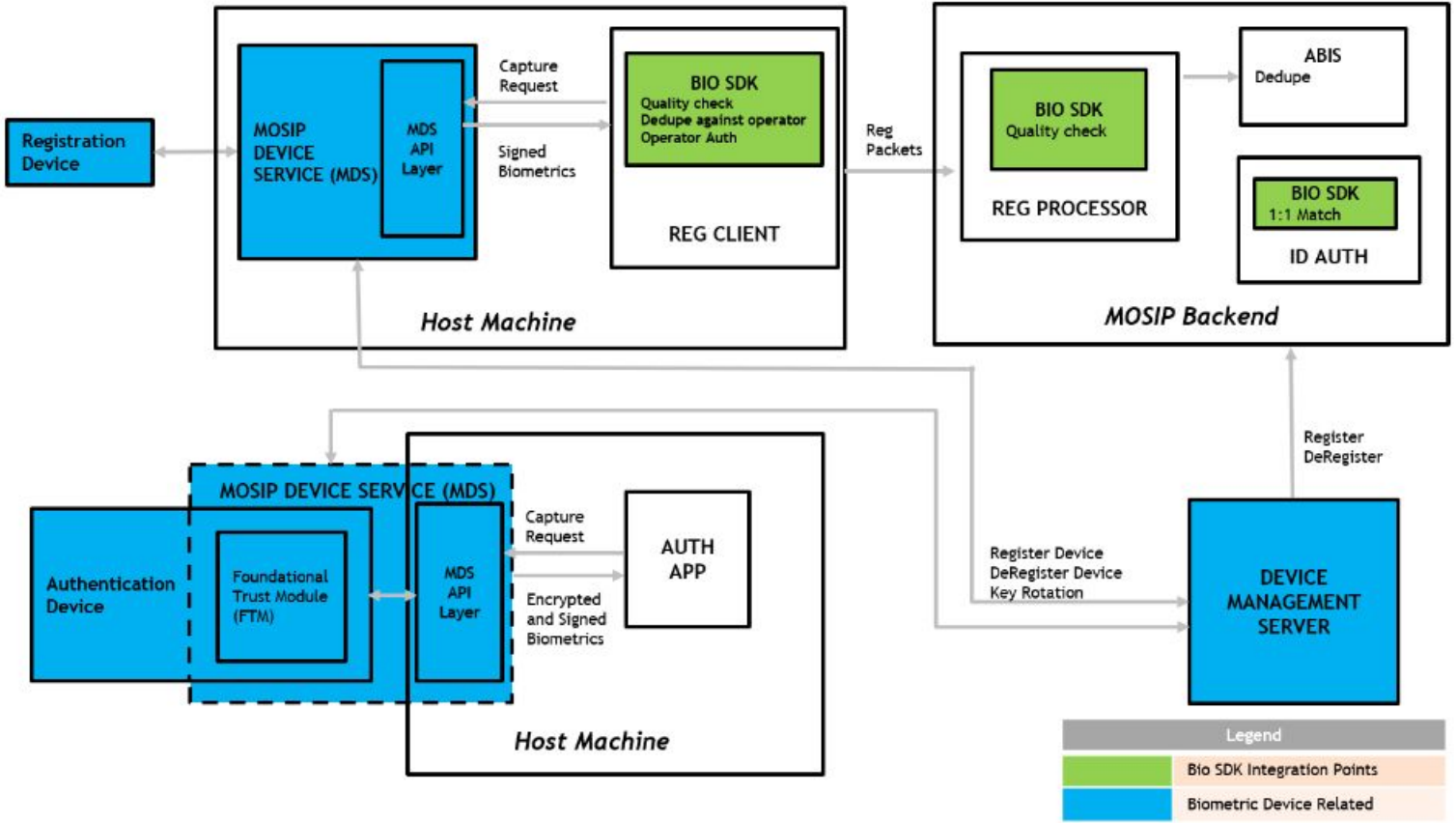
Foundational Trust Module (FTM) - SBI 2.0

- Securely Generate, Process and Store Cryptographic Keys
- Asymmetric and Symmetric Key Generation
- Protect the Keys from tampering/attacks & extraction
- Secure Boot Verify Code
- Run Trusted Applications
- Forward only upgrades
- Validate Integrity
- All required biometric processing
- Certificate Issuance in a secure provisioning facility



Biometric SDK

Biometric SDK – High Level Overview



Biometric SDK - Function

Quality Checker

- Checks the quality of input biometrics and returns quality score for the same.
- When the Biometric image is received by MOSIP in the registration client this method is used to check the quality of the image

Matcher

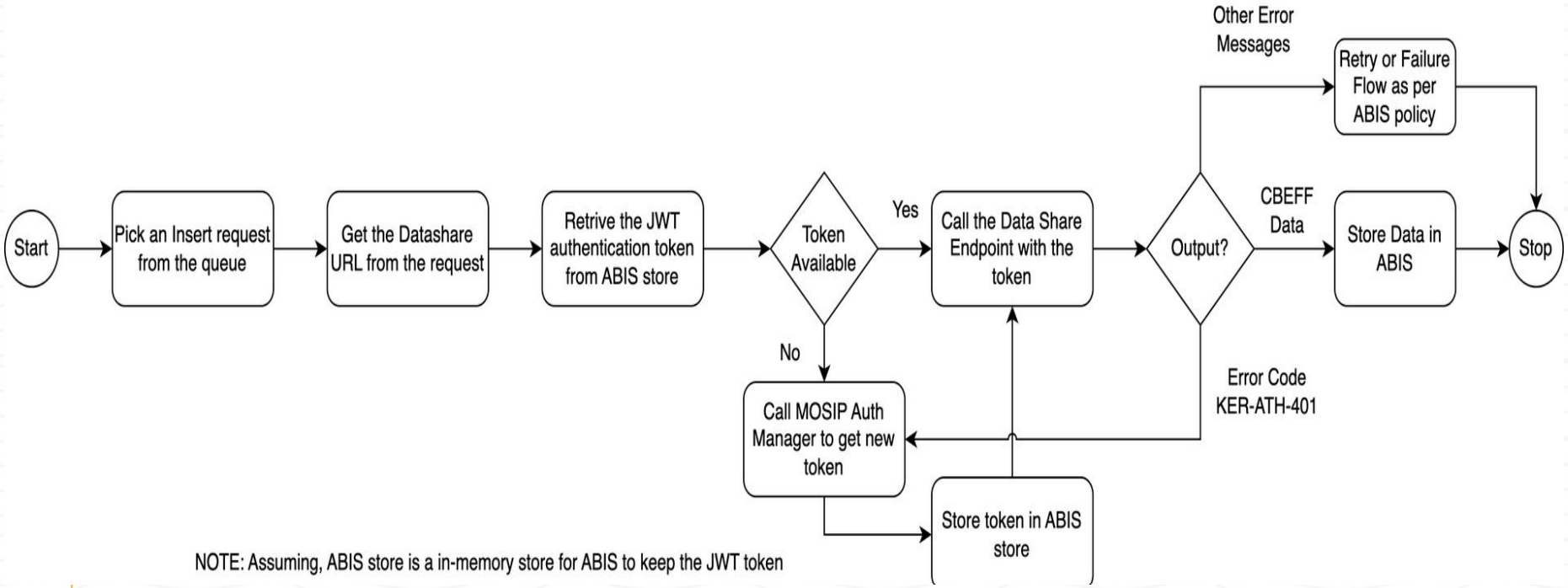
- Matches the captured biometric record or a list of biometric records (based on single match or composite match), matches it against list of stored biometric records. It then returns a matching score against each stored biometric record or a composite matching score for the list of input biometric records.
- Used for authentication of operators in registration client

Extractor

- Extracts salient features and patterns of input biometric record to use in fast comparison. It returns the extracted biometric record, ex:- Finger Minutiae points

ABIS
(Automated Biometric Identification System)

ABIS - Overview



ABIS - Overview

- Providing a unique identity for a resident is one of key features
- ABIS is used for 1:N de-duplication of a resident biometric data
- ABIS system never comes to know about resident's identity. Any Personally Identifiable Information (PII) such as demographic details or RID (Request ID for Registration) is not shared with the ABIS system
- MOSIP maintains a mapping between the ABIS specific referenceID and RID of the resident
- ABIS must support the following types of biometric images:
  - Individual fingerprint images (segmented)
  - Iris images (left, right)
  - Face image
- ABIS Operations – Insert, Identify, Delete, Ping, Reference Count

API Specifications

- https://docs.mosip.io/1.1.5/biometrics/mosip-device-service-specification
- https://docs.mosip.io/1.1.5/biometrics/biometric-specification
- https://docs.mosip.io/1.1.5/biometrics/biometric-sdk
- https://docs.mosip.io/1.1.5/biometrics/automated-biometric-identification-system-abis

Any Questions?

MOSIP

Thank You!

Homepage: www.mosip.io

Source Code: github.com/mosip

Documentation: docs.mosip.io

Community: community.mosip.io