Privacy and Security by Design

CONCEPTS AND DEFINITIONS

What is Privacy?

Level of Anonymity

Protecting user’s identity

Protecting user’s personal information

Foundational ID - Legal Identity + Unique Identity + Digital Identity*

MOSIP Thinks of Security as...

Building trust:

- Can anyone steal my Identity?
- Transparency of usage
- Data sharing and Authorization .

Protection:

- Information Security
- Protection from Hackers

Worries:

- How to beat the security gap between the literates and non-literates.
- Spam/Phishing attacks

MOSIP Objectives on Privacy and Security

Privacy

1. Individual is the owner of the data.
2. Transparency should be built in.

Security

1. Enable individuals/partners/governments to use the system with utmost trust
2. Protection against state attacks and terrorist attacks.
3. Ability of the individual to restrict verification
4. Ability to revoke identity upon need.
5. Stop any proliferation attempts.

CHALLENGES TO PRIVACY AND SECURITY

Challenge Scenarios

Internal Attacks, External Threats, Terrorist, Internal Civil war

Offline Registration, Online/Offline verification.

Ability to revoke.

Ability to quarantine and isolate upon attacks or compromise.

Response to security attack/threats

Challenges with 360 degree profiling - Privacy

Challenges on non tech-savvy users, multi lingual

Fraud and Theft

- Type of fraud
  - Stealing biometrics
  - Stolen phone
  - Social engineering
- Increasing Sophistication
- Recovering from fraud/theft

MOSIP DESIGN - PRIVACY AND SECURITY

Design elements for Privacy - Basics

Treatment of Personally Identifiable Information

- Secure one way hash for anonymous comparisons
- Encryption of data in motion and at rest

ID Repository Access Service

- Restricts querying on the database
- Application handles encryption / decryption
- Offers specific functional stateless APIs that are secured (certificate based authentication - TL1)

User consent

- All access to user's data should have user consent.

Design elements for Privacy - Functionality

UIN

- A unique 12 digit random number assigned to a individual after de-duplication.

Virtual ID

- Enables a revocable identity and prevents stealing of identity

Token ID

- Deters 360 degree profiling

Limited Profile Sharing

- Provides limited sharing of data, user centric policy

History and Alerts

- Provides transparency, Notification and real time awareness of usage with non tamperable data

Lock Authentication

- Provides ability to lock or unlock specific functions of authentication and eKYC.

Secure offline Authentication

- Provides for data privacy even in offline authentication mode

Virtual ID - How does this work?

VID is generated on user request

- Random ID with validatable format

Allows access to limited information

Policy driven validity

- User can revoke any time
- One time use
- Valid for 30 minutes
- Valid for one time use within 30 minutes
- Long term validity of VID associated for offline usage

Token ID - How does this work?

User uses UIN / VID for one time authentication and authorization of eKYC

- Happens on a separate secure channel where 3rd party does not have access to user provided information.

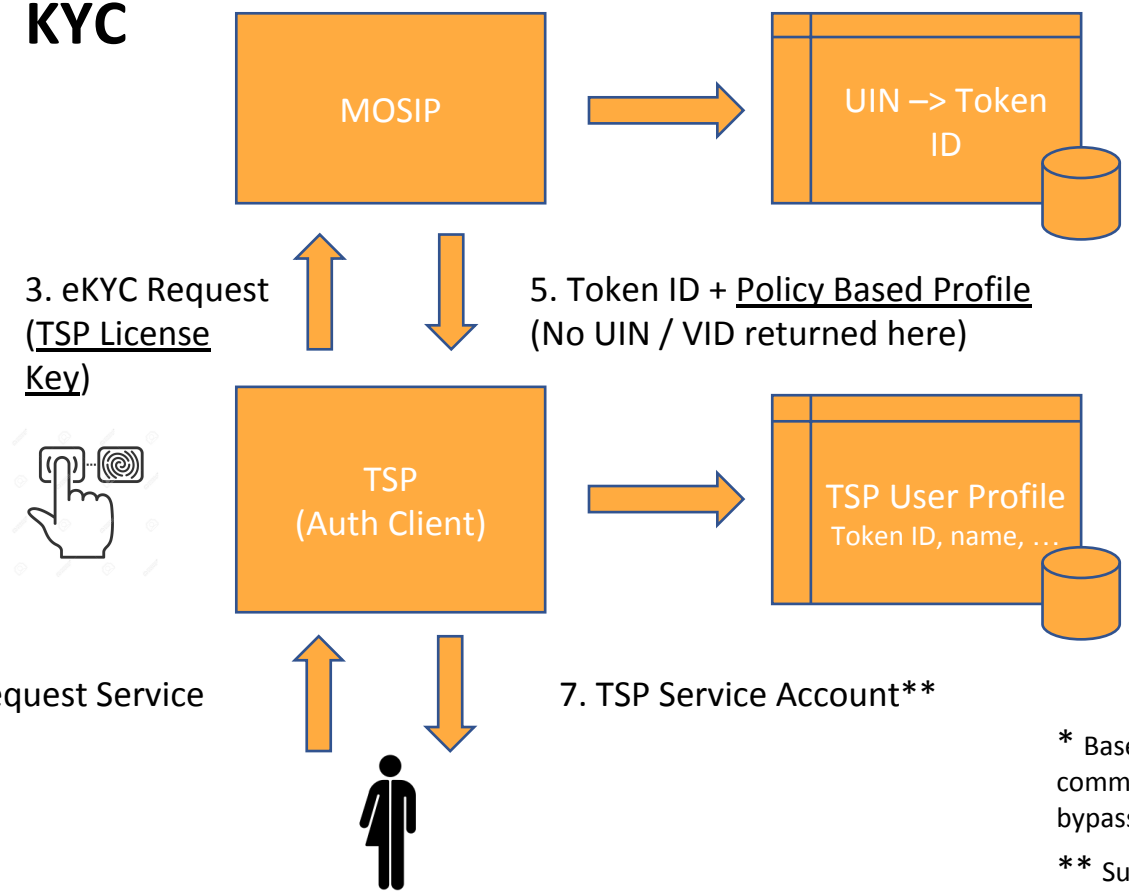
3rd Party Agency does not get UIN, they get a Token ID

- Future transactions with agency will use the same Token ID

Token ID is different for each 3rd Party agency deterring profiling across providers

Token ID can be revoked or blocked

Token ID – UIN Abstraction, Limited KYC



* Based on type of device the communication with MOSIP could be direct, bypassing the TSP software

** Subsequent requests for the same user for the TSP will use the same Token ID

User controlled authentication, Offline Support

Lock Authentication:

- Authentication.
- Ekyc
- Biometric
- Auto lock

Offline authentication.

- Download the latest ID in QR Code format.
- Encrypted and digitally signed QR code is provided to validate.
- One time encryption key shared with user ala OTP
- Well defined issuance and expiry of the QR code.
- Minimal KYC or Full KYC could be stored in QR code.

Foundational Principles for Security

Data that moves out of MOSIP environment should be digitally signed with timestamp.

All PII data (to be defined as part of the integration) & all configuration data (defined as part of the development of system) will be encrypted at rest and in motion.

Every third-party interaction will be built over the mutually trusted channel with the respective PKI validation. All events are auditable and non repudiable.

All data and trust should be cryptographically validatable by all parties involved in the transaction at any point in time.

Design elements for Security (1/2)

Trusted Execution Environment (TL1 - TL3)

Identification

Key management

Encryption

OTP

Data protection

Insert only design on audit

Transparency

Data anonymization

Password standards & Storage

Design elements for Security (2/2)

Container Security

CA Structure

API abuse protection

Hardened tools

Secure By default

Api Protection

Any time Audit

Devsec OPS

Advisory

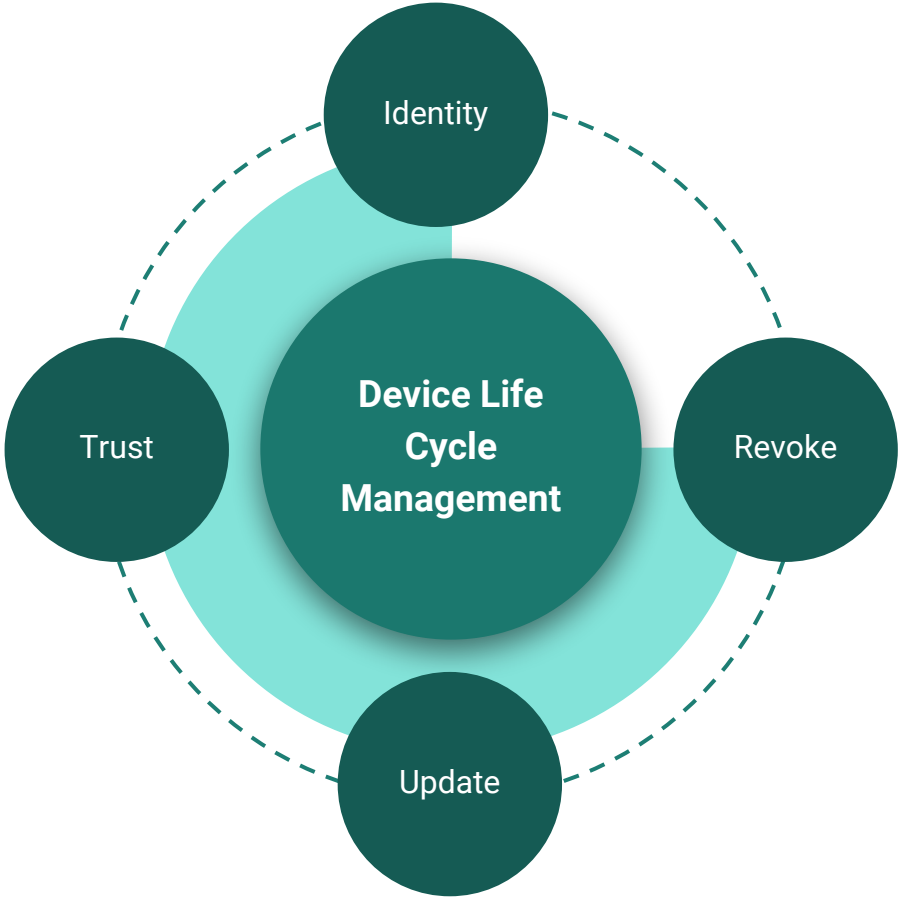
Support for Log aggregation

Support for Endpoint Security

Layering through eco system partners

Device Management

- Registration
- Update
- Authentication



IMPLEMENTING SECURITY

Zero Knowledge Storage

The following techniques are employed for the data at Rest.

1. The actual individual data as provided will remain in encrypted form throughout its lifecycle. Never ever the data is decrypted and stored.
2. The processed data is stored in application encrypted database.
    a. Each column is encrypted with a key
    b. Key:Data
    c. Each row has a HMAC which protects any change in the data.
    d. All keys used for encryption is stored in a special database which is in turn encrypted with a single master key.
    e. Access rights to the key database is monitored and maintained.
3. The copy of the data stored for authentication, ekyc
    a. Each record is digitally signed.
    b. Always stored against a VID as primary key.
    c. Data is encrypted as a single record.
        i. Hash(VID) -> enc(Kid(hash(VID), record) where Kid is the AES key for a given VID.
        ii. Kid is derived from a master AES key in the HSM.

Device Trust

- Every device used within the MOSIP ecosystem to collect biometrics will be a trusted and registered device.
- The device has a trust module certified by the vendor for MOSIP.
  - Secure boot
  - Safe key storage
  - Downgrade protection
- The trusted keys are derived from the Centralized MOSIP CA.
- Every data from the device is digitally signed.
- Centralised device repository to revoke a device or a OEM.
- Ability to cryptographically validate a device from anywhere.

Audit Records

Every request and response is stored in the audit records

Chained with Merkel tree to ensure no record deletion

Transparent access.

Out of the Box

Trust levels are auto associated out of the box for the system.

Encryption is deployed by default with auto key generation.

OTP key generation and seeding is based on the the request.

Certificate Authority configuration and issuance upon first run with auto renewal

Digital Signature for all API response

Default key rotation policies.

Database encryption.

Log aggregation framework support

Extending Security Measures

Trust level for new softwares and integration.

Support for higher key size

Common authentication support

OPERATIONS

Handling Vulnerabilities and Threats

- Default Prioritized Assets (Dockers)
- Official vulnerability reporting by researchers
- Threats modeled with DREAD and rated with STRIDE
- DevSecOps scan for dependency, SAST & container (OpenSCAP) vulnerability on every build.
- Official Security advisory publications
- Recommended Security Policy handbook
- Vulnerability scan
    - Monthly once internal scan
    - Every day external scan
- Update notification
- Active bounty programs

Threat Management Center

- A basic log aggregation is built in.
  - Logs are automatically shipped to a central syslog server .
- Advanced users can integrate Metron, Graffna or any other commercial tools of their need.
- Security analytics, Threat hunting, SOC is part of the Apache Metron - Should we worry about this or will this be part of the SI?

Audit Framework

Platform - IV&V Process

Deployment - Audit and Validation against Guidelines

Operations Excellence - Periodic Audit, Self Managed