Safeguarding Identity Data

Strategies for Ensuring Security and Privacy

Sasikumar Ganesan | Head of Engineering – MOSIP

01 Security Principles
Security Principles that drive MOSIP's Design

02 Threat Landscape Matrix
A matrix of threats and how MOSIP deals with it

03 Secure By Design
Security design choices

04 Security Beyond MOSIP
What should I do for security beyond what MOSIP offers?

Principles

- Keep it Simple
- Trust but Verify
- Reduce Attack Surface Area
- Fail Securely
- Defence in Depth

Keep it Simple

- Mass usage of digital systems need to have simple easy to use ID. An ID that lets the user feel comfortable and reduces the learning curve and reduces the attackers choice

- Biometric with revocable ID
- Mobile based authentication

- Ready to use Infrastructure as a code pre-built with zero trust

- Simple database administration with guaranteed data integrity and confidentiality

- Automatic key management

Trust
but Verify

- **Built over Zero Trust Architecture with Trust but Verify at:**
  - Microservices
  - Third Party access
  - User access

- **Seamless support for TPM built in to services and onboarding process**
  - Biometric devices
  - Registration client
  - HSM

- **Upgrades built over signed artifacts preventing untrusted execution**

- **Built in customisable AV to verify incoming data**

Reduce
Attack Surface

- **Segregation of Services:** MOSIP micro services are segregated to reduce attack surface and increase efficiency.
- **Segregation of Administration:** Role based segregation of users
- **Isolation through Policies:** All data transfer between the identity system and parties are governed through machine readable policies
- Very **few services** are exposed outside of the network

Fail Securely

An attack could originate anywhere within the system. Typically, we could classify the attacker as:

1. Internal
2. External

Internal

- Access to data, system and configuration are clearly segregated That no one admin would have access to all this information.
- Configurations are version controlled
- Data integrity protected against tamper and swap.

External

- Errors are handled at global level to reduce any possible leakage.
- Ingress deployed to stop propagation of errors
- Segregation of namespaces to limit the and contain any failure.

Defence
in Depth

App:
Authentication,
Authorisation,
Availability

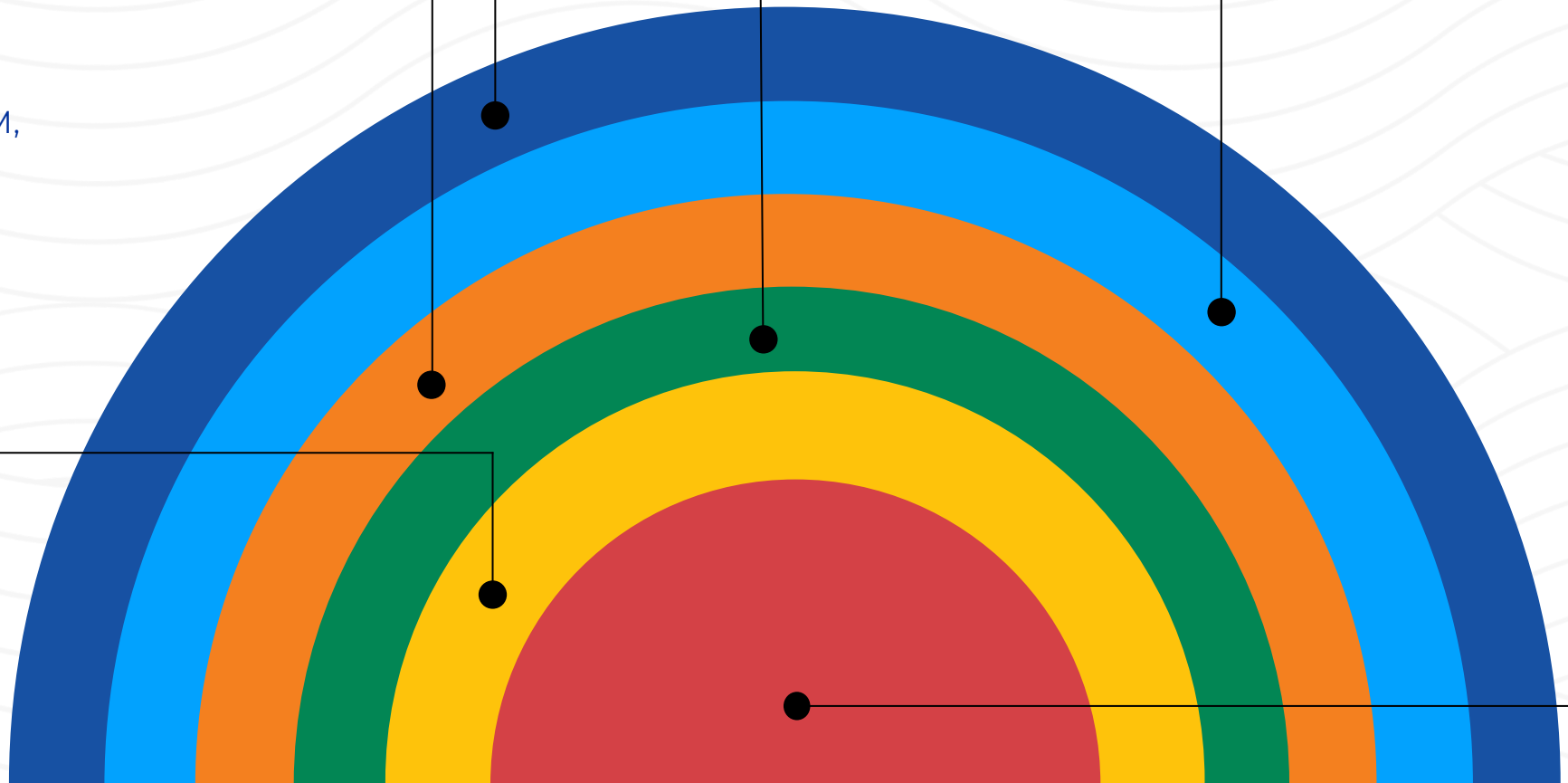
Perimeter:
Firewall,
Intrusion,
Wireguard

People:
Onboarding,
Segregation of
Duties, Roles

Zone:
Segregation
and layering of
microservices

Machine:
Onboarding,
Identity & TPM,
Notary

Data:
Database,
Integrity,
Encryption,
Signing, Silo



Threat Landscape

- Good Protection
- Average Protection
- No Protection

31% Ransomware

21% DDos

2% Zero Day

20% Data

3% Web Threat

4.8% Information Manipulation

2% Suppy Chain

8.2% Malware

7.9% Social Engineering

Secure
By Design

01
Improved Trust

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

02
Mutually-Trusted Partners

Third-party interaction built over mutually trusted channel. All events are auditable and non-repudiable.

03
Trust, But Verify

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

04
Data Protection

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

Security
Beyond MOSIP

Identify & Predict

- List
- Monitor
- Governance
- Risk Management

Prevent & Detect

- Awareness & Training
- Deploy defensive tools
- Access Control
- Process & Procedure

Respond

- Incident Response
- Plan for Disaster
- Planning
- Improve

Recover

- Backup
- Business Continuity
- Segregate
- Communications

MOSIP

MOSIP Homepage: www.mosip.io

MOSIP Source Code: github.com/mosip

MOSIP Documentation: docs.mosip.io

MOSIP Community: community.mosip.io