



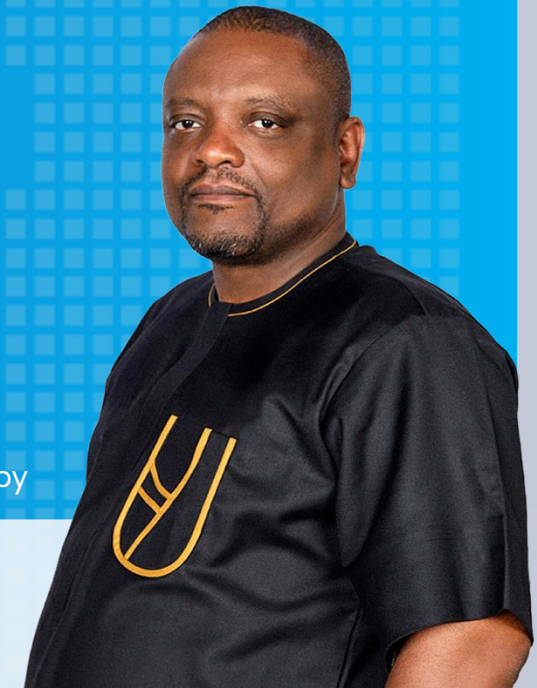
Securing National Identity Systems

Lessons from Real Implementation

A Presentation by

George Williams

Ag. Chief IT Infrastructure of
Margins ID Group



A Layered Security Model

Security controls mapped across the OSI stack

| | | |
|------|-------------------------------|---|
| L7 | Application | Credential issuance systems Access controls Application hardening |
| L5-6 | Session / Presentation | Biometric template protection Encryption protocols Format standards |
| L4 | Transport | TLS channels API security gateways Mutual authentication |
| L3 | Network | Segmentation Firewalls Intrusion detection systems APN SIM whitelisting |
| L2 | Data Link | Secure enrollment station connectivity MAC filtering |
| L1 | Physical | Enrollment center hardening Biometric device tamper protection |

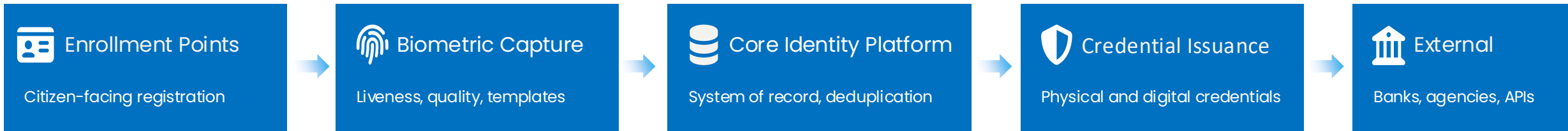
Key principle: No single layer provides complete protection. Security emerges from the interaction of controls across all layers – tested and validated under operational conditions.

REFERENCE ARCHITECTURE

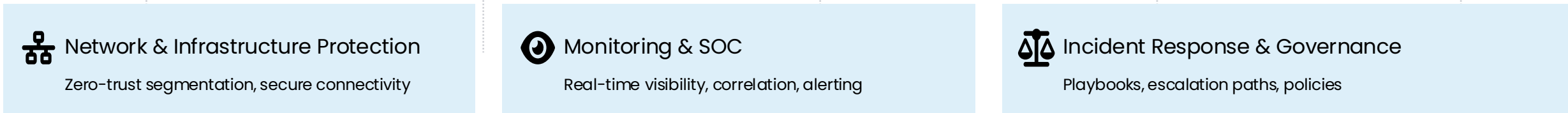
National Identity Ecosystem

Field-tested security and operational components

FUNCTIONAL LAYER



SECURITY



Architecture reflects field-tested deployment patterns – not theoretical design.

Biometric Enrollment Under Constraints

Remote stations, no connectivity, high-volume deadlines

CHALLENGE

Biometric data captured and stored locally before sync to core platform, creating a vulnerability window at remote stations with limited physical security.

RISK

Device tampering, local data exposure, and man-in-the-middle attacks during transmission to the central platform.

TRADE-OFF

Real-time online validation was most secure but infeasible given network conditions; offline capability was essential for inclusion but introduced security gaps.

SOLUTION

Edge-hardened enrollment kits, encrypted local storage, sync with integrity verification, biometric deduplication.

LESSON

Security must adapt to operational reality. Harden offline capability and build compensating controls matched to the actual threat model and constraints.

What Proves Effective in the Field

Operational insights across five critical domains

Architecture Decisions

- Zero-trust segmentation between identity subsystems
- API gateways with mutual TLS at every integration point
- Immutable audit logging from capture to credential issuance

Biometric Security

- Liveness detection at the capture point
- Template encryption
- Biometric authentication for operators
- Supervised biometric capture to prevent injection of morphs

Credential Issuance

- Secure printing with cryptographic verification
- PKI-backed digital credentials with real-time revocation

Incident Response

- Pre-defined playbooks for identity-specific scenarios
- Cross-agency communication protocols established pre-incident

Institutional Coordination

- Clear RACI matrices for security decisions
- Shared threat intelligence and regular joint assessments

Key insight: Technical controls alone are insufficient. Institutional coordination determines whether security architecture translates into operational reality.

Moving Forward

Implementation Priorities

01

Harden the Foundations

Infrastructure protection and monitoring must be in place before scale.

02

Secure the Citizen Journey

From enrollment through credential lifecycle - every touchpoint is an attack surface.

03

Build Institutional Resilience

Coordination, response capability, and continuous assessment separate secure design from secure reality.

The most secure identity system balances

technical rigor

with

operational practicality.

That balance is only achievable through sustained collaboration between implementers, institutions, and oversight bodies.

Thank You

Scan to visit our website



 5th Floor, The Octagon,
Accra - Ghana.
info@marginsgroup.com

 +233 (0) 0308251212

 info@marginsgroup.com

 info@marginsgroup.com