LESOTHO COMMUNICATIONS AUTHORITY

ITU DFS SECURITY WEBINAR SERIES · EPISODE 10

Operationalizing a Joint DFS Security Lab

Insights from the Kingdom of Lesotho

Navigating Inter-Regulatory Collaboration, Technical Baselines, and Ecosystem Trust

Mr. Tumane Mahloane

Cybersecurity & Ls ComCSIRT Manager · Lesotho Communications Authority · 28 May 2026

LESOTHO COMMUNICATIONS AUTHORITY

Overview

01 Foundation & Collaboration

The inter-regulatory partnership and institutional setup behind the Lab

02 Challenges in Implementation

The practical hurdles encountered in standing up the Lab

03 A Mature Engagement Model

Shifting from isolated testing to inclusive, collaborative assessment

04 Technical Baseline & Assessments

Testing scope and a summary of the five app evaluations

05 Common Weaknesses & Maturity

Common technical weaknesses and the fields where providers are strong

06 Takeaways & Recommendations

Key lessons and recommendations for regulators and DFS Providers

The Foundation: Evolution & Timeline

The lab rests on a deliberate partnership between Lesotho's telecom and financial regulators — built to secure the national digital-payments ecosystem.

Strategic Partnership| Joint Inter-Regulatory Team:

- Built upon a long-standing MOU between LCA and CBL.
- The DFS Security Lab has transitioned into a fully operated team of specialized engineers from both institutions

The Lab Journey | Milestones to Operation:

- Followed a rigorous runway from early ITU DFS Clinics to infrastructure setup (April–October 2025).
- The lab formally went live in December 2025 with an initial baseline phase led by LCA engineers following ITU technical handover

The Policy Runway | ENACTING THE GUIDELINES:

- In parallel, a cross-agency track adapted global ITU recommendations into domestic DFS Security Guidelines
- Following industry consultation, the framework was officially approved and enacted in May 2026

Challenges in Lab Implementation

1 Operational Sequencing

Early baseline assessments were executed while the **DFS Security Guidelines** were still undergoing development => Operating the lab without statutory legal framework

2 Mismatched Notification Philosophies

Regulator 1: favoured rapid testing to quickly establish national baseline risk metrics vs Regulator 2: Prioritized advance provider notification to maintain institutional trust

3 Admin Approval Bottlenecks

Differing institutional structures resulted in mismatched speeds regarding internal operational approvals

4 Single-Agency Data Ownership

Siloed Testing: Initially Apps evaluations were executed by a single technical team => Delayed shared institutional ownership of the findings

Shifting to a Mature Engagement Model

THE COLLABORATIVE PIVOT

Pre-notification › **Joint Testing & Reporting** › **Shared Triage**

Synchronized Testing Schedules: The formal approval of the DFS Security Guidelines established a transparent legal anchor => Overlapping workflows were eliminated, the testing is done under official regulatory framework

Unified Testing Calendar: The Regulators now operate under a shared standard operational timelines => Baseline requirements are balanced with advanced notifications => Preserves industry trust

Cultural Tolerance & Acceptance: Embracing that the two regulators operate under fundamentally different organizational cultures and paces. cultures and structures => Mutual operational acceptance, respect and tolerance

Integrated Technical Execution: The testing workflows transitioned from single-agency to fully integrated cross-regulatory engineering teams => Complete ownership of data Findings

Technical Baseline: Summary of App Assessments

Testing Scope: Evaluation based on:

- ITU-T X.1150 Security Assurance Framework and
- the OWASP Mobile Top 10.

Ecosystem View: Five (5) comprehensive evaluations completed across Android and iOS deployments.

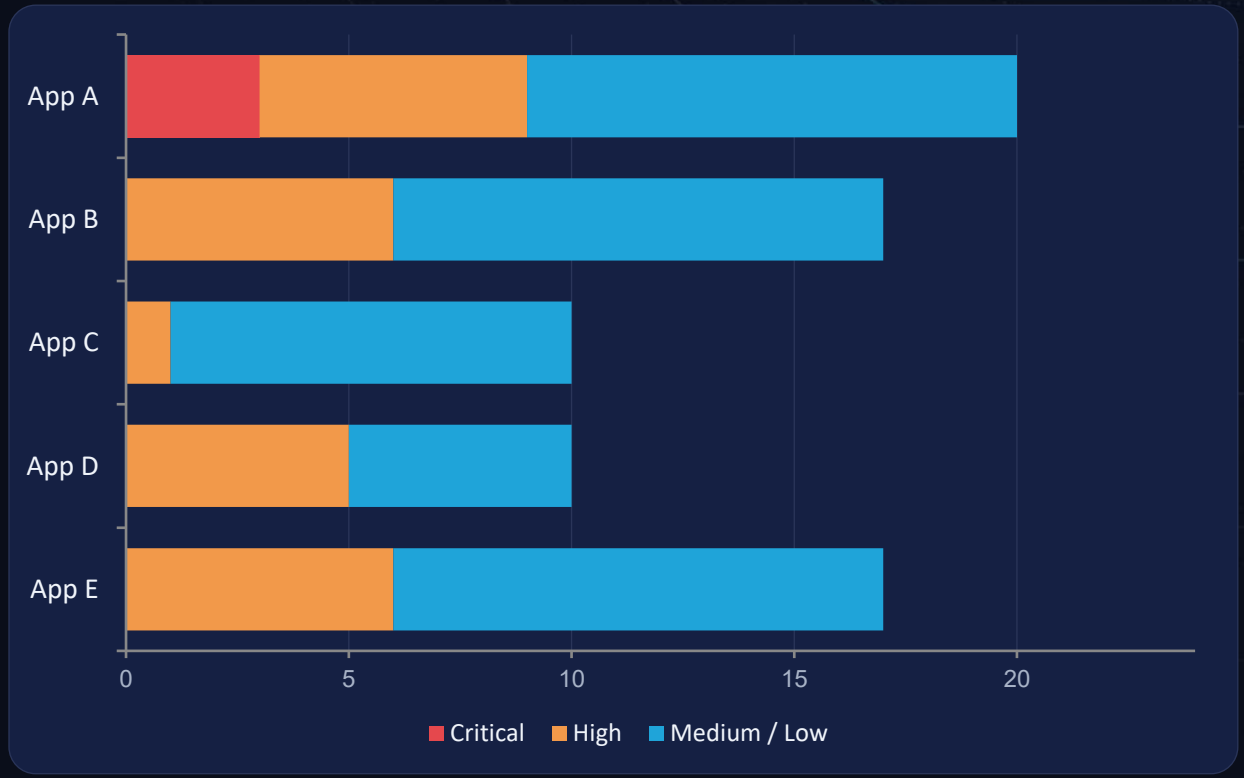
5
Apps assessed
4 Android · 1 iOS

74
Total findings
Across all Apps

3
Critical
in one App

24
High-severity
Across the portfolio

VULNERABILITY SEVERITY BY APPLICATION



Technical Baseline: Per-App Detail

APPLICATION	PLATFORM	FINDINGS	MOST SIGNIFICANT CRITICAL / HIGH FINDINGS
App A	Android	**20** 3 Crit · 6 High	Cleartext HTTP traffic, no certificate pinning, biometric bypass
App B	Android	**17** 0 Crit · 6 High	Weak server TLS (C grade) and no certificate pinning so any accepted certificate is trusted
App C	iOS	**10** 0 Crit · 1 High	Core framework is 7 years out of date, with no binary integrity checks to detect if the app has been tampered with.
App D	Android	**10** 0 Crit · 5 High	Legacy TLS 1.0/1.1 allowed, hardcoded encrypted keys, excessive app permissions
App E	Android	**17** 0 Crit · 6 High	Sensitive functionality accessible without re-authentication after idling, broken runtime integrity checks, and missing APK Signature Scheme v4 protection.

Common Vulnerabilities & Technical Trends

M5 Network & Communication Gaps

- No certificate pinning, so apps trust whatever certificate the device accepts — easy for an attacker to intercept traffic.
- Some traffic still falls back to plain HTTP, and backend servers run old, weak TLS settings.

M7 Binary Protection Failures

- Weak or no runtime checks — the app does not detect when it is being tampered with at execution time.
- Apps still run on rooted, jailbroken, or emulated devices, and the code is not obfuscated — making reverse engineering easy.

M9 Insecure Data Storage & Lifecycle

- Wallet balances and transaction history get captured in the app-switcher preview image.
- Sensitive data is also written to local files in plain text on the device.

M10 Cryptographic Flaws

- Use of outdated, broken hash algorithms (MD5 / SHA-1) that are no longer safe.
- API keys and encryption secrets hardcoded inside the app package, where anyone can extract them.

The Positive Baseline: Fields of Maturity

It's not all gaps — providers show consistent strength in several important areas.

✓ Production Configurations

- Production builds are shipped non-debuggable (android:debuggable="false"), so attackers cannot attach a debugger.

✓ Logging Discipline

- No personal data, wallet codes, or secret keys leak into app logs or console output.

✓ Backup Architecture

- App data is protected from simple extraction via command-line backup tools (adb backup).

✓ Intent Control

- App components are not needlessly exposed, so other apps cannot reach internal screens.

Key Takeaways & Recommendations for Regulators

01 Cultivate Cross-Agency Synergy

- **Regulators:** Appreciate and actively design workflows around differing institutional cultures; build clear operational pipelines to ensure both regulators maintain equal ownership
- **Providers:** Welcome joint regulatory testing as a standardized, unified benchmark rather than navigating separate telecom and banking requirements

02 Harmonize Policy Timelines with Technical Pipelines

- **Regulators:** Sync the rollout of active technical capability testing with the formal enactment of guidelines to ensure clear compliance expectations
- **Providers:** View early baseline diagnostic phases as a collaborative runway to harden internal applications

Key Takeaways & Recommendations for Regulators

03 Shift from Rigid Auditor to Security Partner

- **Regulators:** Frame the lab's technical assessments as a free, specialized diagnostic resource for defensive risk reduction not a **punitive stick**.
- **Providers:** Leverage the lab's findings as an open-access, zero-cost penetration testing resource to fortify production builds against real-world threat actors.

04 Benchmark Globally, Expand Locally

- **Regulators:** Continuously benchmark with regional peers to adopt best practices and broaden the lab's testing scope.
- **Providers:** Map corporate security configurations against global standards to foster domestic resilience and support regional digital financial interoperability

CLOSING

Thank you!

Questions & discussion welcome.

FROM AD-HOC TESTING TO A COLLABORATIVE, STATUTORY DFS SECURITY LAB

Lesotho's lab now operates on an enacted legal framework, an inclusive engagement model with providers, and a measurable technical baseline across DFS applications — a replicable model for the region.

Mr. Tumane Mahloane

Cybersecurity Manager · Lesotho Communications Authority

Ls ComCSIRT · Interim National CSIRT of Lesotho

ITU DFS SECURITY WEBINAR SERIES · EPISODE 10 · 28 MAY 2026

In partnership with ITU