

Gap Analysis survey: DFS Security recommendations implementation

Arnold Kibuuka
Project Officer, ITU

June 2025



Objective

The gap analysis survey focused on establishing to what extent Lesotho has implemented the security best practices outlined in the ITU DFS security recommendations

LESOTHO: DFS Security Recommendations adoption status

Based on the gap analysis survey done on:

[MOU between a
Telecommunicatio
ns Regulator and
Central Bank
related to DFS
Security](#)

Adopted November
2023

Mitigating SS7
vulnerabilities

Protection
against DFS SIM
related risks
(ITU-T X.1456)

Mobile
application
security Best
practices

DFS consumer
competency
framework

Gap Analysis survey results: Mitigating SS7 Vulnerabilities

Non-Mandated Security Baselines:

- ✘ Established baseline security measures for telecom services (2G/3G/4G/5G) are **not mandated** for implementation by telecom operators.

User Interface & Transaction Security:

- ✘ USSD PIN masking has **not** been deployed wherever possible.
- ✘ DFS operators have **not** implemented OTPs bidirectionally.

Core Network Security:

- ? Core network traffic security with TLS v1.2 or higher is still **Under Consideration**.

Consumer Awareness & Protection:

- ✘ Users are **not** educated on secure engagement with DFS (risks of rooted devices, public Wi-Fi, unverified applications).
- ✘ Mechanisms for detecting and mitigating social engineering attacks (including MT-USSD and interception of USSD) are **not** in place.

Implication: Key technical and consumer-facing safeguards are missing or not enforced, potentially exposing users and the DFS ecosystem to preventable risks.

Gap Analysis survey results: SIM Swap & Related Risk Mitigation

Despite some foundational rules, significant gaps exist in robustly addressing SIM swap fraud:

MNO-DFS Provider Collaboration:

- ✗ MNOs are **not** mandated to notify DFS providers about swapped, ported, or recycled numbers.

Verification & Authentication Deficiencies:

- ✗ Biometric verification before a SIM swap is **not** broadly enforced (beyond proxy image).
- ✗ Multifactor user validation before a SIM swap is **not** required.
- ✗ MNOs are **not** required to send SIM swap notifications to users and await a positive response before proceeding.

Procedural & Systemic Weaknesses:

- ✗ **No** mandatory holding time prescribed before activating a swapped SIM.
- ✗ Regulations **do** not encourage/require DFS operators to offer opt-out from less secure channels (USSD/STK).

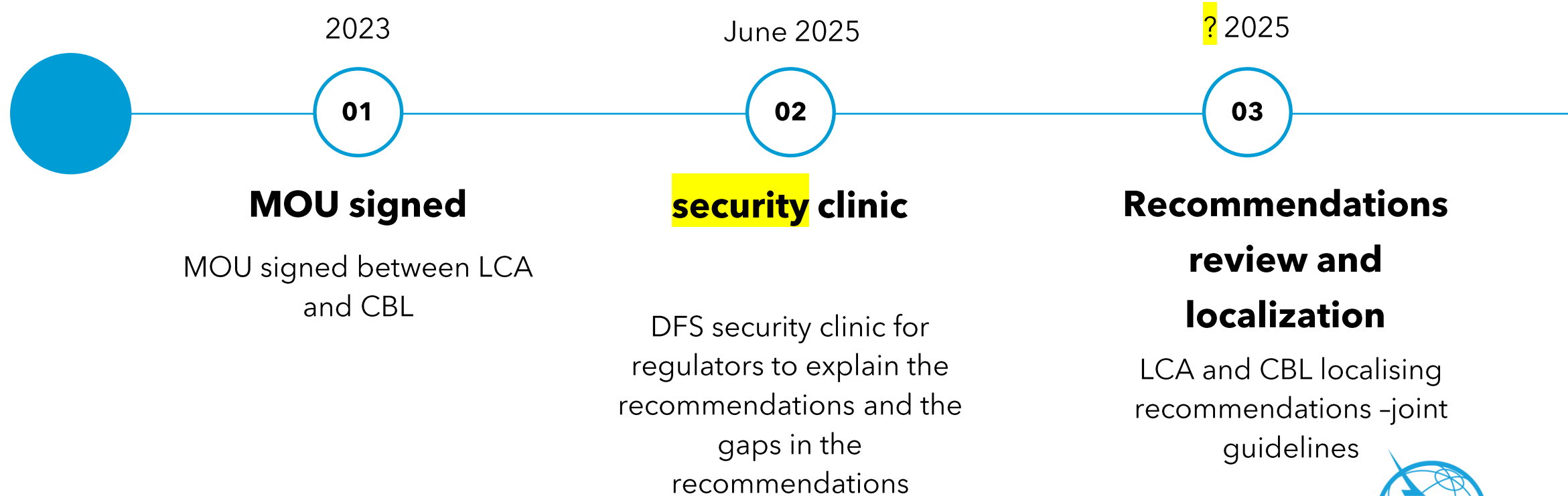
Gap Analysis survey results: DFS Mobile application security Best practices

Current regulations in Lesotho do **NOT** mandate recommended security measures for DFS mobile applications on.

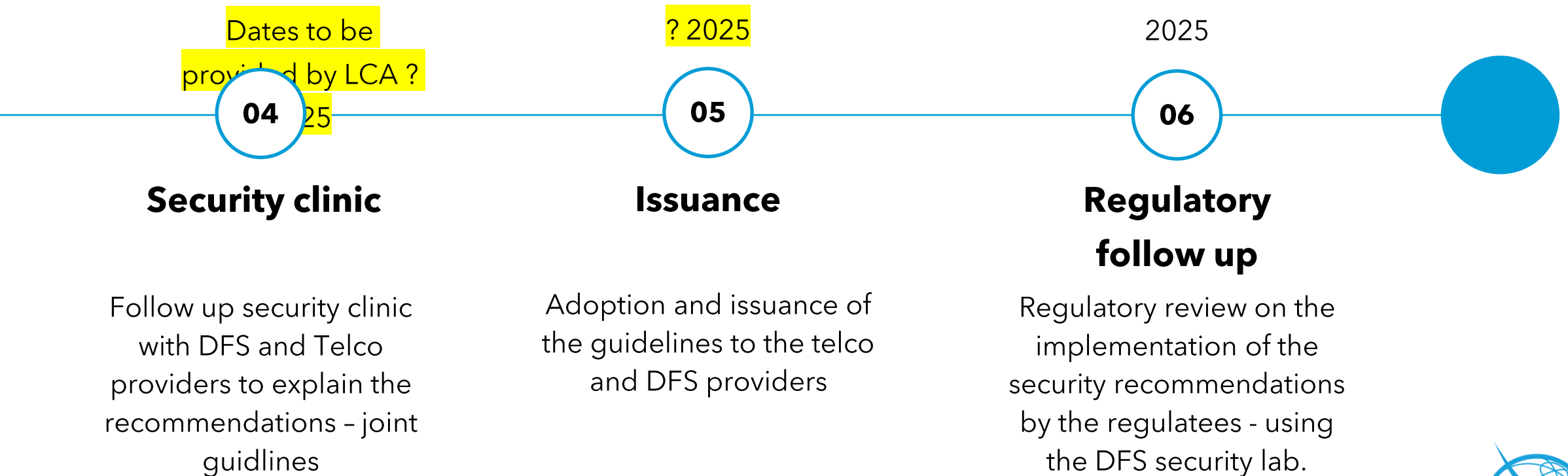
- ✕ Device Integrity & Code Protection:
- ✕ Secure Communication Protocols:
- ✕ Authentication & Credential Management:
- ✕ Data Storage & Handling:
- ✕ Secure Development & Maintenance:

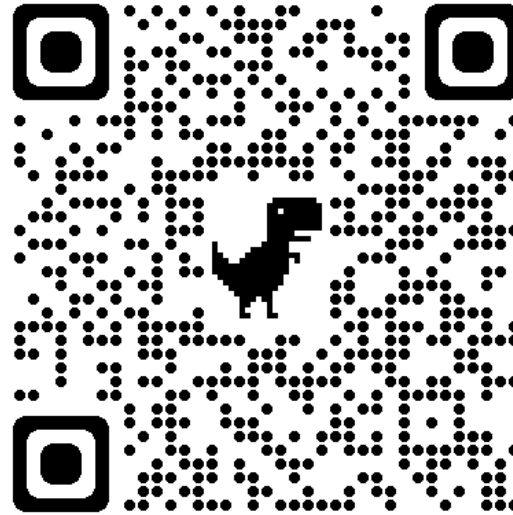
Implication: A critical lack of regulatory oversight for DFS mobile app security, potentially leading to inconsistent and inadequate protection for consumers.

Timeline for DFS security recommendations adoption



Timeline for DFS security recommendations adoption





<http://www.itu.int/go/dfssl>

Contact: dfssecuritylab@itu.int

Thank you!