Digital Financial Services Security Lab

Arnold Kibuuka
Project Officer
Standardization Bureau, ITU

Overview

1. ITU DFS Security recommendations
2. DFS Security Lab
3. USSD, Android and iOS mobile payment app security audit
4. DFS security lab knowledge transfer.
5. Summary and Key take aways

DFS Security Recommendations

Collaborate with DFS regulators and DFS providers to enhance the cybersecurity strategy for DFS and security assurance of the DFS ecosystem **by implementing the recommendations** in:

1. DFS Security Assurance Framework
2. Security testing for USSD and STK based DFS applications
3. Security audit of various DFS applications
4. DFS security audit guideline
5. DFS Consumer Competency Framework

See https://figi.itu.int/figi-resources/working-groups/

DFS Security Recommendations

The DFS Security Recommendations contain the following specific guidelines that may be adopted by regulators

1. Model Memorandum of Understanding between a Telecommunications Regulator and a Central Bank Related to Security for Digital Financial Services

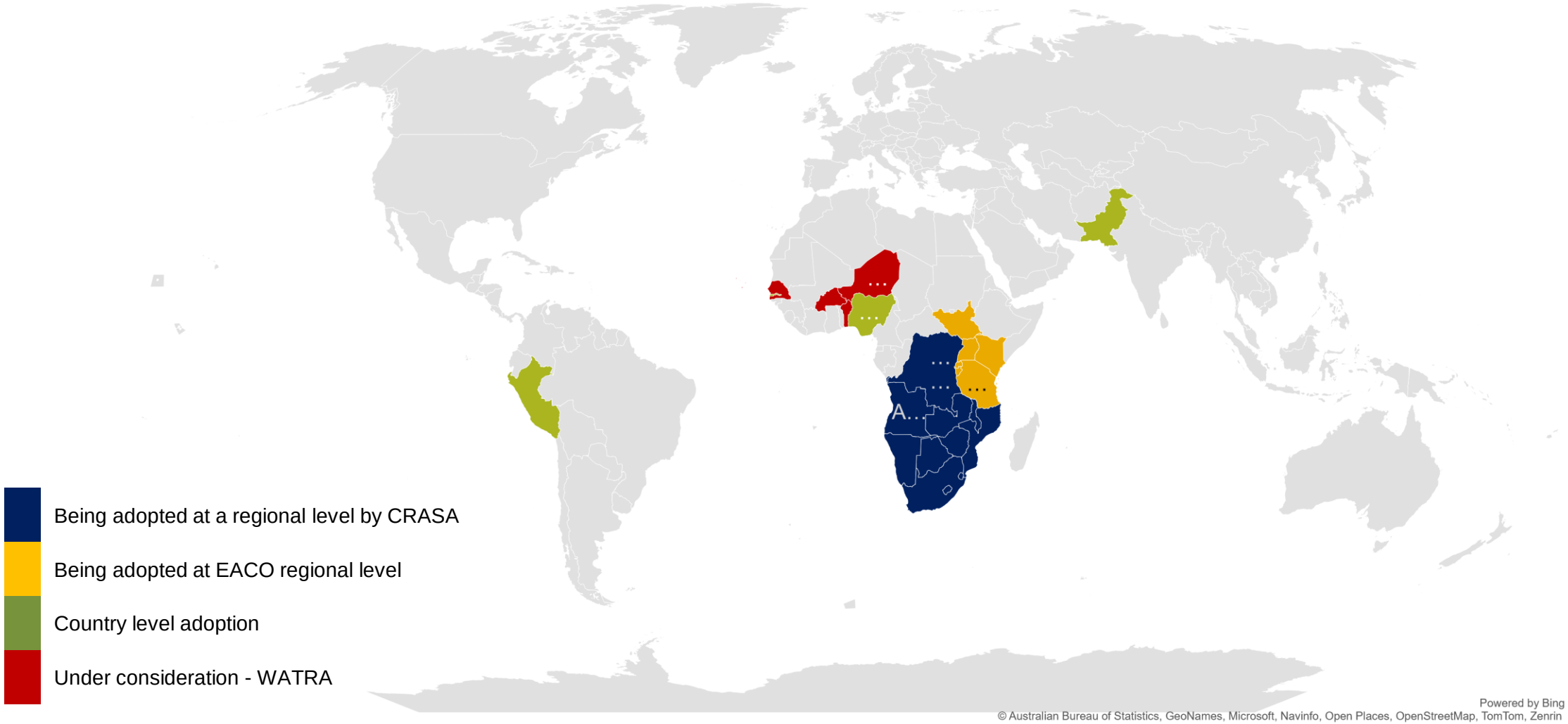
2. Recommendations to mitigate SS7 vulnerabilities

3. Recommendations for securing mobile payment apps

4. Recommendations for operators and regulators for SIM card risks such as SIM swap fraud and SIM card recycling.

See https://figi.itu.int/figi-resources/working-groups/

Countries and Regions adopting the recommendations



Examples: Adoption of the recommendations

Business Rules & Operational Processes for Implementation of the SIM Replacement Guidelines 2022

April 2022

[NCC Sim replacement rules]

[SBP Mobile Application security guidelines]

DFS Security Lab

Provides a standard methodology to conduct security audit for mobile payment apps (USSD, Android and iOS) and address systemic vulnerabilities and verify compliance against security best practices and standards.

Website: https://figi.itu.int/figi-resources/dfs-security-lab/

DFS Security Lab - Objectives

Collaborate with regulators to adopt DFS security recommendations from FIGI

Perform **security audits** of mobile payment apps (USSD, Android and iOS)

Encourage adoption of **international standards on DFS security and participate in ITU-T SG17**

Organise **security clinics & Knowledge transfer** for Security Lab

Assist regulators to **evaluate** the **cyberresilience of DFS critical infrastructure**

Networking platform for regulators for knowledge sharing on threats and vulnerabilities

ITU Knowledge Sharing Platform for Digital Finance Security

Objective

- Collaborate with ITU to keep up to date the DFS security assurance framework security controls and DFS security recommendations.
- Share experiences, challenges, and lessons learned from the implementation of security measures across various jurisdictions.
- Communicate directly with their peers on issues relating to security of digital financial services.

Knowledge Sharing Platform for Digital Finance Security (itu.int)

Security audit for USSD & STK, Android and iOS Mobile Payment apps

USSD and STK

1. **SIM Swap**
2. **SIM cloning**
3. susceptibility to **binary OTA attacks** (SIM jacker, WIB attacks)
4. **man-in-the-middle attacks** on STK based DFS applications
5. **remote USSD** execution attacks

Android and iOS

18 and 21 tests best on the OWASP Mobile Top 10 Risks.

- M1 Improper Platform Usage
- M2 Insecure Data Storage
- M3 Insecure Communication
- M4 Insecure Authentication
- M5 Insufficient Cryptography
- M8 Code Tampering
- M9 Reverse engineering

DFS Security Lab Knowledge Transfer

Phase 1

- Lab team and Equipment in place
- verify equipment is configured
- DFS Security Clinic

Phase 2

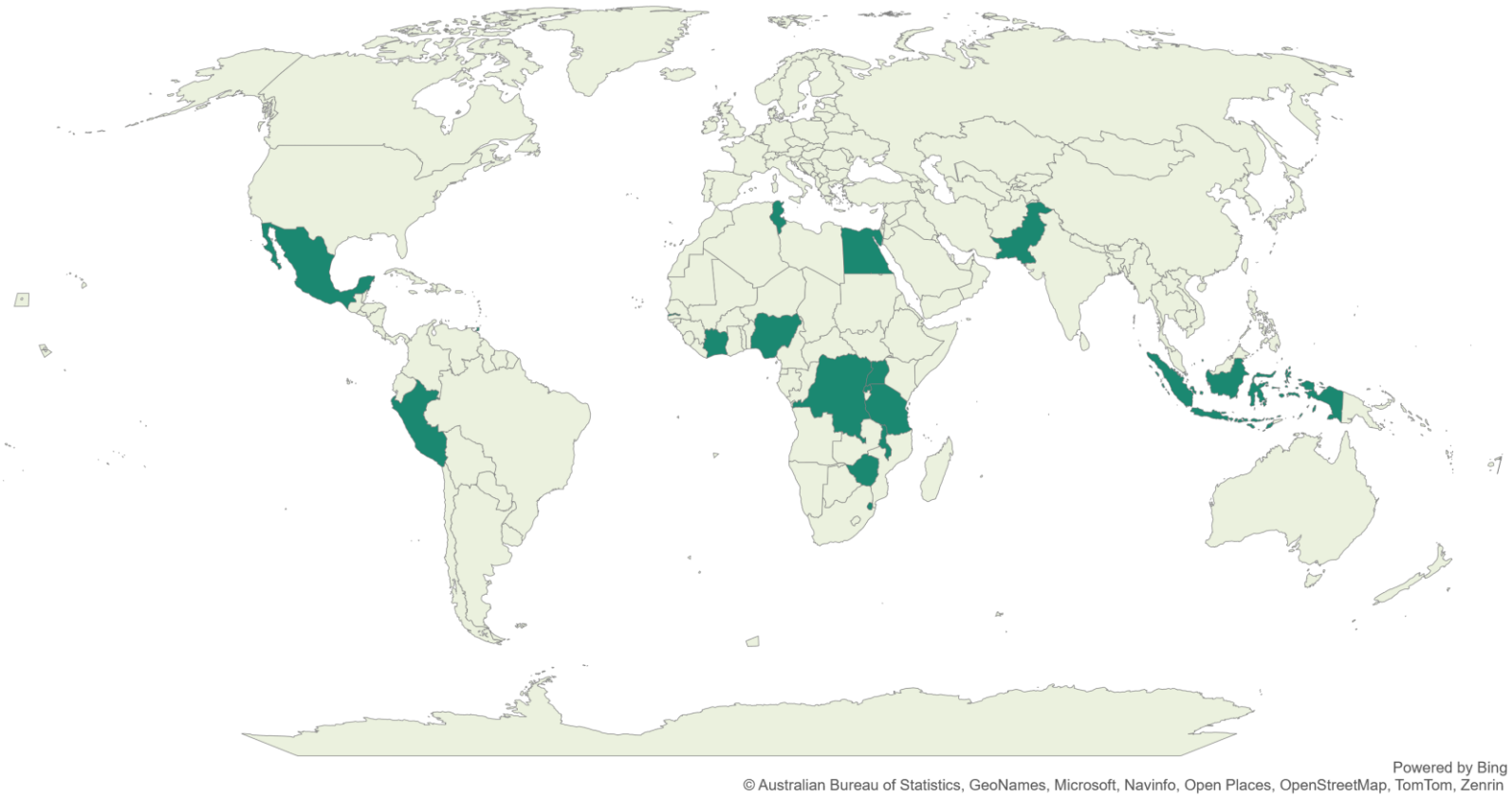
- Select mobile payment app
- Security walkthroughs online workshops

Phase 3

- Organise training on iOS, Android and USSD security testing
- Independent testing by Lab team
- Report on testing done

Phase 4

- 6-9 months period of oversight by ITU
- Mobile payment app testing reviewed by ITU
- Lessons learned of new threats and vulnerabilities



DFS security clinics held in 2021, 2022, 2023

Security Clinics were held in some 21 countries

Summary DFS Security Lab areas of Focus

1. Organizing DFS Security clinics with a focus on knowledge sharing on DFS security recommendations from FIGI
2. Guidance on implementing DFS security recommendations
3. Knowledge transfer for regulators: (setting up of the DFS security lab for Tanzania, Peru and Uganda, The Gambia, Zimbabwe, Rwanda)
4. Conduct security audits of mobile payment applications and SIM cards (Zambia, Zimbabwe, The Gambia, Peru).
5. ITU Knowledge Sharing Platform for Digital Finance Security
6. ITU Cyber Security Resilience Assessment toolkit for DFS Critical Infrastructure

Questions

Contact: dfssecuritylab@itu.int

https://figi.itu.int/figi-resources/dfs-security-lab/