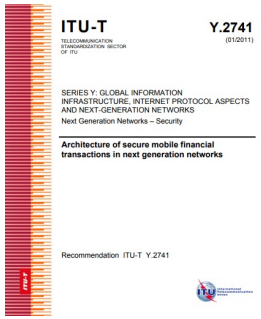
Digital Financial Services Security Lab

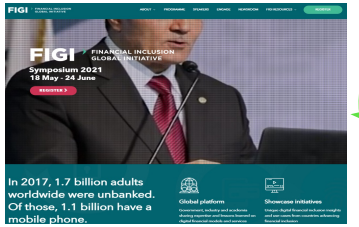
Vijay Mauree
Programme Coordinator
Standardization Bureau, ITU

Overview

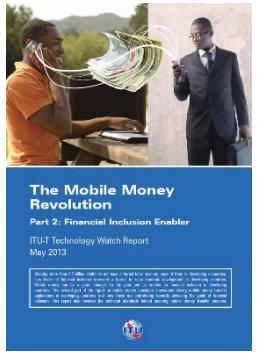
1. ITU & Digital Finance
2. Security challenges
3. DFS Security Lab
4. Security recommendations for digital finance
5. USSD, Android and iOS mobile payment app security audit
6. Setting up the security lab & Knowledge transfer for regulators
7. Actions being implemented

ITU Digital Finance & Inclusion Journey

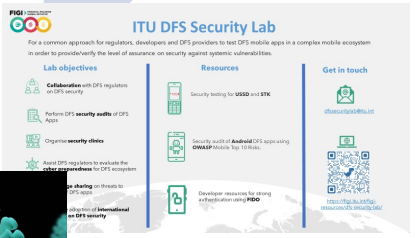




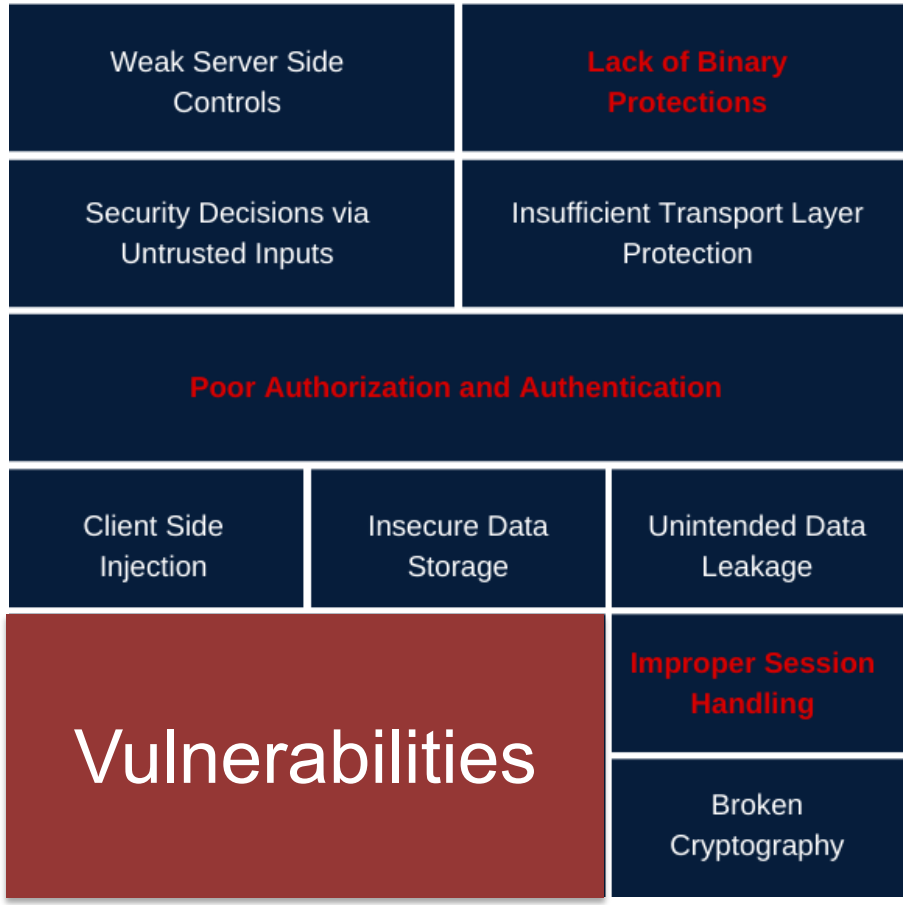
2010-2012 | 2013 | 2014 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022



Tech Watch Report Mobile Money



DFS security challenges for regulators



DFS Security Lab

- Cybersecurity capability of regulators
- Security audit of mobile payment applications
- Adoption of security best practices for digital finance

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

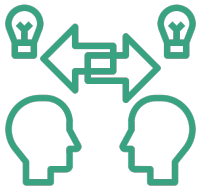
Collaborate with regulators to adopt DFS security recommendations from FIGI

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

Adoption of 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/

Adoption of Security Recommendations

The recommendations contain the following specific guidelines that may be adopted by regulators.

1. Recommendations to mitigate SS7 vulnerabilities

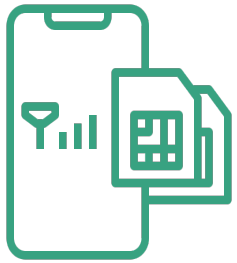
2. Model Memorandum of Understanding between a Telecommunications Regulator and a Central Bank Related to Security for Digital Financial Services

3. Recommendations for securing mobile payment apps

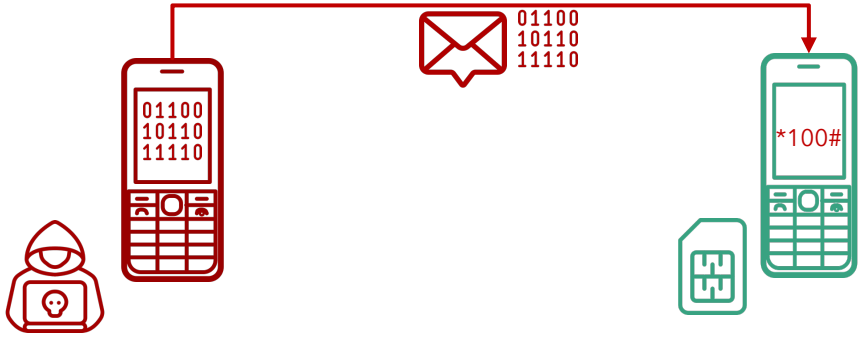
4. Recommendations for operators and regulators for SIM card risks such as SIM swap fraud and SIM card recycling

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

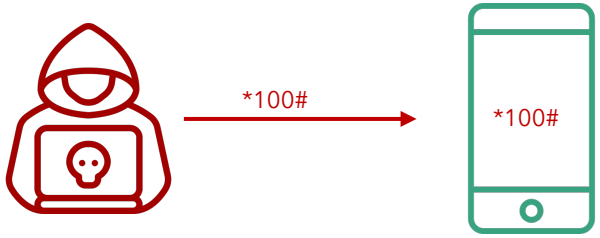
USSD & STK tests



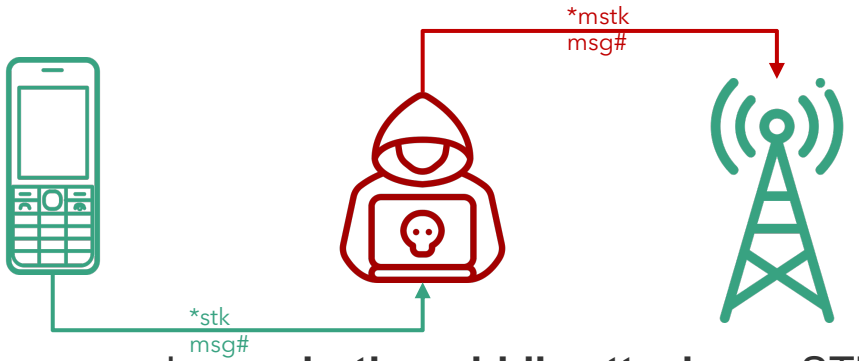
a. **SIM Swap** and **SIM cloning**



b. susceptibility to **binary OTA attacks** (SIM jacker, WIB attacks)



c. **remote USSD** execution attacks



d. **man-in-the-middle attacks** on STK based DFS applications

Android and iOS app security tests

Risks	Security test
M1 Improper Platform Usage	Check misuse of platform features or failing to use platform security controls provided
M2 Insecure Data Storage	Check that malware and other apps do not have access to DFS sensitive information
M3 Insecure Communication	Check that communication channels are encrypted
M4 Insecure Authentication	Authentication cannot easily be bypassed
M5 Insufficient Cryptography	Check crypto algorithms used
M8 Code Tampering	Check whether it is possible to modify the code
M9 Reverse engineering	Decompile source code

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

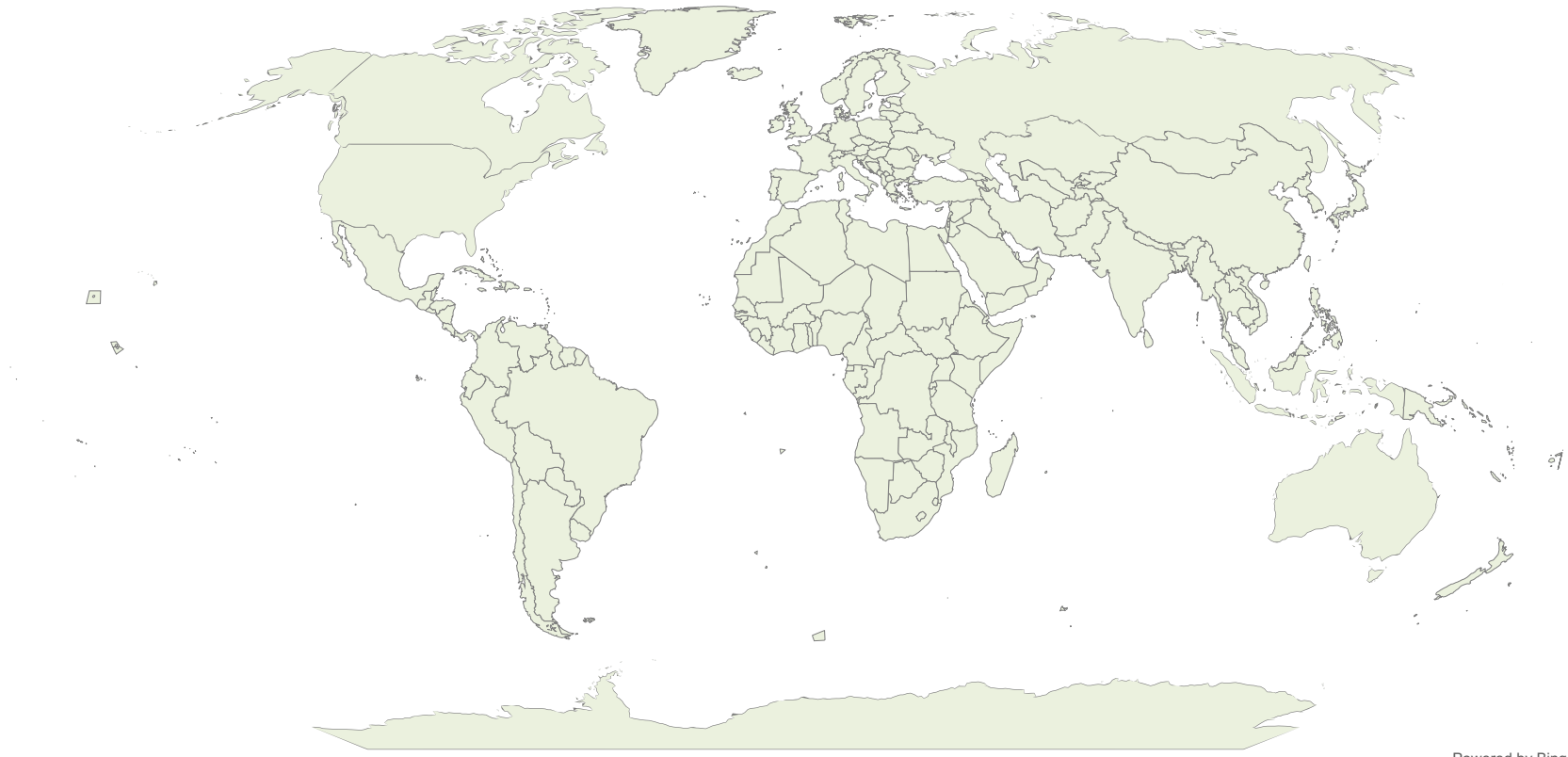
- Organise training on iOS, Android and USSD security testing
- Independent testing by Lab team
- Report on testing done

Phase 4

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

Actions being implemented

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



DFS security clinics held in 2021, 2022, 2023

Security Clinics were held in some 18 countries

Countries and Regions adopting the recommendations

Examples: Adoption of the recommendations

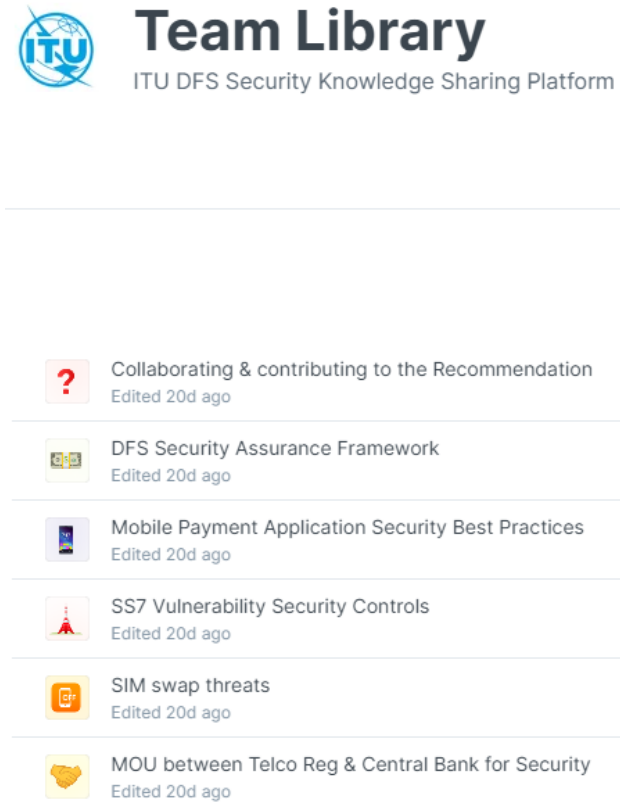
Business Rules & Operational Processes for Implementation of the SIM Replacement Guidelines 2022

April 2022

[NCC Sim replacement rules]

[SBP Mobile Application security guidelines]

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)]

ITU Knowledge Sharing Platform for Digital Finance Security

The collaboration tools

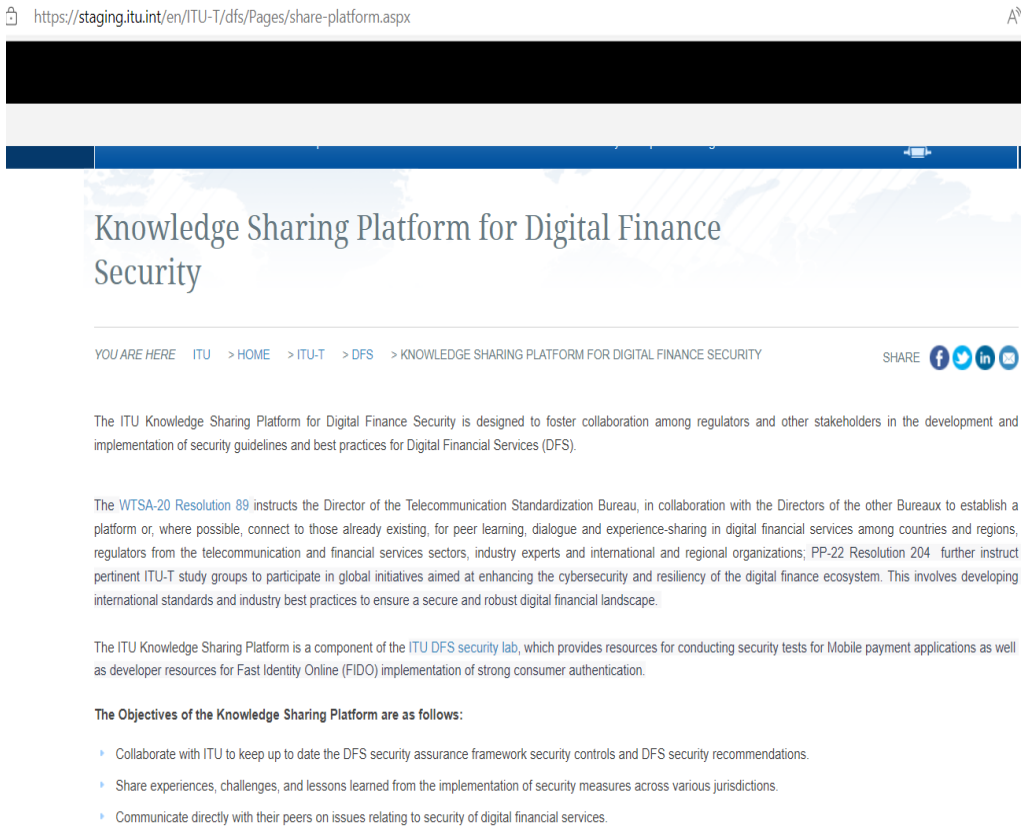
slack

discussions amongst members

GitBook

Manages agreed changes and comments

Visit website to find more on how to join:
[Knowledge Sharing Platform for Digital Finance Security (itu.int)]



ITU Cyber Security Resilience Assessment toolkit for DFS Critical Infrastructures

Objectives

1. **Facilitate Cyber Resilience Self-Assessments:** To empower DFS entities, users, and actors to proactively assess their existing security protocols and identify potential vulnerabilities.
2. **Enhance DFS Infrastructure Resiliency:** Reinforce both peripheral and internal defences of the DFS infrastructure, bolstering resistance against potential cyber threats.
3. **Provide Stakeholder Education:** Equip stakeholders from various sectors within the DFS ecosystem, including telecommunications and finance, with the knowledge to prepare for and defend against malicious cyber operations and unauthorized access attempts.
4. **Establish Best Practices:** Encourage the adoption and implementation of effective cyber defence practices tailored to each DFS entity's unique needs

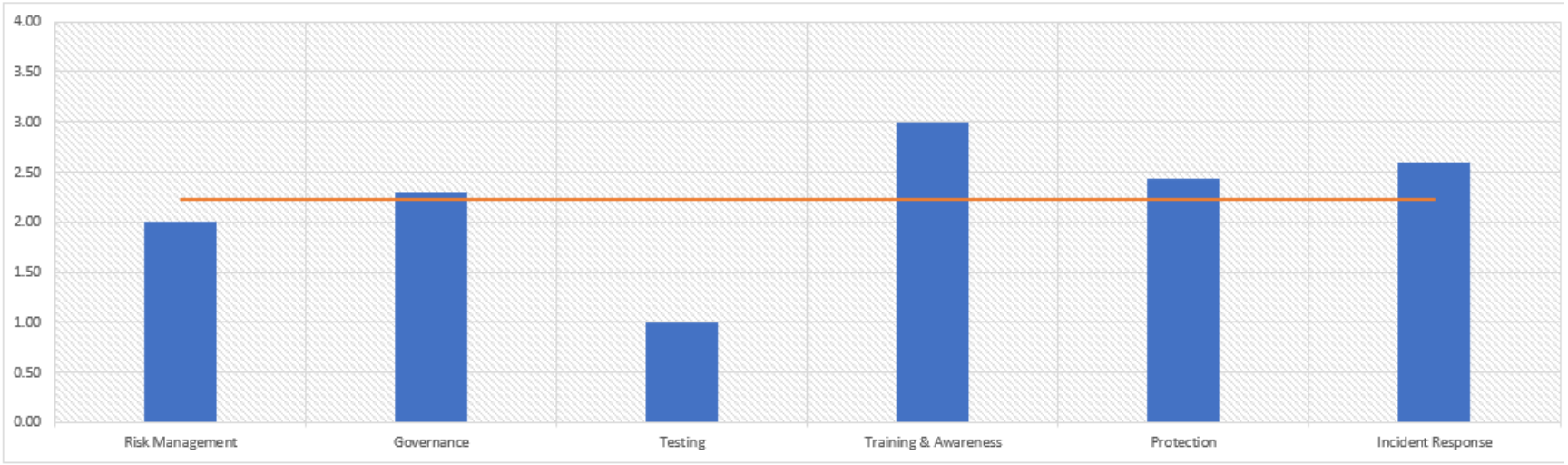
Results assessment summary: Cyber Security Resilience Assessment toolkit

Results Summary

This section provides an overview of the results and lays the foundation for a mitigation roadmap to be identified, structured, and presented to the decision-maker. All results presented here aggregate the sub-pillars of each methodological question. For a more granu results, the user is advised to review the results in the radar charts section.

Pillar	Resiliency Level
Risk Management	2.00
Governance	2.30
Testing	1.00
Training & Awareness	3.00
Protection	2.44
Incident Response	2.60

Overall score	2.22



Questions

Contact: dfssecuritylab@itu.int

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