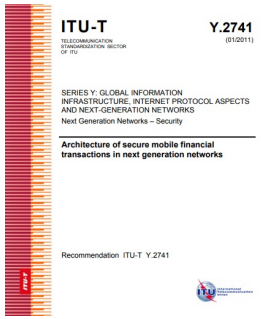
# Digital Financial Services Security Lab

Vijay Mauree
Programme Coordinator
Standardization Bureau, ITU

# Overview

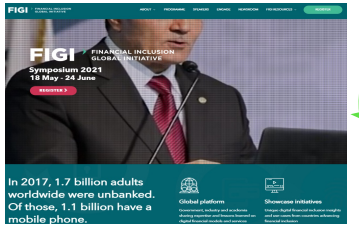
1. ITU & Digital Finance
2. DFS Security Lab
3. Security recommendations for digital finance
4. Knowledge transfer for regulators
5. Actions being implemented

# ITU Digital Finance & Inclusion Journey



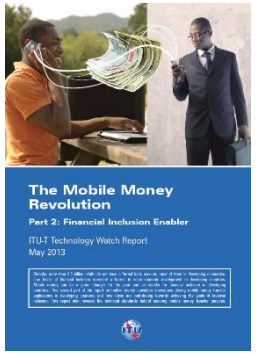






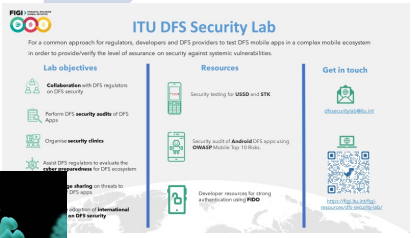


2010-2012 | 2013 | 2014 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022

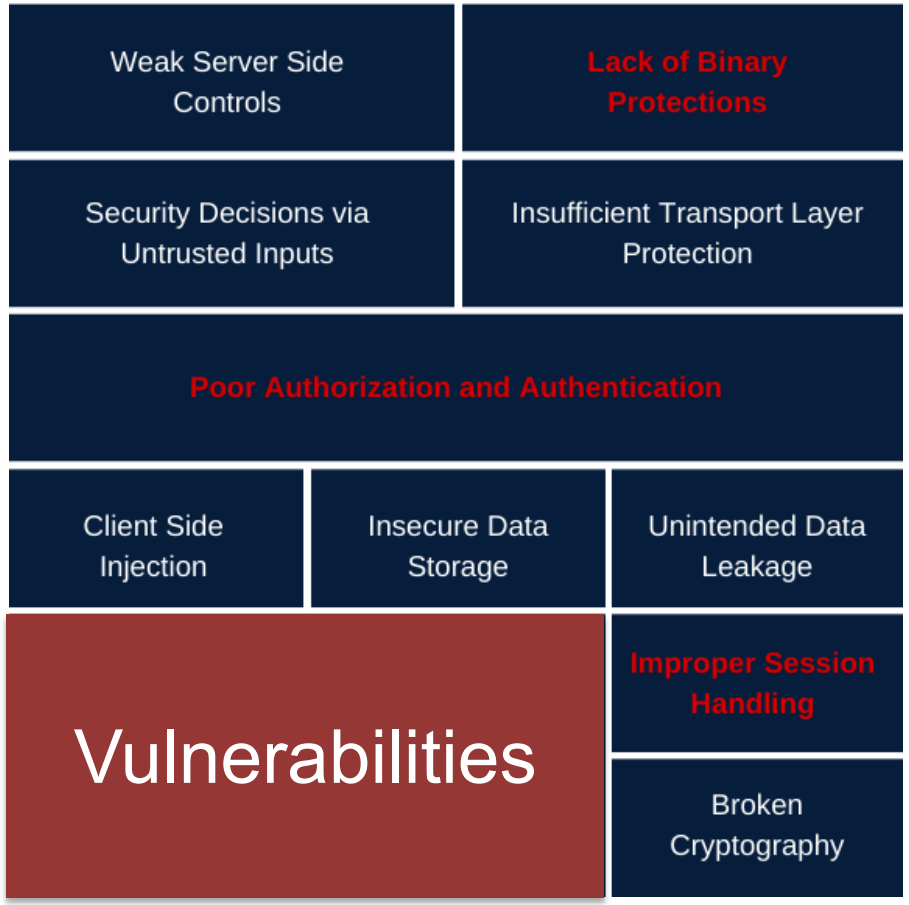



Tech Watch Report Mobile Money



# 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

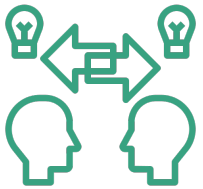
**Collaborate** with regulators to adopt DFS security recommendations from FIGI

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:

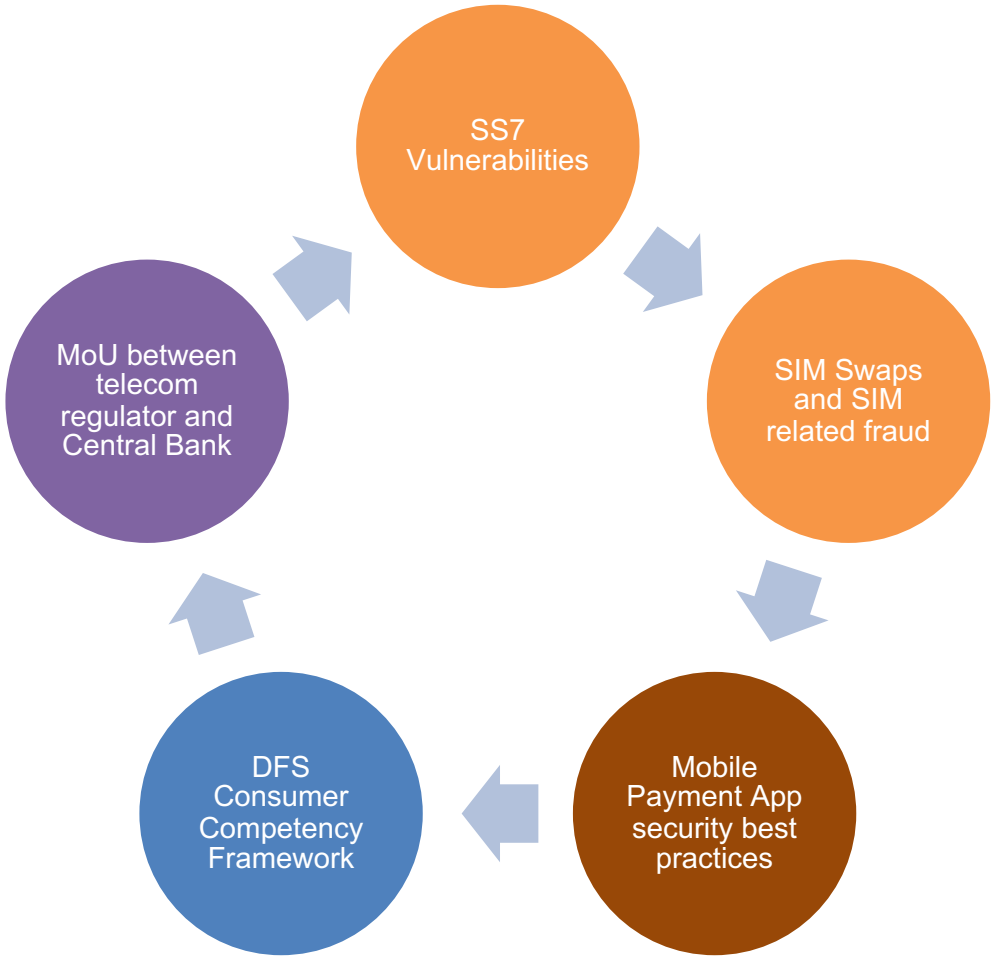
1. DFS Security Assurance  Framework
2. Security testing for USSD and STK based DFS applications
3. Security audit of various DFS applications
4. SS7 Vulnerabilities and mitigation measures for DFS
5. DFS security audit guideline
6. DFS Consumer Competency Framework


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

# DFS Security Recommendations

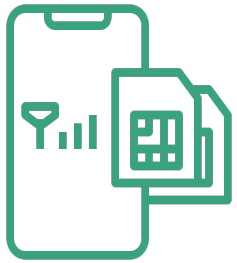
The recommendations contain the following specific guidelines that may be adopted by regulators.

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 (Mobile Payment Apps security best practices)
4. DFS Consumer Competency Framework
5. Recommendations for operators and regulators for SIM card risks such as SIM swap fraud and SIM card recycling

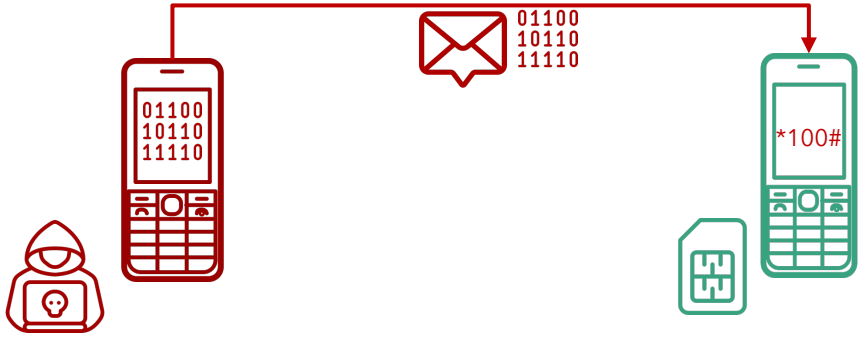



See https://www.itu.int/en/ITU-T/dfs/PublishingImages/Pages/default/DFS_security_recommendations.pdf

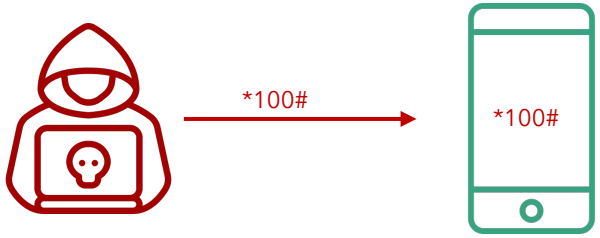
# USSD & STK tests



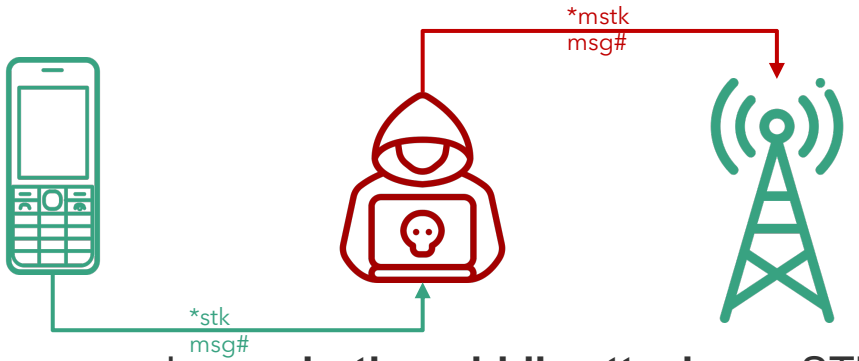
a. **SIM Swap** and **SIM cloning**




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

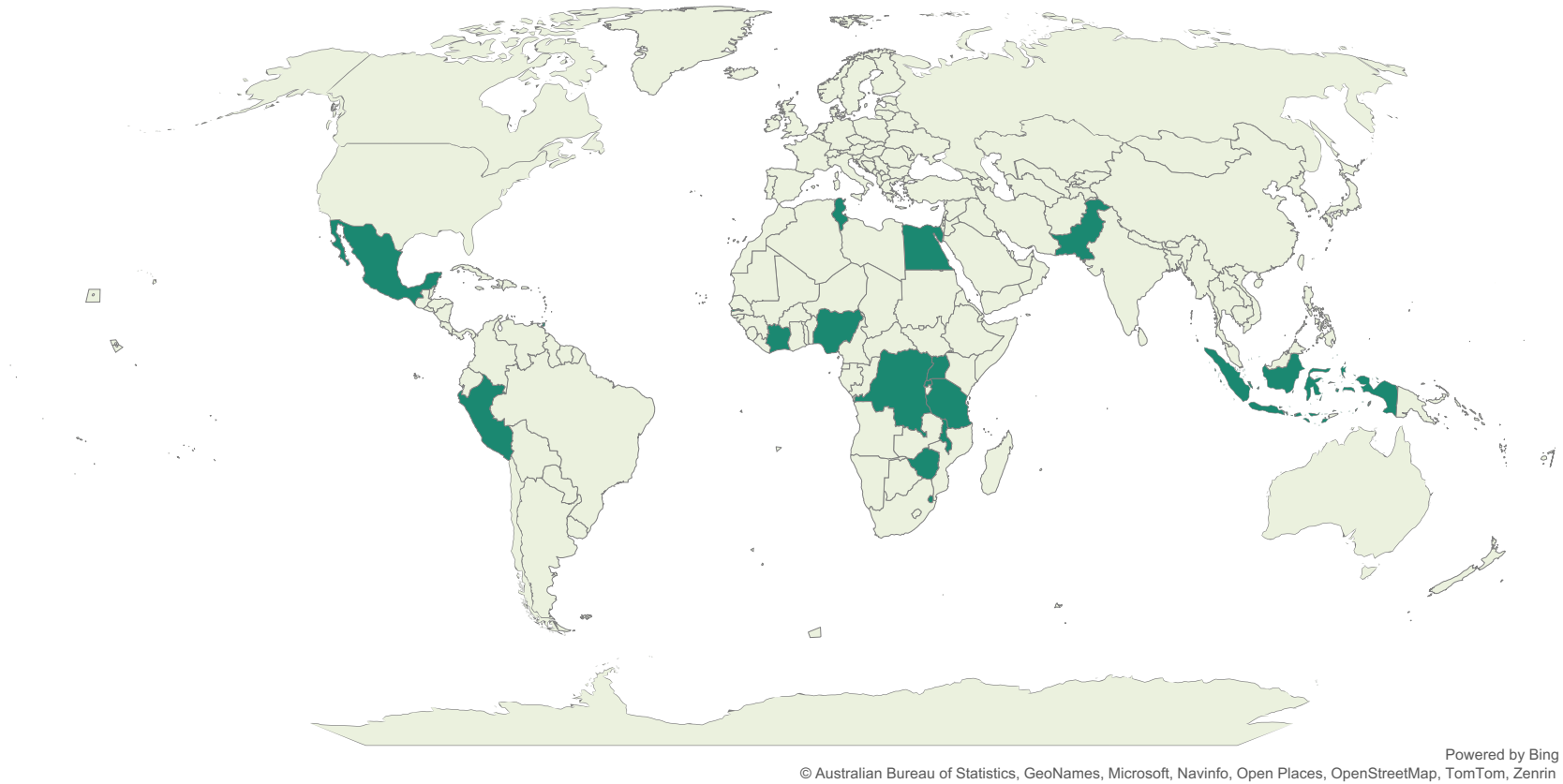
- Organise training on iOS, Android and USSD security testing
- Independent testing by Lab team
- Report on testing done

## 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

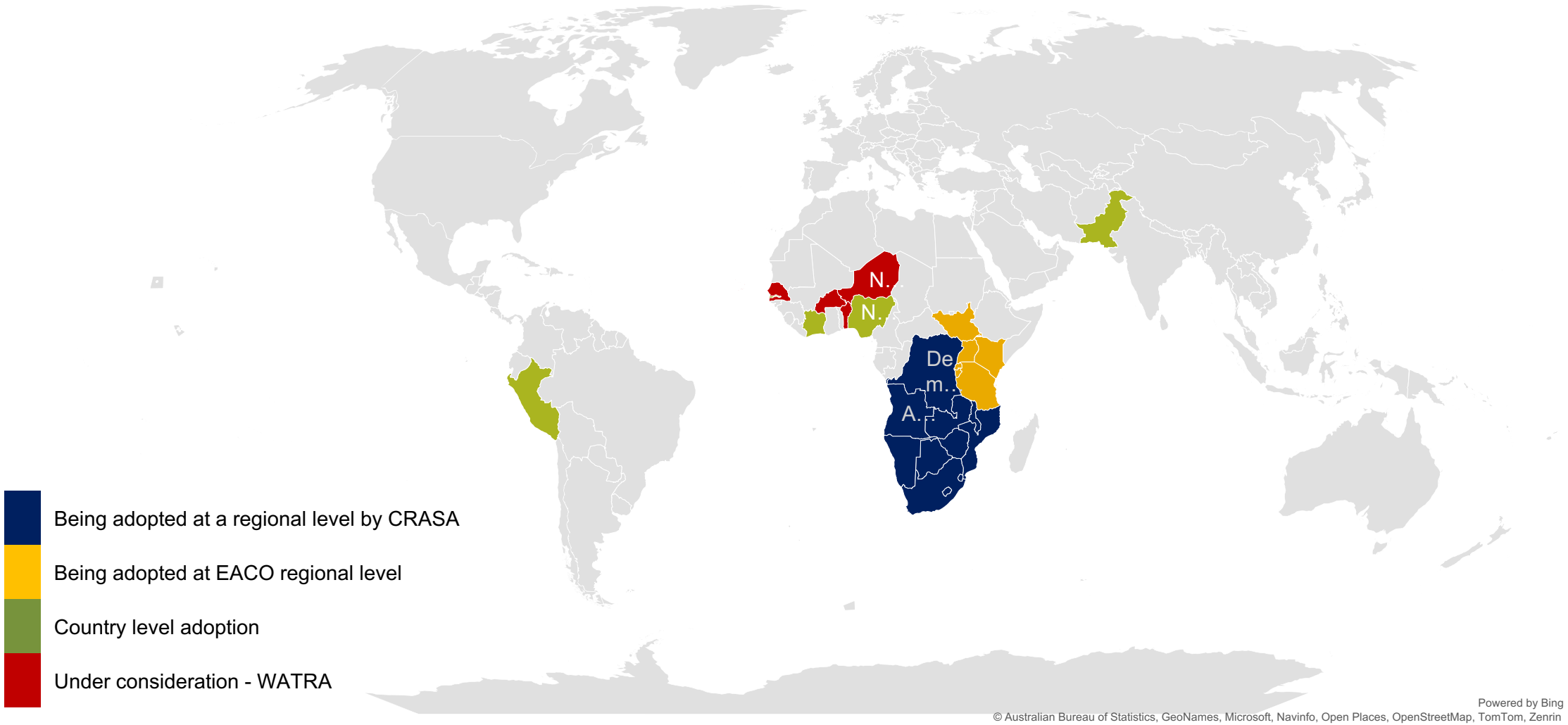
1. Organisation of DFS Security clinics with a focus on knowledge sharing on DFS security recommendations from FIGI
2. Knowledge transfer for regulators of Tanzania, Uganda and Peru to set up DFS Security Lab
3. Guidance on implementing  recommendations DFS security recommendations
4. Conduct security 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




- Being adopted at a regional level by CRASA
- Being adopted at EACO regional level
- Country level adoption
- Under consideration - WATRA


# Questions

Contact: dfssecuritylab@itu.int

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