

ITU Digital Financial Services Security Lab

Vijay Mauree, Programme Cordinator, ITU
<http://www.itu.int/go/dfssl>

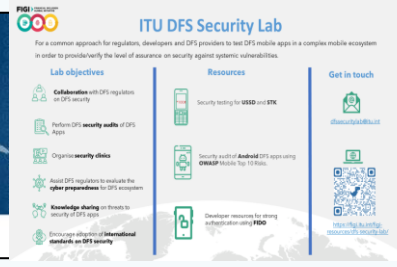
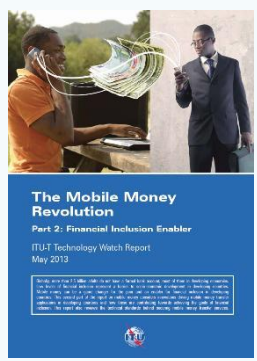
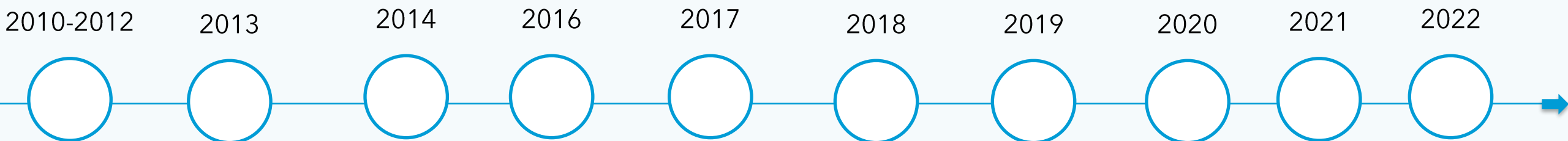
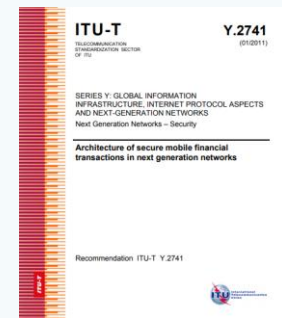
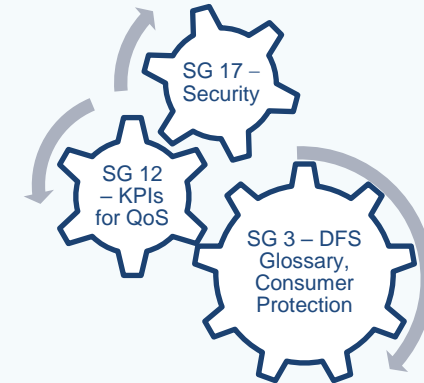
19-20 March 24



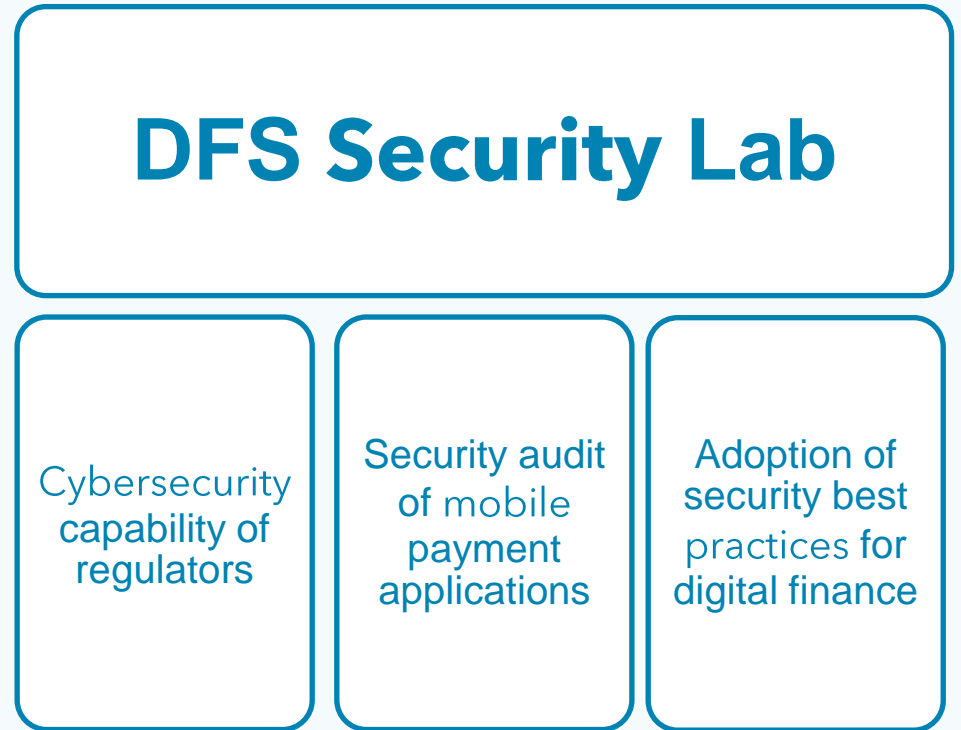
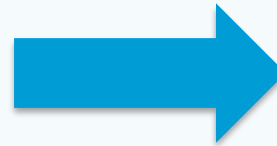
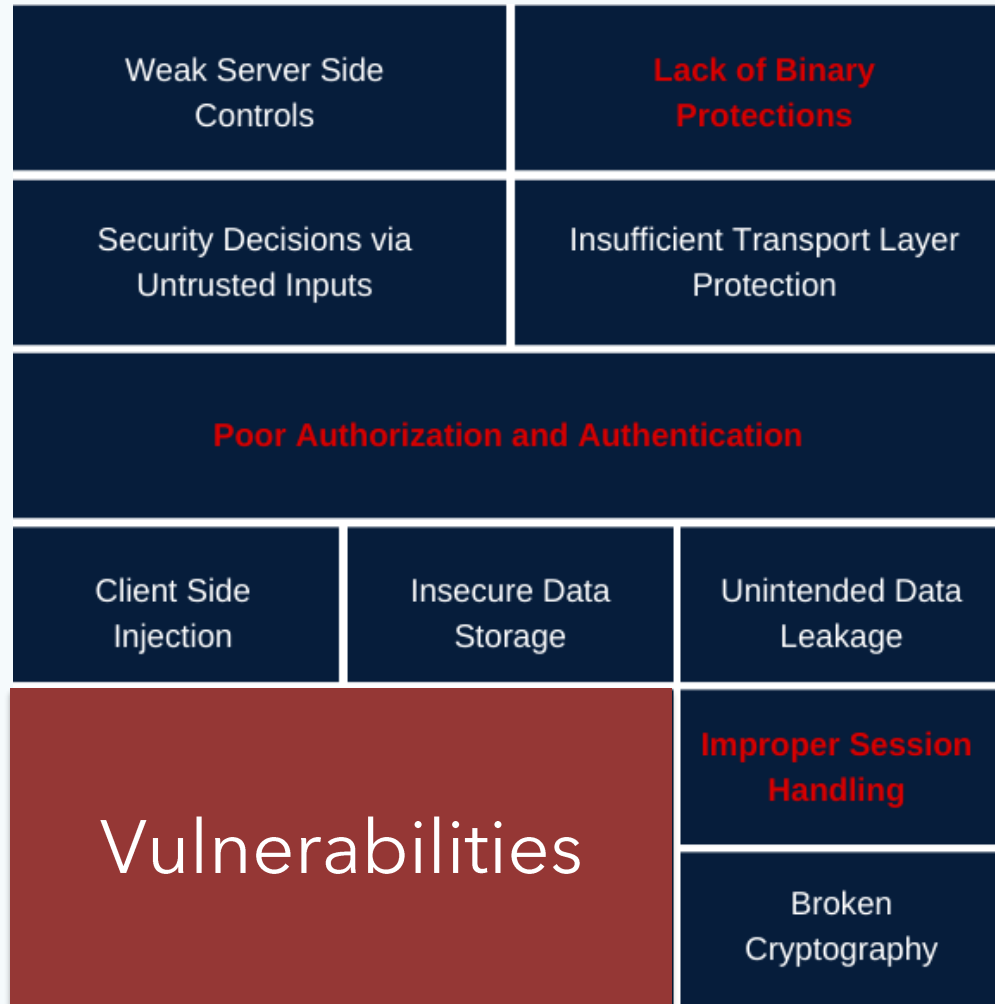
Overview

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

1. ITU & Digital Finance



2. DFS security challenges for regulators



3. 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.

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

3. 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



4. Security recommendations for digital finance

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 the following reports:

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](#)

<https://figi.itu.int/figi-resources/working-groups/>



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

Link: [DFS Security recommendations for regulators and DFS providers developed under FIGI](#)



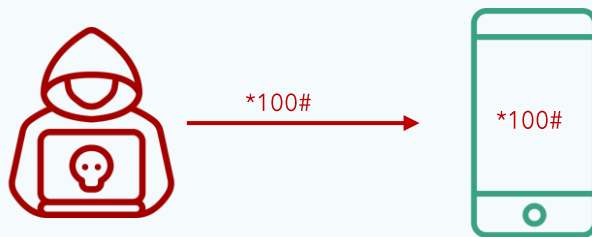
USSD & STK tests



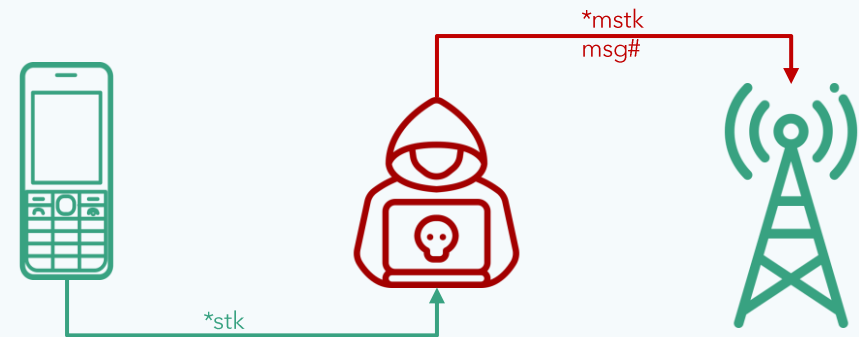
a. **SIM Swap** and **SIM cloning**



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

Source: ITU DFS security lab Android testing Manual



DFS Security Lab Knowledge Transfer

01

Phase 1

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

02

Phase 2

- Select mobile payment app
- Security walkthroughs online workshops

03

Phase 3

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

04

Phase 4

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

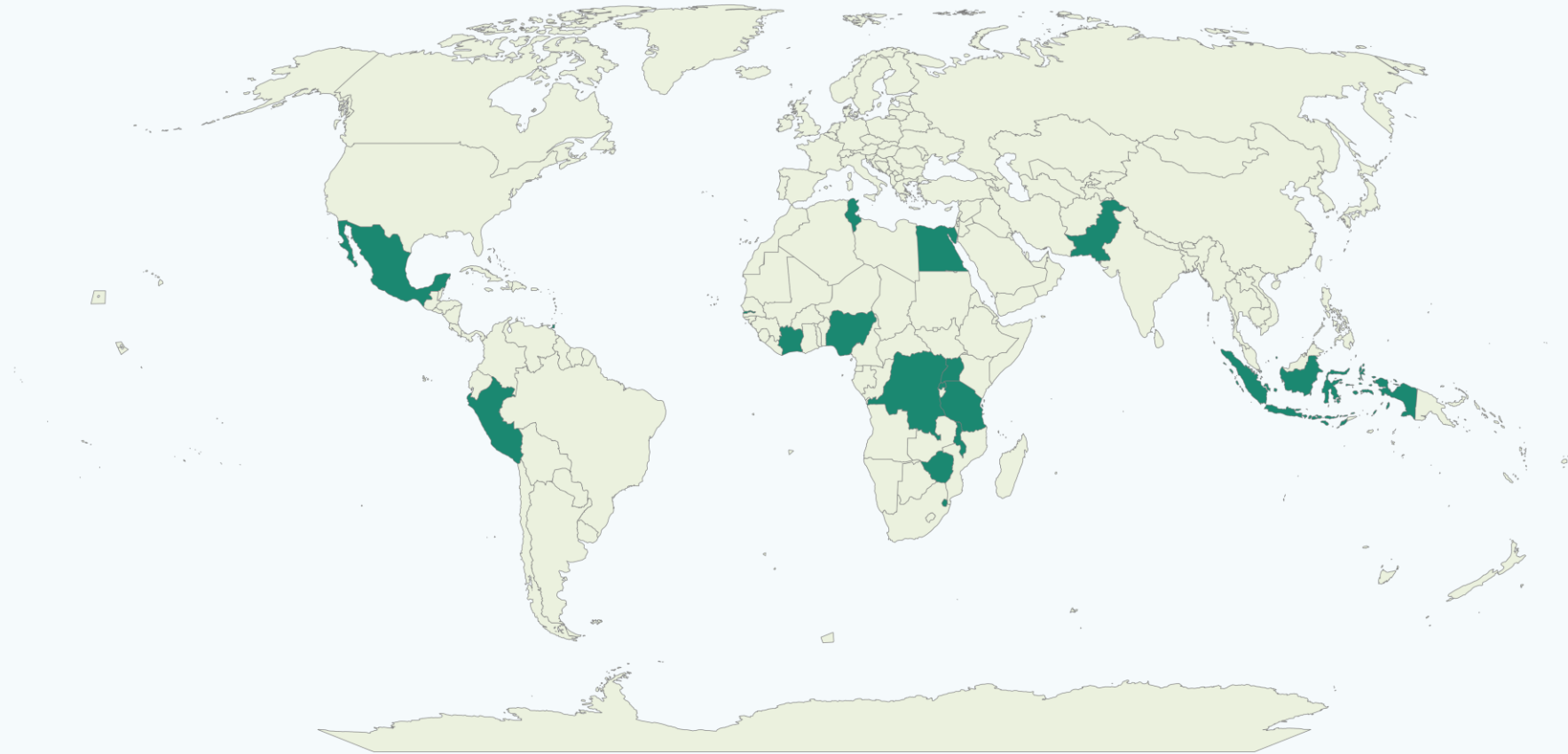


Actions being implemented

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, DRC, 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

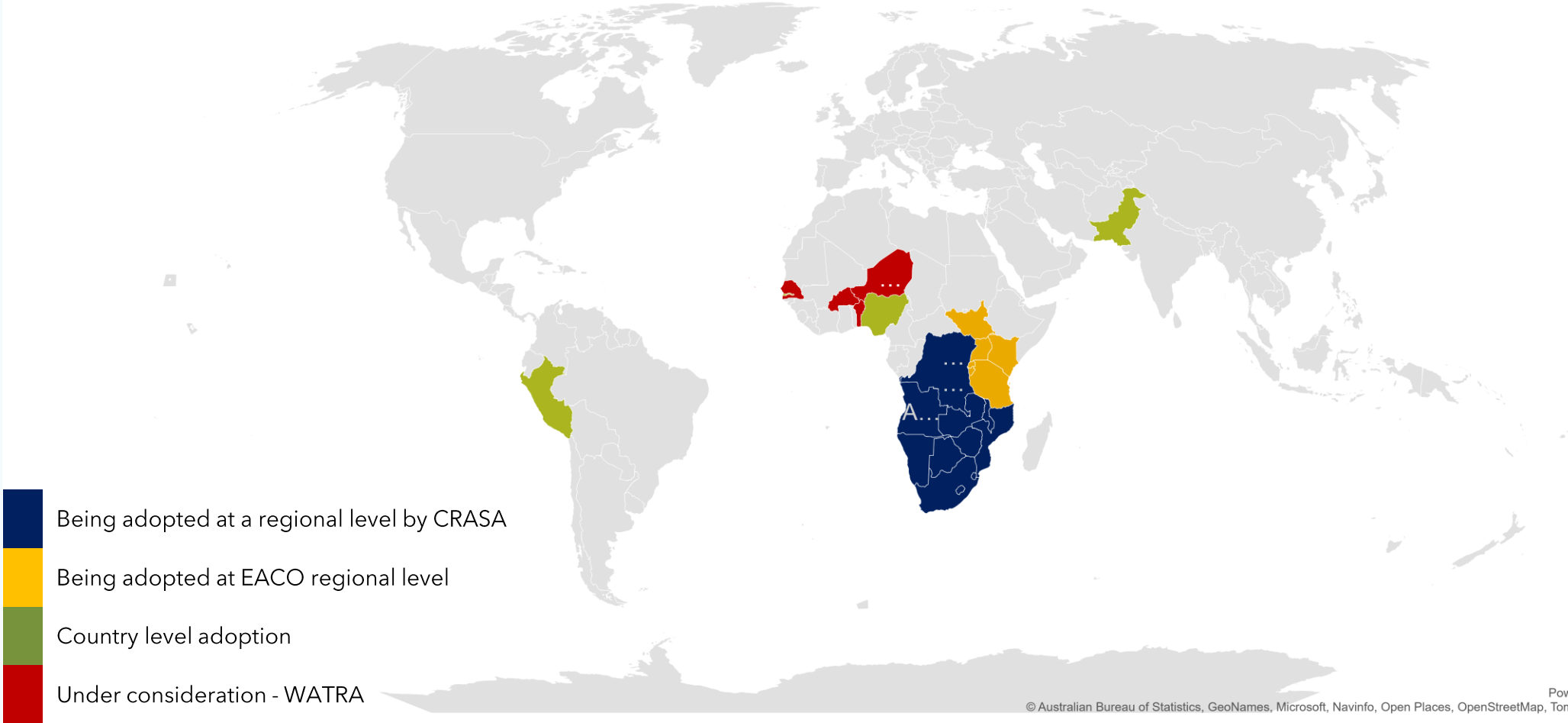


Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Security Clinics were held in some 18 countries



Countries and Regions adopting the recommendations



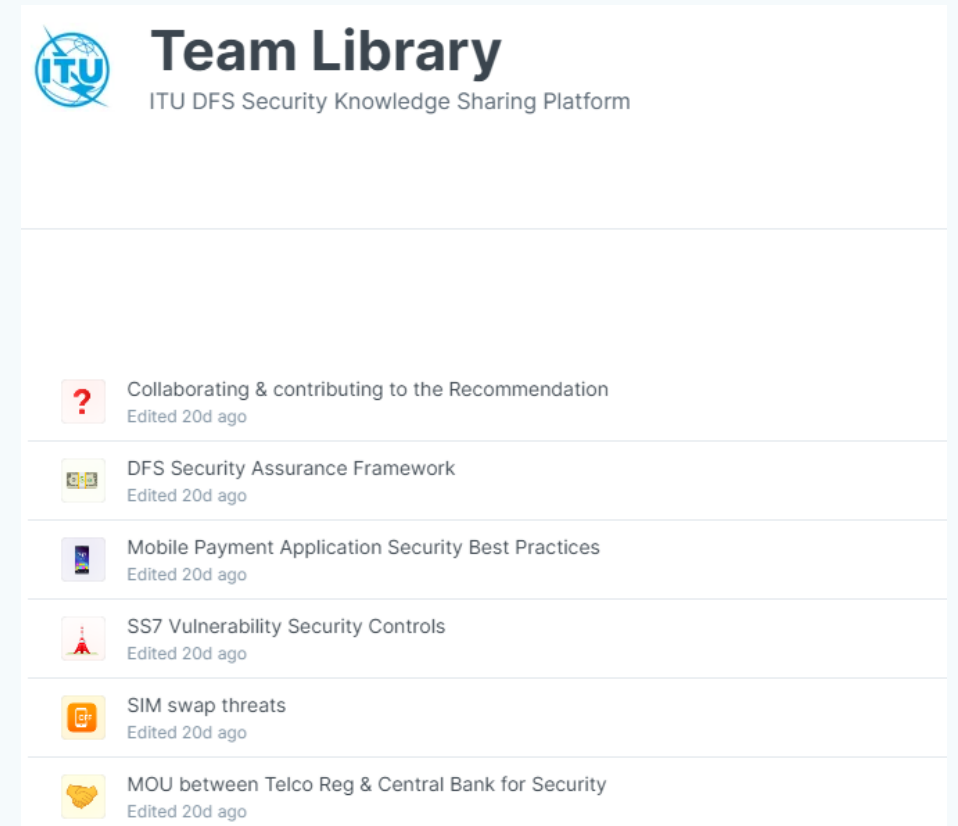
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin









Knowledge Sharing Platform for Digital Finance Security

Objective

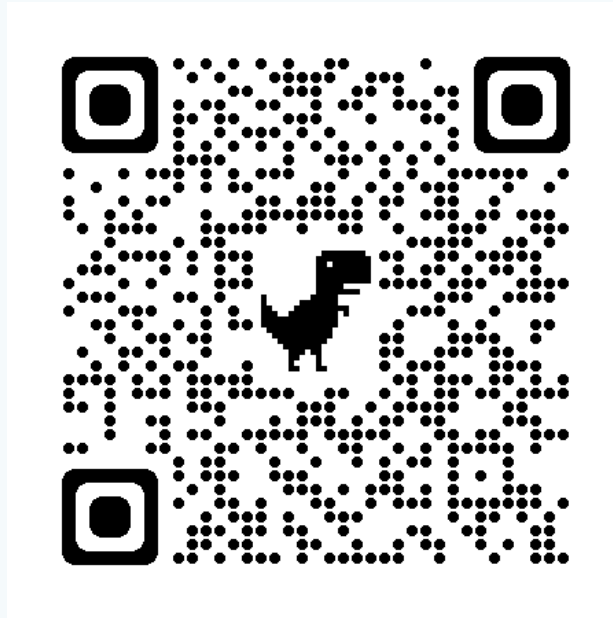
- Collaborate with ITU to keep up to date the DFS security assurance framework security controls and DFS security recommendations.
- Share experiences, challenges, and lessons learned from the implementation of security measures across various jurisdictions.
- Communicate directly with their peers on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



The screenshot displays the 'Team Library' interface for the ITU DFS Security Knowledge Sharing Platform. It features a list of documents with their respective icons, titles, and edit dates. The documents listed are:

-  Collaborating & contributing to the Recommendation
Edited 20d ago
-  DFS Security Assurance Framework
Edited 20d ago
-  Mobile Payment Application Security Best Practices
Edited 20d ago
-  SS7 Vulnerability Security Controls
Edited 20d ago
-  SIM swap threats
Edited 20d ago
-  MOU between Telco Reg & Central Bank for Security
Edited 20d ago

<https://www.itu.int/en/ITU-T/dfs/Pages/share-platform.aspx>



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

Contact: dfssecuritylab@itu.int



Thank you!