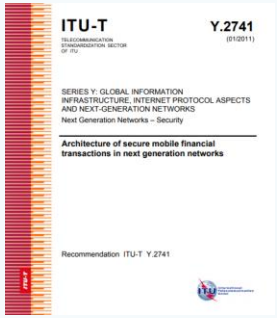
# ITU Digital Financial Services Security Lab

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

# Overview

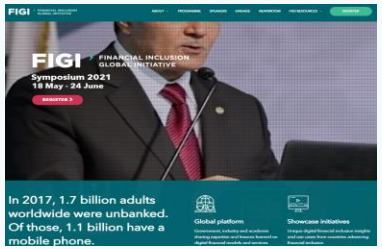
1. ITU & Digital Finance
2. Security challenges
3. DFS Security Lab
4. Security recommendations for digital finance
5. USSD, Android and iOS mobile payment app security audit
6. Setting up the security lab & Knowledge transfer for regulators
7. Actions being implemented

# 1. ITU & Digital Finance



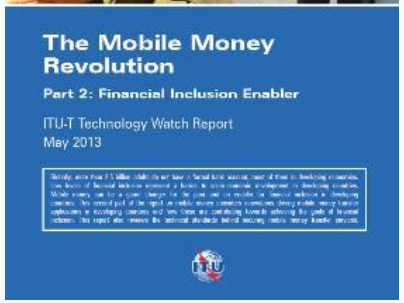








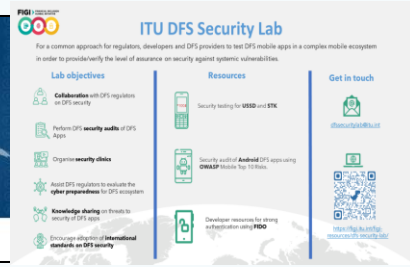
2010-2012 | 2013 | 2014 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022











# DFS Security Lab

Cybersecurity capability of regulators

Security audit of mobile payment applications

Adoption of security best practices for digital finance

# 3. DFS Security Lab

Provides a standard methodology to conduct security audit for mobile payment apps (USSD, Android and iOS), 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:

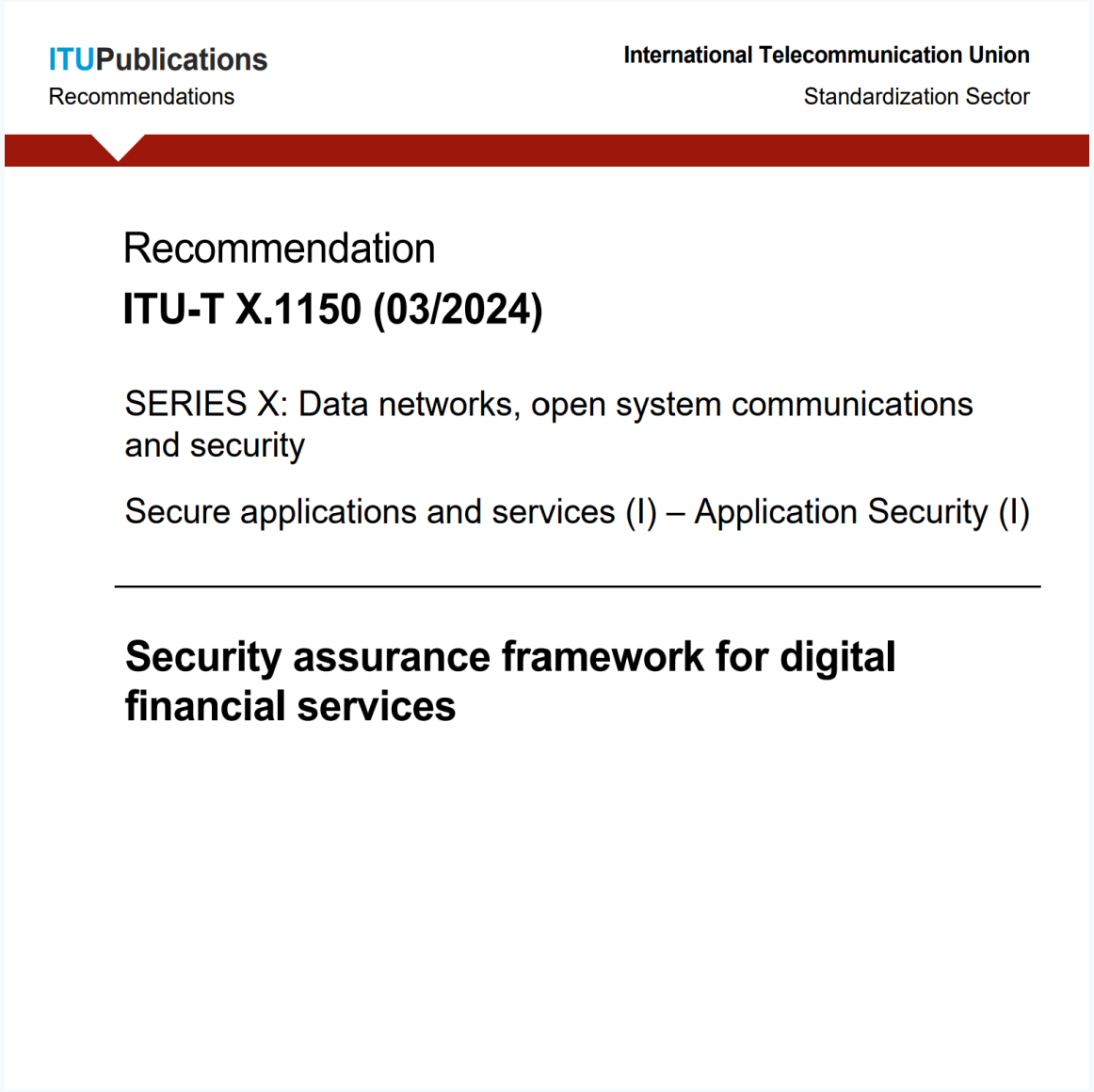
1. DFS Security Assurance  Framework
2. Security testing for USSD and STK based DFS applications
3. Security audit of various DFS applications
4. DFS security audit guideline
5. DFS Consumer Competency Framework


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

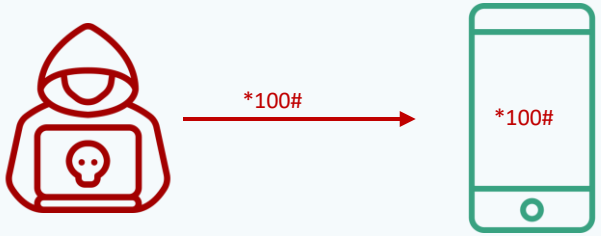



Link: DFS Security recommendations for regulators and DFS providers developed under FIGI

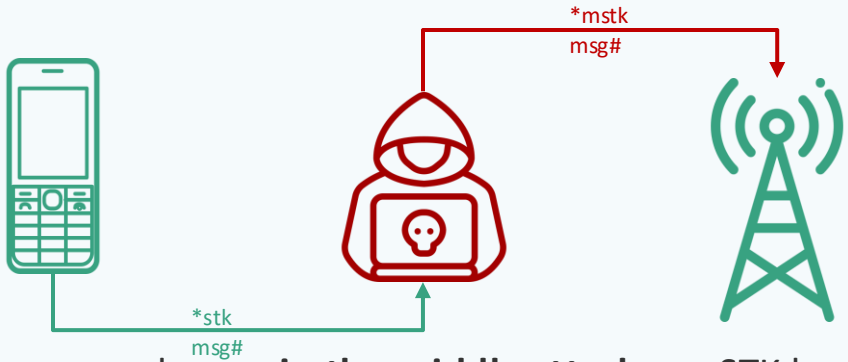
# USSD & STK security audit tests

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 mobile payment app security audit 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 phases

The Lab has a knowledge transfer programme for regulators to verify the security assurance of mobile payment applications based on Android, iOS, and USSD. conducted om 4 phases

01

## Phase 1

- Regulator Identifies Lab team and equipment in place
- verify equipment is configured
- DFS Security Clinic – Share recommendations on Digital Finance

02

## Phase 2

- Select mobile payment app to be tested during the knowledge transfer
- 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

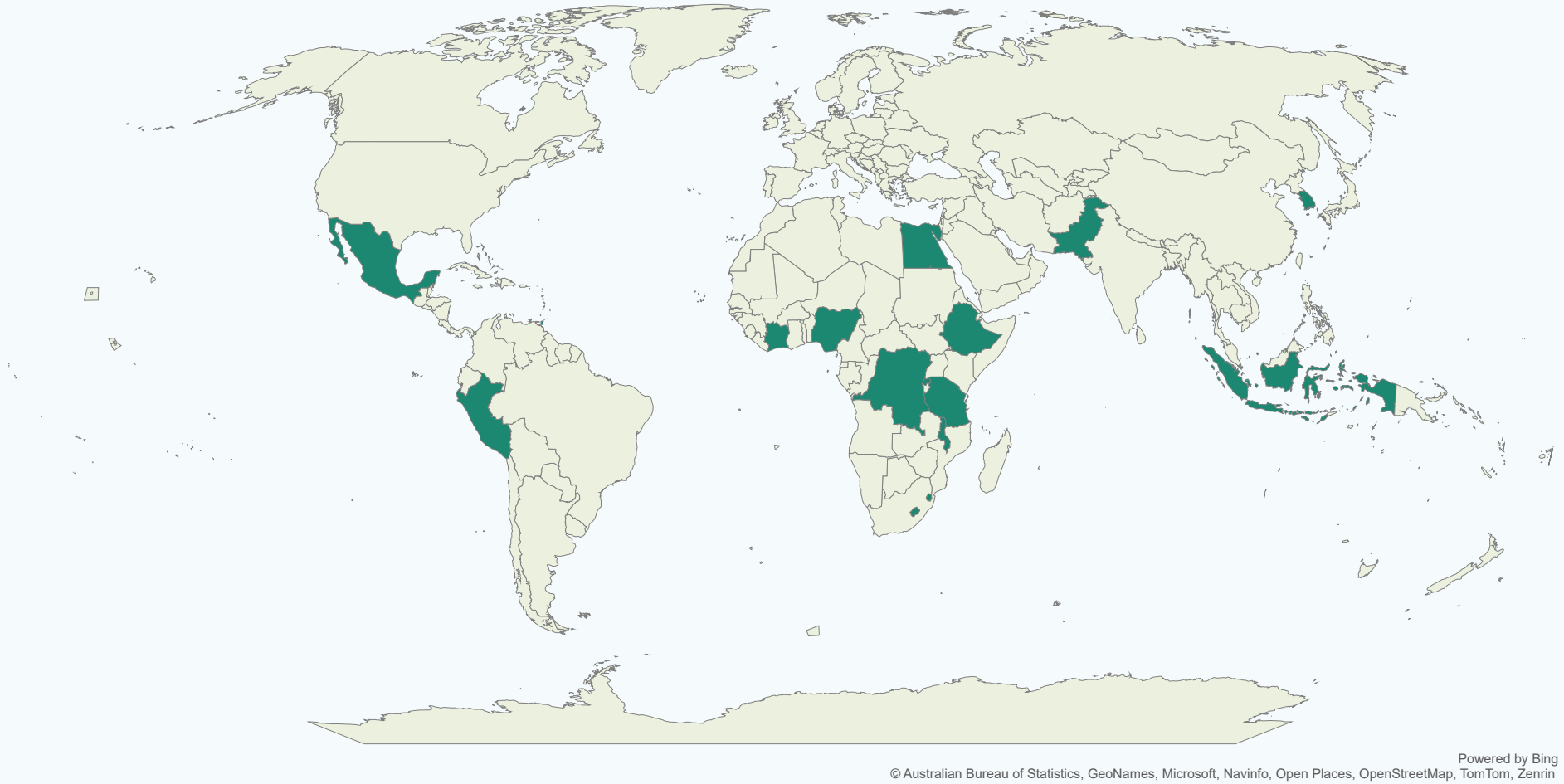
## Phase 4

- 6-9 months period of oversight by ITU
- Mobile payment app testing review by ITU
- Sharing lessons learned of new threats and vulnerabilities

# Actions being implemented

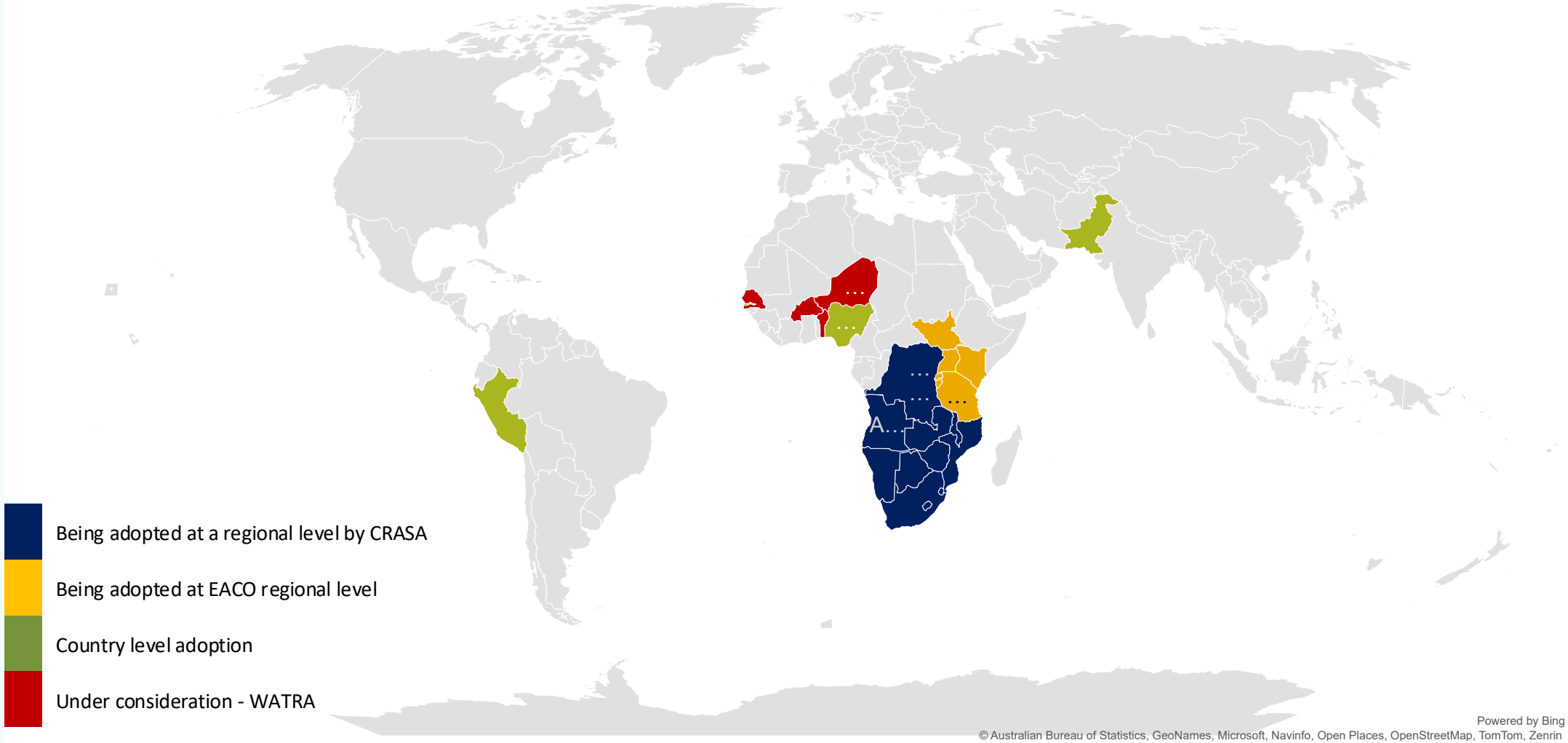
1. Organisation of DFS Security clinics with a focus on knowledge sharing on DFS security recommendations
2. Knowledge transfer for regulators (Ghana, Tanzania, Uganda, St. Lucia, Antigua and Barbuda, Zimbabwe, South Sudan, Ghana, The Gambia and Peru)
3. Guidance on implementing  recommendations DFS 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 2021-2024




Security Clinics were held in some 21 countries, 3 regional bodies

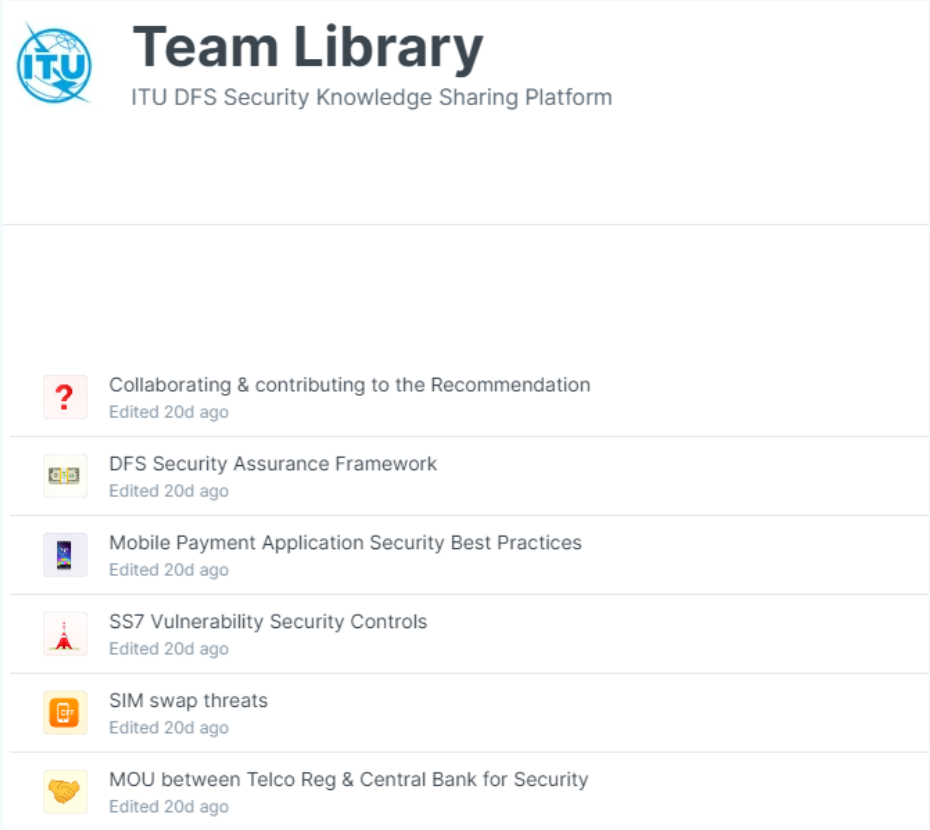
# Countries and Regions adopting the recommendations



# ITU Knowledge Sharing Platform for Digital Finance Security

**Objective**

- Collaborate with ITU to keep up to date the DFS security assurance framework & 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.




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

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

**Contact:** dfssecuritylab@itu.int

**Thank you!**