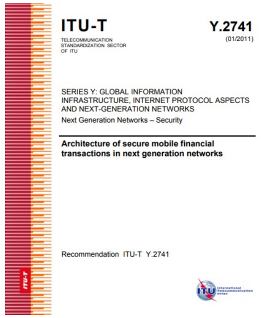
# Digital Financial Services Security Lab

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 implemented

# ITU Digital Finance & Inclusion Journey



ITU-T

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

Y.2741 (01/2011)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Security

**Architecture of secure mobile financial transactions in next generation networks**

Recommendation ITU-T Y.2741

> ITU FOCUS GROUP DIGITAL FINANCIAL SERVICES: MAIN RECOMMENDATIONS

ITU-T FOCUS GROUP ON DIGITAL FINANCIAL SERVICES

FIGI symposium

29 November – 1 December 2017
Bengaluru, India

#financialinclusion

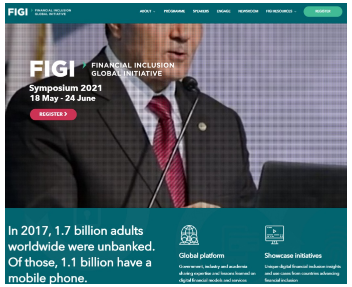
FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE

Bengaluru
Hosted by
Organized by
Sponsored by
DEPARTMENT OF TELECOMMUNICATIONS MINISTRY OF COMMUNICATIONS GOVERNMENT OF INDIA
WORLD BANK GROUP
Committee on Payments and Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS
BILL & MELINDA GATES foundation

FIGI Symposium

22 - 24 January 2019
Cairo, Egypt

FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE



FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE

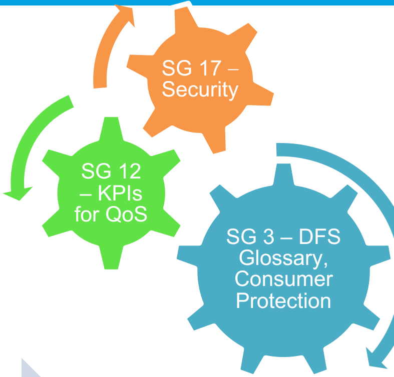
FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE

Symposium 2021
18 May - 24 June

In 2017, 1.7 billion adults worldwide were unbanked. Of those, 1.1 billion have a mobile phone.

**Global platform**
Government, industry and academia sharing expertise and lessons learned on digital financial models and services

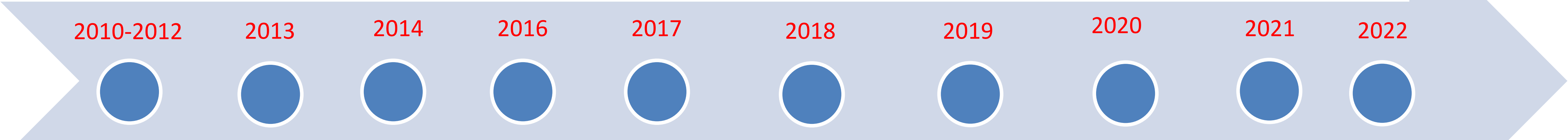
**Showcase initiatives**
Unique digital financial inclusion insights and use cases from countries advancing financial inclusion

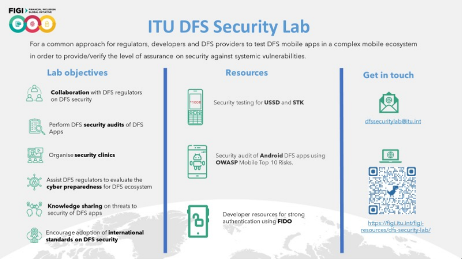


SG 17 – Security

SG 12 – KPIs for QoS

SG 3 – DFS Glossary, Consumer Protection





## ITU DFS Security Lab

For a common approach for regulators, developers and DFS providers to test DFS mobile apps in a complex mobile ecosystem in order to provide/verify the level of assurance on security against systemic vulnerabilities.

**Lab objectives**

- **Collaboration** with DFS regulators on DFS security
- Perform DFS **security audits** of DFS Apps
- Organise **security clinics**
- Assist DFS regulators to evaluate the **cyber preparedness** for DFS ecosystem
- **Knowledge sharing** on threats to security of DFS apps
- Encourage adoption of **international standards on DFS security**

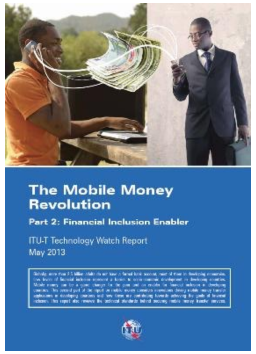
**Resources**

- Security testing for **USSD** and **STK**
- Security audit of **Android** DFS apps using **OWASP** Mobile Top 10 Risks.
- Developer resources for strong authentication using **FIDO**

**Get in touch**

dfssecuritylab@itu.int

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



**The Mobile Money Revolution**

**Part 2: Financial Inclusion Enabler**

ITU-T Technology Watch Report
May 2013

Globally, more than 2.5 billion adults do not have a formal bank account, most of them in developing economies. Low levels of financial inclusion represent a barrier to socio-economic development in developing countries. Mobile money can be a game changer for the poor and an enabler for financial inclusion in developing countries. This second part of the report on mobile money considers innovations driving mobile money transfer applications in developing countries and how these are contributing towards achieving the goals of financial inclusion. This report also reviews the technical standards behind securing mobile money transfer services.

Tech Watch Report Mobile Money

FOCUS GROUP

**Digital Currency including Digital Fiat Currency**

Standards for digital fiat currency for financial inclusion

#DigitalFinanceITU

Res. 89

wtsa16 TUNISIA

WORLD TELECOMMUNICATION STANDARDIZATION ASSEMBLY

25 OCTOBER - 3 NOVEMBER
HAMMAMET, TUNISIA

国际电联第一次法定数字货币焦点组工作会议
First Workshop on Standards for Digital Fiat Currency for Universal Financial Access
2017年10月12日 中国・北京
October 12, 2017 Beijing China

**Workshop on standardizing Digital Fiat Currency and its Applications**

18 - 20 July 2018
New York City, USA

In partnership with: Cornell University

Organized by

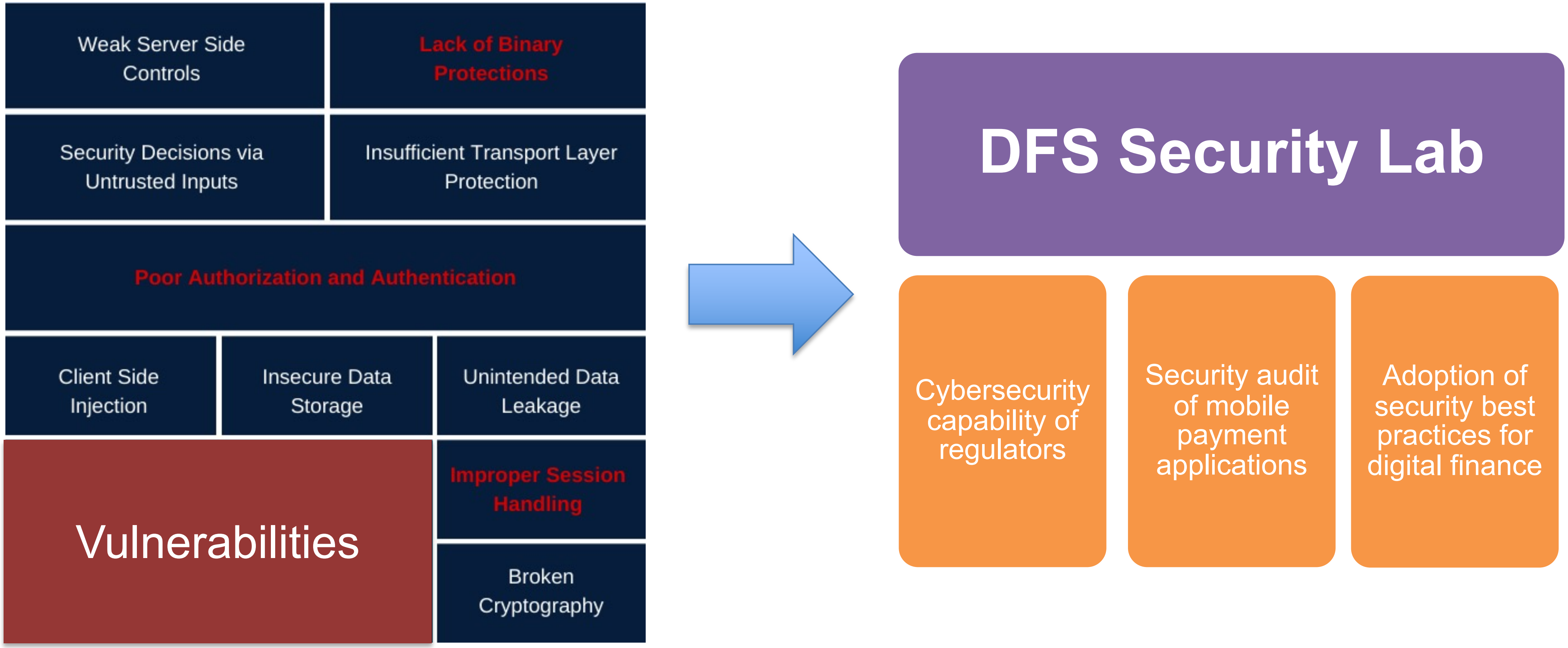
**Digital Currency Global Initiative**

Contribute to: SUSTAINABLE DEVELOPMENT GOALS

ITUEvents

**Insights on Digital Financial Services during COVID-19 Webinar Series**

# DFS security challenges for regulators



Weak Server Side Controls

Lack of Binary Protections

Security Decisions via Untrusted Inputs

Insufficient Transport Layer Protection

Poor Authorization and Authentication

Client Side Injection

Insecure Data Storage

Unintended Data Leakage

Vulnerabilities

Improper Session Handling

Broken Cryptography

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

FIGI
FINANCIAL INCLUSION GLOBAL INITIATIVE
SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP
Digital Financial Services security assurance framework
SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP
Security audit of various DFS applications
REPORT OF THE SECURITY WORKSTREAM
SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP
Digital Financial Services security audit guideline
SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP
Security testing for USSD and STK based Digital Financial Services applications
REPORT OF SECURITY WORKSTREAM
ITU

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

# Adoption of Security Recommendations

These reports 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

FIGI
FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services security assurance framework

FIGI
FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Security audit of various DFS applications

RT OF THE SECURITY WORKSTREAM

FIGI
FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services security audit guideline

FIGI
FINANCIAL INCLUSION GLOBAL INITIATIVE

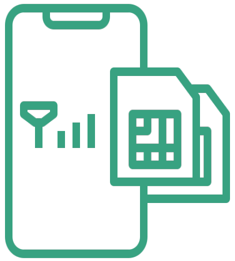
SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Security testing for USSD and STK based Digital Financial Services applications

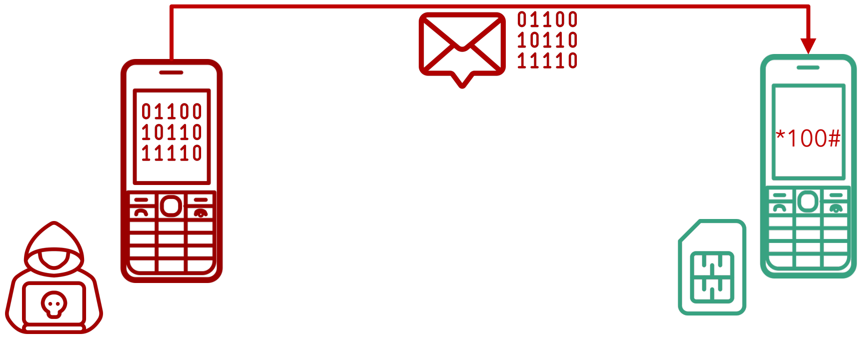
REPORT OF SECURITY WORKSTREAM

*See [https://figi.itu.int/figi-resources/working-groups/](https://figi.itu.int/figi-resources/working-groups/)*

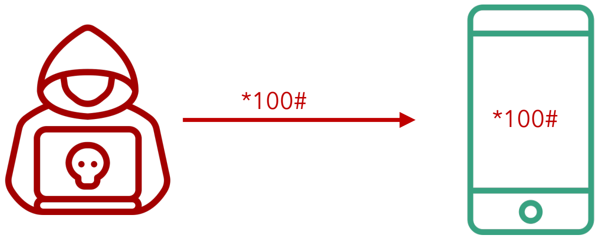
# USSD & STK tests



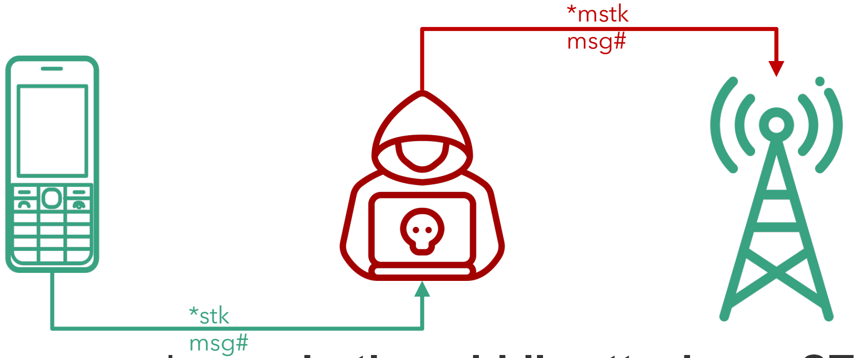
a. **SIM Swap** and **SIM cloning**



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



c. **remote USSD** execution attacks

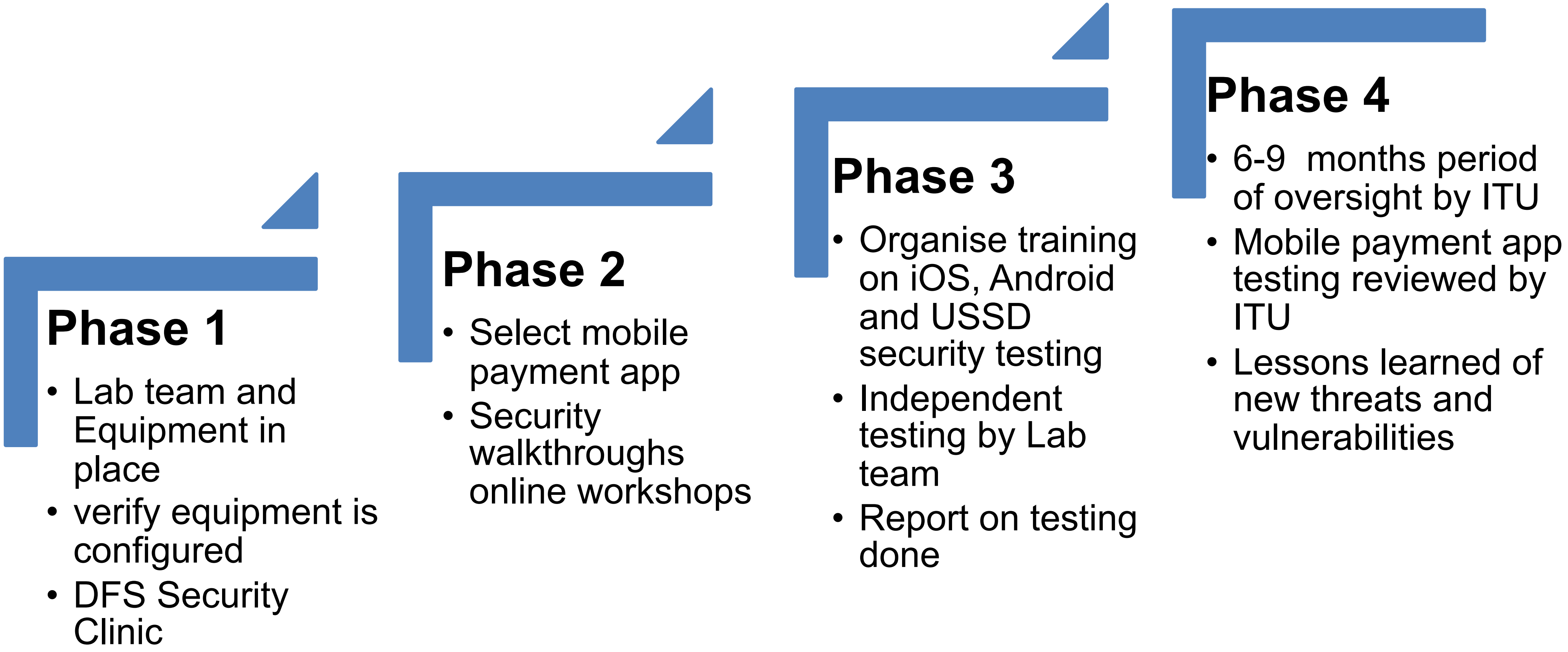


d. **man-in-the-middle attacks** on STK based DFS applications

# 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

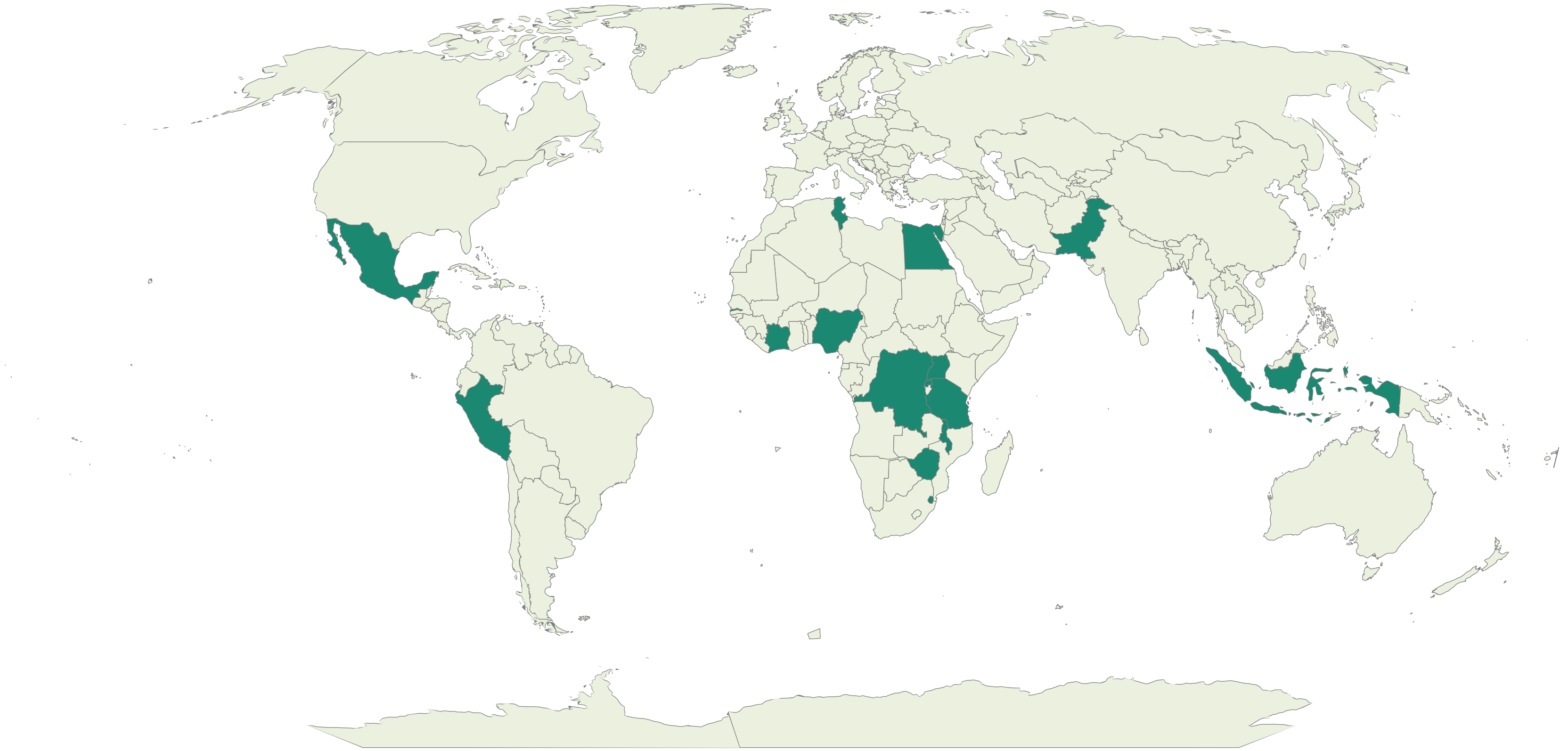
# Actions Implemented

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).

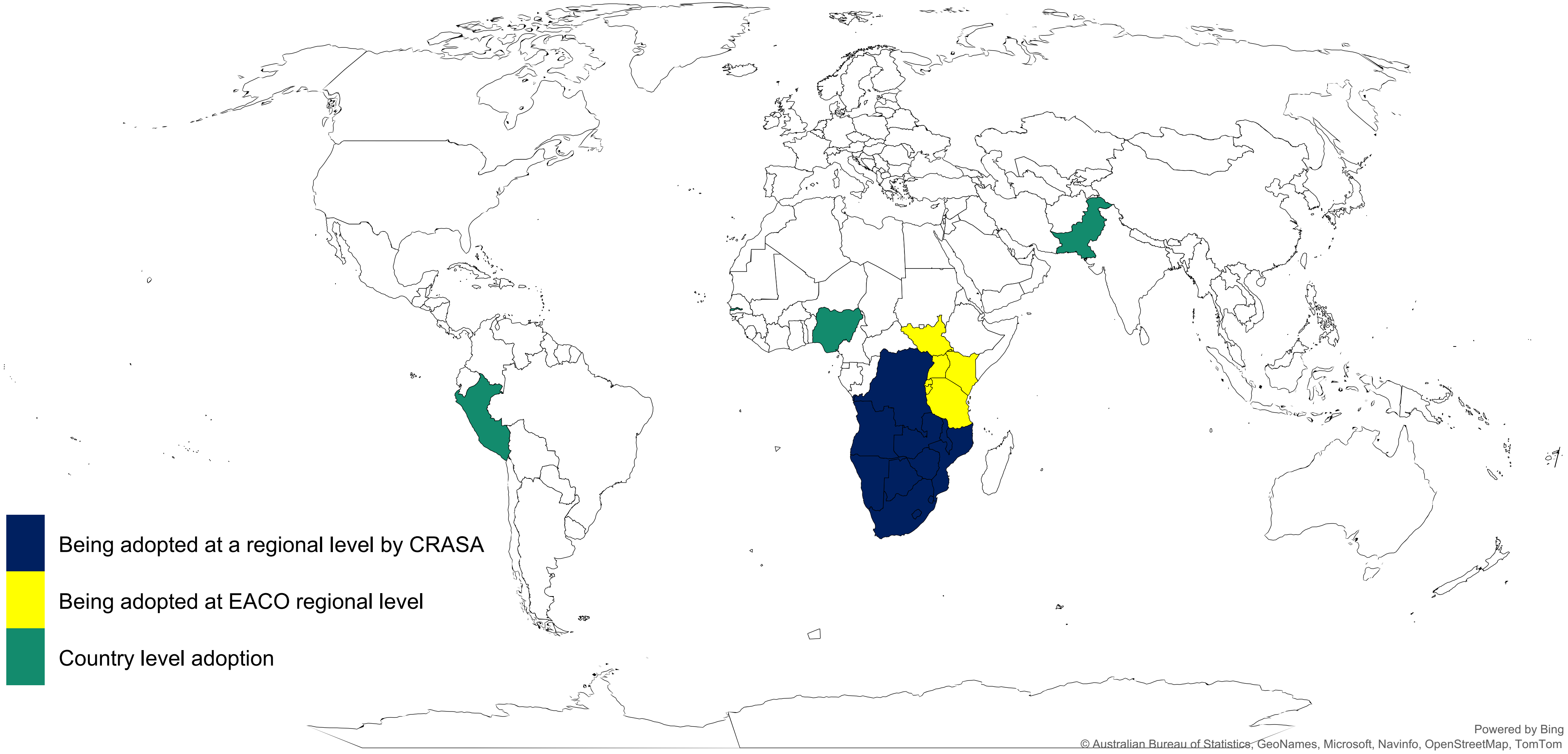


Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

## DFS security clinics held in 2021 and 2022

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

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