ITU Digital Financial Services Security Lab

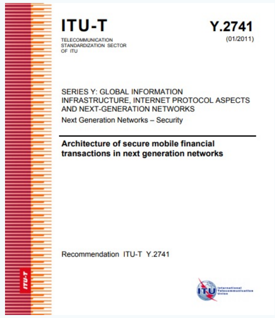
Vijay Mauree, Programme Cordinator, ITU
http://www.itu.int/go/dfssl

11 April 2024

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



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

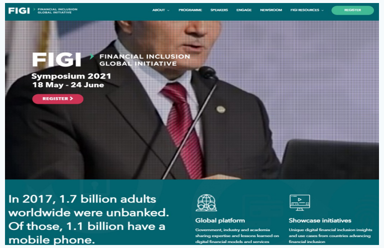
ITU-T FOCUS GROUP ON DIGITAL FINANCIAL SERVICES

FIGI symposium
29 November – 1 December 2017
Bengaluru, India
#financialinclusion

FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE

FIGI Symposium
22 - 24 January 2019
Cairo, Egypt

FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE

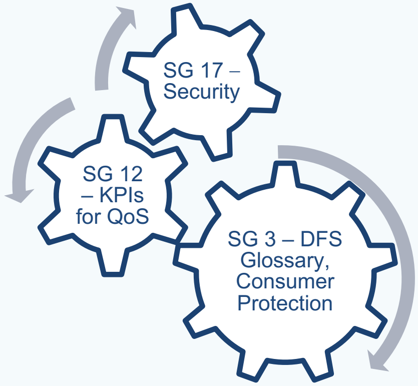


FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE
Symposium 2021
18 May - 24 June

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

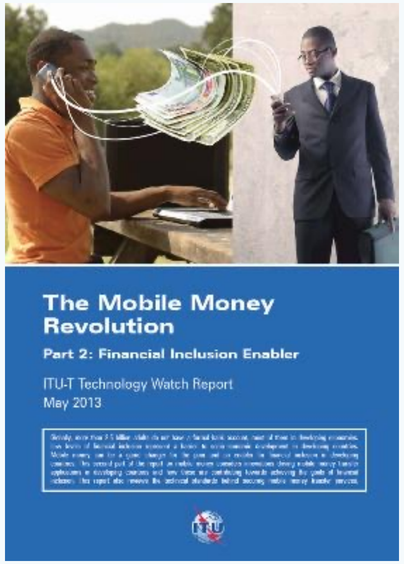


SG 17 – Security

SG 12 – KPIs for QoS

SG 3 – DFS Glossary, Consumer Protection

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



The Mobile Money Revolution
Part 2: Financial Inclusion Enabler
ITU-T Technology Watch Report
May 2013

[illegible]

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

Host: Institute of World Economics and Politics (IWEP), CASS
International Telecommunication Union (ITU)
Honorable sponsor: Institute of Digital Money, People's Bank of China
Support: China Academy of Information and Communications Technology
Digital Fiat Currency Institute (DFCI, USA)

2017年10月12日 中国・北京
October 12, 2017 Beijing China

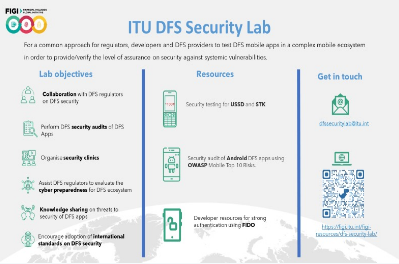
Workshop on standardizing Digital Fiat Currency and its Applications
18 - 20 July 2018
New York City, USA

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



FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE

ITU DFS Security Lab

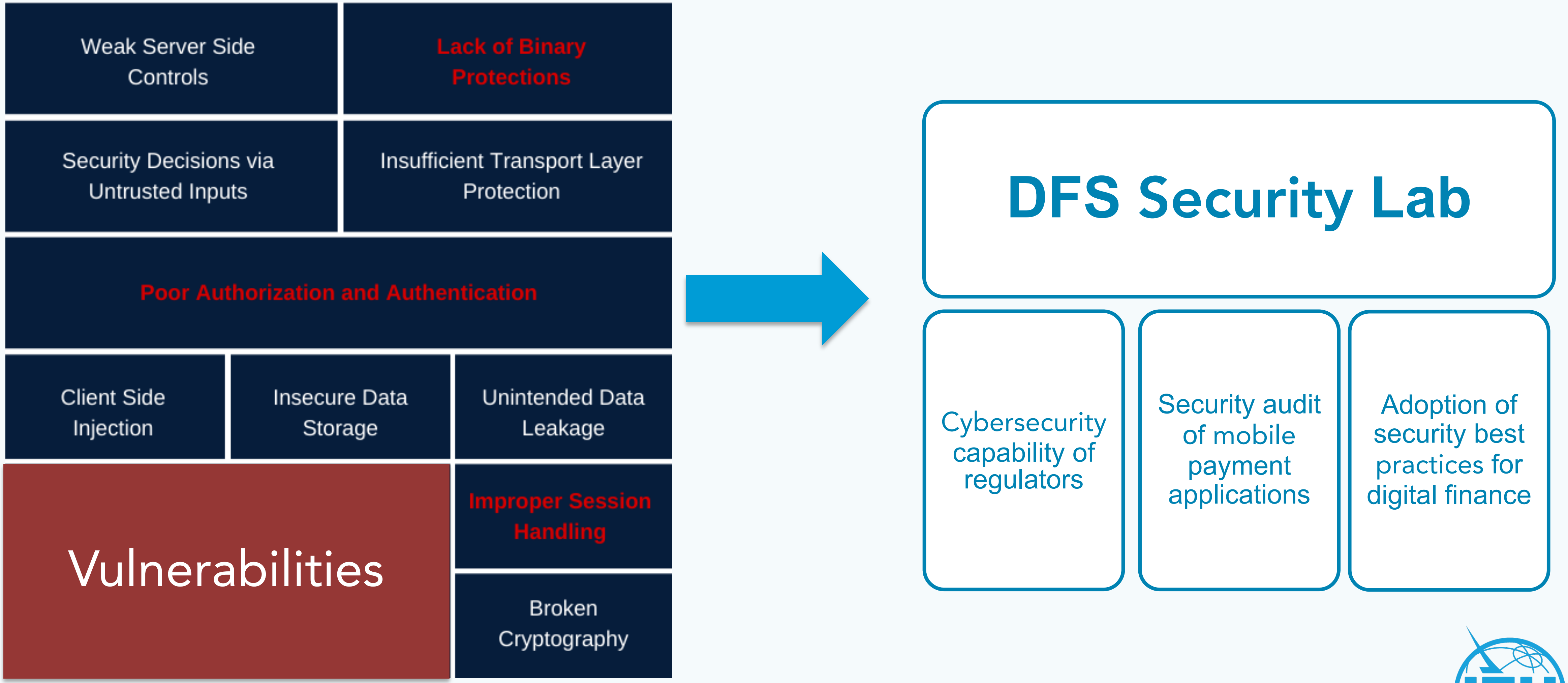
For a common approach for regulators, developers and DFS providers to test DFS mobile apps in a complex mobile ecosystem in order to provide/verify the level of assurance on security against systemic vulnerabilities.

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/

2. 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

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/

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services security assurance framework

REPORT OF SECURITY WORKSTREAM

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Security audit of various DFS applications

REPORT OF THE SECURITY WORKSTREAM

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

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services security audit guideline

REPORT OF SECURITY WORKSTREAM

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

FIGI
FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services security assurance framework

REPORT OF SECURITY WORKSTREAM

FIGI
FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Security audit of various DFS applications

REPORT OF THE SECURITY WORKSTREAM

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

ITU

FIGI
FINANCIAL INCLUSION GLOBAL INITIATIVE

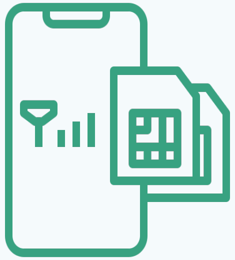
SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services security audit guideline

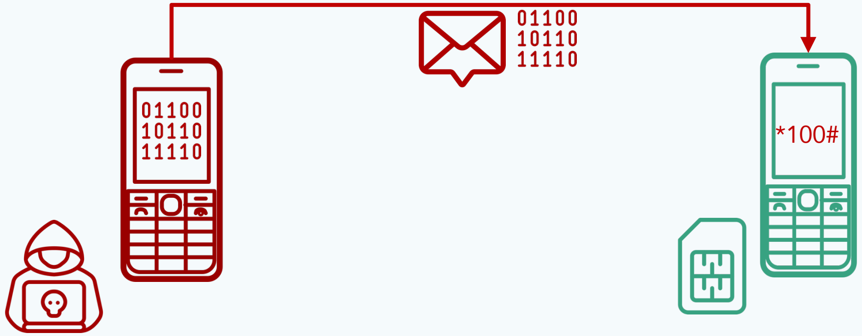
REPORT OF SECURITY WORKSTREAM

ITU

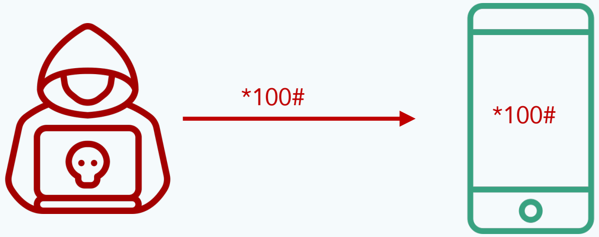
USSD & STK tests



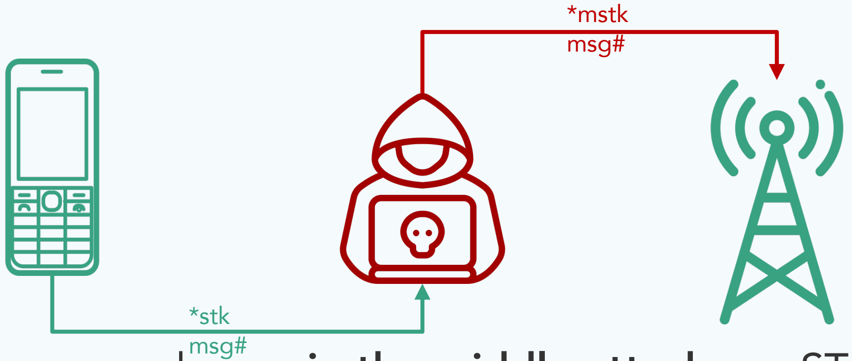
a. **SIM Swap** and **SIM cloning**



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



c. **remote USSD** execution attacks



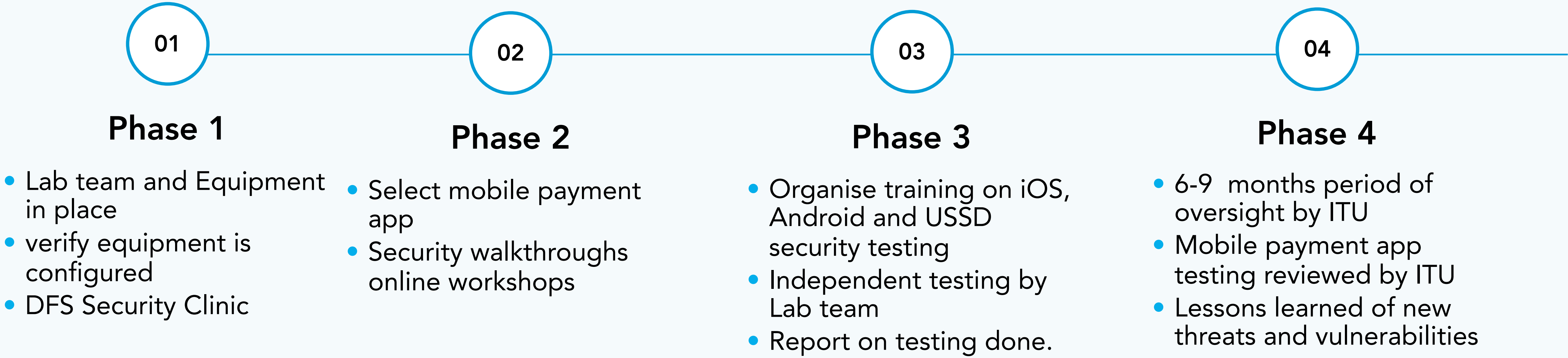
d. **man-in-the-middle attacks** on STK based DFS applications

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 2021-2024

Security Clinics were held in some 18 countries, 3 regional bodies

Countries and Regions adopting the recommendations

🟦 Being adopted at a regional level by CRASA

🟨 Being adopted at EACO regional level

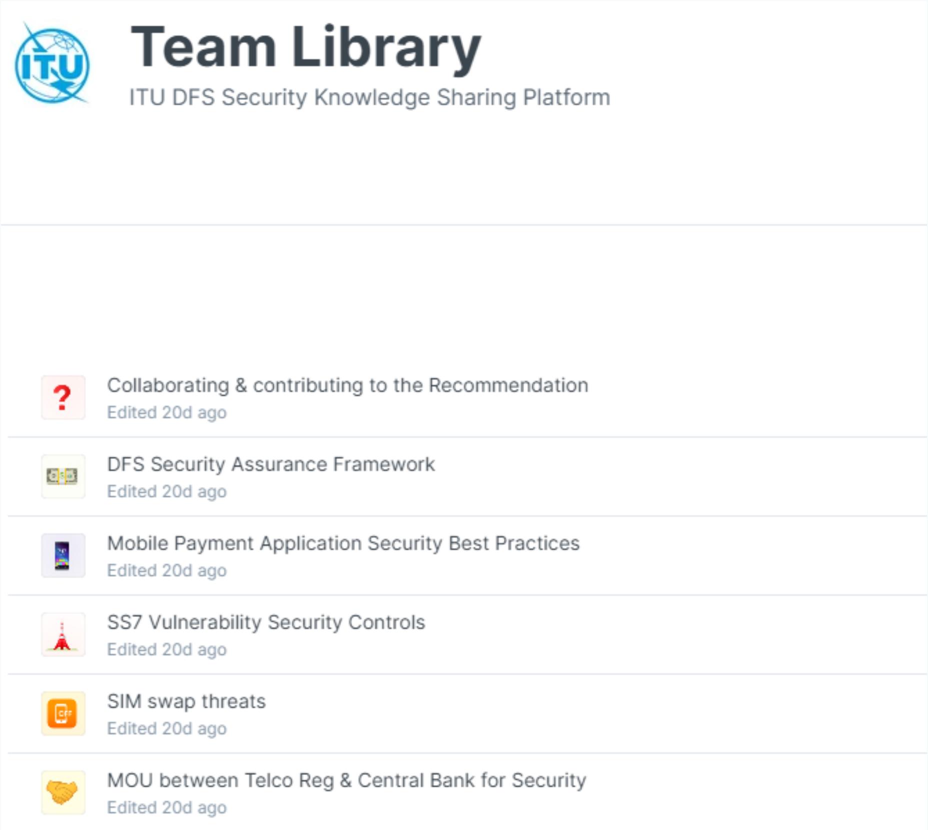
🟩 Country level adoption

🟥 Under consideration - WATRA

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.



Team Library

ITU DFS Security Knowledge Sharing Platform

- 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!