

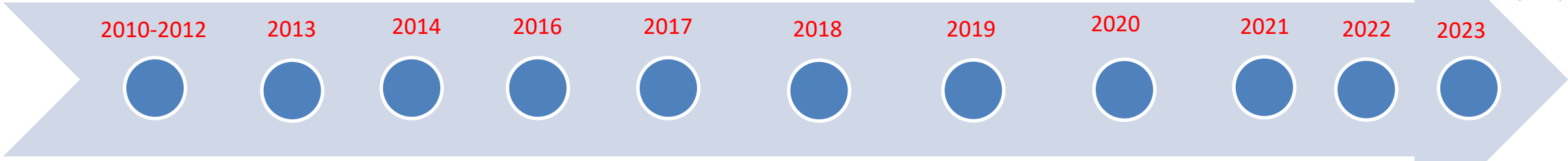
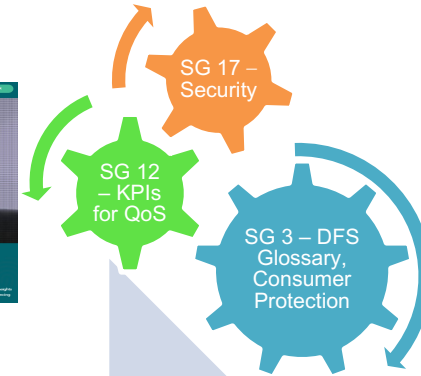
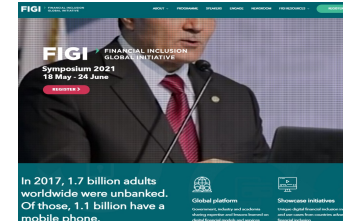
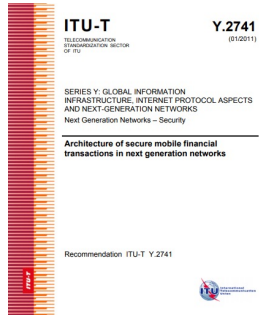
ITU Digital Financial Services Security Lab

Vijay Mauree
Programme Coordinator
Standardization Bureau, ITU

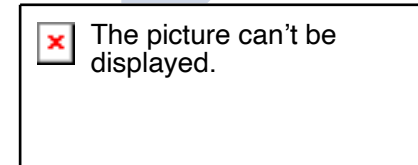
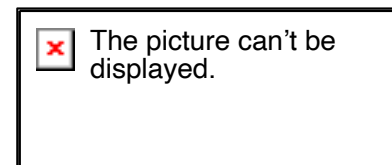
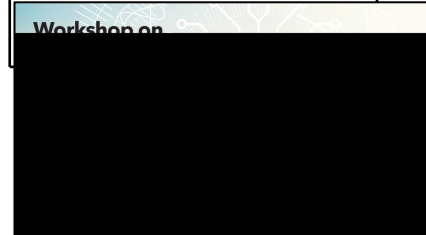
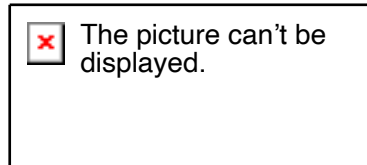
Overview

1. ITU & Digital Finance
2. Security challenges
3. DFS Security recommendations
4. DFS Security Lab
5. Testing security of mobile payment apps
6. Assistance to developing countries

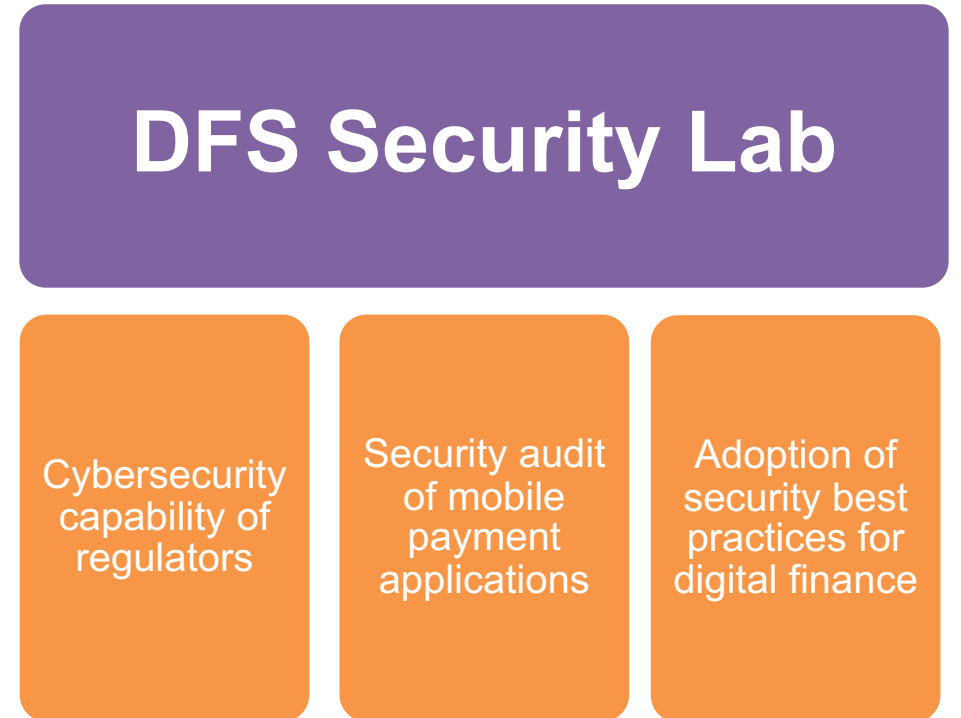
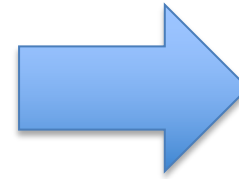
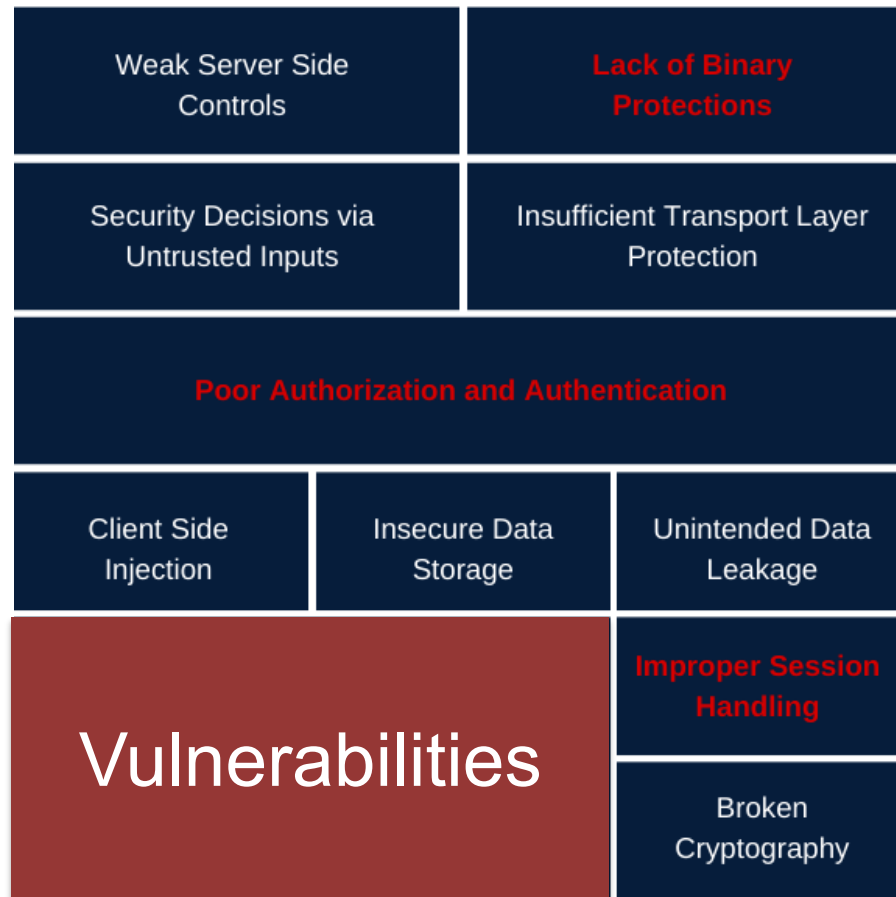
ITU Digital Finance & Inclusion Journey



Tech Watch Report Mobile Money

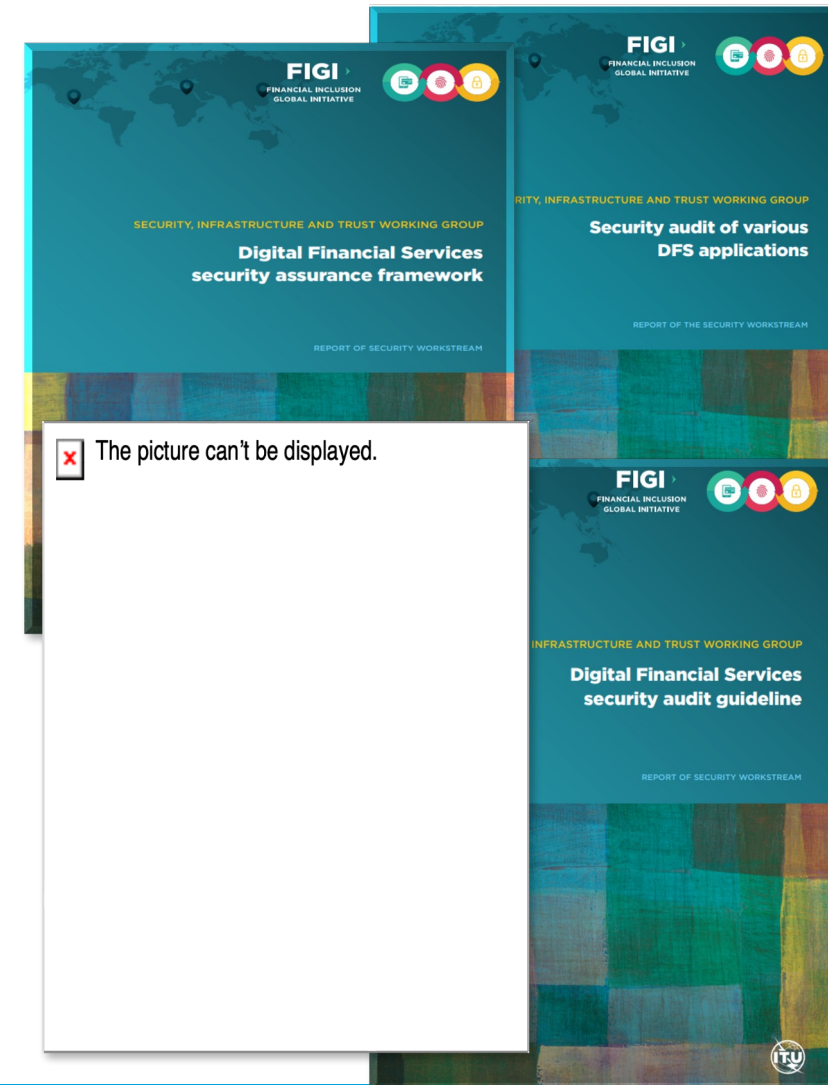


DFS security challenges for regulators



DFS Security Reports

1. [Mitigating SS7 Vulnerabilities](#)
2. [DFS Security Assurance Framework](#)
3. [Security testing for USSD and STK based DFS applications](#)
4. [Security audit of various DFS applications](#)
5. [DFS security audit guideline](#)
6. [DFS Consumer Competency Framework](#)

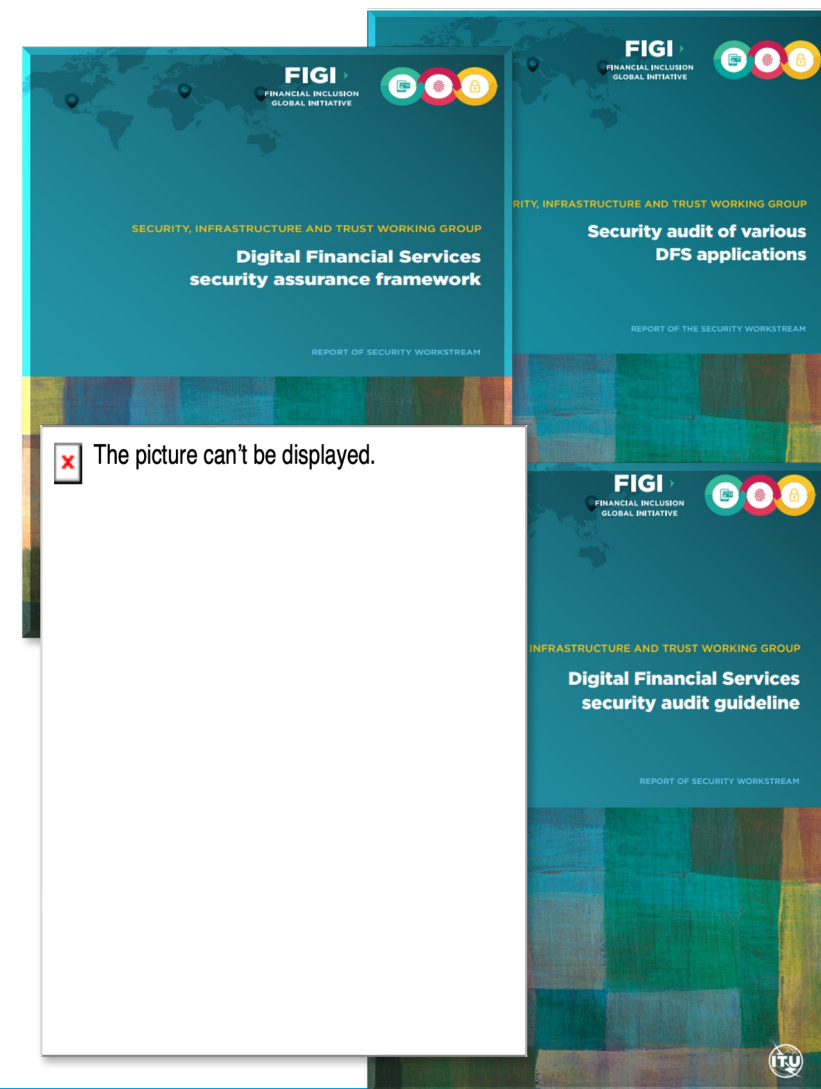


See <https://figi.itu.int/figi-resources/working-groups/>

DFS Security Recommendations

The [DFS Security Recommendations](#) contain the following specific guidelines that may be adopted by regulators.

1. Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security
2. Security recommendations to protect against DFS SIM related risks like SIM swap fraud and SIM recycling
3. Recommendations to mitigate SS7 vulnerabilities
4. Mobile Application Security Best practices
5. [DFS Consumer Competency Framework](#)

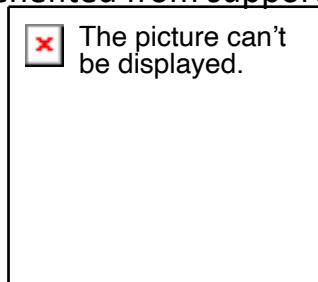


See <https://figi.itu.int/figi-resources/working-groups/>

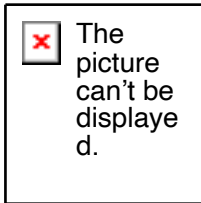
DFS Security Lab

Provides a standard methodology based on OWASP Mobile Top 10 Security Risks to conduct security audit for mobile payment apps and verify compliance against security best practices and standards.

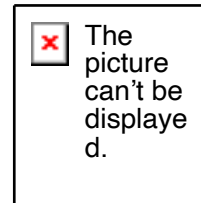
Benefited from support of



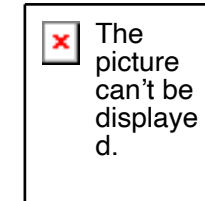
DFS Security Lab - Objectives



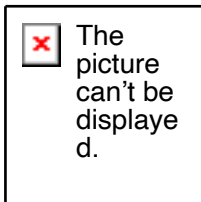
Collaborate with regulators to adopt DFS security recommendations from FIGI



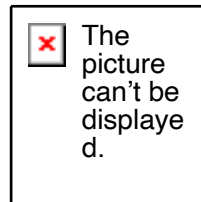
Perform **security audits** of mobile payment apps (USSD, Android and iOS)



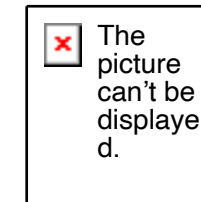
Encourage adoption of **international standards on DFS security and participate in ITU-T SG17**



Organise **security clinics & Knowledge transfer** for Security Lab



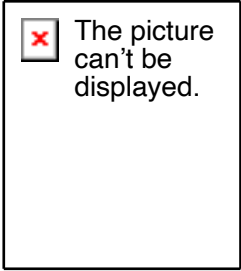
Assist regulators to **evaluate the cyberresilience of DFS critical infrastructure**



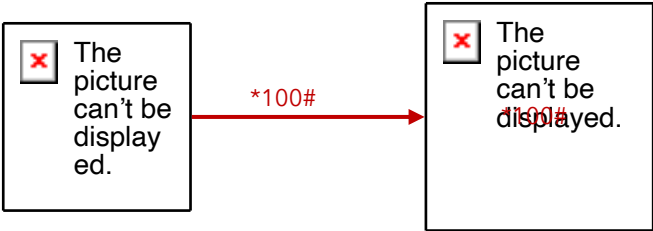
Networking platform for regulators for knowledge sharing on threats and vulnerabilities

Testing security of mobile payment apps

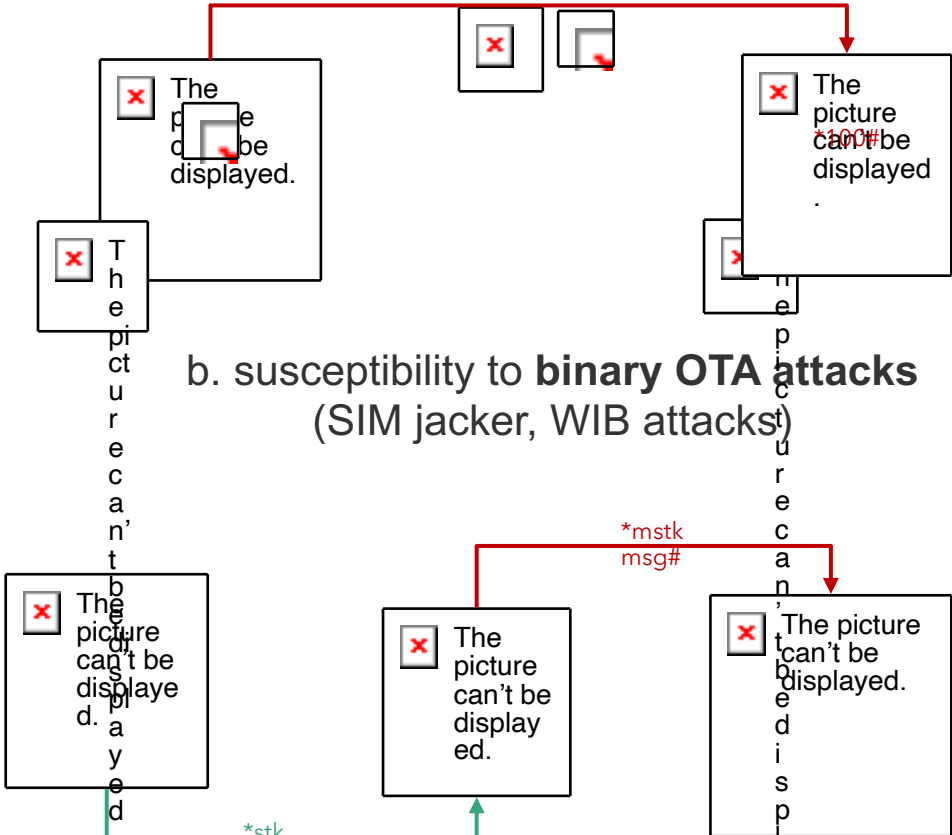
USSD & STK tests



a. SIM Swap and SIM cloning



c. remote USSD execution attacks



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

Based on OWASP Mobile
Top 10 Security Risks 2016

DFS Security Lab – Assistance for developing countries

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 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


 The picture can't be displayed.

Questions

 The picture can't be displayed.

Contact: dfssecuritylab@itu.int

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

 The picture can't be displayed.