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 tests
- 6. DFS Security Lab Knowledge Transfer phases
- 7. Actions being implemented



ITU DFS Security Lab

1. ITU & Digital Finance













2010-2012

ITU DFS Security Lab











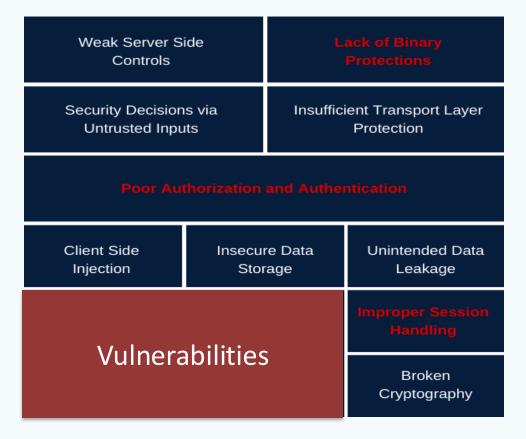








2. DFS application security challenges for regulators





3. DFS Security Lab

Set up and managed by TSB

Objective

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

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 - 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. <u>Security testing for USSD and STK based DFS applications</u>
- 3. <u>Security audit of various DFS applications</u>
- 4. DFS security audit guideline
- 5. DFS Consumer Competency Framework



Adoption of DFS Security Recommendations

The recommendations contain the following specific guidelines that may be adopted by regulators.

- 1. Recommendations for regulators to mitigate SS7 vulnerabilities
- 2. <u>Security recommendations to protect against DFS SIM risks and SIM swap fraud</u>
- 3. <u>Mobile Application Security Best practices</u> (From <u>ITU-T X.1150</u> Section 9)
- 4. <u>Template for a Model MOU between a Telecommunications</u>

 <u>Regulator and Central Bank on Digital Financial Services Security</u>
- 5. DFS consumer competency framework



International Telecommunication Union

Standardization Sector

Recommendation

ITU-T X.1150 (03/2024)

SERIES X: Data networks, open system communications and security

Secure applications and services (I) – Application Security (I)

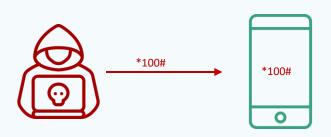
Security assurance framework for digital financial services

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

5. USSD & STK security audit tests



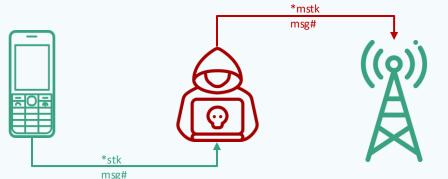
a. SIM Swap and SIM cloning



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 mobile payment app security audit tests

- M1: Improper Credential Usage
- M2: Inadequate Supply Chain Security
- M3: Insecure Authentication/Authorization
- M4: Insufficient Input/Output Validation
- M5: Insecure Communication
- M6: Inadequate Privacy Controls
- M7: Insufficient Binary Protections
- M8: Security Misconfiguration
- M9: Insecure Data Storage
- M10: Insufficient Cryptography



6. DFS Security Lab Knowledge Transfer phases

ITU has a knowledge transfer programme for regulators to verify the security assurance of mobile payment applications based on Android, iOS, and USSD.

The objective is to empower the staff of the regulator to be able to conduct the security tests and adopt the DFS security recommendations.

01

Phase 1

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

Phase 2

02

- Select mobile payment app to be tested during the knowledge transfer
- Security walkthroughs online workshops

Phase 3

03

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

Phase 4

04

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

7. ITU Cyber Security Resilience Assessment toolkit for DFS Critical Infrastructure





Assessing cyber resilience

Risk Management

Governance

Testing

Training and Awareness

Incident Response





The process related to the efficient implementation of risk assessment and treatment activities. These processes allow DFS entities and relevant third-parties to structure and update mechanisms to anticipate, evaluate and mitigate risks, ensuring critical resiliency



The framework for DFS entities to achieve strategic and resiliency objectives. DFS entities' governance bodies define strategic objectives and prorates to address critical resiliency and ensure a robust cyber resilience approach implementation to face prevailing and emerging cyber-focused threats



The use of a wide range of cyber resilience assessment tools and techniques to understand how effective the entity's cybersecurity capabilities and measures implemented are in preventing and defending against malicious cyber-threat actors



The process that provides participants with an overview of strategies, approaches, and procedures in place within a DFS entity. Such processes aim to upskill staff to a predetermined understanding of a given matter



The ability of an entity to handle cybersecurity incidents. This includes policies and strategies that structure the incident response process and required cybersecurity capabilities to prevent, detect, manage and recover from ICTrelated incidents

- Risk Assessment
- Asset Management
- Risk Treatment
- Monitor and Review

- Roles and Responsibilities
- Communication Channels
- · Availability of Official Documentation
- Monitoring and Review Processes

- **Red Teaming**
- Penetration Testing
- Vulnerability Assessment
- Simulations and War Gaming

- **Employee Training**
- Information-Sharing **Practices**

- Incident Response Life Cycle
- Protection
- Incident Response Governance
- Incident Response Reporting



Technical assistance for Cyber Resilience Assessment toolkit

Technical assistance for regulators to facilitate cyber resilience self-assessments and enhance the resiliency of the Digital Financial Services (DFS) infrastructure.



Phase 1: Planning and Focal Point Identification (Month 1-2)

- First meeting
- Identify Focal Points
- Identify Critical Infrastructure for DFS
- Identify Key Personnel
- ITU Mission for the capacity building
- Briefing of the critical infrastructure service providers identified

Phase 2: Explaining the Cyber resilience assessment toolkit with a tabletop exercise. (Month 3-4)

- Phase 3 planning
- Capacity building on the cyber resilience assessment toolkit
- Knowledge transfer for the regulator on filling out and evaluating a real case questionnaire for the cyber resilience

Phase 3: Cyber resilience Assessment of Critical Infrastructure (Month 4-5)

- Coordination with the service providers to respond to the questionnaire for the cyber resilience assessment and assist wherever necessary.
- Analysis of the responses received.
- Report Preparation and review
- Communication of results
- Prioritize Enhancements
- Development of Road Map for monitoring cyber resilience of DFS

Phase 4: Roadmap for Cyberresilience and follow up (Duration: 12 months after phase 3)

- Coordination meetings for roadmap implementation.
- Second cyber resilience assessment after 1 year.

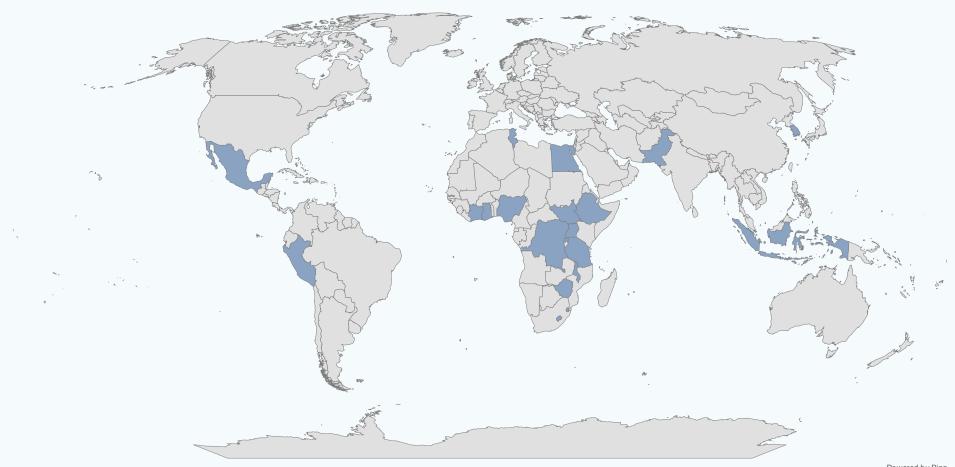


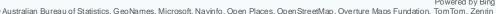
7. Actions being implemented

- 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, Indonesia).
- 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

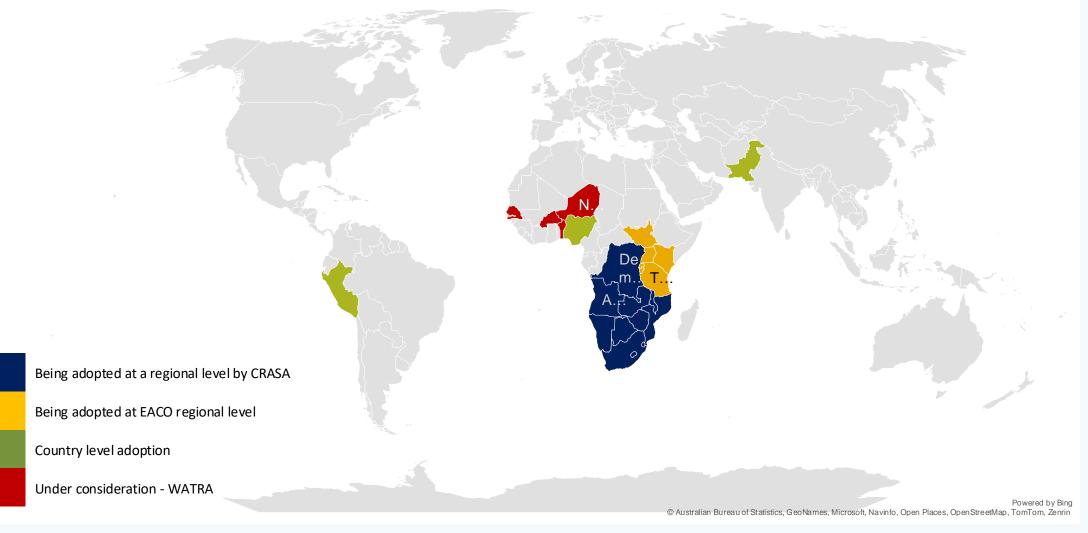






ITU DFS Security Lab

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

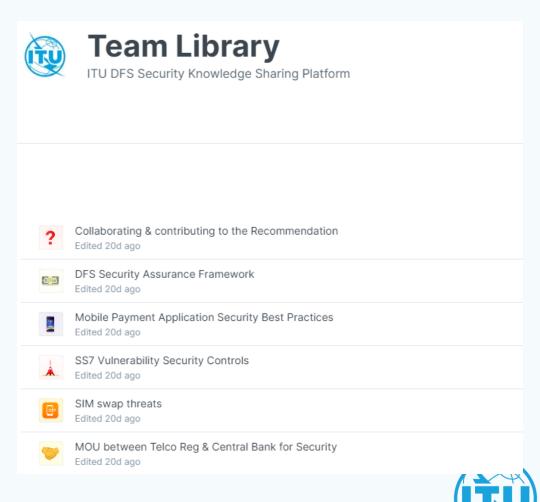


ITU DFS Security Lab

How to register to the ITU Knowledge Sharing Platform for Digital Finance Security

Scan qrcode to go to registration page







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

Contact: dfssecuritylab@itu.int



Thank you!