# ITU Digital Financial Services Security Lab

Arnold Kibuuka

Project Officer, ITU



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



### **Overview**

- 1. ITU & Digital Finance
- 2. DFS 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. Cyber Security Resilience Assessment toolkit for DFS Critical Infrastructure
- 8. Actions being implemented



# 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

## **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.



## 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 <u>DFS</u> <u>security recommendations</u>



Organize security clinics & Knowledge transfer for Security

Lab



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



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



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



Networking platform for regulators for knowledge sharing on threats and vulnerabilities

## 4. DFS Security Recommendations

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

- 1. Recommendations to mitigate SS7 vulnerabilities
- 2. <u>Security recommendations to protect against DFS SIM related risks</u>
  (ITU-T X.1456)
- 3. DFS Mobile application security Best practices (From ITU-T X.1150)
- 4. <u>Template for a Model MOU between a Telecommunications</u>

  Regulator and Central Bank related to DFS Security
- 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)

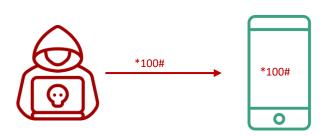
## Security assurance framework for digital financial services



## 5. USSD & STK Security Audit Tests



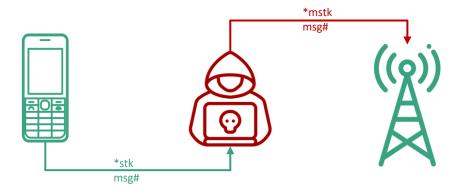
a. SIM Swap and SIM cloning



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. ITU DFS Security Lab Knowledge Transfer Phases

The 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.



#### Phase 1

- Regulator identifies Lab team
- Regulator ensures equipment in place
- DFS Security Clinic Share recommendations on Digital Finance

#### Phase 2

- Select mobile payment app to be tested during the knowledge transfer
- Security walk throughs for testing manuals
- Verify equipment is configured

#### Phase 3

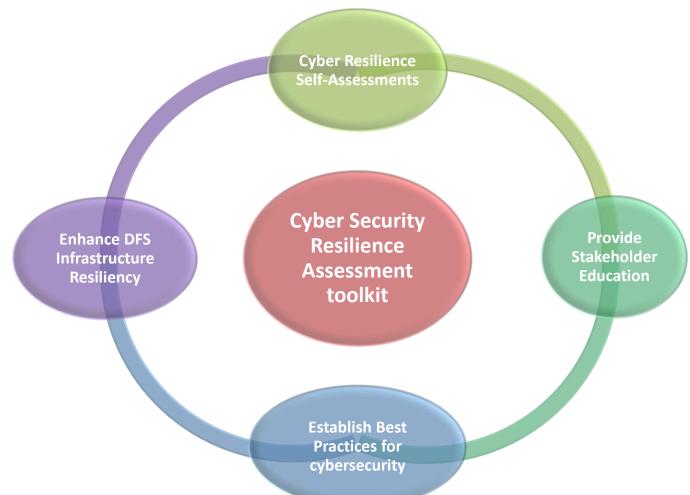
- Organize training on iOS, Android and USSD security testing
- Independent testing by Lab team
- Report on testing done.

#### Phase 4

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

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

## 7. ITU Cyber Security Resilience Assessment Toolkit for DFS Critical Infrastructure



Risk Management

4

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

resiliency

- Asset Management
- Risk Treatment
- Monitor and Review

### Assessing cyber resilience

Governance

Testing

Training and Awareness

**Incident Response** 



to achieve strategic and

resiliency objectives. DFS

entities' governance bodies

prorates to address critical

cyber resilience approach

implementation to face

cyber-focused threats

prevailing and emerging

define strategic objectives and

resiliency and ensure a robust

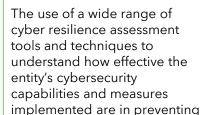
Roles and Responsibilities

Communication Channels



The framework for DES entities





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

mitigate risks, ensuring critical

- · Availability of Official Documentation
  - Monitoring and Review Processes

- **Red Teaming**
- **Penetration Testing**

and defending against

- **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**



## 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.



## **Cyber Security Resilience Assessment Toolkit**

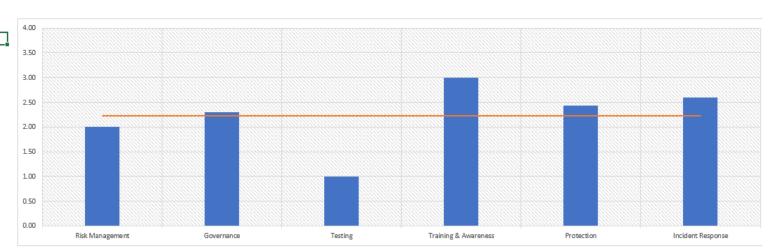


#### **Results Summary**

This section provides an overview of the results and lays the foundation for a mitigation roadmap to be identified, structured, and presented to the decision-maker. All results presented here aggregate the sub-pillars of each methodological question. For a more granu results, the user is advised to review the results in the radar charts section

Resiliency Level
2.00
2.30
1.00
3.00
2.44
2.60







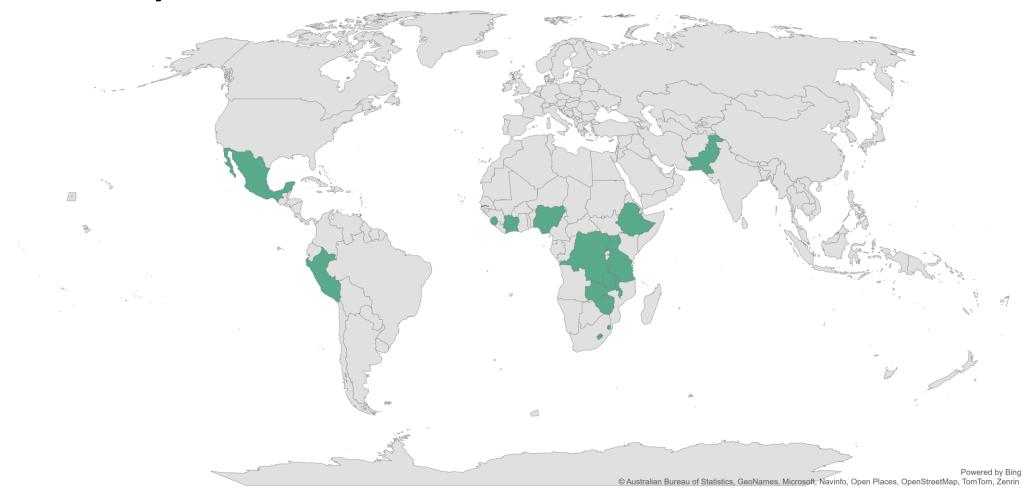
http://www.itu.int/go/dfssl

## 7. Actions Being Implemented

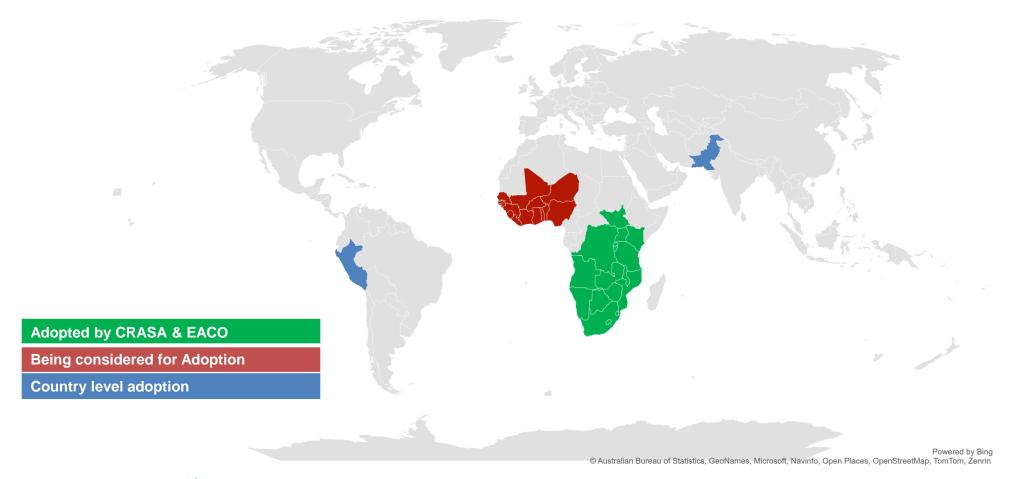
- 1. Organizing of <a href="DFS Security clinics">DFS Security clinics</a> with a focus on knowledge sharing on DFS security recommendations
- 2. Knowledge transfer for regulators (Tanzania, St. Lucia, Antigua and Barbuda, Uganda, Peru, Zimbabwe, South Sudan, Ghana, The Gambia and Ethiopia)
- 3. Supporting regulators on implementing DFS security recommendations
- 4. Conducting security audits of mobile payment applications (conducted tests for Zambia, Zimbabwe, DRC, The Gambia, Peru, Tanzania, 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**



## **Countries and Regions Adopting the Recommendations**





## **ITU Knowledge Sharing Platform for DFS**

### **Objective**

- 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.

How to join the knowledge sharing platform





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

Contact: <a href="mailto:dfssecuritylab@itu.int">dfssecuritylab@itu.int</a>

Thank you!