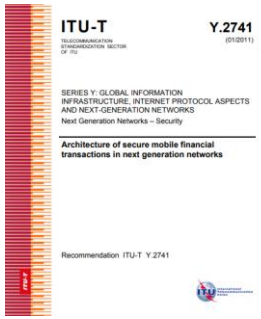
ITU Digital Financial Services Security Lab

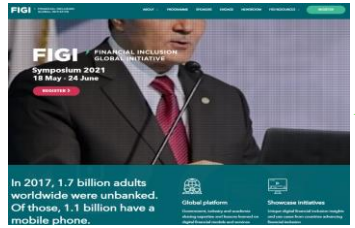
Vijay Mauree
Programme Coordinator
Standardization Bureau, ITU

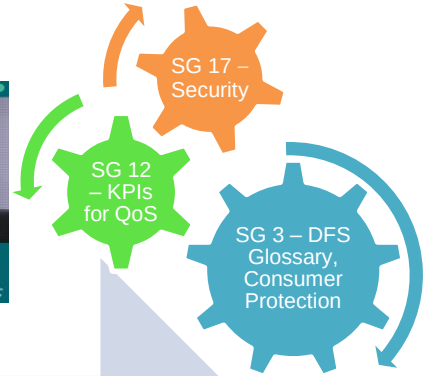
Overview

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

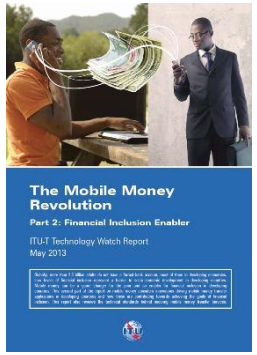
ITU Digital Finance & Inclusion Journey



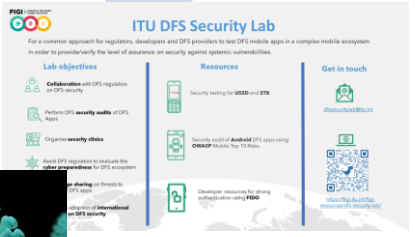




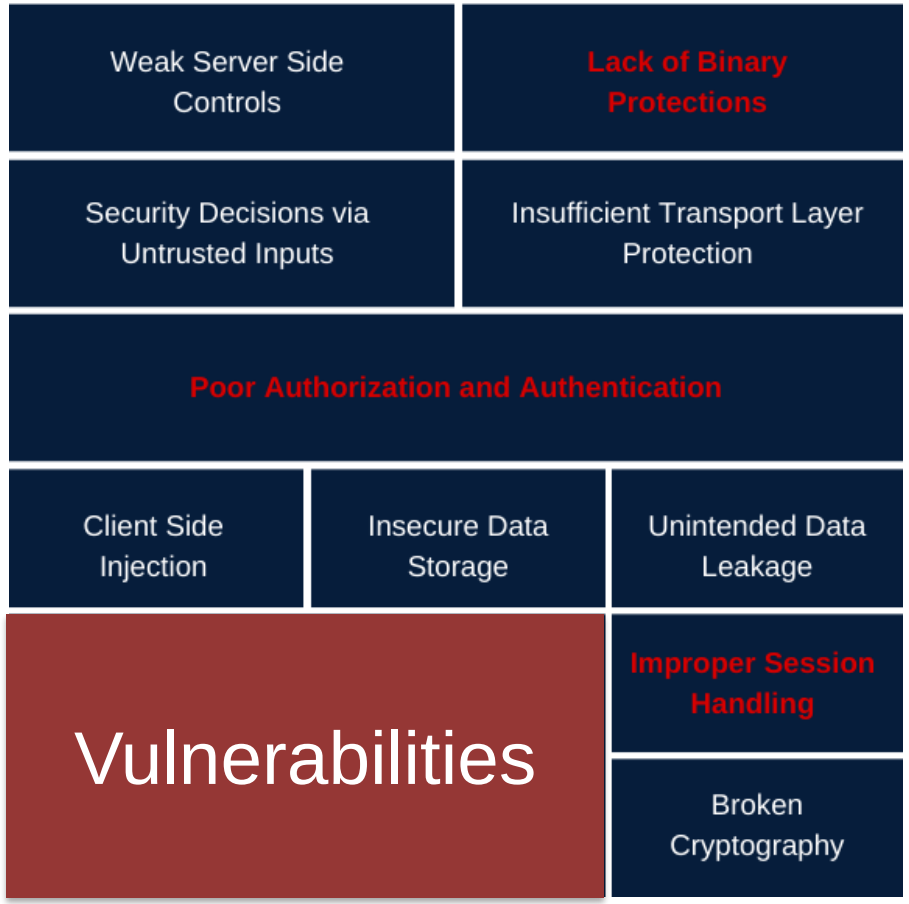
2010-2012 | 2013 | 2014 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023



Tech Watch Report Mobile Money



DFS security challenges for regulators



DFS Security Lab

- Cybersecurity capability of regulators
- Security audit of mobile payment applications
- Adoption of security best practices for digital finance

DFS Security 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

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. Security recommendations to protect against DFS SIM related risks like SIM swap fraud and SIM recycling
2. Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security
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

과학기술정보통신부
Ministry of Science and ICT

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

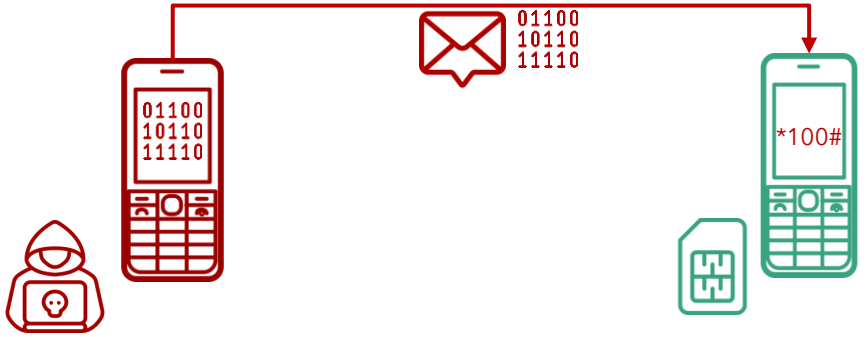
Assist regulators to **evaluate** the **cyberresilience of DFS critical infrastructure**

Networking platform for regulators for knowledge sharing on threats and vulnerabilities

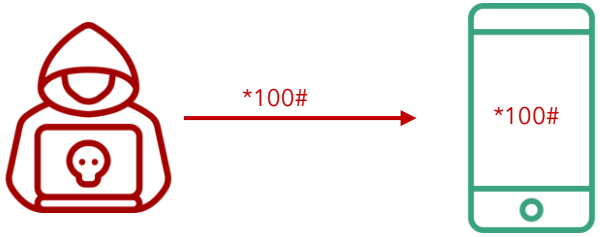
Testing security of mobile payment apps

USSD & STK tests

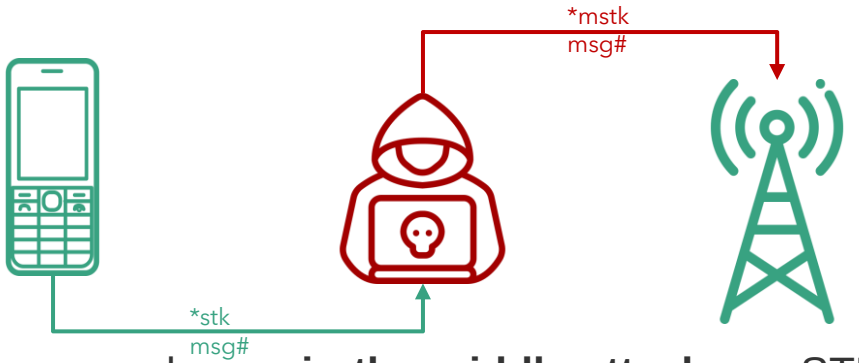
a. **SIM Swap** and **SIM cloning**



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

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

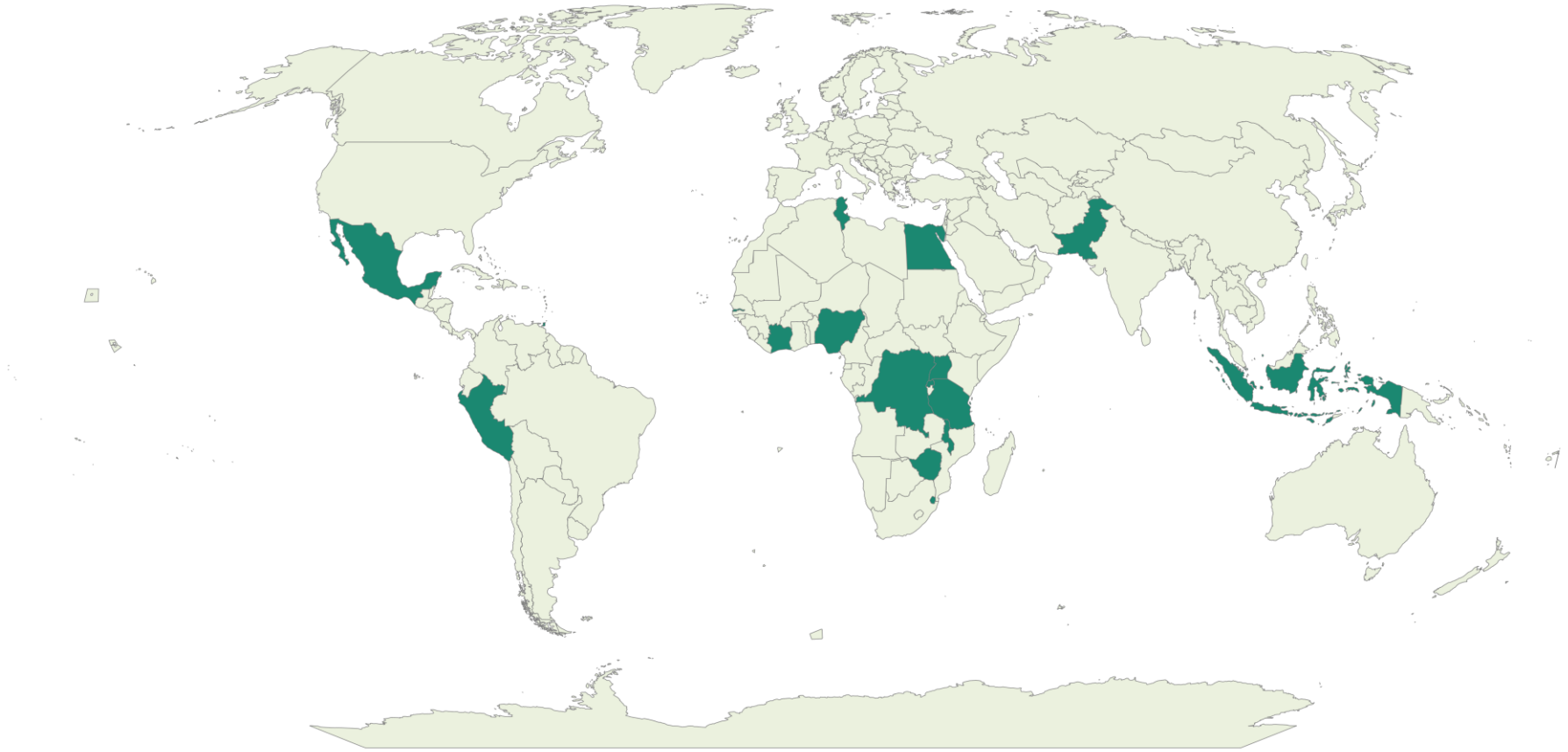
- Select mobile payment app
- Security walkthroughs online workshops

Phase 3

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

Phase 4

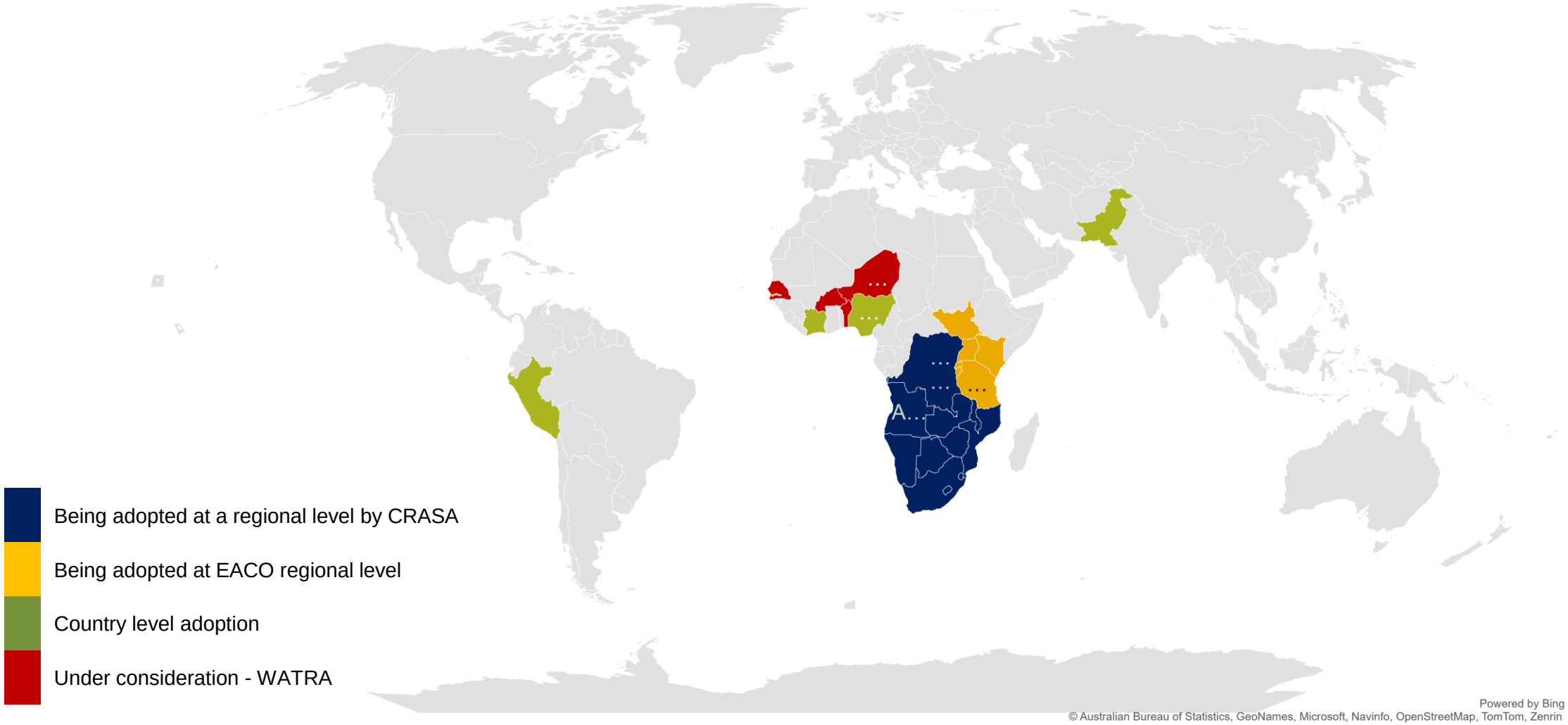
- 6-9 months period of oversight by ITU
- Mobile payment app testing reviewed by ITU
- Lessons learned of new threats and vulnerabilities



DFS security clinics held in 2022, 2023

Security Clinics were held in some 18 countries

Countries and Regions adopting the recommendations



ITU DFS Security Recommendations

Vijay Mauree
Programme Coordinator
Standardization Bureau, ITU

DFS Security Recommendations

1. SIM related risks like SIM swap fraud and SIM recycling
2. Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security
3. Mitigate SS7 vulnerabilities
4. Mobile Application Security Best practices
5. DFS Consumer Competency Framework

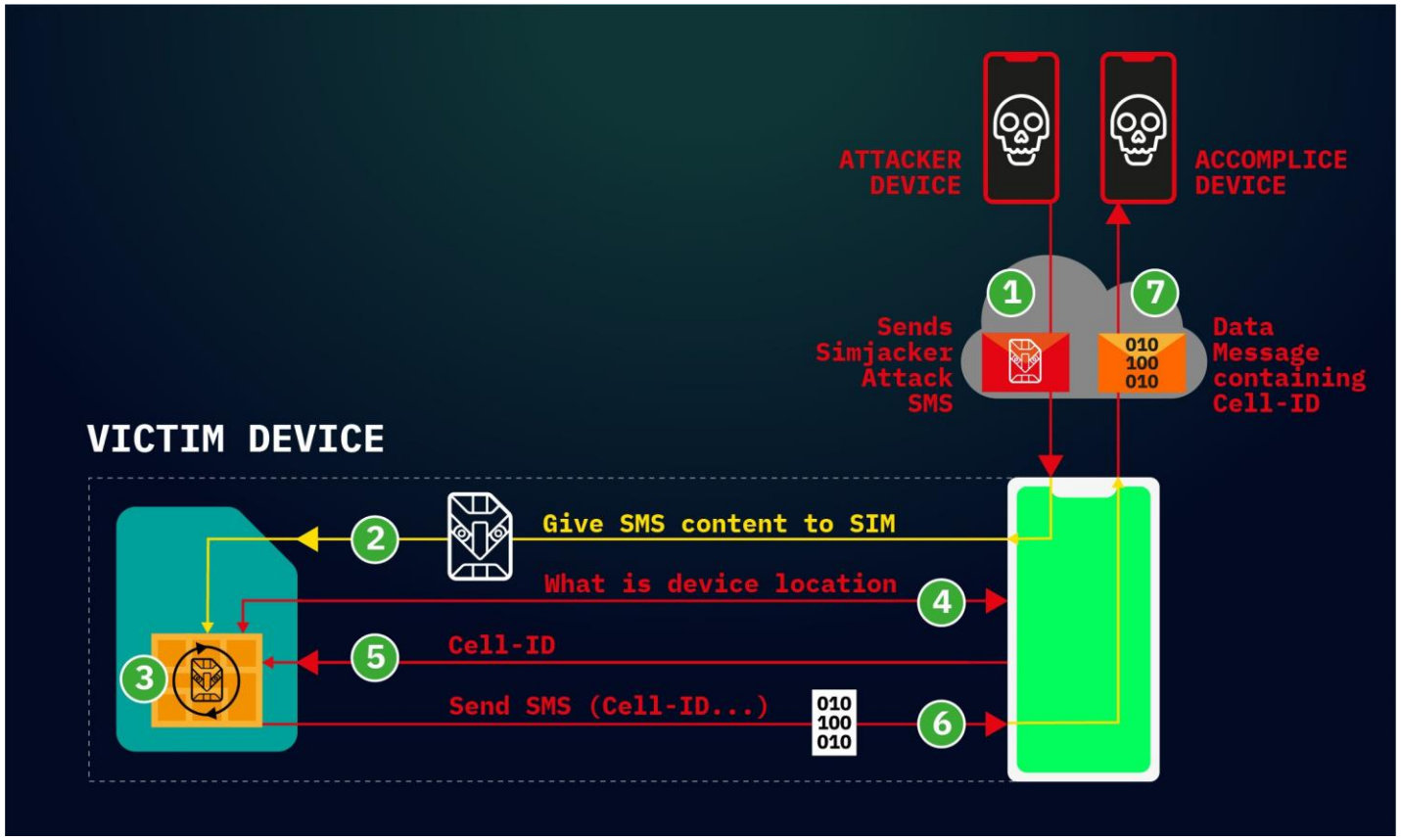
Access Recommendations Here

Regulatory guidance to mitigate SIM risks

Related report:
Security testing for USSD and STK based DFS applications

SIM risks

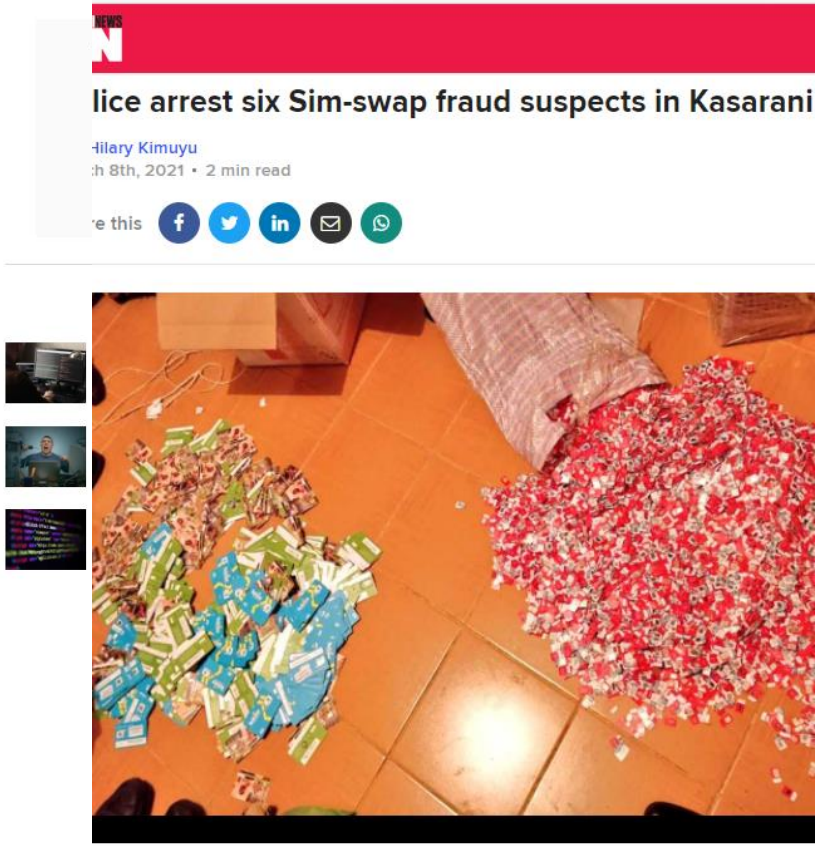
1. SIM Cloning
2. SIM Swaps
3. SIM Recycling
4. Binary over the air attacks (Sim jacker and WIB browser attacks)



Source: adaptive mobile

Examples of DFS attacks

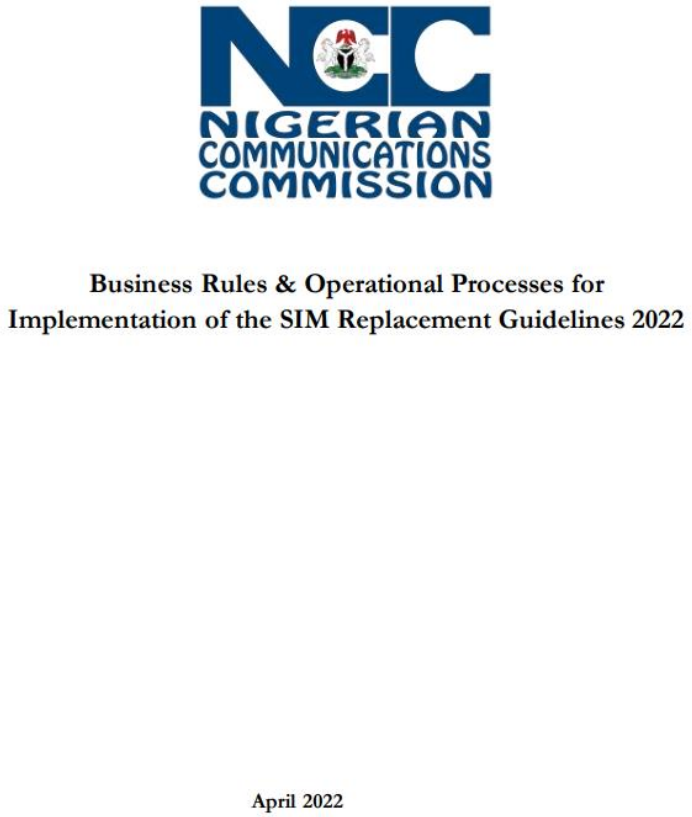
Source: znet



Source: Nairobi News

- March 2021, Times Of India, **2 duped of Rs 82k in SIM swap fraud**
- March 2021, Nairobi News: **Police arrest six Sim-swap fraud suspects in Kasarani**
- The Daily Monitor: **Thieves use 2,000 SIM cards to rob banks**
- Ghana Chamber of Telecommunications: **Mobile Money Fraudsters Now Target Bank Accounts Linked To MoMo Accounts**
- February 2021, CNN: **Police arrest eight after celebrities hit by SIM-swapping attacks**

Regulatory Guidance to mitigate SIM risks



a. Regulatory coordination between telco and DFS regulator on SIM vulnerabilities.

   - e.g. An MOU between the DFS regulator and Telco regulator

b. Standardization by regulators of SIM swap rules amongst MNOs/MVNOs

c. Recommending security measures for DFS operators on SIM risks.

Source: NCC

MOU between the Central bank and Telco regulator

- A bilateral Memorandum of Understanding (MOU) related DFS should be in place between the telecommunications regulator and the central bank.
- The MOU would identify clearly the responsibilities of the central bank and Telco regulator for security of DFS (for example in the area of SIM swap fraud, SS7, consumer protection etc.)
- The MOU should include modalities around the creation of a Joint Working Committee on DFS security and risk-related matters.

MNO controls on SIM swaps (SIM swap rules for MNOs and MVNOs)

a. Where SIM replacement is carried out by proxy, the MNO/MVNO or its agents must capture a biometric, facial image of the proxy which must be kept for a specified period.

b. MNOs should notify DFS providers on swapped SIMs, ported and recycled numbers.

c. SIM swap notifications to users

d. Biometric SIM swap verification

e. Multifactor user validation before SIM swap

f. Secure SIM data protection

g. Holding time before activation of a swapped SIM

h. Service support representatives training

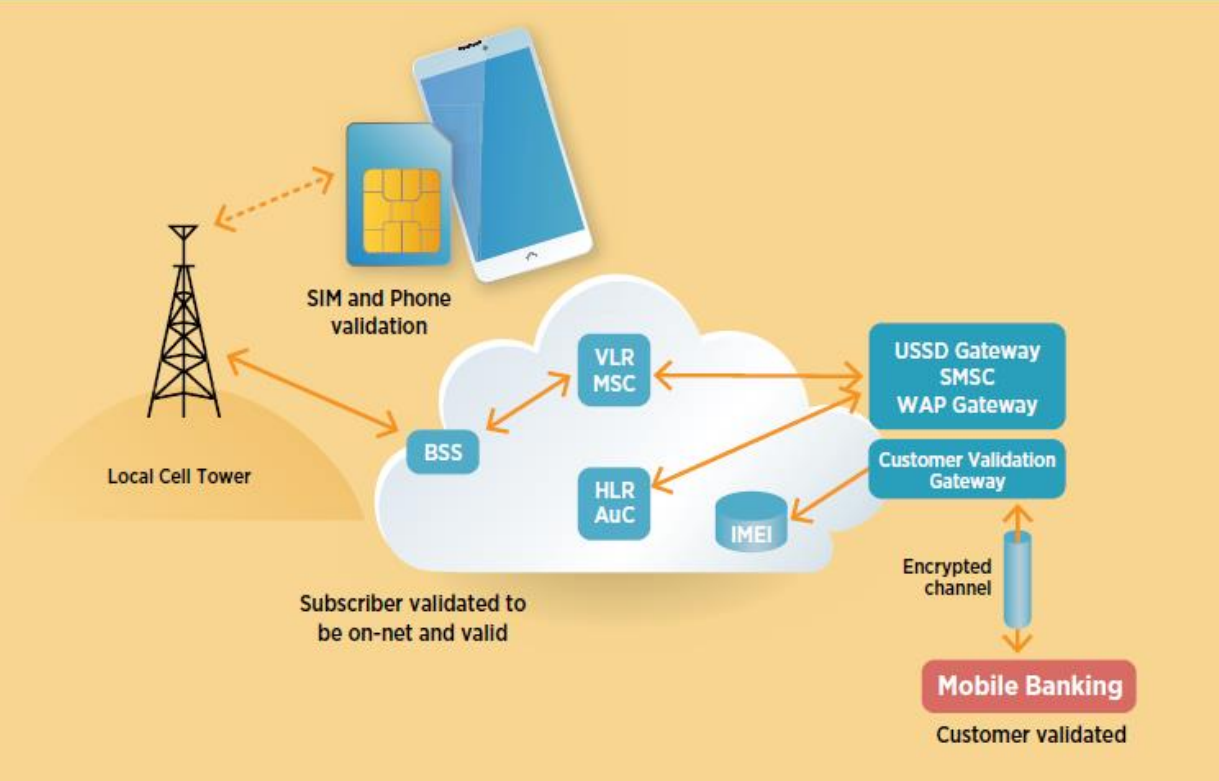
DFS operators controls to mitigate SIM swaps

a. Real time IMSI/ICCID detection

b. Real time device change detection – device to DFS account binding

c. Encourage use of secure DFS access through apps.

IMSI validation gateway



Architectural implementation of IMSI validation gateway.
Source: ITU Report on SS7

Category: PREMIUM

API Name	API Definition
Sim Swap API	API which allows a corporate customer to check if a given MSISDN has performed a SIM swap. Returns 'MSISDN',' date of last SIM swap'
Authentication API	API which allows a corporate customer to use MTN Service to send OTPs . A customer is onboarded on the MTN instance and the OTP service is configurable to them
KYC Premium API	API allows a customer to check if the KYC info provided by its customers matches with that provided at Sim registration. Returns one or more actual customer details. This requires customer consent

Example implementation of IMSI validation gateway by MTN.
source: MTN website

An IMSI validation gateway can be used to ensure to FSPs and banks that the real, registered customer is using the system via **USSD to detect USSD interception**.

Guidance to mitigate SS7 threats

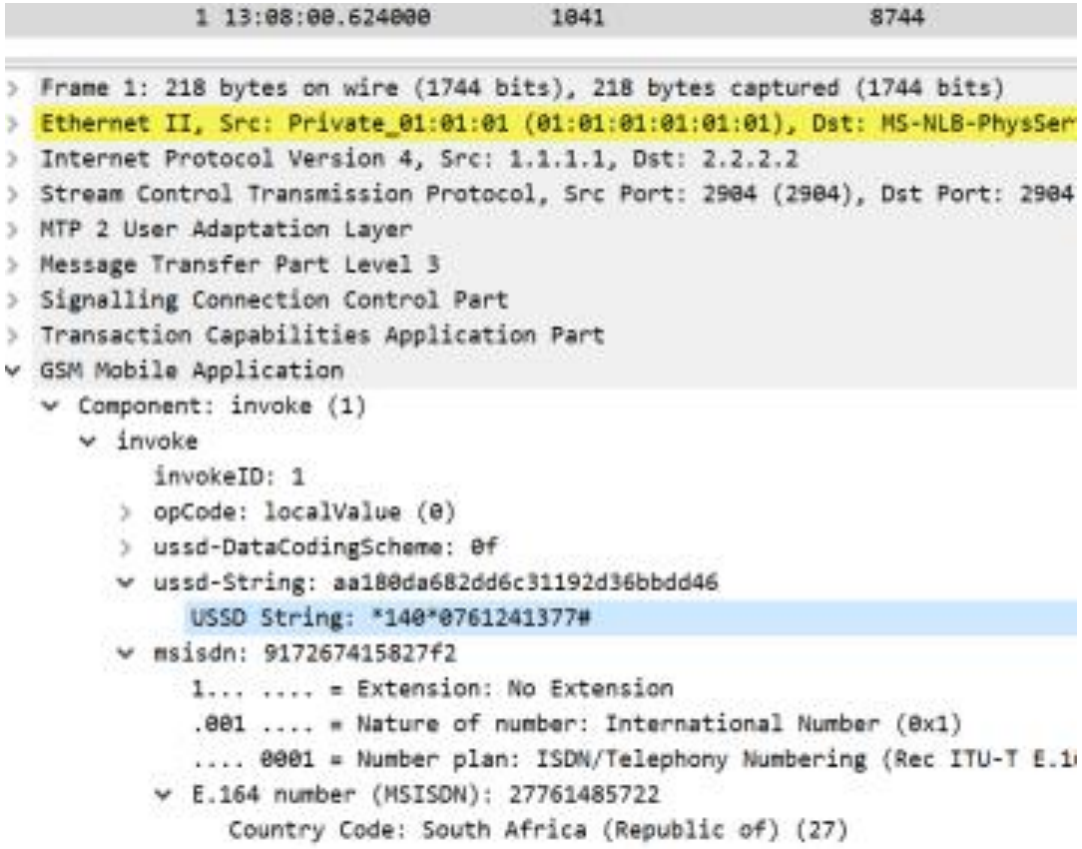
Related report:
Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions

Regulatory Guidance to mitigate SS7 risks

- Regulatory coordination between telco and DFS regulator on SS7 vulnerabilities.
- Incentivize the industry
- Education for telecom and financial services regulators on SS7 vulnerabilities and impact to DFS
- Telecom regulators to establish baseline security measures for each SS7 risk category
- IMSI validation gateway: An API that provides status of a mobile number and real time country where client is located,

Recommendations for MNO to mitigate SS7 risks

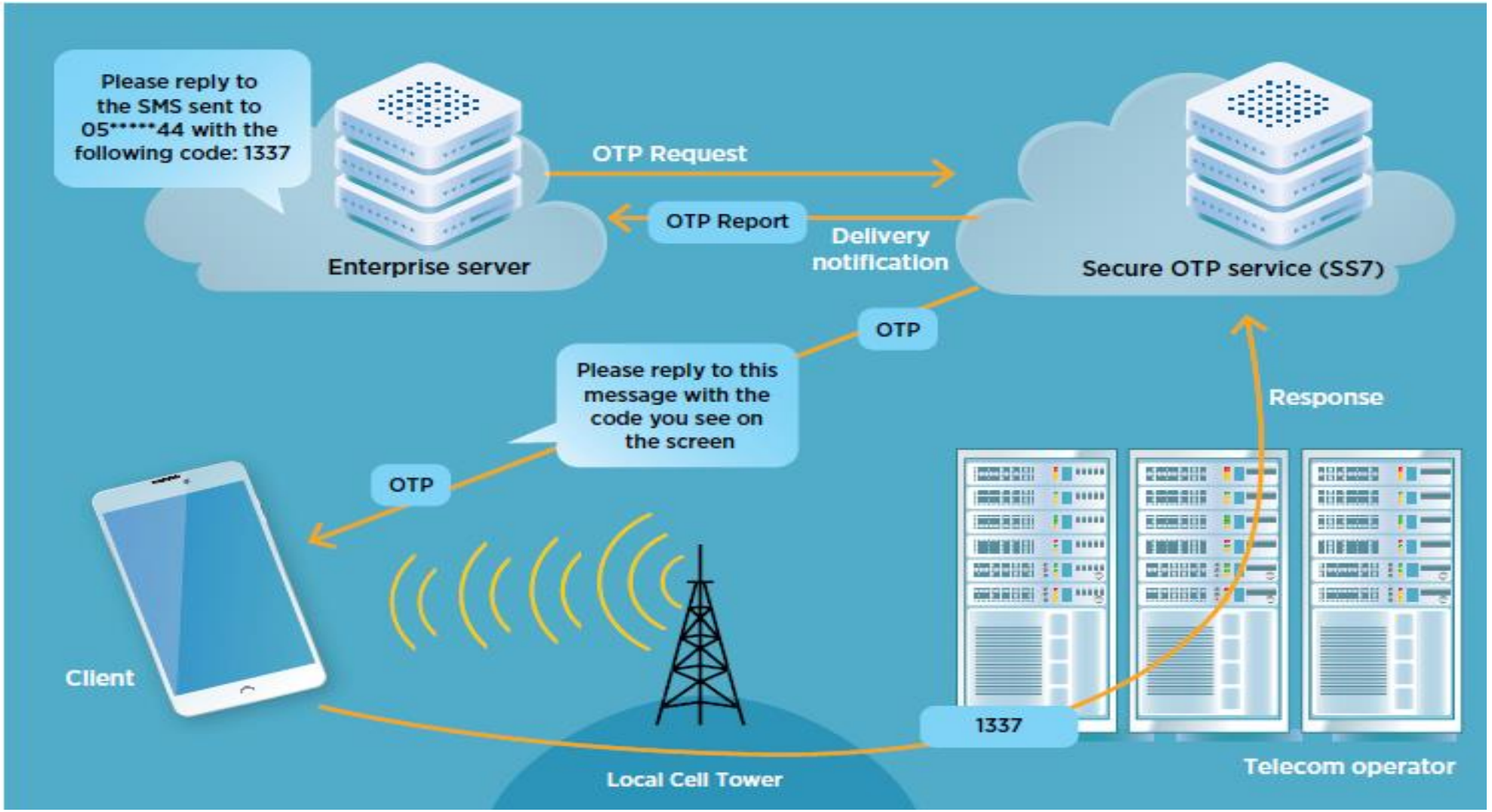
- Session time out
- USSD PIN masking
- Secure and monitor core network traffic
- Limit access to traces and logs
- SMS filtering
- SMS home routing



DFS operator controls to mitigate SS7 risks

- Session time out for USSD, STK and OTP SMS for DFS
- Transaction limits for insecure channels (e.g USSD)
- User education
- Detecting and mitigating social engineering attacks with USSD
- Bidirectional OTP SMS flow

Bidirectional OTP SMS flow



Mobile Payment App Security framework

Related report: DFS Security Assurance Framework

Mobile Payment App Security Framework

- Draws upon:
    - GSMA study on mobile money best practices,
    - ENISA smartphone security development guidelines,
    - State Bank of Pakistan mobile payment applications security framework
- Template can be used as input to an app security policy by DFS providers to provide minimum security baselines for app developers and DFS providers as well as setting criteria for verifying compliance of apps
- Template considerations:
    i. device and application integrity.
    ii. communication security and certificate handling.
    iii. user authentication.
    iv. secure data handling.
    v. secure application development.

Mobile Application Security best practices

Device and Application Integrity

Use platform services for integrity checks;

remove extraneous code

maintain high-integrity state server-side.

Communication Security and Certificate Handling

Standardized cryptographic libraries

up-to-date TLS certificates;

Use strong cipher suites

limit certificate lifetimes (825 days);

contingency for untrusted CA; secure TLS configuration;

certificate pinning recommended;

correct server certificate validation by user device.

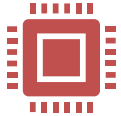
User Authentication

Disallow easily guessable credentials;

encourage multi-factor authentication;

prefer authenticator apps over SMS for OTPs;

secure storage of biometric information.



Secure Data Handling

Secure storage of confidential info;

trusted hardware for sensitive data;

avoid external storage;

Disable screenshots;

clean caches/memory;

`fine-grained permissions for data sharing;

avoid hard-coding sensitive info;

validate client input for database storage.

Secure Application Development

Adhere to secure coding practices and standards;

provide secure application updates;

regular internal or external code reviews.

Mobile Application Security -> OWASP Mobile Top 10

Device and Application Integrity

T1.2 Android:debuggable

`T1.4 Dangerous permissions

T8.1 The application should refuse to run on a rooted device

Communication Security and Certificate Handling

T3.1 Application should only use HTTPS connections

T3.2 Application should detect Machine-in-the-Middle attacks with untrusted certificates

T3.3 Application should detect Machine-in-the-Middle attacks with trusted certificates

T3.4 App manifest should not allow clear text traffic

T5.1 The app should not use unsafe crypto primitives

T5.2 The HTTPS connections should be configured according to best practices

T5.3 The app should encrypt sensitive data that is sent over HTTPS

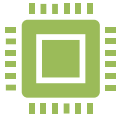
User Authentication

T4.1 Authentication required before accessing sensitive information

T4.2 The application should have an inactivity timeout

T4.3 If a fingerprint is added, authentication with fingerprints should be disabled

T4.4 It should not be possible to replay intercepted requests



Secure Data Handling

T1.1 Android:allowBackup

T1.3 Android:installLocation

T2.1 Android.permission.WRITE_EXTERNAL_STORAGE

T2.2 Disabling screenshots

Secure Application Development

T9.1 The code of the app should be obfuscated

Mobile Payment App Security Best Practices

- Can be adopted as technical guideline or regulation for mobile payment app security
- Provides a minimum security baseline that developers need to adhere to for building security in mobile payment applications
- Compliance can be verified using the security tests developed by the DFS Security Lab

DFS Consumer Competency Framework

Related Report: DFS Consumer Competency Framework

Objectives

1. **Digital Transaction Engagement:** Enable consumers to confidently engage in financial transactions using digital channels.

2. **Informed Decision-Making:** Empower consumers to make informed choices and thoroughly understand pricing, terms, and conditions.

3. **Safety and Fraud Avoidance:** Equip consumers to operate safely, circumventing fraudulent or deceptive marketing practices.

Objectives

4. **Data Privacy Comprehension:** Ensure consumers understand the risks of failing to protect data privacy within digital financial services.

5. **Grievance Redress Mechanisms:** Guide consumers to effectively engage with grievance redress and recourse mechanisms in case of discrepancies.

6. **Competencies for Vulnerable Populations:** Identify and build necessary skills for vulnerable groups (e.g., women, youth, elderly, disabled) to facilitate informed, safe, and confident use of DFS.

Consumer Competences & DFS Transaction Lifecycle

1. **Pre-transaction Phase**
    - When the consumer is contemplating the use of DFS services.
    - **Important Skills/Knowledge**: Understanding of service offerings, pricing, and benefits; comparison of providers.
2. **Transaction Phase**
    - Engaging with the service provider and using or purchasing the financial service.
    - **Important Skills/Knowledge:** Understanding of the transaction process; knowledge of potential risks and safeguards.

Consumer Competences & Transaction Lifecycle

3. Post-transaction Phase

- Includes engagement with the provider for quality assurance or redress when the Quality of Service (QoS) was not up to standards.
- **Important Skills/Knowledge:** Understanding of rights and obligations; ability to seek redress.

15 Core competences

DFS transaction Phase	Competences
Pre-transaction (CA1)	CA 1.1 Search for information about costs, quality and terms of conditions of the service.
	CA 1.2 Compare information on costs, quality and terms of conditions of the service.
	CA 1.3 Evaluate the commercial information provided and suitability for purpose.
	CA 1.4 Manage digital identity and credit profile.
	CA 1.5 Understand how to access digital financial service in a secure manner.
	CA 1.6 Understand what is personal data and the related risks to personal data.
Transaction (CA2)	CA 2.1 Understand how an electronic payment is initiated using digital channels[15] and the conditions for the transactions to be completed (i.e. receiver receives payment).
	CA 2.2 Make payments and accessing finance through digital channels.
	CA 2.3 Understand the terms and conditions of the DFS provider, including related costs and risks.
	CA 2.4 Manage personal data and privacy.
	CA 2.5 Protect health and safety.
Post-transaction (CA3)	CA 3.1 Share information with the service providers (i.e. feedback) and other consumers online.
	CA 3.2 Know consumer rights and how to obtain redress.
	CA 3.3 Know the responsible regulator to approach with intractable problems and the mechanism for doing so.
	CA 3.4 Keep up to date on developments in digital financial services.

Knowledge, skills and proactive step

1.1 Search for information about cost, quality and terms of conditions of the service To search for and access information related to digital finance. To know where to obtain the information needed regarding the various cost (direct and indirect) options for a DFS provider service and the terms and conditions of the service.	
Knowledge area	CA1.1-K1 Recognize that consumers should understand the exact costs (both direct and indirect) and evaluate affordability for using the service if they want to bear these costs before engaging in the transaction. [For gender sensitivity: Include also information about the relevance of the digital financial inclusion service product]. CA1.1-K2 Understand that they need to read, watch, listen and comprehend the DFS provider terms and conditions, including steps to use before accepting to use the service. CA 1.1-K3 Differentiate the selected product from similar products. CA 1.1-K4 Understand the audio or visual medium used for advertising the product or service.
Skills area	CA1.1-S1 Know how to identify the costs for using the service. CA1.1-S2 Know whether the terms and conditions stated are fair to consumers and legislation in place. CA 1.1-S3 Know how to compute the cost of the service. CA 1.1-S4 [For gender sensitivity: Know the range of financial products and services women can access from the DFS provider].
Proactive steps	CA1.1-P1 Search for information about the costs for the service in the appropriate locations. CA1.1-P2 If unsure, contact the DFS provider consumer information contact to obtain relevant information or if necessary, the appropriate regulator. CA1.1-P3 Contact other users of the DFS service to confirm the cost and terms of conditions. CA1.1-P4 Take advice from consumer advocacy organizations about costs, terms and conditions and service provision of service provider. CA1.1-P5 Searching and analysing different DFS options and comparing them with available savings and desired objective to be met by DFS service providers.

Consumer Competency Framework

1. Identifies consumer competences according to the DFS transaction cycle
2. For each competence, the skills and knowledge required by the consumer is identified and outlined
3. Provides a curriculum outline for regulators and DFS providers for use in their DFS user awareness programmes.

Questions

Contact: dfssecuritylab@itu.int

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