

ITU Initiatives

Digital financial services security lab

itu.int/go/dfs




ITU DFS Security Recommendations

Arnold Kibuuka
Project Officer
Standardization Bureau, ITU

ITU DFS Security Recommendations

- [Recommendations for regulators to mitigate SS7 vulnerabilities](#)
- [Security recommendations to protect against DFS SIM risks and SIM swap fraud](#)
- [Mobile Payment Application security best practices](#)
- [Template for a Model MOU between a Telecommunications Regulator and Central Bank on Digital Financial Services Security](#)
- [DFS consumer competency framework](#)

 Times of India

10 hack man's mobile phone, withdraw money

Police have booked 10 persons accused of duping a 61-year-old man of Rs 35 lakh in a case of cyber fraud. The accused hacked his mobile...

1 month ago

 Techish Kenya

MTN, Airtel & Stanbic 'lose Billions' in Uganda Mobile Money Hack

MTN, Airtel & Stanbic 'lose Billions' in Uganda Mobile Money Hack. Pegasus Source: techjaja.com.

6 Oct 2020

 PML Daily

Police detectives grill two Pegasus Technologies employees over Oct. 3 major mobile money hack

KAMPALA — Two prime suspects in connection with a major hack carried out on MTN, Airtel Uganda and two banks Stanbic and Bank of Africa...

11 Oct 2020

 WeeTracker

Multiple Kenyan Digital Services Knocked Offline Amid Hack Fears

On Thursday, M-Pesa, the prominent digital payment system run by Kenya's leading telecoms company Safaricom, went down mysteriously.

27 Jul 2023

Google news search

 Daily Nation

Bomet SIM swap fraud: Ten suspects arrested

The suspects had 14 unused SIM cards, nine used Safaricom SIM cards and 11 national identity cards.

1 month ago

 Telecompaper

Digi Spain fined another EUR 200000 in SIM swap fraud case

Spain's data protection authority (AEPD) has fined Digi Spain a total of EUR 200000 for failing to apply adequate verification procedures to...

5 Dec 2023

 Phone Arena

SIM swap costs woman \$17K in scam you need to watch out for

A Verizon customer was scammed out of \$17000 by a thief ripping her off by using her phone number to obtain a new SIM card.

1 week ago

 Australian Broadcasting Corporation

Medion Australia hit with \$260,000 fine after SIM-swapping scam leads some telco customers to lose thousands

Authorities say nine customers had their SIM cards illegally swapped without them knowing, and five of them together lost more than \$160000.

3 weeks ago

 Kenya Broadcasting Corporation

1. MOU between the Central bank and Telco regulator

- Bilateral.
- Includes responsibilities of the central bank and Telco regulator on DFS Security(e.g. SIM swap fraud, SS7, consumer protection, QoS etc.)
- A Joint Working Committee on DFS security and risk-related matters.

2. Security recommendations to protect against DFS SIM risks

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

SIM Swap

SIM Cloning

SIM Recycling

Binary over the air attacks



Business Rules & Operational Processes for
Implementation of the SIM Replacement Guidelines 2022

April 2022

Source: NCC

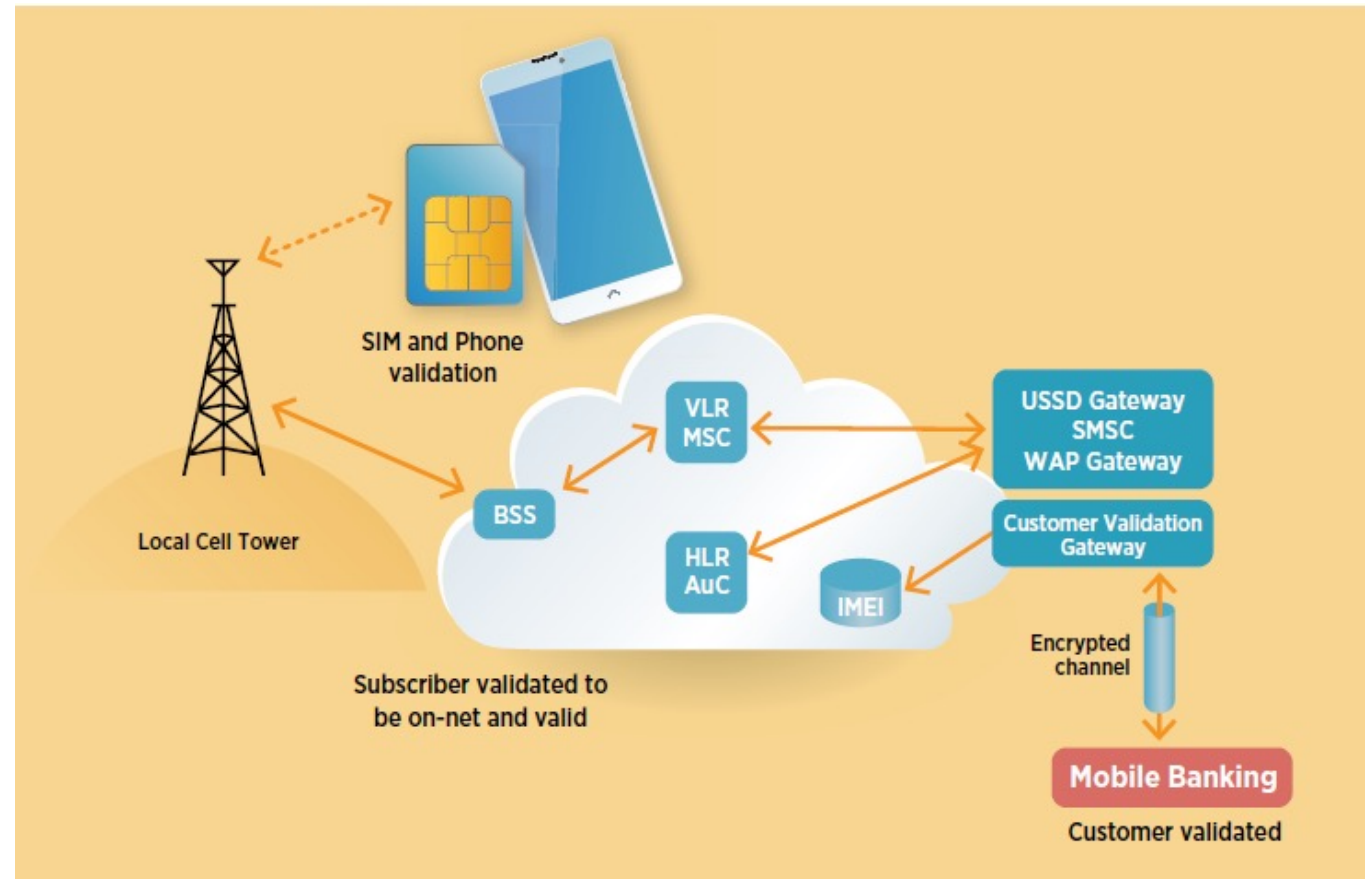
Regulatory Guidance to mitigate SIM risks

- 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.

Recommendations contain

- MNO controls on SIM swaps
- DFS operators controls to mitigate SIM swaps

IMSI validation gateway



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

3. Recommendations to mitigate SS7 vulnerabilities

Related report:

[Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions](#)

| 1 | 13:08:00.624000 | 1041 | 8744 |
|---|---|------|------|
| > | Frame 1: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) | | |
| > | Ethernet II, Src: Private_01:01:01 (01:01:01:01:01:01), Dst: MS-NLB-PhysSer | | |
| > | Internet Protocol Version 4, Src: 1.1.1.1, Dst: 2.2.2.2 | | |
| > | Stream Control Transmission Protocol, Src Port: 2904 (2904), Dst Port: 2904 | | |
| > | MTP 2 User Adaptation Layer | | |
| > | Message Transfer Part Level 3 | | |
| > | Signalling Connection Control Part | | |
| > | Transaction Capabilities Application Part | | |
| ∨ | GSM Mobile Application | | |
| ∨ | Component: invoke (1) | | |
| ∨ | invoke | | |
| | invokeID: 1 | | |
| > | opCode: localValue (0) | | |
| > | ussd-DataCodingScheme: 0f | | |
| ∨ | ussd-String: aa180da682dd6c31192d36bbdd46 | | |
| | USSD String: *140*0761241377# | | |
| ∨ | msisdn: 917267415827f2 | | |
| | 1... = Extension: No Extension | | |
| | .001 = Nature of number: International Number (0x1) | | |
| | 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.1) | | |
| ∨ | E.164 number (MSISDN): 27761485722 | | |
| | Country Code: South Africa (Republic of) (27) | | |

Regulatory Guidance to mitigate SS7 risks

- Regulatory coordination (telco and DFS)
- Incentivize the industry
- Sensitization
- Baseline security measures on SS7.

4. Mobile Payment App Security Best Practices

Related report:
[Security testing for USSD and STK based DFS applications](#)



Circulars/Notifications - Payment System Department

PSPOD Circular No 01 of 2022

April 26, 2022

The Presidents/CEOs
All Banks/ MFBs/ PSOs/ PSPs/ EMIs

Dear Sir/Madam,

Mobile Applications (Apps) Security Guidelines

Mobile payment applications (mobile apps) have become an alternate payment channel for a growing number of users. SBP regulated entities have been offering innovative products and services through mobile applications. Consequently, opportunities for the fraudsters to exploit vulnerabilities in mobile apps and defraud the customers have also increased manifold.

2. In line with international standards and best practices, SBP has developed comprehensive Mobile App Security Guidelines (the "Guidelines") providing baseline security requirements for app owners in order to ensure confidentiality and integrity of customer data and availability of app services in a secure manner, when developing payment applications for mobile or other smart devices.

3. App owners shall use these Guidelines for the architecture, design, development and deployment of mobile payment apps and associated environment that consumers use for digital financial services.

4. App owners shall ensure that their mobile apps and associated infrastructure are compliant with the requirements of these Guidelines latest by December 31, 2022.

Enclosure: Mobile Applications (Apps) Security Guidelines

Yours sincerely,

Sd/-

(Shoukat Bizinjo)
Additional Director

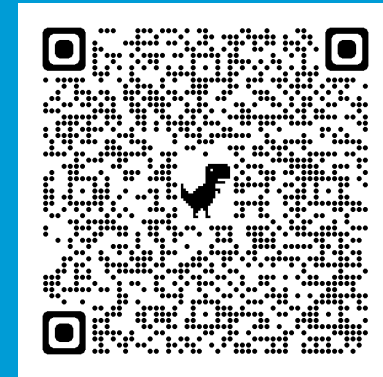
Mobile Payment App Security Best Practices

Considerations:

- i. device and application integrity.
- ii. communication security and certificate handling.
- iii. user authentication.
- iv. secure data handling.
- v. secure application development.

5. DFS Consumer Competency Framework

- Guide for policymakers, national regulators, and DFS providers.
- For developing consumer awareness and literacy programs.
- Identifies competencies (knowledge areas, skills and attitudes) for safe engagement of users in DFS.



Contact: dfssecuritylab@itu.int

