

DFS Security recommendations for regulators and providers

Arnold Kibuuka, Project Officer, ITU

dfssecuritylab@itu.int

11 April 2024



DFS Security Recommendations

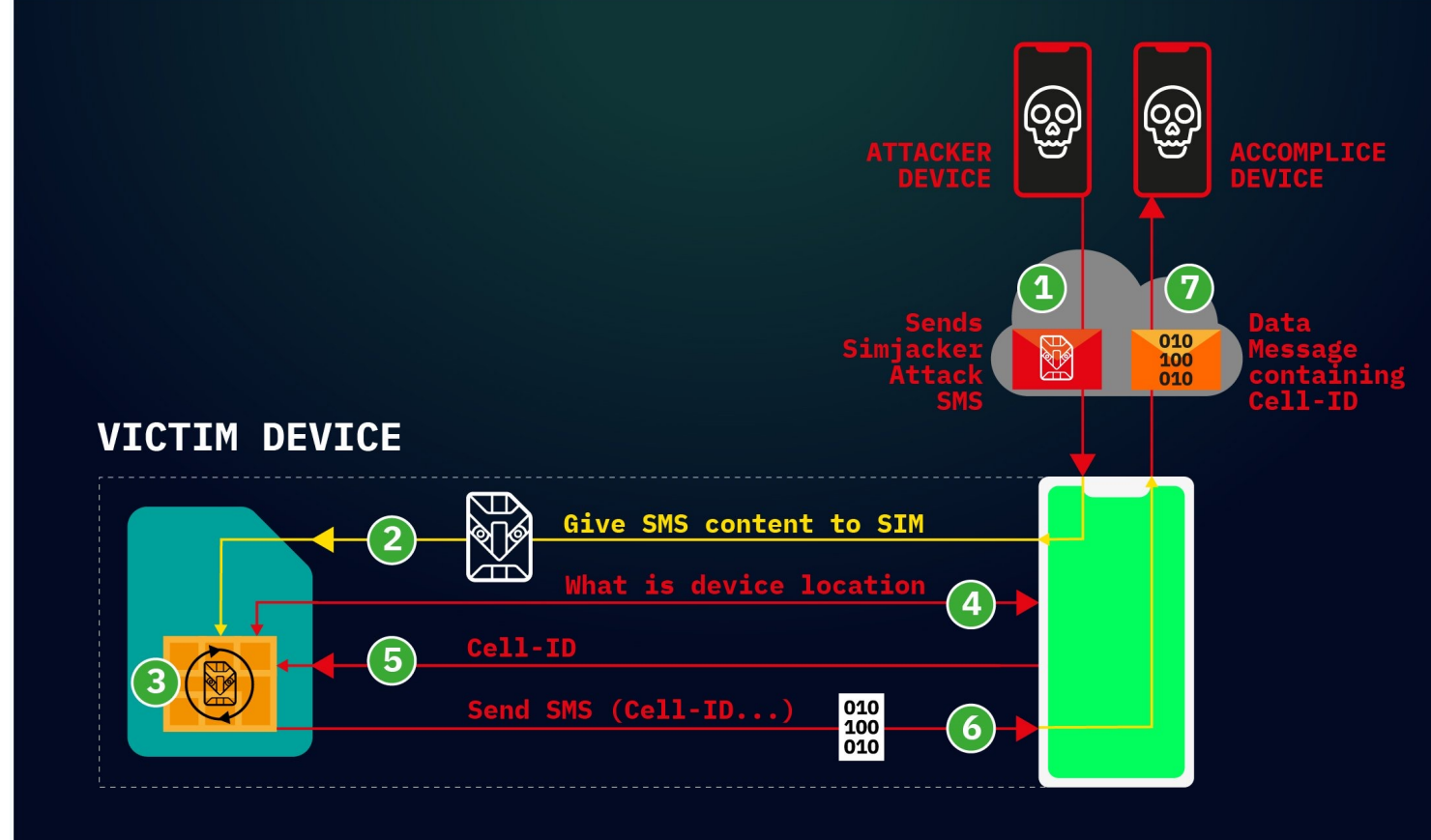
1. [Security recommendations to protect against DFS SIM related risks like SIM swap fraud and SIM recycling](#)
2. [Recommendations to mitigate SS7 vulnerabilities](#)
3. [Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security](#)
4. [Mobile Application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

Regulatory Guidance to mitigate SIM risks

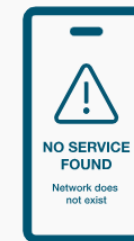
[Related report:
Security testing for USSD and STK based DFS applications](#)

SIM risks

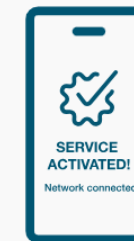
- SIM cloning
- SIM swaps
- SIM Recycling
- Binary over the air attacks (Sim jacker and WIB browser attacks)



Your phone



Attacker's phone



A SIM swap will deactivate your phone, and if done by an attacker, the attacker will receive your calls and texts on their device.

SIM risks

- 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**
- February 2021, CNN: **Police arrest eight after celebrities hit by SIM-swapping attacks**

LEAD STORY ICT

Another suspect in elaborate **Mobile Money and SIM swap fraud** arrested

On Mar 28, 2024



The Economic and Organized Crime Office (EOCO) has arrested another person reportedly involved in a “sophisticated mobile money and sim swap fraud scheme.”

EOCO officials appeared before an Accra Circuit Court and filed an amended charge and facts sheet, after which the court retook the pleas of the

accused persons.

The five accused persons namely Richmond Donkor Alias Chino, Cecilia Asabre, Salifu Eshum, Daniel Asomani Baawiah and Shadrack Anthony alias Target have been jointly charged with conspiracy to steal **GH¢113,947.57.**

Regulatory Guidance to mitigate SIM risks

- Regulatory coordination between telco and DFS regulator on SIM vulnerabilities.
 - e.g. An MOU between the DFS regulator and Telco regulator
- Standardization by regulators of SIM swap rules amongst MNOs/MVNOs
- Recommending security measures for DFS operators on SIM risks.



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

April 2022

Sources: 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.

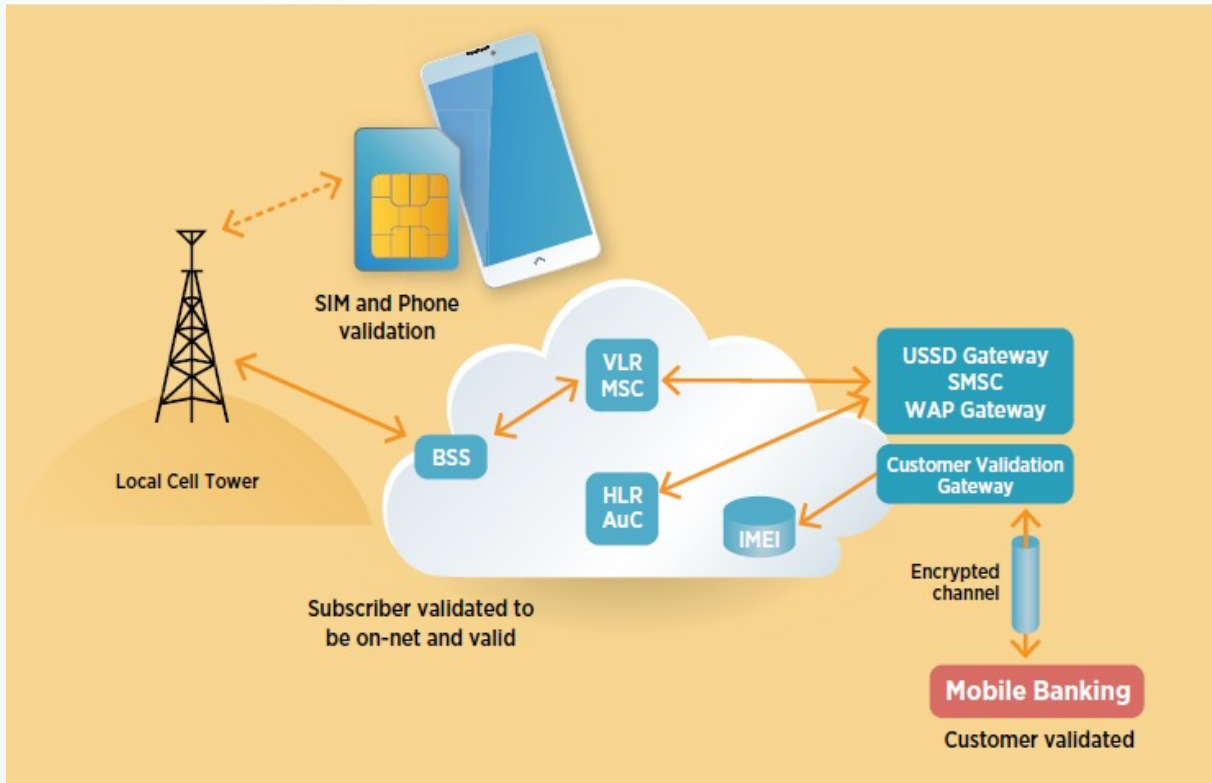
MNO controls on SIM swaps (SIM swap rules for MNOs and MVNOs)

- 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

Guidance to mitigate SS7 threats

Related report:

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



Next

or

Sign Up

```
assaf@DESKTOP-MCKINNK:~$ cd /mnt/c/Work/Vaulto/Vaulto/tests/
```

```
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ clear
```

```
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ python demo_ul_sms_intercept.py 972502138133 ne
```

w

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 number and real time country where client is located,

Recommendations for MNO to mitigate SS7 risks

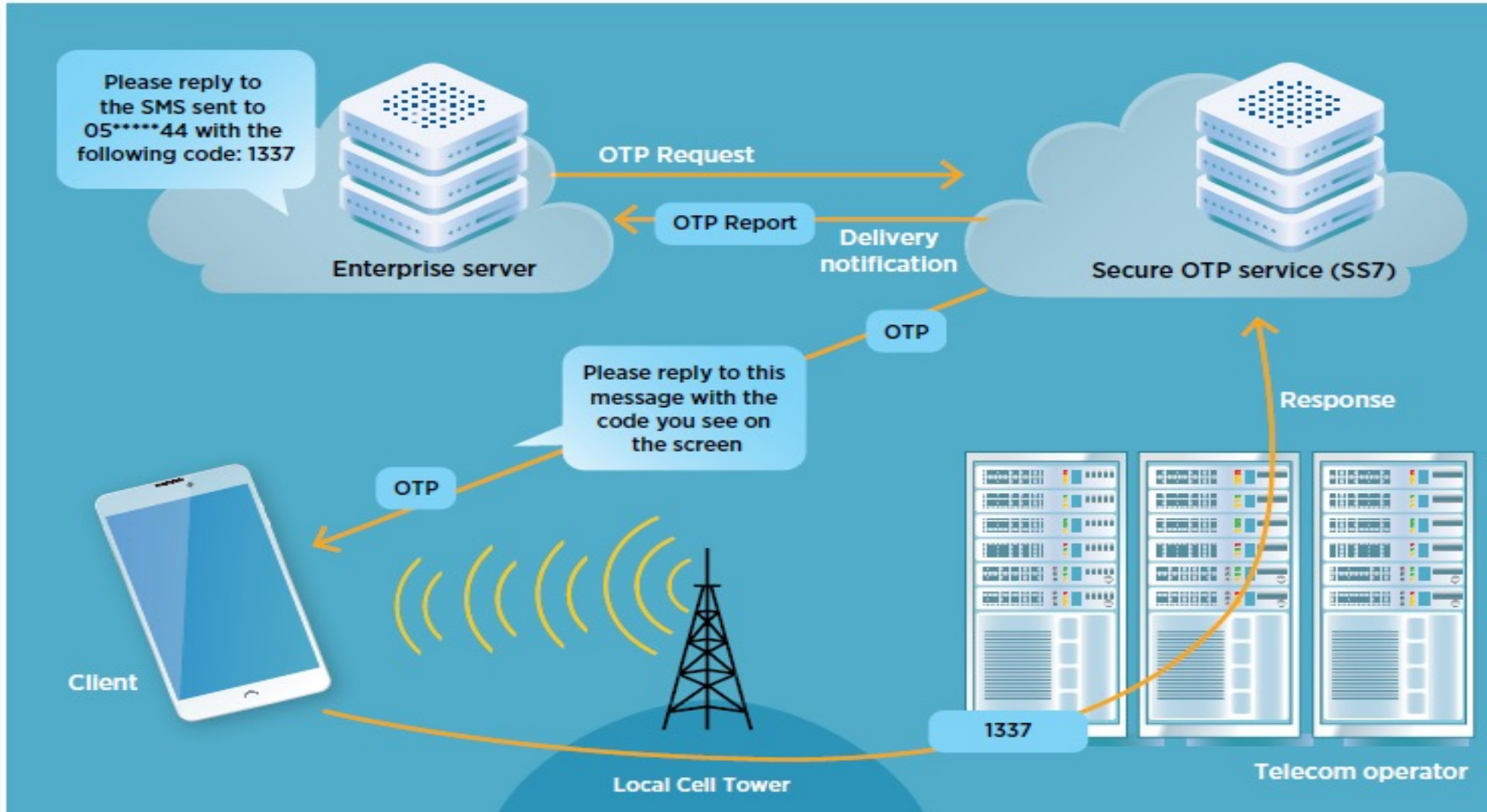
- Session time out
- USSD PIN masking
- Secure and monitor core network traffic
- Limit access to traces and logs
- SMS filtering
- SMS home routing

```
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
v GSM Mobile Application
  v Component: invoke (1)
    v invoke
      invokeID: 1
      > opCode: localValue (0)
      > ussd-DataCodingScheme: 0f
      v ussd-String: aa180da682dd6c31192d36bbdd46
        USSD String: *140*0761241377#
      v msisdn: 917267415827f2
        1... .... = Extension: No Extension
        .001 .... = Nature of number: International Number (0x1)
        .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.1
      v E.164 number (MSISDN): 27761485722
        Country Code: South Africa (Republic of) (27)
```

DFS operator controls to mitigate SS7 risks

- Session time out
- Transaction limits for insecure channels
- User education
- Detecting and mitigating social engineering attacks with MT-USSD and interception of USSD
- Bidirectional OTP SMS flow

Bidirectional OTP SMS flow



DFS Consumer Competence Framework

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

Objectives

1. Digital Transaction Engagement
2. Informed Decision-Making
3. Safety and Fraud Avoidance
4. Data Privacy Comprehension.
5. Grievance Redress Mechanisms.
6. Competencies for Vulnerable Populations

Transaction Phases

1. Pre-transaction Phase
2. Transaction Phase
3. Post-transaction Phase

DFS CCF encompasses 15 core competences

DFS transaction Phase	Competences
Pre-transaction (CA1)	<p>CA 1.1 Search for information about costs, quality and terms of conditions of the service.</p> <p>CA 1.2 Compare information on costs, quality and terms of conditions of the service.</p> <p>CA 1.3 Evaluate the commercial information provided and suitability for purpose.</p> <p>CA 1.4 Manage digital identity and credit profile.</p> <p>CA 1.5 Understand how to access digital financial service in a secure manner.</p> <p>CA 1.6 Understand what is personal data and the related risks to personal data.</p>
Transaction (CA2)	<p>CA 2.1 Understand how an electronic payment is initiated using digital channels¹⁵ and the conditions for the transactions to be completed (i.e. receiver receives payment).</p> <p>CA 2.2 Make payments and accessing finance through digital channels.</p> <p>CA 2.3 Understand the terms and conditions of the DFS provider, including related costs and risks.</p> <p>CA 2.4 Manage personal data and privacy.</p> <p>CA 2.5 Protect health and safety.</p>
Post-transaction (CA3)	<p>CA 3.1 Share information with the service providers (i.e. feedback) and other consumers online.</p> <p>CA 3.2 Know consumer rights and how to obtain redress.</p> <p>CA 3.3 Know the responsible regulator to approach with intractable problems and the mechanism for doing so.</p> <p>CA 3.4 Keep up to date on developments in digital financial services.</p>

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	<p>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].</p> <p>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.</p> <p>CA 1.1-K3 Differentiate the selected product from similar products.</p> <p>CA 1.1-K4 Understand the audio or visual medium used for advertising the product or service.</p>
Skills area	<p>CA1.1-S1 Know how to identify the costs for using the service.</p> <p>CA1.1-S2 Know whether the terms and conditions stated are fair to consumers and legislation in place.</p> <p>CA 1.1-S3 Know how to compute the cost of the service.</p> <p>CA 1.1-S4 [For gender sensitivity: Know the range of financial products and services women can access from the DFS provider].</p>
Proactive steps	<p>CA1.1-P1 Search for information about the costs for the service in the appropriate locations.</p> <p>CA1.1-P2 If unsure, contact the DFS provider consumer information contact to obtain relevant information or if necessary, the appropriate regulator.</p> <p>CA1.1-P3 Contact other users of the DFS service to confirm the cost and terms of conditions.</p> <p>CA1.1-P4 Take advice from consumer advocacy organizations about costs, terms and conditions and service provision of service provider.</p> <p>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.</p>

Mobile Payment App Security framework

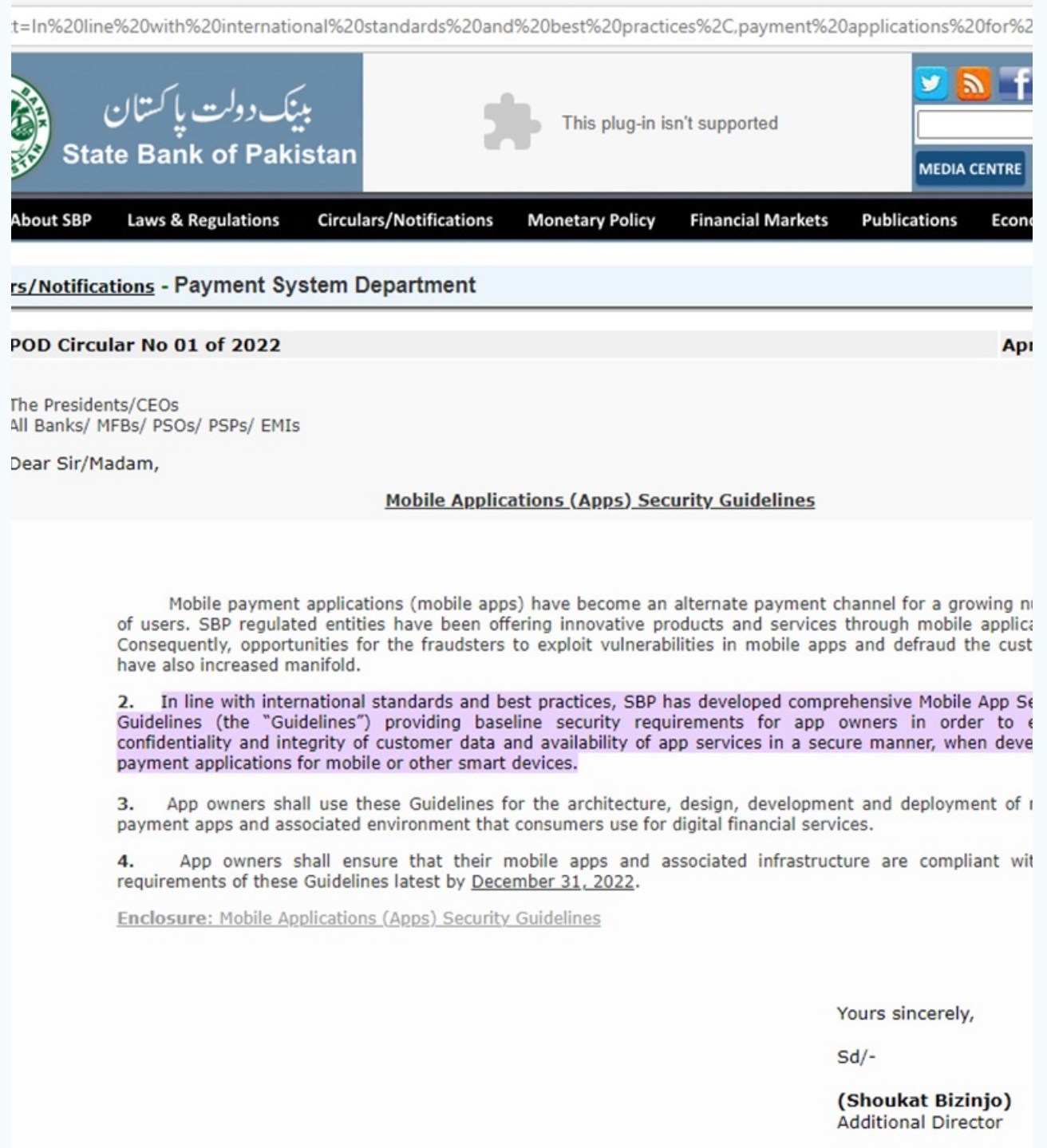
Mobile Payment App Security Best Practices (Section 9)

- Draws upon:
 - GSMA study on mobile money best practices,
 - ENISA smartphone security development guidelines,
- 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.

Application security best considerations:

- device and application integrity.
- communication security and certificate handling.
- user authentication.
- secure data handling.
- secure application development.

t=In%20line%20with%20international%20standards%20and%20best%20practices%2C,payment%20applications%20for%2



The screenshot shows the State Bank of Pakistan website. The header includes the SBP logo and name in Urdu and English. A navigation menu lists various sections like 'About SBP', 'Laws & Regulations', etc. The main content area is titled 'Circulars/Notifications - Payment System Department' and features a circular titled 'POD Circular No 01 of 2022'. The circular is addressed to 'The Presidents/CEOs of All Banks/ MFBs/ PSOs/ PSPs/ EMIs' and is dated 'April 2022'. The subject is 'Mobile Applications (Apps) Security Guidelines'. The text of the circular discusses the importance of mobile payment applications and the need for security guidelines. It states that SBP has developed comprehensive Mobile App Security Guidelines (the "Guidelines") providing baseline security requirements for app owners to ensure confidentiality and integrity of customer data. The guidelines are effective from December 31, 2022. The circular is signed by Shoukat Bizinjo, Additional Director.

State Bank of Pakistan

This plug-in isn't supported

MEDIA CENTRE

About SBP Laws & Regulations Circulars/Notifications Monetary Policy Financial Markets Publications Econ

rs/Notifications - Payment System Department

POD Circular No 01 of 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 Application Security best practices



Device and Application Integrity

Use platform services for integrity checks;
remove extraneous code
maintain high-integrity state server-side.



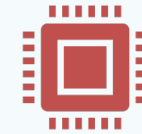
Communication Security and Certificate Handling

Standardized cryptographic libraries;
strong, up-to-date TLS certificates; limit certificate lifetimes (825 days);
contingency for untrusted CA; secure TLS configuration;
certificate pinning;
correct server certificate validation.



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;
clean caches/memory;
fine-grained permissions for data sharing;
avoid hard-coding sensitive info;
validate client input for database storage.

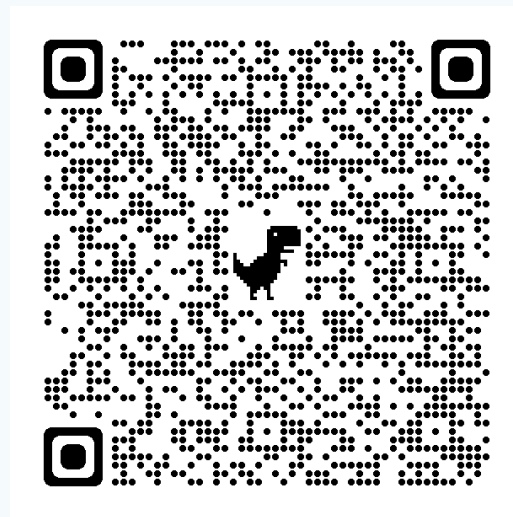


Secure Application Development

Adhere to secure coding practices and standards;
provide secure application updates;
regular internal or external code reviews.

DFS Security Recommendations

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



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

Contact: dfssecuritylab@itu.int

Thank you!