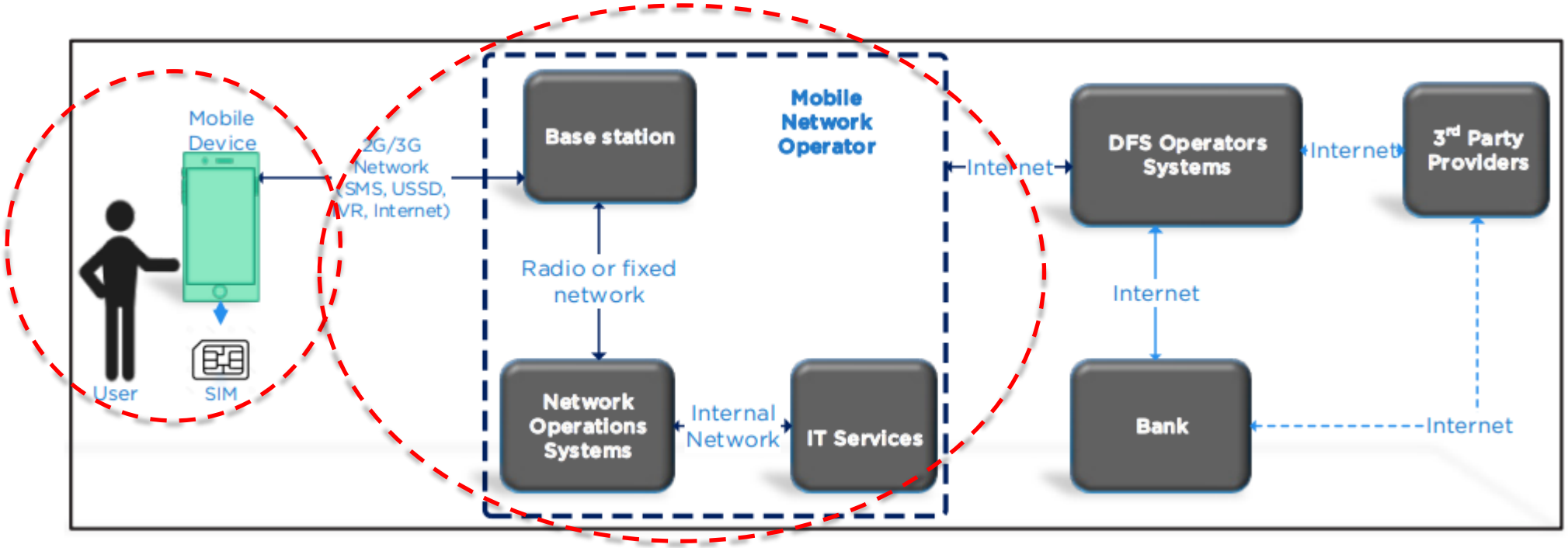
# DFS Security recommendations for regulators and providers

Arnold Kibuuka, Project Officer, ITU

dfssecuritylab@itu.int

September 2024

# Elements of a DFS Ecosystem




**User**

is target audience for DFS, uses mobile banking/payment application on a mobile device to access the DFS ecosystem

**MNO**

provides communication infrastructure from wireless link through the provider network

**DFS Provider**

application component, interfaces with payment systems and third-party providers.

# DFS Security Recommendations

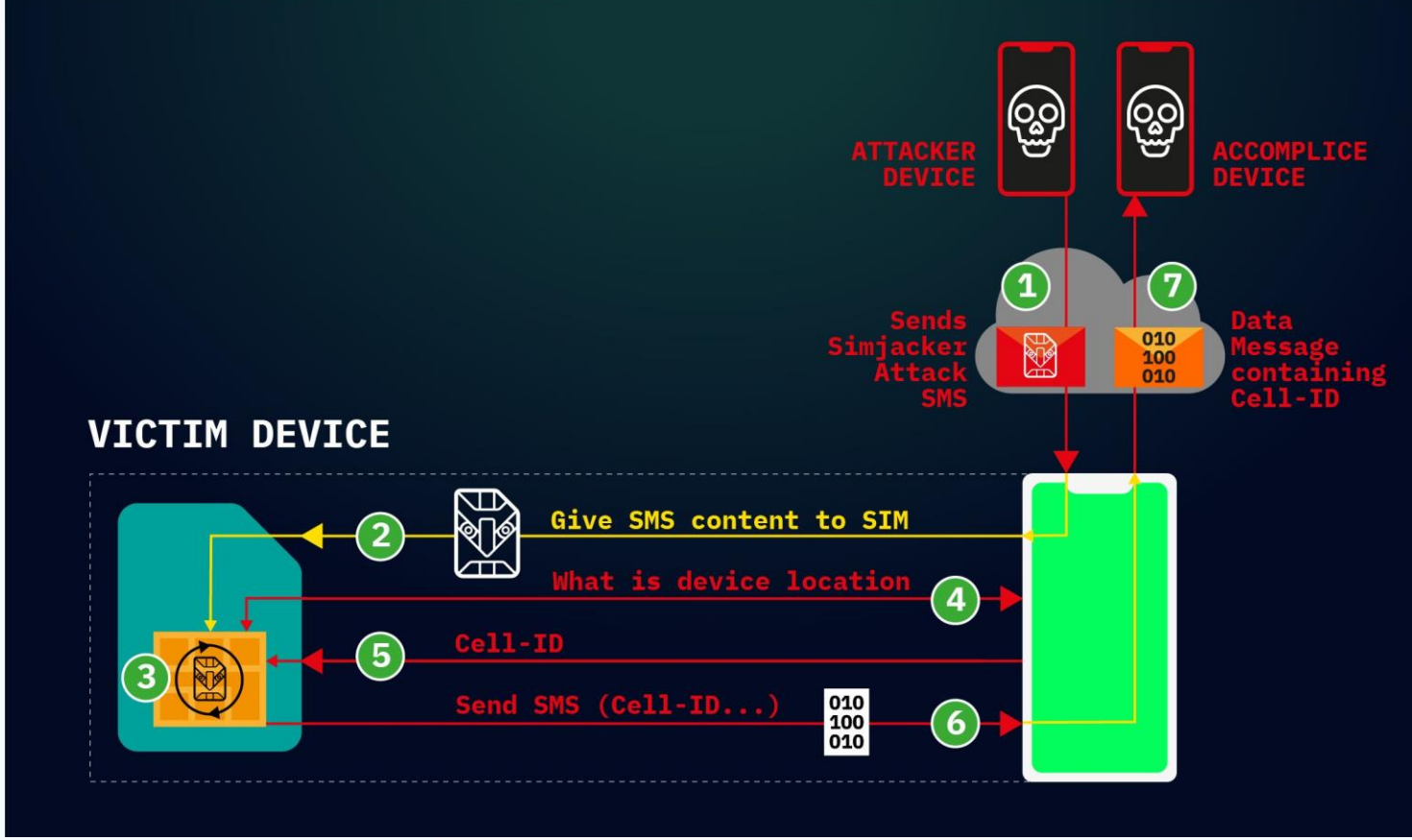
1. Security recommendations to protect against DFS SIM related risks like SIM swap fraud and SIM recycling
2. Recommendations to mitigate SS7 vulnerabilities
3. Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security
4. Mobile Application Security Best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



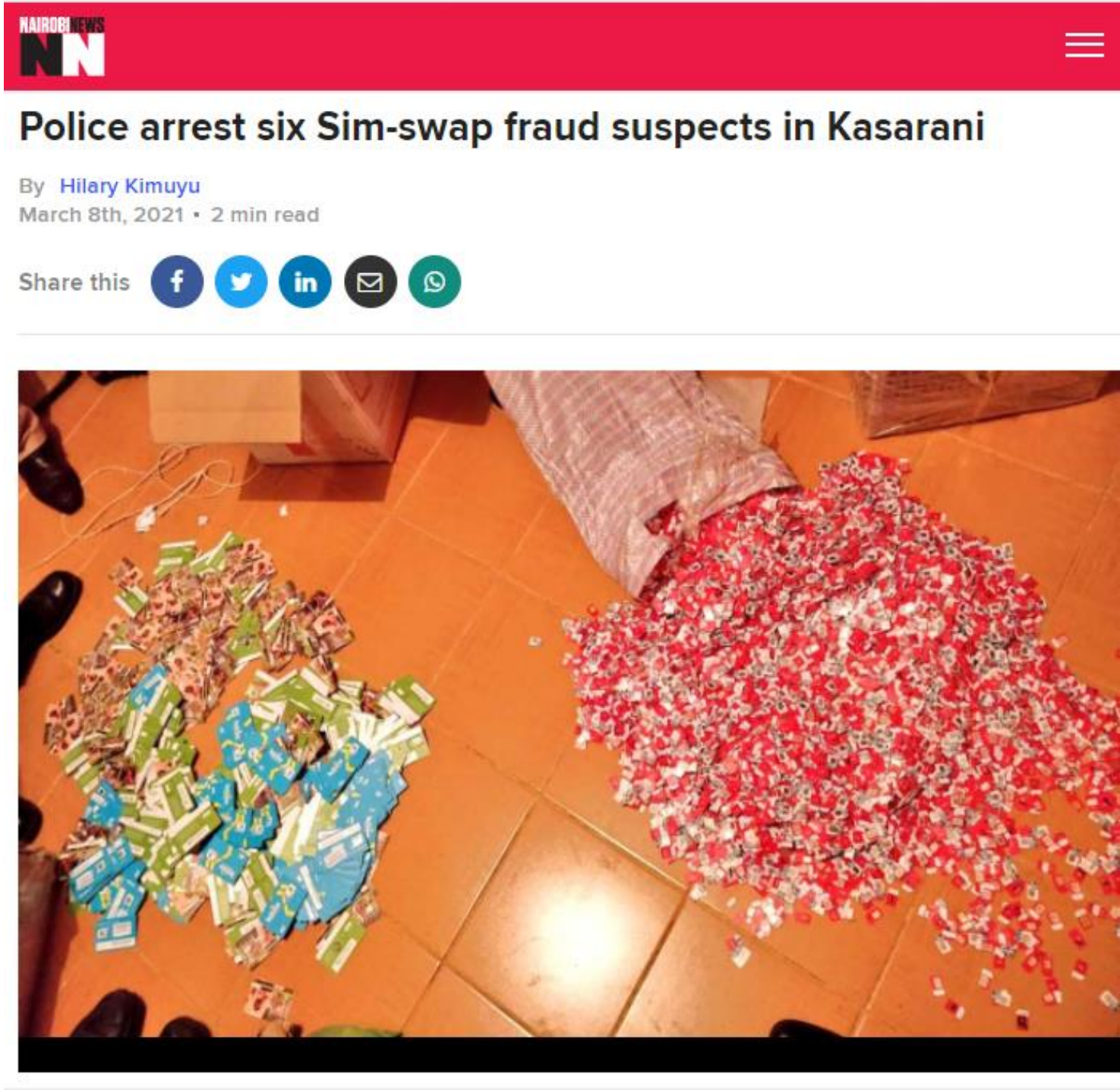


A SIM swap will deactivate your phone, and if done by an attacker, the attacker will receive your calls and texts on thier device.

Sources: Positive Technologies, Yubico

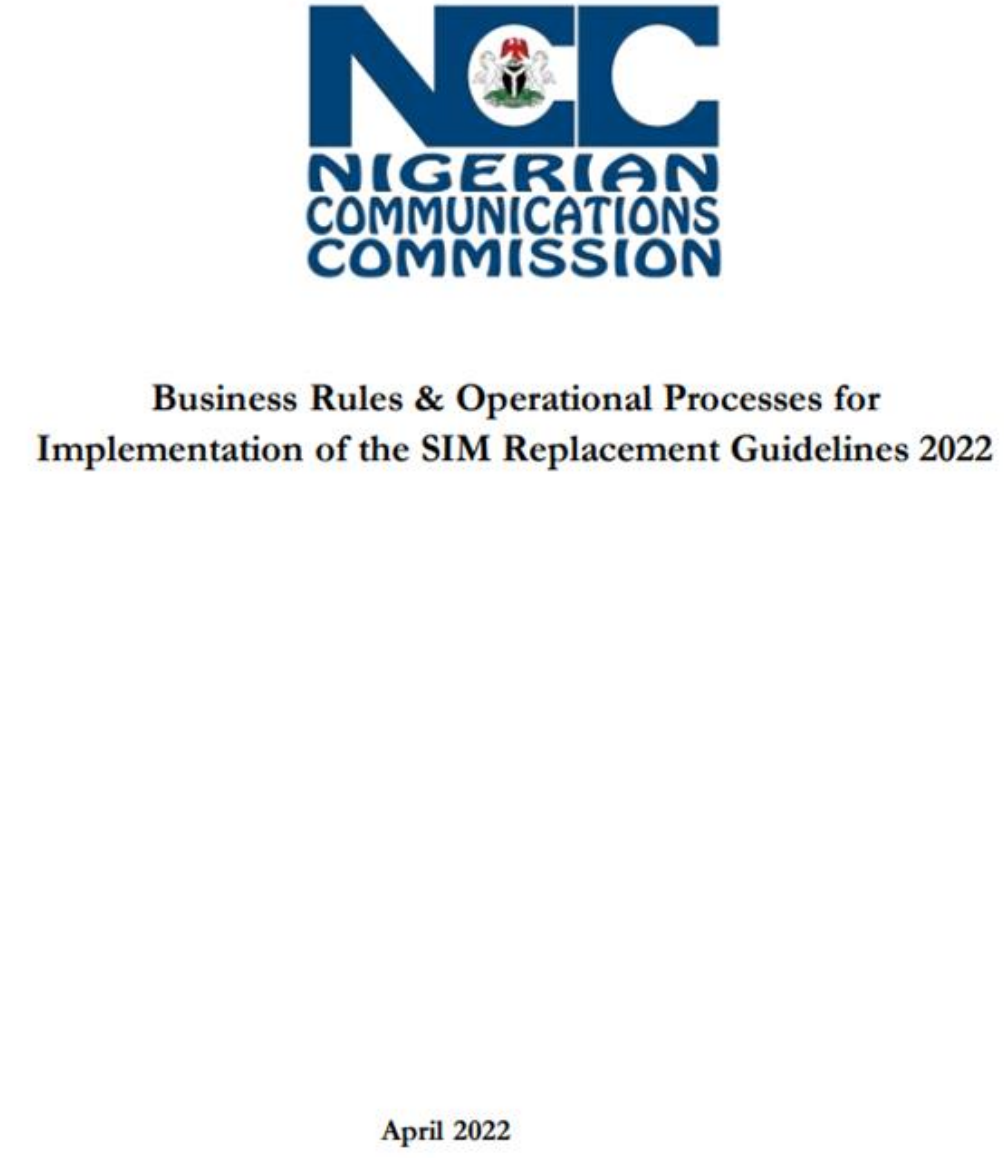
# SIM risks

- 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

- 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.




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

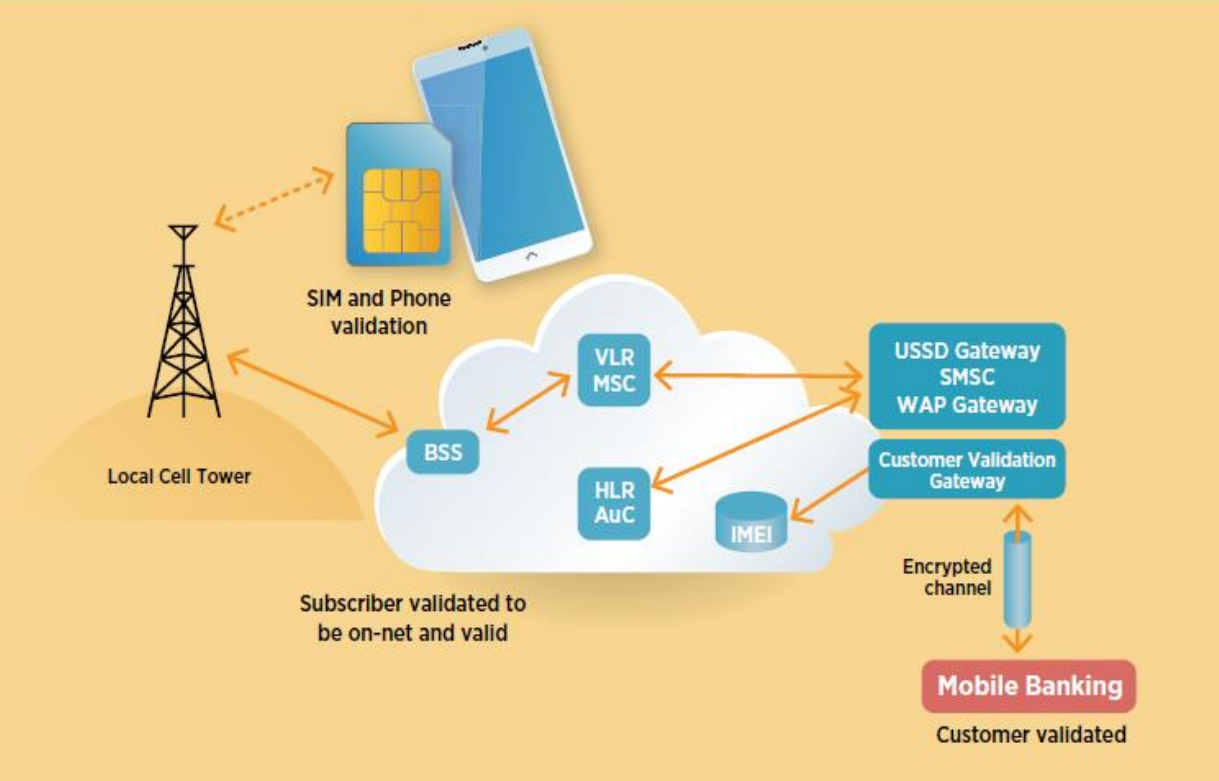
## DFS operators controls to mitigate SIM swaps

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 |

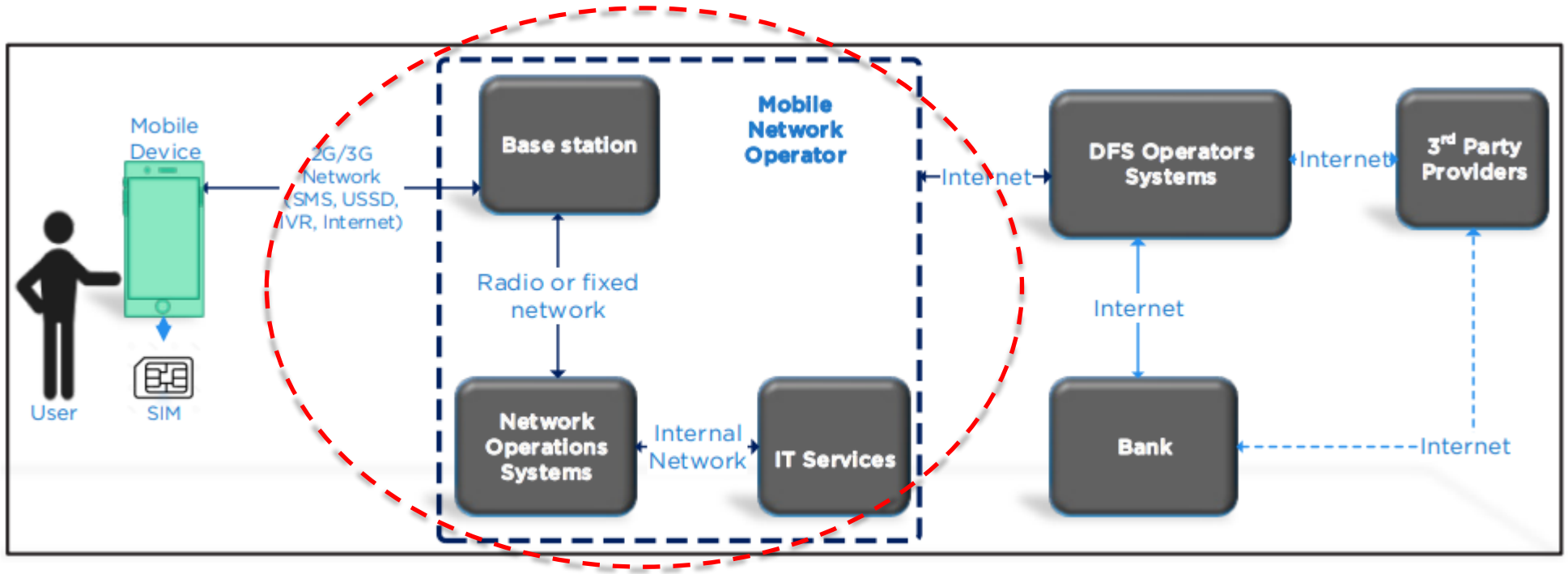
Example implementation of IMSI validation gateway by MTN. source: MTN website

# Guidance to mitigate SS7 threats

Related report:

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

# Elements of a DFS Ecosystem




**User**

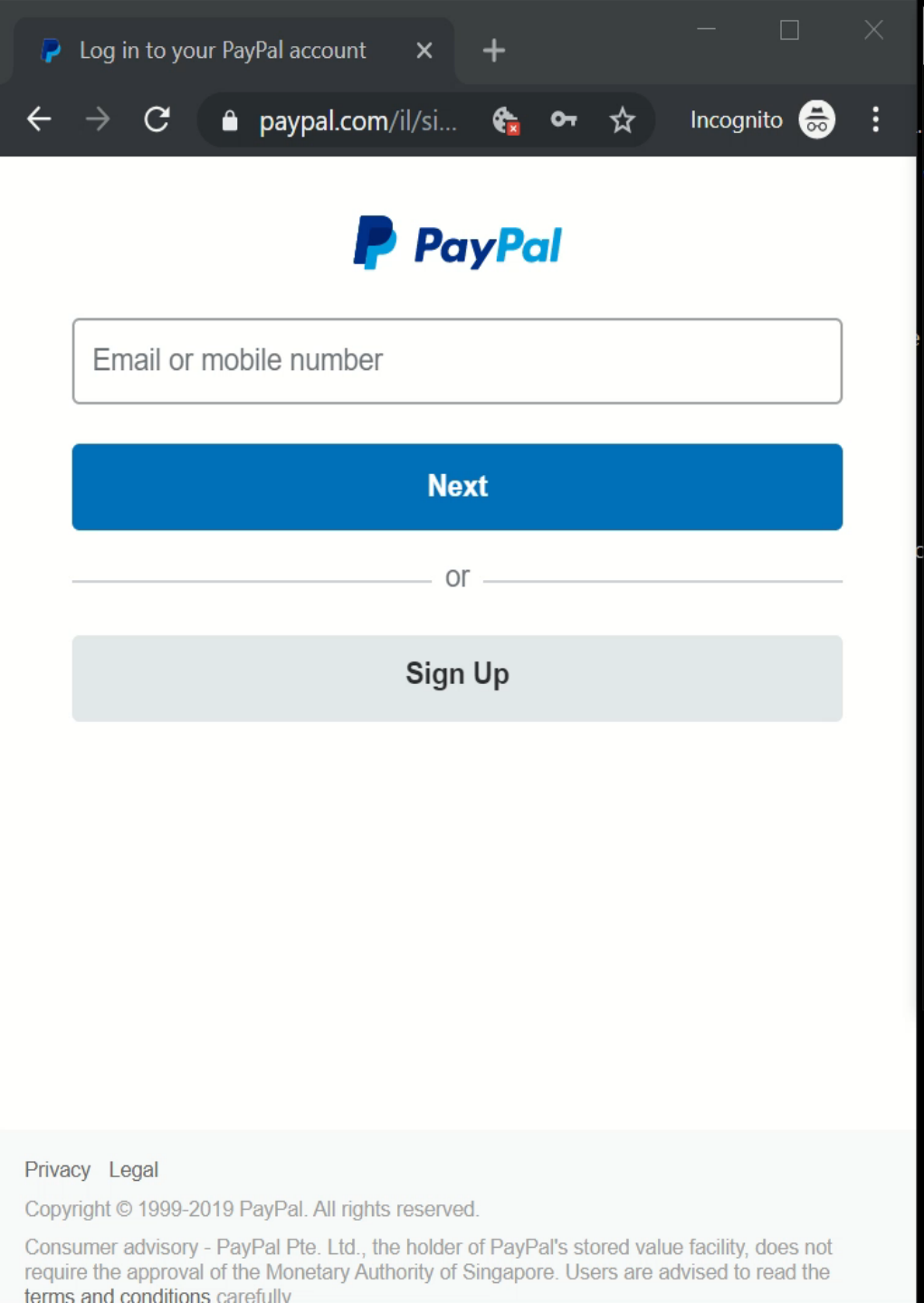
is target audience for DFS, uses mobile banking/payment application on a mobile device to access the DFS ecosystem

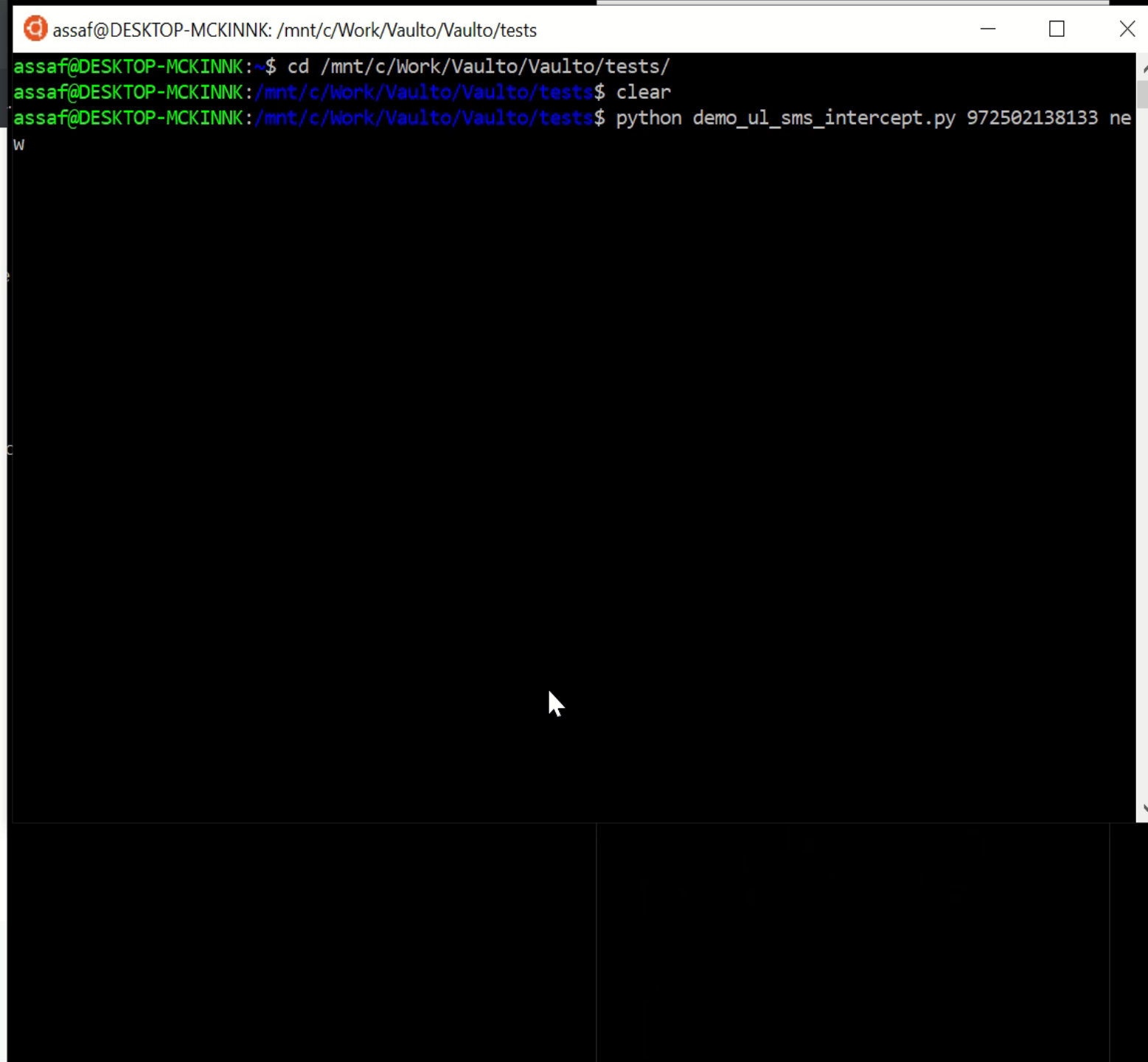
**MNO**

provides communication infrastructure from wireless link through the provider network

**DFS Provider**

application component, interfaces with payment systems and third-party providers.


Log in to your PayPal account
paypal.com/il/si...
Incognito
PayPal
Email or mobile number
Next
or
Sign Up
Privacy
Legal
Copyright © 1999-2019 PayPal. All rights reserved.
Consumer advisory - PayPal Pte. Ltd., the holder of PayPal's stored value facility, does not require the approval of the Monetary Authority of Singapore. Users are advised to read the terms and conditions carefully

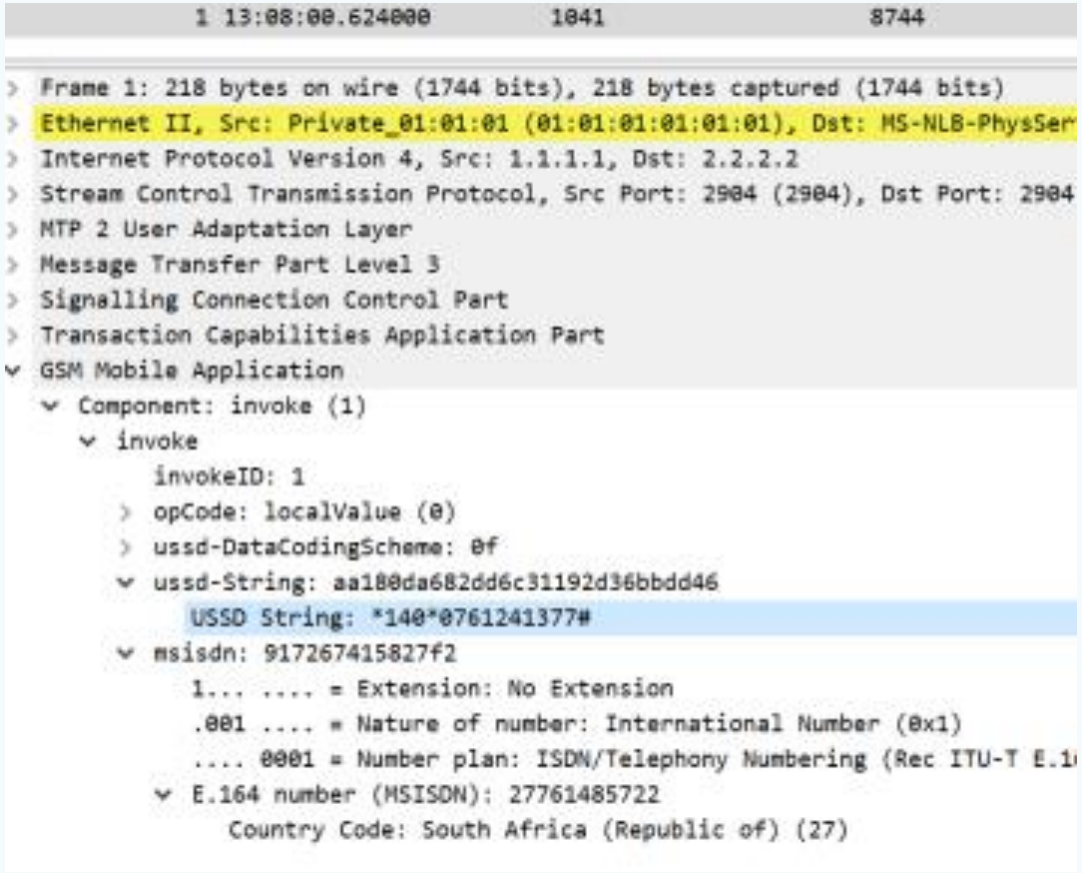

assaf@DESKTOP-MCKINNK: /mnt/c/Work/Vaulto/Vaulto/tests
assaf@DESKTOP-MCKINNK:~$ cd /mnt/c/Work/Vaulto/Vaulto/tests/
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ clear
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ python demo_ul_sms_intercept.py 972502138133 ne
w

# 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

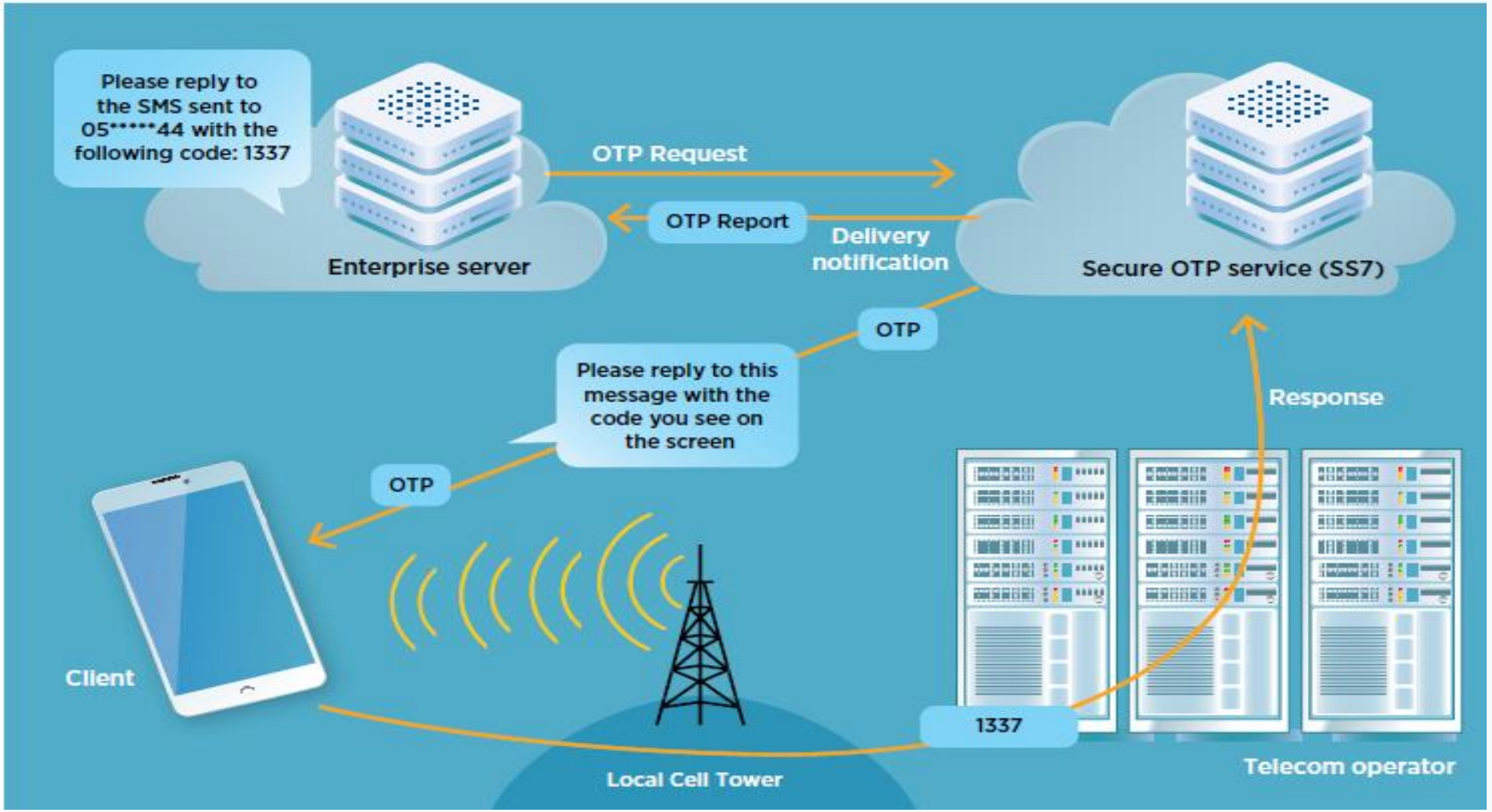
- Session time out
- USSD PIN masking
- Secure and monitor core network traffic
- Limit access to traces and logs
- SMS filtering
- SMS home routing



# 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

# DFS Consumer Competence Framework

Empowers Consumers to:

- confidently engage in financial transactions using digital channels.
- make informed choices and thoroughly understand pricing, terms, and conditions.
- operate safely, circumventing fraudulent or deceptive marketing practices.
- understand the risks of failing to protect data privacy within digital financial services.

# Transaction 3 phases

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

### 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.

# DFS CCF encompasses 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.<br>CA 1.2 Compare information on costs, quality and terms of conditions of the service.<br>CA 1.3 Evaluate the commercial information provided and suitability for purpose.<br>CA 1.4 Manage digital identity and credit profile.<br>CA 1.5 Understand how to access digital financial service in a secure manner.<br>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).<br>CA 2.2 Make payments and accessing finance through digital channels.<br>CA 2.3 Understand the terms and conditions of the DFS provider, including related costs and risks.<br>CA 2.4 Manage personal data and privacy.<br>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.<br>CA 3.2 Know consumer rights and how to obtain redress.<br>CA 3.3 Know the responsible regulator to approach with intractable problems and the mechanism for doing so.<br>CA 3.4 Keep up to date on developments in digital financial services. |

# DFS consumer competence framework

| **1.5 Understand how to access digital financial service in a secure manner**<br>To understand how to use DFS services securely and protect oneself from online threats. To understand the risks of disclosing login credentials and how to manage them in a secure manner. | |
|---|---|
| Knowledge area | CA1.5-K1 Know how to recognize and detect fraudulent emails, (phishing, vishing and social engineering scams), texts and calls.<br>CA1.5-K2 Know not to disclose login credentials to third parties to help perform transactions.<br>CA1.5-K3 Know how to protect the mobile phone used for DFS transactions, including protection against SIM swaps.<br>CA1.5-K4 Know the risks and dangers that come when transacting online and using digital financial services.<br>CA1.5-K5 Know basic good practices to prevent common types of cyber threats.<br>CA1.5-K6 Know how to use multifactor authentication and biometrics and why they are safer for accessing DFS (may not be applicable in all countries[19]). |
| Skills Area | CA1.5-S1 Evaluate one's phone security feature/detect weak security features[20].<br>CA1.5-S2 Assess the DFS platform and make sure it is safe and secure.<br>CA1.5-S3 Manage different usernames and passwords for login to one's online profile and access different digital services, and avoid use of the same username/password for multiple online services[21].<br>CA1.5-S4 Apply critical thinking when receiving social engineering scams (i.e.: recognizing the methods used by scammers)[22].<br>CA1.5-S5 Do not leave money with agents to carry out transactions on one's behalf[23].<br>CA1.5-S6 Do not engage with Smishing emails or messages – i.e. use of phone calls or SMS to gather personal information such as account details, PINs or passwords or other consumer identification details.<br>CA1.5-S7 Use multifactor authentication and biometrics for accessing digital financial services.<br>CA1.5-S8 Protect your biometrics. |
| Proactive steps | CA1.5-P1 Set strong passwords which are changed frequently.<br>CA1.5-P2 Engage with reputable and trusted DFS providers.<br>CA1.5-P3 Secure devices (lock screen) when not using one's device and set passwords to prevent unauthorised access to financial app.<br>CA1.5-P4 Customize privacy settings on one's online accounts.<br>CA1.5-P5 Discontinue use of any agent who asks for customers' PIN immediately.<br>CA1.5-P6 Check financial statements regularly.<br>CA1.5-P7 Use SMS update facility. |

CA1.5-K1 Know how to recognize and detect fraudulent emails, (phishing, vishing and social engineering scams), texts and calls.

CA1.5-K2 Know not to disclose login credentials to third parties to help perform transactions.

CA1.5-K3 Know how to protect the mobile phone used for DFS transactions, including protection against SIM swaps.

CA1.5-K4 Know the risks and dangers that come when transacting online and using digital financial services.

CA1.5-K5 Know basic good practices to prevent common types of cyber threats.

CA1.5-K6 Know how to use multifactor authentication and biometrics and why they are safer for accessing DFS (may not be applicable in all countries[19]).

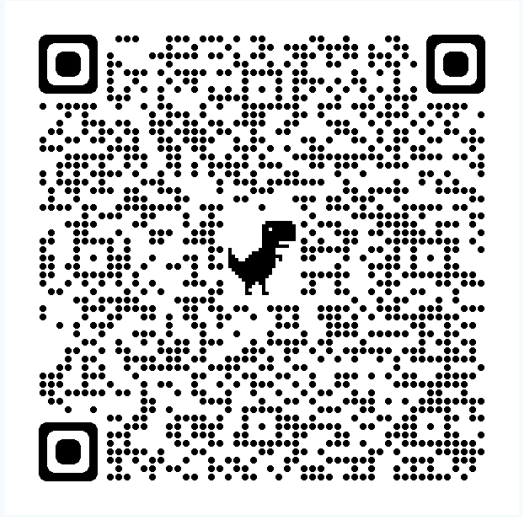
**Extracted from:** ITU DFS Consumer Competence Framework

# ITU DFS security Lab and ITU Recommendations on Digital Finance

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

# DFS Security Recommendations

- ITU-T Rec. X.1150 : Security assurance framework for digital financial services
- Security recommendations to protect against DFS SIM related risks like SIM swap fraud and SIM recycling
- Recommendations to mitigate SS7 vulnerabilities
- Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security
- Mobile Application Security Best practices
- ITU DFS Consumer Competence Framework



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

**Contact:** dfssecuritylab@itu.int

# Thank you!