DFS Security recommendations for regulators and providers

Arnold Kibuuka, Project Officer, ITU

dfssecuritylab@itu.int

November 2024

DFS Security Recommendations

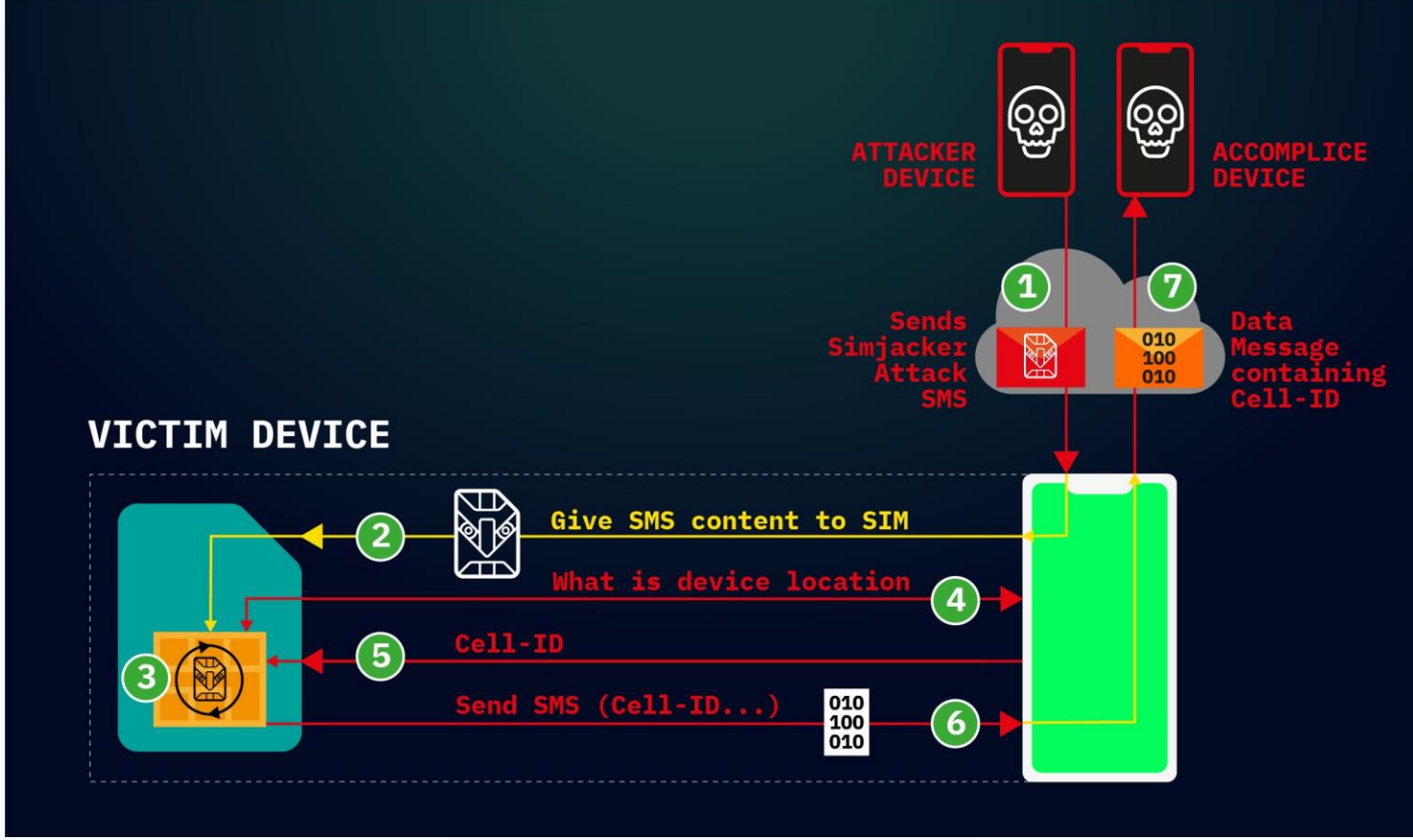
1. Security recommendations to protect against DFS SIM related risks like SIM swap fraud and SIM recycling
2. Recommendations to mitigate SS7 vulnerabilities
3. Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security
4. Mobile Application Security Best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

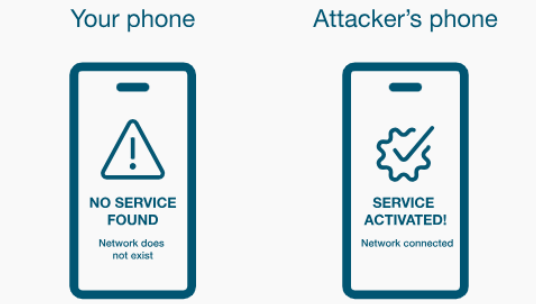
Regulatory Guidance to mitigate SIM risks

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)





Sources: Positive Technologies, Yubico

Sources: The Economic Times

SIM risks

THE ECONOMIC TIMES | wealth

English Edition | Today's ePaper

Airtel issues fraudster duplicate SIM without proper verification, Soldier loses lakhs from SBI a/c: How to protect yourself

By Neelanjit Das, ET Online • Last Updated: Aug 20, 2024, 08:33:00 PM IST

Synopsis

SIM card fraud: Bharti Airtel has issued a duplicate mobile SIM card to a fraudster and as a result of this a Indian Army soldier posted in Jammu & Kashmir lost Rs 2.87 lakh from this State Bank of India (SBI) a/c. The soldier fought with Airtel for 7 years and finally won the case with Rs 4.83 lakh compensation to be payable by Airtel; NCDRC.

A soldier who was a long-term Airtel customer lost Rs 2,87,630 from his State Bank of India (SBI) savings bank account due to a mobile 'SIM swap fraud'. The fraud happened when Airtel issued a duplicate mobile SIM card to an unknown person without

Sources: NCC

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.

NIGERIAN COMMUNICATIONS COMMISSION

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

www.itu.int/go/dfssl

MOU between the Central bank and Telco regulator

A bilateral MOU related DFS should be in place between the ICT and Financial regulators.

responsibilities of the central bank and ICT regulator for security of DFS (SIM swap fraud, SS7, consumer protection etc.)

modalities around the creation of a Joint Working Committee on DFS security and risk-related matters.

1 Basis of the Memorandum of Understanding

In recognition of the growing convergence of telecommunications and financial services in what has been identified as 'Digital Financial Services,' the Authorities have identified a need for Regulatory interaction and collaboration to ensure the integrity, security, stability and protection of participants and end users relating to the provision of these services.

The Central Bank and the National Telecommunications Regulator shall cooperate with each other for the oversight and supervision of DFSPs and MNO communications networks under their respective financial and telecommunications mandates to ensure the highest levels of security, reliability, consumer protection, fair and equitable access to facilities, and confidentiality.

Recognizing too that both the Central Bank and the National Telecommunications Regulator each have limited scope of supervision and oversight of components of DFS, this MOU is entered into to establish the manner in which the authorities will jointly oversee, supervise, and interact with each other in respect of any matters relating to DFS that touch on their respective mandates and remits, and so together strengthen and/or address any gaps in the Regulatory, supervisory and oversight framework for DFS in (the country).

This MOU is entered on the basis of mutual respect, in a spirit of goodwill, and does not affect the independence of the two Authorities hereto.

This MOU aims to promote the integrity, efficiency, and efficacy of participants by improving effective regulation and enhancing the supervision of DFS.

2 Areas of cooperation and cooperation strategies general provisions

2.1 The parties agree to cooperate in their respective roles in dealing with matters relating to:

a) DFS generally;
b) Full and fair access to, security, and reliability of all components of DFS in (the country);
c) Consumer Protection; and
d) Any other relevant areas of possible collaboration between the Authorities.

2.2 The cooperation between the Central Bank and National Telecommunications Regulator shall focus around the following issues and processes:

a) Exchange of any relevant information;
b) Mutual capacity building;
c) Investigation of any incident, issues and cases relating to the scope of this MOU;
d) Joint or individual hearings, as needed;
e) Use of common systems for DFS transaction monitoring
f) Fostering competition and promoting a level playing field for all participants of a DFS ecosystem;
g) Dispute resolution between providers, and between consumers as end users;
h) Development, monitoring and enforcement of relevant provisions of respective laws, by-laws, guidelines, or regulations where these may relate to DFS;

www.itu.int/go/dfssl

Recommendations on SIM Swaps

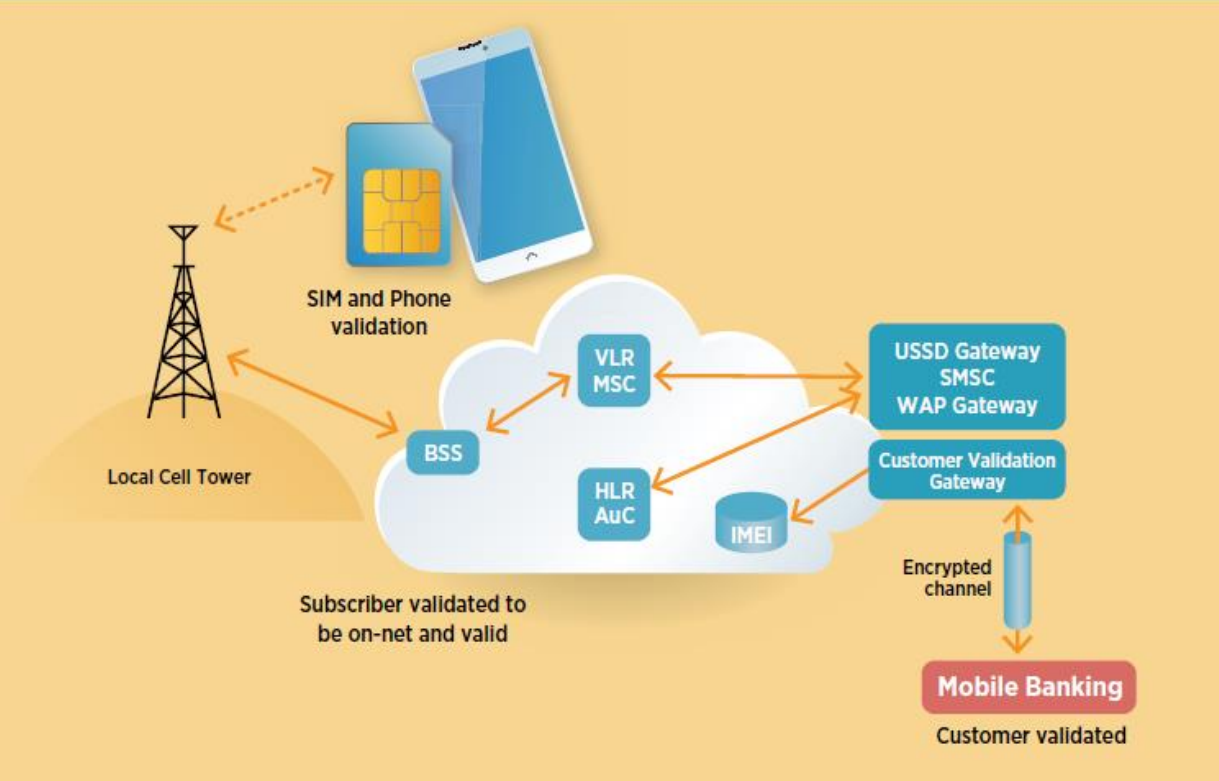
Security controls to be implemented by MNOs and MVNOs

- the MNO/MVNO or its agents must capture a biometric, facial image of the proxy which must be kept for a specified period.
- MNOs should notify DFS providers on swapped SIMs, ported and recycled numbers.
- SIM swap notifications to users
- Biometric SIM swap verification
- Multifactor user validation before SIM swap
- Secure SIM data protection
- Holding time before activation of a swapped SIM
- Service support representatives training

Security controls to be implemented by DFS operators

- Real time IMSI/ICCID detection
- Real time device change detection – device to DFS account binding
- Encourage use of secure DFS access through apps.

IMSI validation gateway



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

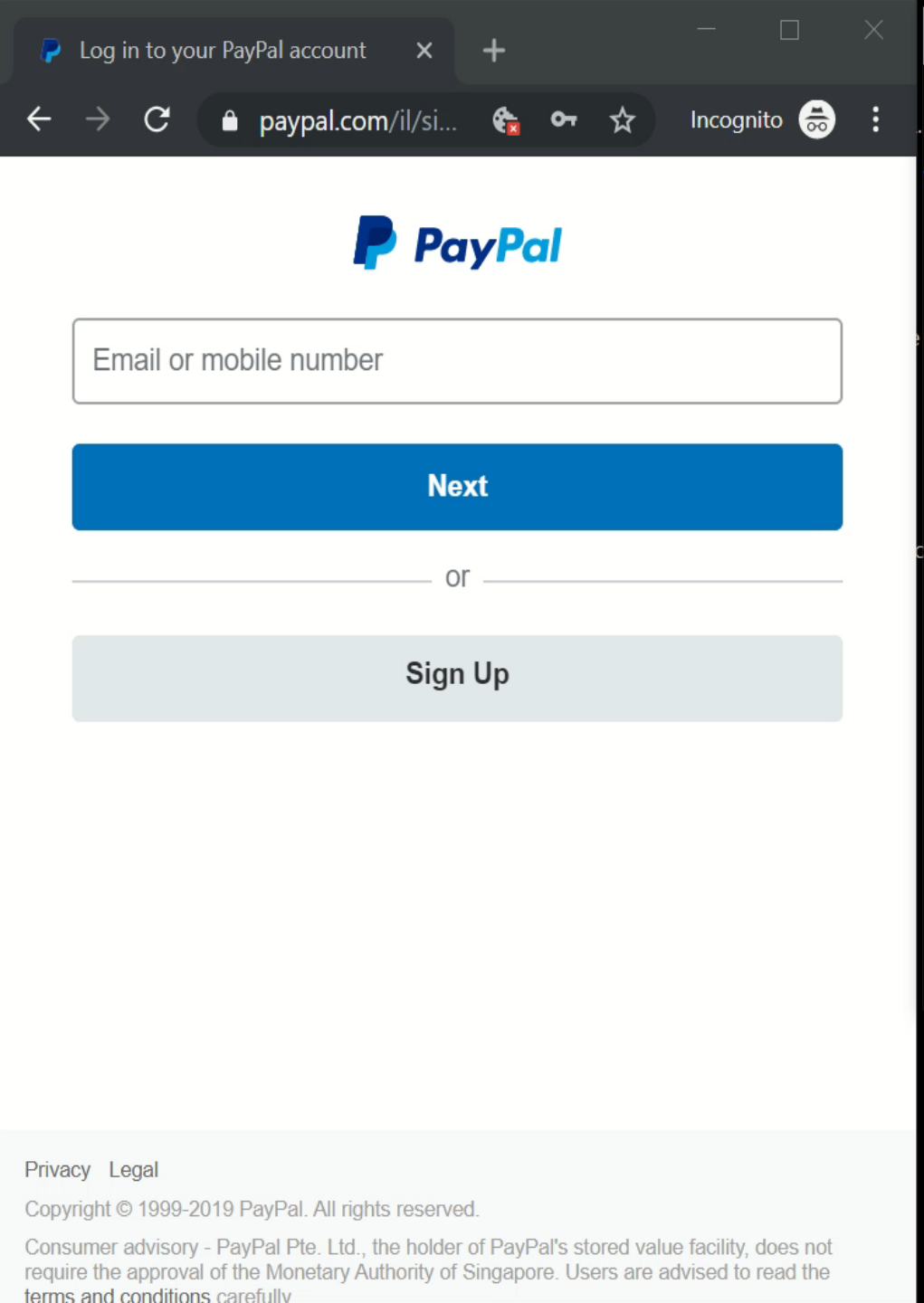
Category: PREMIUM

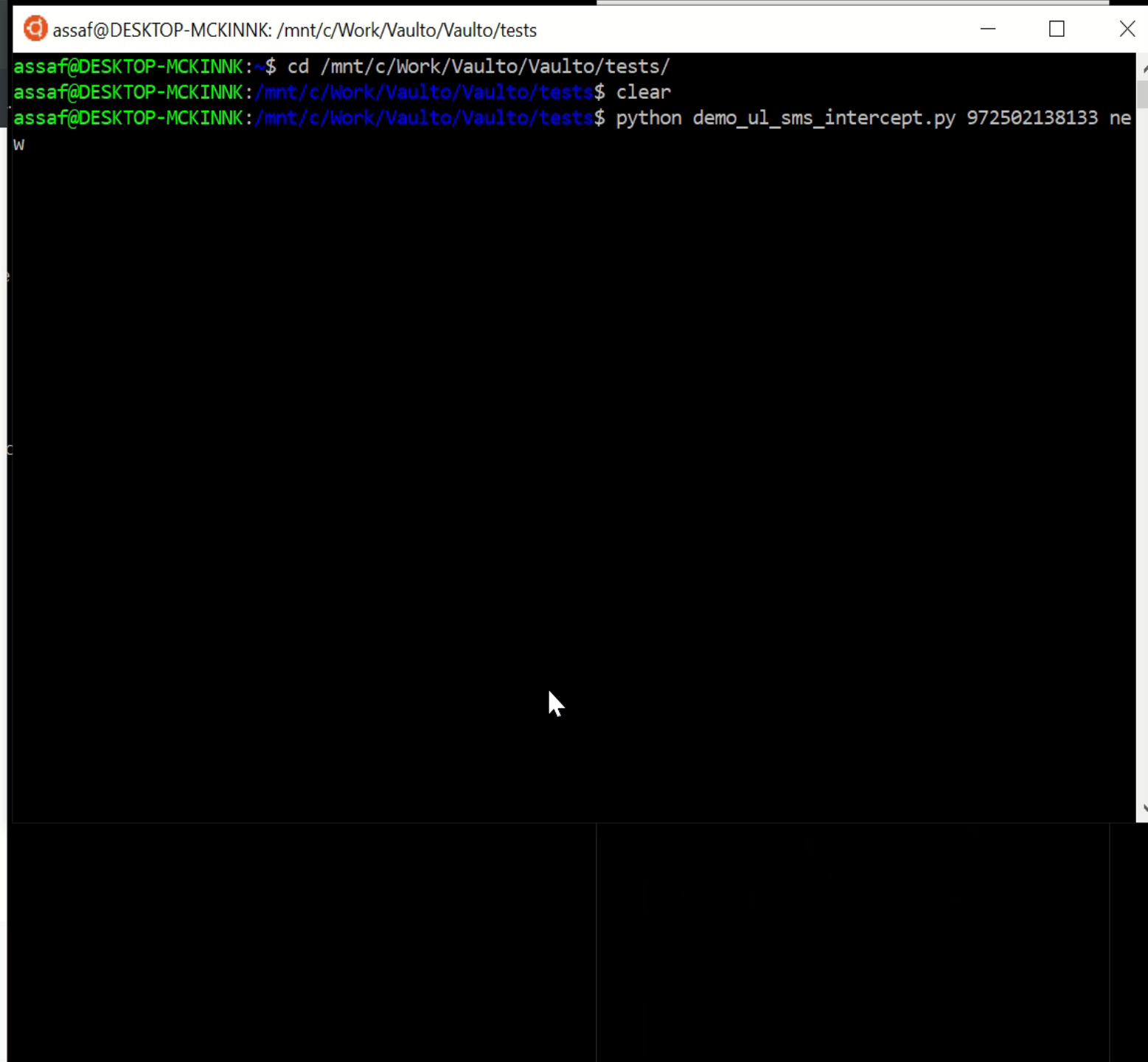
API Name	API Definition
Sim Swap API	API which allows a corporate customer to check if a given MSISDN has performed a SIM swap. Returns 'MSISDN',' date of last SIM swap'
Authentication API	API which allows a corporate customer to use MTN Service to send OTPs . A customer is onboarded on the MTN instance 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


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

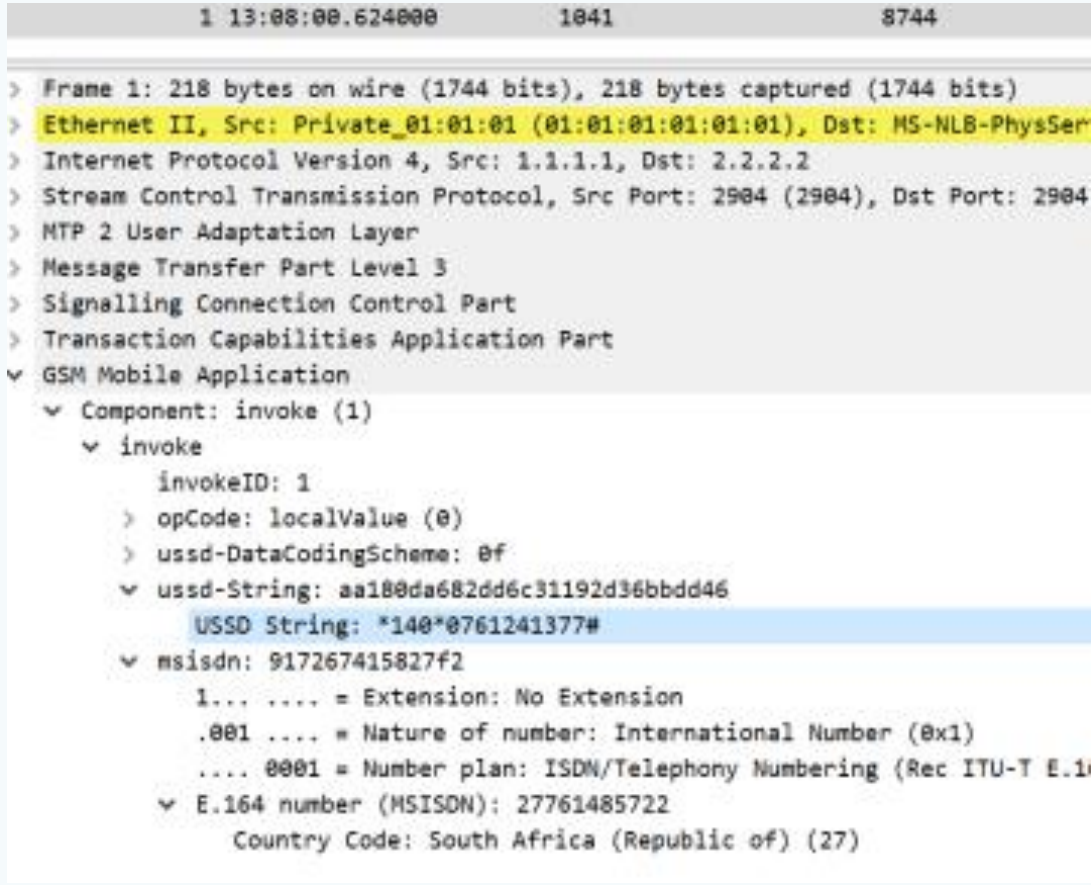

assaf@DESKTOP-MCKINNK: /mnt/c/Work/Vaulto/Vaulto/tests
assaf@DESKTOP-MCKINNK:~$ cd /mnt/c/Work/Vaulto/Vaulto/tests/
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ clear
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ python demo_ul_sms_intercept.py 972502138133 ne
w

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.

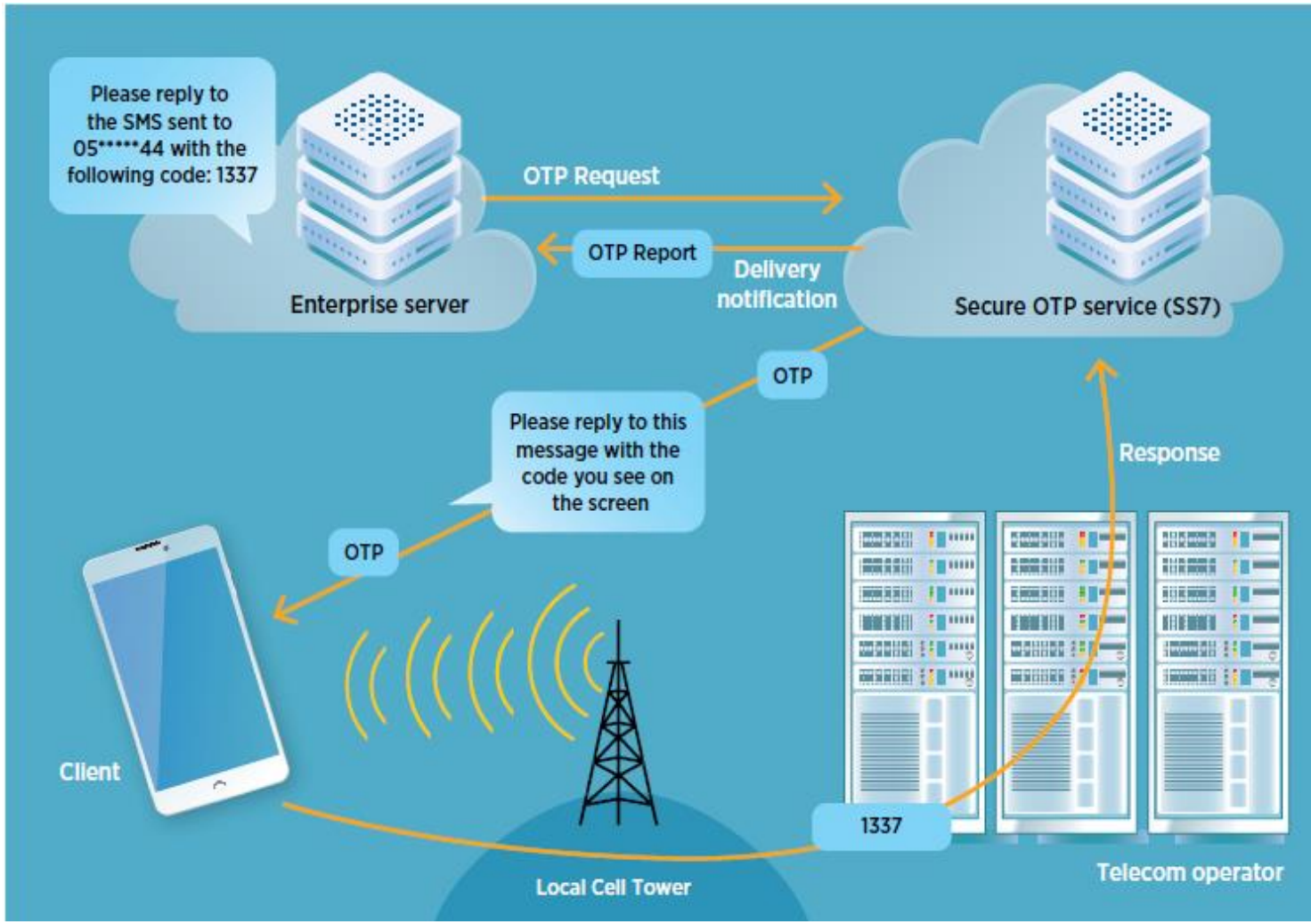
Recommendations for MNO to mitigate SS7 risks

- 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



ITU-T Study Group 11 work on SS7

- **Published Recommendations and Technical Reports:**
- ITU-T QSTR-SS7-DFS (2019): SS7 vulnerabilities and mitigation measures for digital financial services transactions
- ITU-T QSTR-USSD (2021) Low resource requirement, quantum resistant, encryption of USSD messages for use in financial services
- ITU-T Q.3062 (2022): Signalling procedures and protocols for enabling interconnection between trustable network entities in support of existing and emerging networks
- ITU-T Q.3063 (2022) : Signalling procedures of calling line identification authentication
- **Ongoing**
- Draft Q.TSCA: Requirements for issuing End-Entity and Certification Authority certificates for enabling trustable signalling interconnection between network entities.
- Draft Q.DMSA: Principles for detection and mitigation of signalling attacks in security signalling gateway

DFS Consumer Competency Framework

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

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., youth, elderly, disabled) to facilitate informed, safe, and confident use of DFS)

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

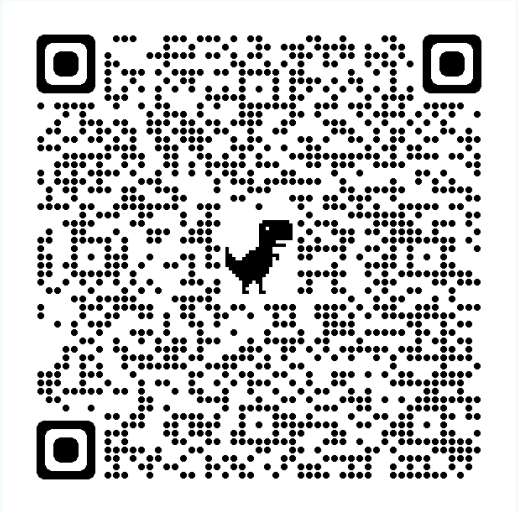
3. **Post-transaction Phase**
   - Includes engagement with the provider for quality assurance or redress when the Quality of Service (QoS) was not up to standards.
   - **Important Skills/Knowledge:** Understanding of rights and obligations; ability to seek redress.

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. 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.



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

Contact: dfssecuritylab@itu.int

Thank you!