DFS Security recommendations for regulators and providers

Arnold Kibuuka, Project Officer, ITU

January 2025

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

DFS Security Recommendations

1. Security recommendations to protect against DFS SIM related risks
2. Recommendations to mitigate SS7 vulnerabilities
3. DFS Mobile application security Best practices (From ITU-T X.1150)
4. Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security
5. DFS consumer competency framework

Regulatory Guidance to mitigate SIM risks

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

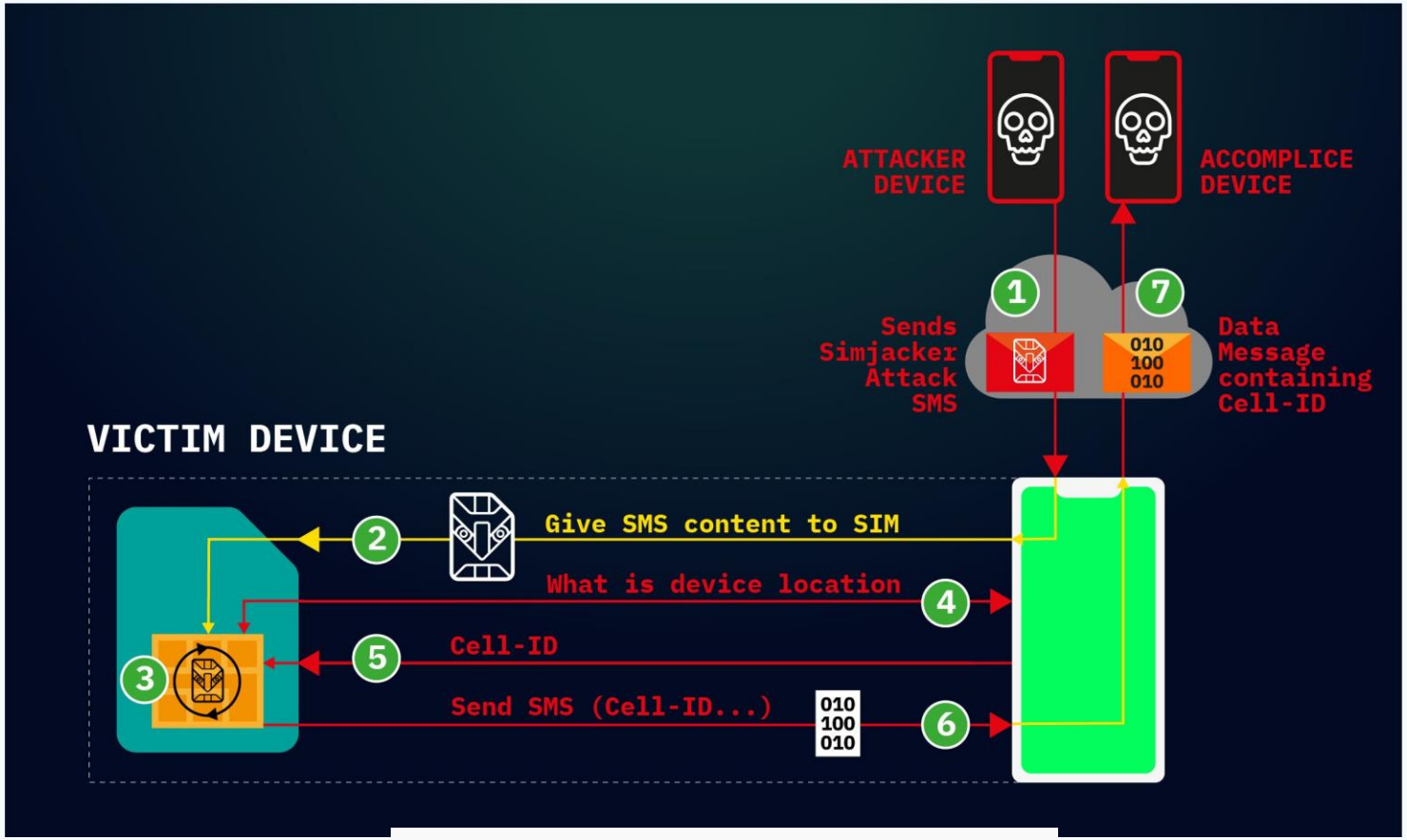
Poll Question

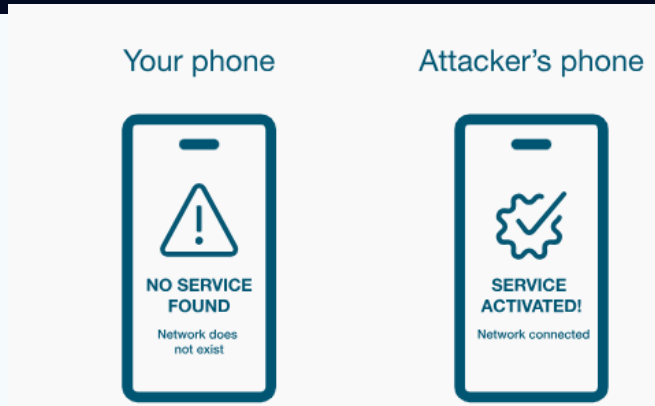
Which of these SIM card-related security risks are you familiar with?

4

SIM risks

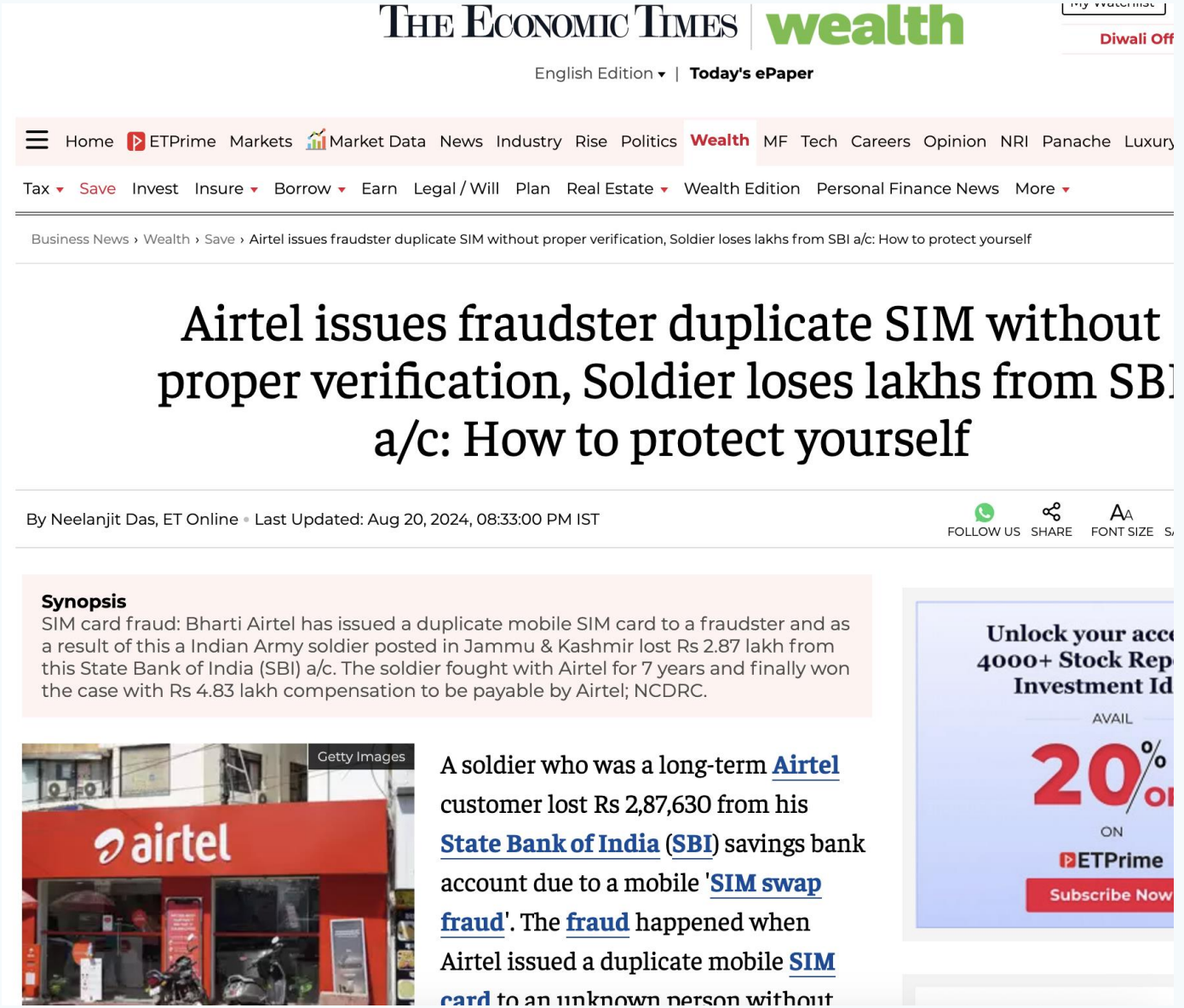
- SIM cloning
- SIM swaps
- SIM Recycling
- Binary over the air attacks (Sim jacker and WIB browser attacks)





Sources: Positive Technologies, Yubico

SIM risks



THE ECONOMIC TIMES | wealth

English Edition | Today's ePaper

Home ETPrime Markets Market Data News Industry Rise Politics Wealth MF Tech Careers Opinion NRI Panache Luxury

Tax Save Invest Insure Borrow Earn Legal / Will Plan Real Estate Wealth Edition Personal Finance News More

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

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

FOLLOW US SHARE FONT SIZE

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.

Getty Images

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

Unlock your acc
4000+ Stock Rep
Investment Id
AVAIL
20%
ON
ETPrime
Subscribe Now

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.

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.

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

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;

MNO controls on SIM swaps (SIM swap rules for 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

iv. **Biometric SIM swap verification**: Mobile providers should adopt biometric verification before a SIM swap/SIM replacement is performed.

v. **Multifactor user validation before SIM swap:** Mobile providers should use using a combination of something they are, something they have, or something they know authenticate users before a sim swap. User authentication challenges should include verification of personal details (address, email address, DOB), Account information (activation date, last payment, service type), device information (IMEI, ICCID), usage information (recent numbers), knowledge (PIN or password, security question), possession (email OTP, SMS OTP).

vi. **Information sharing with DFS provider on SIM swaps and SIM recycling**: MNO should design a mobile number recycling process that involves communicating with DFS providers on Mobile Subscriber Identification Numbers (MSIDN) churned or recycled. (In this context: number recycling is when the MNO reallocates a dormant/inactive Mobile Subscriber Identification Number (MSISDN) to a new customer). When a SIM is recycled, the mobile operator reports the new IMSI related to the account phone number. The DFS provider should block the account until the identity of the new person holding the SIM card is verified as the account holder.

vii. **SIM swap notifications to users:** On request for a SIM swap, sending of notifications via SMS, IVR or Push USSD of the SIM swap request to the (current) SIM/phone number owner, in case the SIM is still live, and then waiting for a positive response from the owner for a certain time before undertaking the SIM swap

viii. **Secure SIM data protection**: The mobile operator should safeguard personal information that can be used during SIM swaps and securely store SIM data like IMSI and SIM secret key values (KI values).

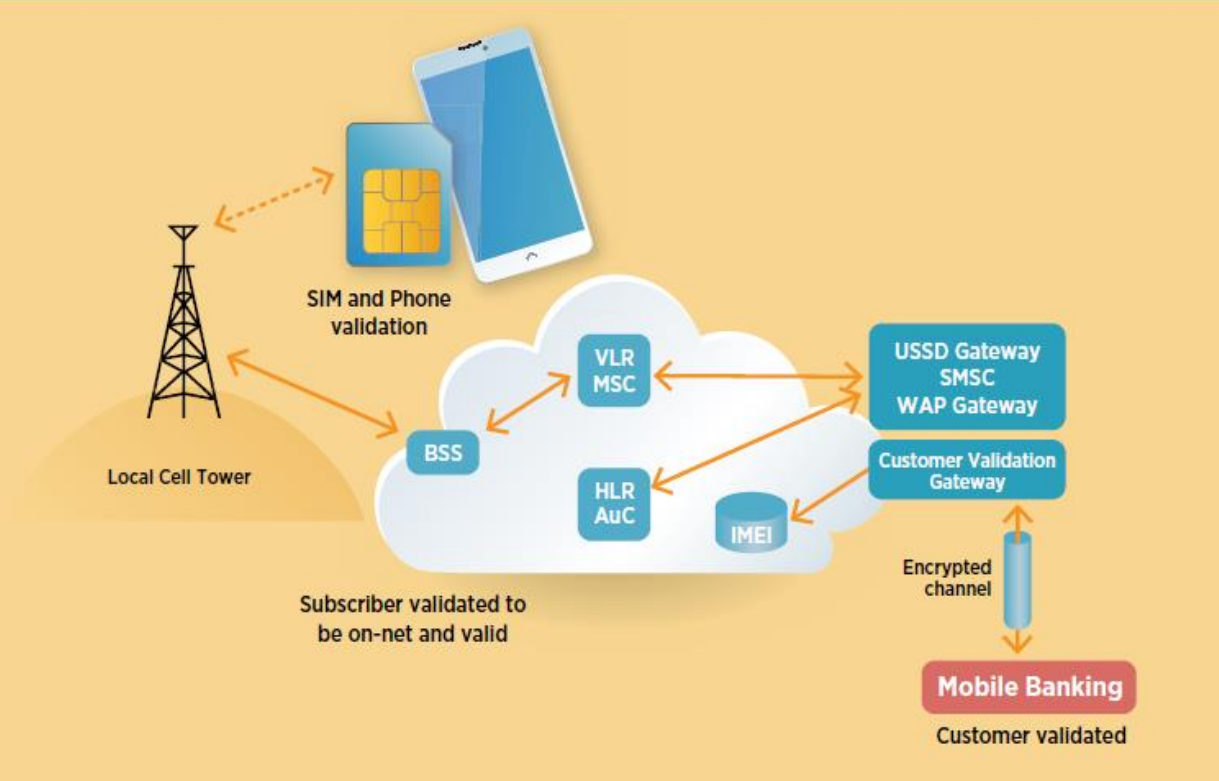
ix. **Holding time before activation of a swapped SIM**: A general holding time from the time of a SIM card request to providing the new SIM card to the requestor

x. **Customer support representatives training**: Provide better training to customer support representatives. Representatives should thoroughly understand how to authenticate customers and that deviations from authentication methods or disclosure of customer information prior to authentication is impermissible.

DFS operators controls to mitigate SIM swaps

- 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

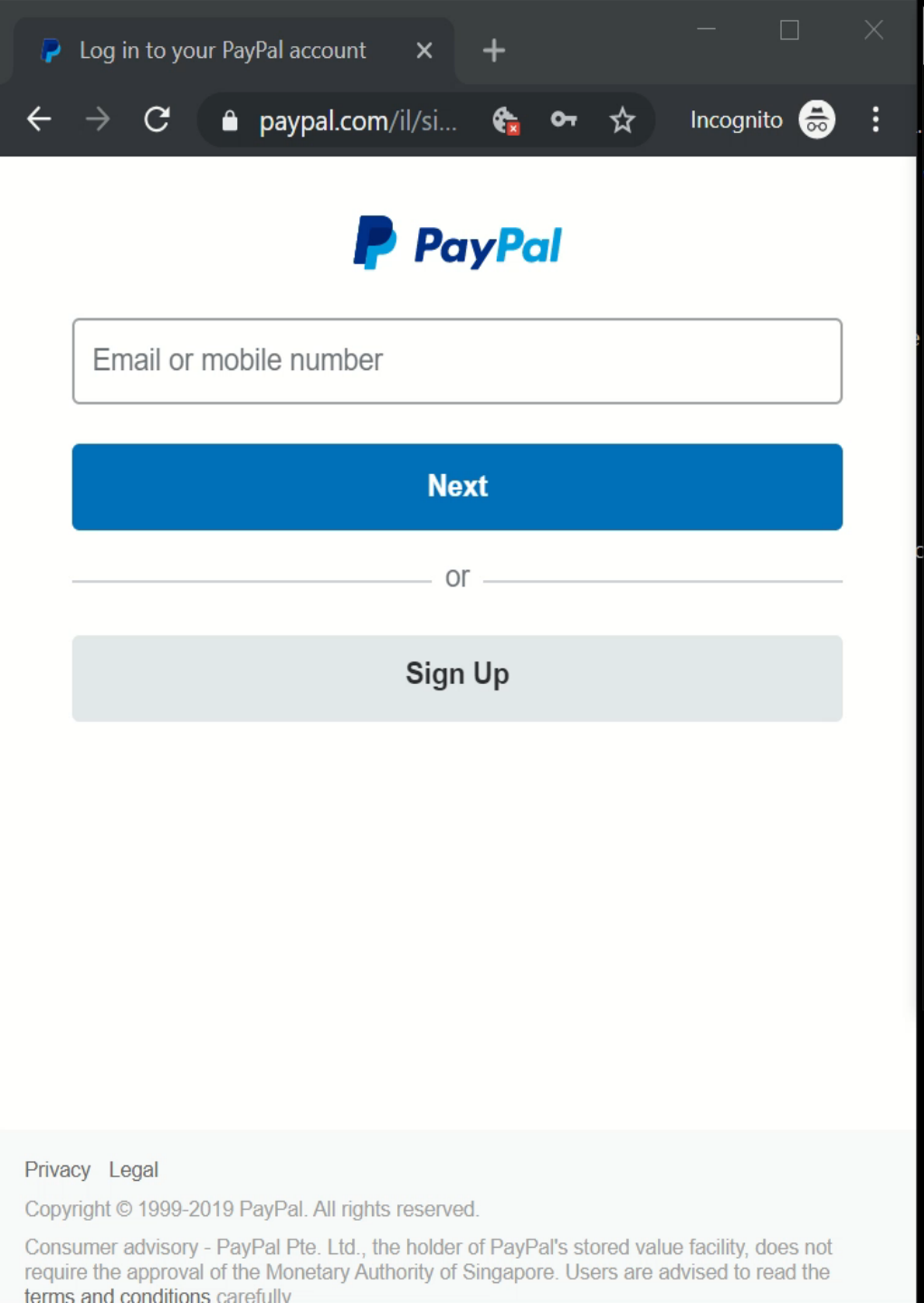
Guidance to mitigate SS7 threats

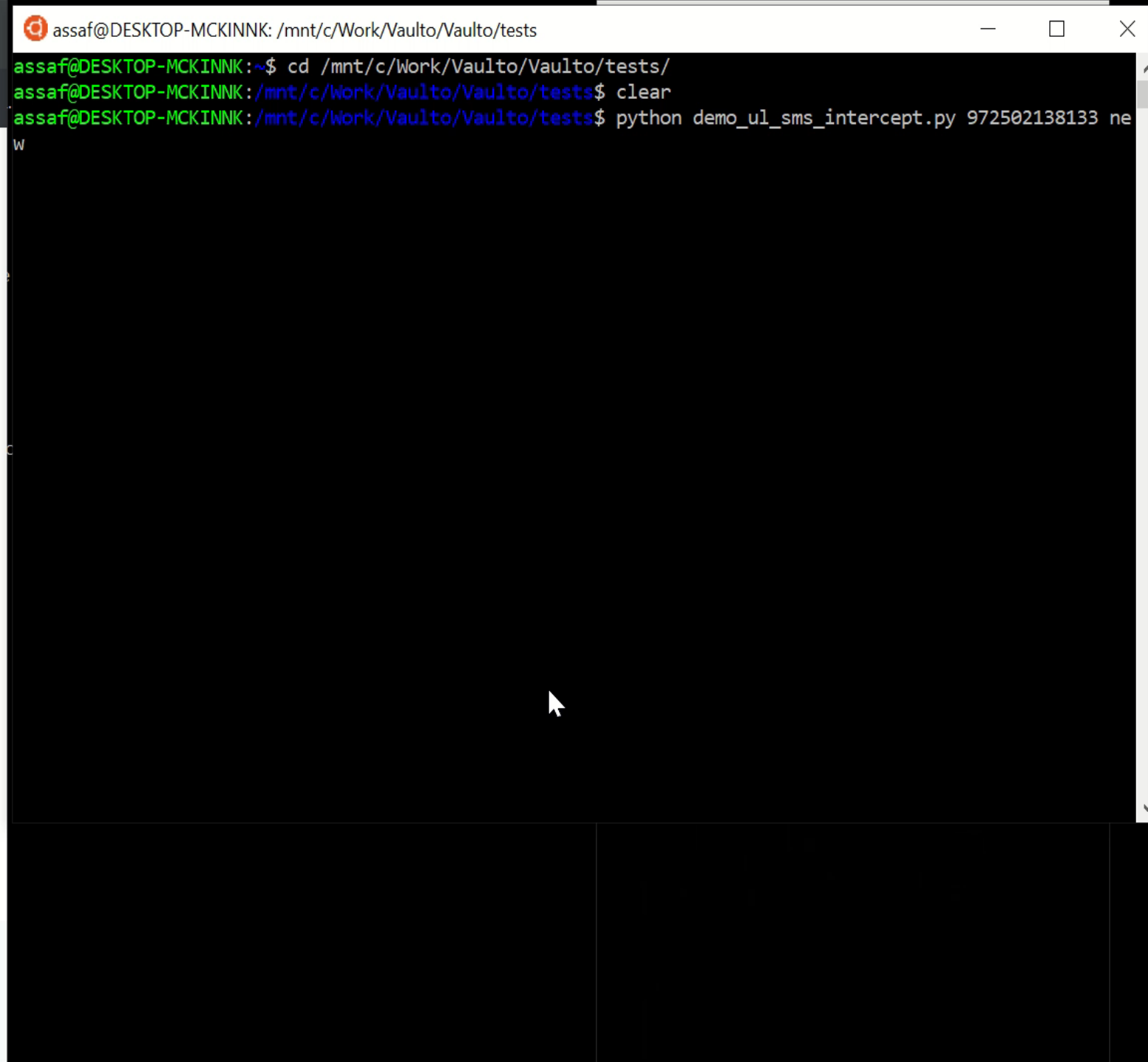
Related report: Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions

Poll Question

SS7 (Signaling System No. 7) is a network protocol used by telecom companies. Vulnerabilities in SS7 can impact the security of Digital Financial Services (DFS). ***How familiar are you with SS7 and its potential impact on DFS?***

13


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

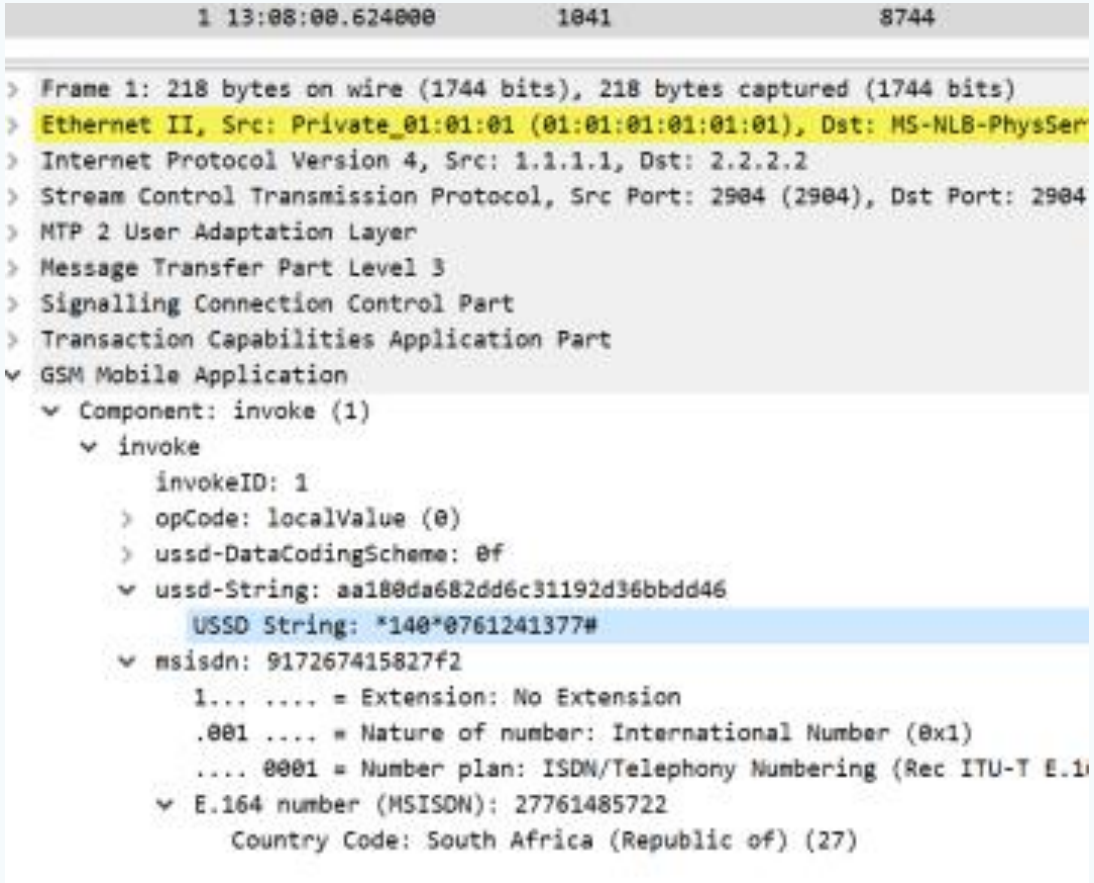

assaf@DESKTOP-MCKINNK: /mnt/c/Work/Vaulto/Vaulto/tests
assaf@DESKTOP-MCKINNK:~$ cd /mnt/c/Work/Vaulto/Vaulto/tests/
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ clear
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ python demo_ul_sms_intercept.py 972502138133 new

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.

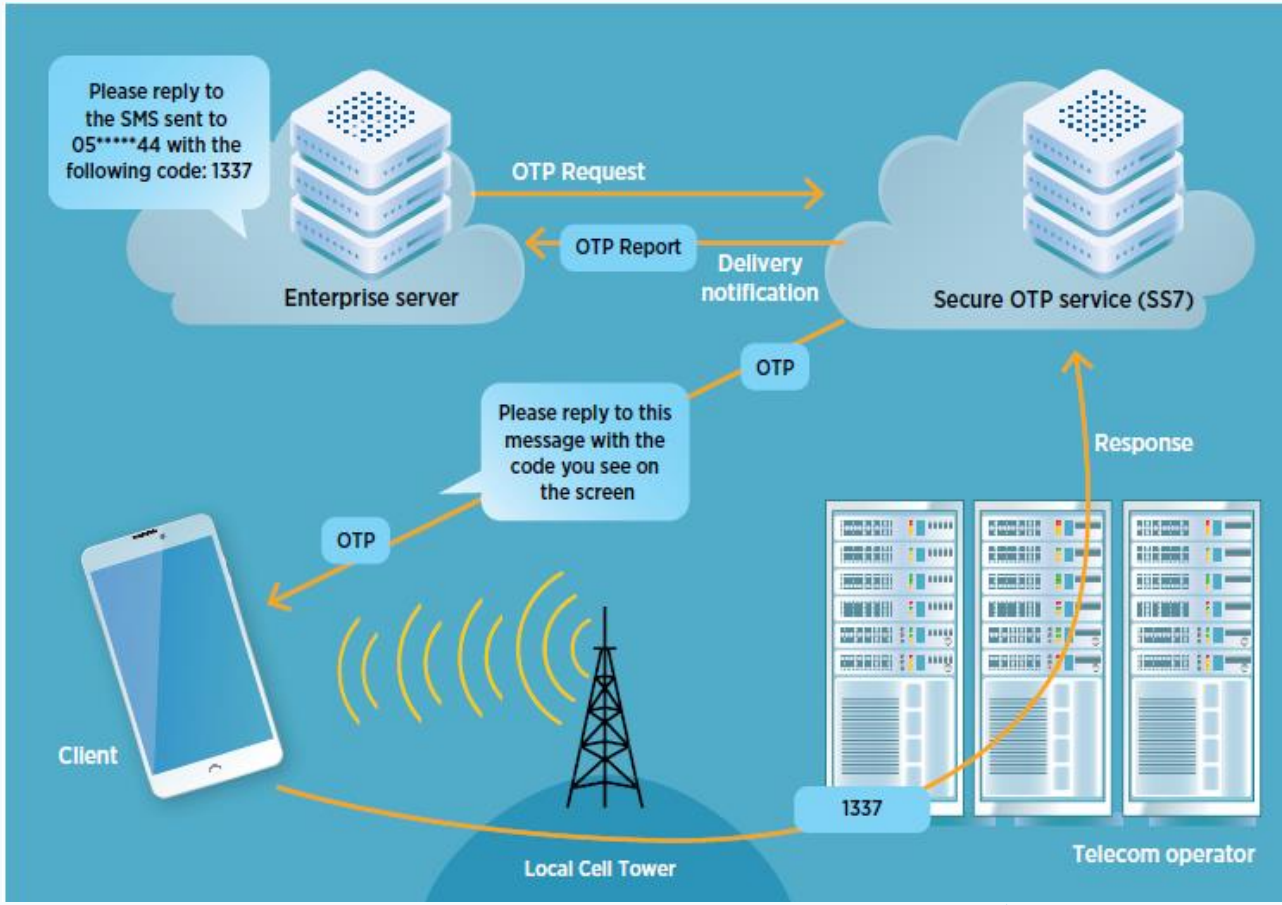
Recommendations for MNO to mitigate SS7 risks

- 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): Signaling procedures and protocols for enabling interconnection between trustable network entities in support of existing and emerging networks
- ITU-T Q.3063 (2022) : Signaling procedures of calling line identification authentication
- Draft Q.TSCA: Requirements for issuing End-Entity and Certification Authority certificates for enabling trustable signaling interconnection between network entities.
- Draft Q.DMSA: Principles for detection and mitigation of signaling attacks in security signaling gateway

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

Contact: dfssecuritylab@itu.int

Thank you!