

ITU DFS Security Recommendations Part 2

Arnold Kibuuka
Project Officer
Standardization Bureau, ITU



DFS Security Recommendations

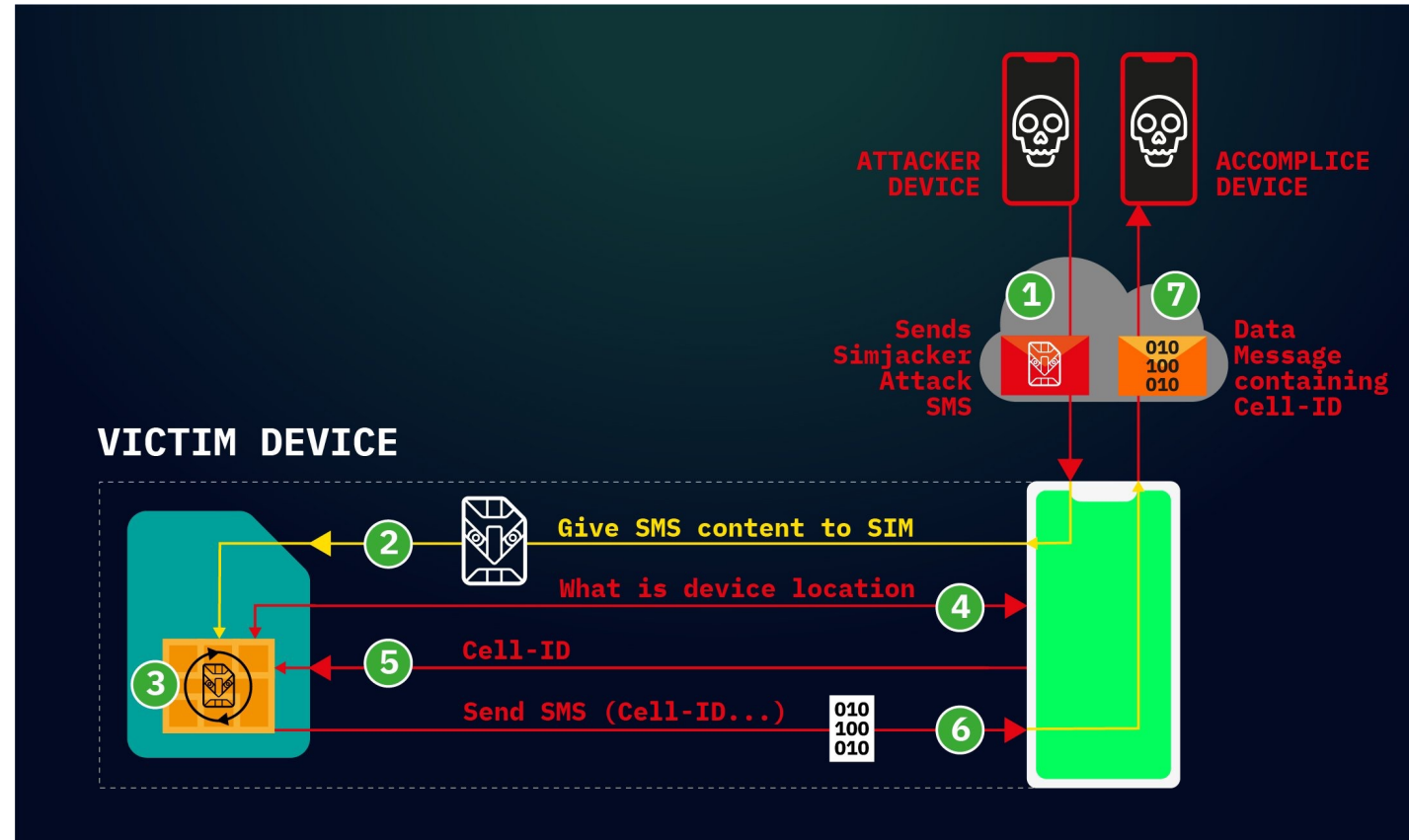
1. [Security recommendations to protect against DFS SIM related risks like SIM swap fraud and SIM recycling](#)
2. [Recommendations to mitigate SS7 vulnerabilities](#)
3. [Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security](#)
4. [Mobile Application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

Regulatory Guidance to mitigate SIM risks

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

SIM risks

1. SIM Cloning
2. SIM Swaps
3. SIM Recycling
4. Binary over the air attacks (Sim jacker and WIB browser attacks)



Source: adaptive mobile

Examples of DFS attacks

These are the 29 countries vulnerable to Simjacker attacks

Adaptive Mobile publishes the list of countries where mobile operators ship SIM cards vulnerable to Simjacker attacks.



Source: znet



Source: Nairobi News

- 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

- 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
 - including SIM swaps leading to porting of numbers to other MNOs/MVNOs
- c. Recommending security measures for DFS operators on SIM risks.

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.

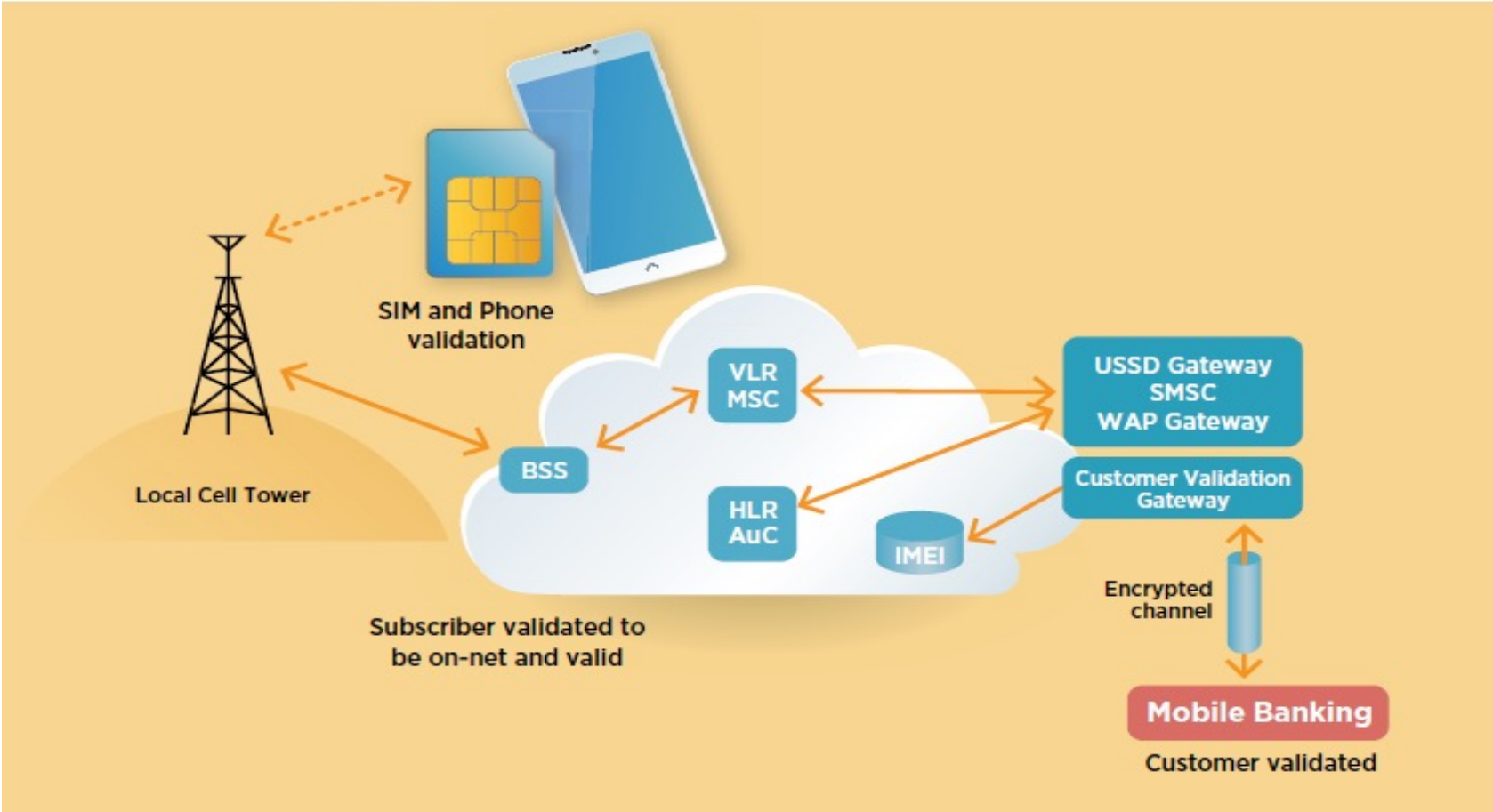
MNO controls on SIM swaps (SIM swap rules for MNOs and MVNOs)

- 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. Biometric SIM swap verification
- d. Multifactor user validation before SIM swap
- e. Information sharing with DFS provider on SIM swaps and SIM recycling:
- f. SIM swap notifications to users
- g. Secure SIM data protection
- h. Holding time before activation of a swapped SIM
- i. Customer support representatives training

DFS operators controls to mitigate SIM swaps

- a. Real time IMSI/ICCID detection
- b. Real time device change detection – device account binding
- c. Encourage use of secure DFS access

IMSI validation gateway



Guidance to mitigate SS7 threats

Related report:

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



Email or mobile number

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](#)

Recommendations for MNO to mitigate SS7 risks

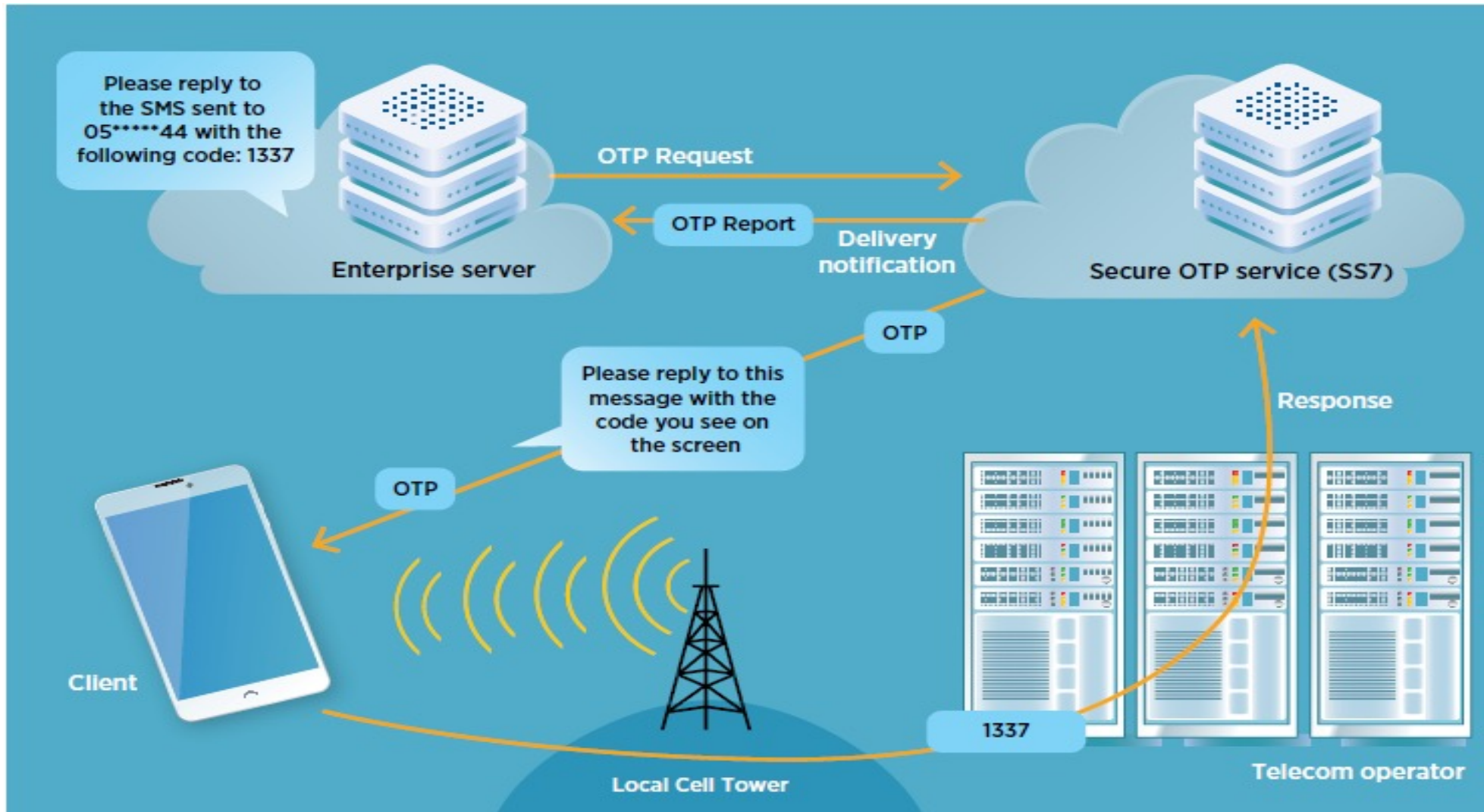
- Secure GSM ciphers for radio network traffic
- Session time out
- USSD PIN masking
- Secure and monitor core network traffic
- Limit access to traces and logs
- SMS filtering
- SMS home routing

```
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

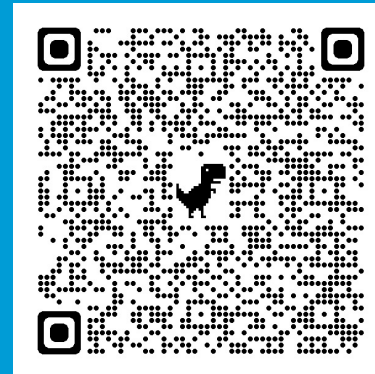
- Session time out
- Transaction limits for insecure channels
- User education
- Detecting and mitigating social engineering attacks with MT-USSD and interception of USSD
- Bidirectional OTP SMS flow

Bidirectional OTP SMS flow





Questions



Contact: dfssecuritylab@itu.int

<https://figi.itu.int/figi-resources/dfs-security-lab/>

