FIGI

FINANCIAL INCLUSION
GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

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

REPORT OF SECURITY WORKSTREAM

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

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

DISCLAIMER

The Financial Inclusion Global Initiative (FIGI) is a three-year program implemented in partnership by the World Bank Group (WBG), the Committee on Payments and Market Infrastructures (CPMI), and the International Telecommunication Union (ITU) funded by the Bill & Melinda Gates Foundation (BMGF) to support and accelerate the implementation of country-led reform actions to meet national financial inclusion targets, and ultimately the global 'Universal Financial Access 2020' goal. FIGI funds national implementations in three countries—China, Egypt and Mexico; supports working groups to tackle three sets of outstanding challenges for reaching universal financial access: (1) the Electronic Payment Acceptance Working Group (led by the WBG), (2) The Digital ID for Financial Services Working Group (led by the WBG), and (3) The Security, Infrastructure and Trust Working Group (led by the ITU); and hosts three annual symposia to gather national authorities, the private sector, and the engaged public on relevant topics and to share emerging insights from the working groups and country programs.

This report is a product of the FIGI Security, Infrastructure and Trust Working Group, led by the International Telecommunication Union.

The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Financial Inclusion Global Initiative partners including the Committee on Payments and Market Infrastructures, the Bill & Melinda Gates Foundation, the International Telecommunication Union, or the World Bank (including its Board of Executive Directors or the governments they represent). The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters. The FIGI partners do not guarantee the accuracy of the data included in this work. The boundaries, colours, denominations, and other information shown on any map in this work do not imply any judgment on the part of the FIGI partners concerning the legal status of any country, territory, city or area or of its authorities or the endorsement or acceptance of such boundaries.

About this report

This report was written by Assaf Klinger with special thanks to Dr. Leon Perlman for his helpful support and contribution and the members of the Security, Infrastructure and Trust Working Group for their comments and feedback. Vijay Mauree, ITU provided overall guidance for this report.

For queries regarding the report, please contact, Vijay Mauree at ITU (email: tsbfigisit @itu.int)

Contents

Executive Summary

The world of digital financial services (DFS) relies heavily on the underlying telecommunications infrastructure to enable users to send and receive money. In most developing countries where DFS is popular, most of the end-users do not have reliable and accessible means to connect to Internet and thus rely heavily on the mobile communications infrastructure. The communication channels with which the end-user communicates with the DFS provider are mostly Unstructured Supplementary Service Data (USSD), Short Messaging Service (SMS). USSD and SMS have long been known as "broken" and have many published vulnerabilities, some over 20 years old, which enables attackers to commit fraud and steal funds.

The core issue that inhibits the mitigation of these vulnerabilities is a misalignment of interests and misplaced liability between the telecom and the financial regulators. ITU and GSMA have long ago published guidelines and advisories to telecom operators (telco) on how to mitigate many of these vulnerabilities; however, the implementation rate of these mitigation measures is extremely low. According to surveys performed by this working group and the European Union Agency for Network and Information Security (ENISA), less than 30% of the telcos in the European Union (EU) and less than 0.5% of telcos in developing countries have implemented these mitigation strategies. This low rate of implementation is attributed to lack of awareness to the existence of these vulnerabilities and the prohibitive cost set on the telcos to implement mitigation measures. Since the telcos are not liable in cases of DFS fraud, there is no financial incentive for the telcos to mitigate these telecom vulnerabilities.

In order to advance the issue and mitigate many of these vulnerabilities, the working group recommends the following:

- Educate telecom and financial services regulators on the vulnerabilities that plague the "DFS over telecom" ecosystem;
- Telecom and financial services regulators should implement regulation that puts the liability where it should be and forces the telcos to put mitigation measures in place;
- Telecom and financial services regulators should ensure signalling security is covered in the legal framework in terms of reporting incidents and adopting minimum security requirements;
- Telecom regulators are encouraged to establish baseline security measures for each category (3G/4G/5G) which should be implemented by telecom operators to ensure a more secure interconnection environment. ITU-T Study Group 11 could develop technical guidelines for the baseline security measures;
- Create dialogue between the DFS providers and telecom regulators with the telecom security industry, by means of round tables to expose the DFS providers and regulators to the existing mitigation solutions already in the market and create an incentive for the industry to develop more solutions;
- Incentivize both the telcos, DFS providers and industry to work together and implement solutions, by either levying fines or providing grants, to build a more secure DFS ecosystem.

Abbreviations and acronyms

BTS	Base Transceiver Station for 2G/3G also know as cell tower
CISO	Chief Information Security Officer
DFS	Digital Financial Service
eNodeB	Base station for LTE a.k.a cell tower (LTE radio access element)
ENISA	European Union Agency for Network and Information Security
GTP	GPRS Tunnelling Protocol
GSMA	GSM Association
HLR & VLR	Home / Visitor Location Register, the central database that holds the telco's subscriber's information, both native and roaming subscribers.
IMEI	International Mobile Equipment Identity; An identifier used by the telecom network to uniquely identify a UE.
IMSI & TMSI	International Mobile Subscriber Identity; The mobile subscriber unique identifier, used internally in the telecom network.
LTE	Long Term Evolution, the fourth generation of cellular networks more commonly known as 4G
MAP	Mobile Application Part, an SS7 protocol that defines the signalling required for mobile, e.g. roaming, calling, SMS etc.
MO-SMS	Mobile Originated SMS, an SMS sent from the UE to the network.
MO-USSD	Mobile Originated USSD transaction, a USSD transaction initiated by the UE.
MSISDN	Mobile Station International Subscriber Directory Number
MT-SMS	Mobile Terminated SMS, an SMS sent from the network to the UE.
MT-USSD	Mobile Terminated USSD transaction, a USSD transaction initiated by the mobile network to a specific UE
MOU	Memorandum of Understanding
OTP	One Time Password.
POP	Post Office protocol
PIN	Personal Identification Number
SMS	Short Messaging Service
SS7	Signalling System No. 7—The signalling protocol used for interconnection between telecom networks and between internal sub components of each telecom network (land and mobile networks alike)
STK	Sim Tool Kit
Telco	Telecom Operator
UE	User Equipment, the user's end device, in our case the mobile phone (feature or smart)
USSD	Unstructured Supplementary Service Data

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

1 INTRODUCTION

The world of Digital Financial Services (DFS) is based mostly on telecom, since in most countries where DFS is popular, most of the end-users do not have reliable and accessible means to connect to the internet, DFS has adopted telecom as its main bearer. Due to the dominance of feature phones among users in developing economies, which comprise the majority of DFS end-users, the communication channels in which the end-user communicates with the DFS provider are mostly Unstructured Supplementary Service Data (USSD), Short Messaging Service (SMS) and Sim Tool Kit (STK). Moreover, today the signalling network is not isolated, and this allows an intruder to exploit its flaws and intercept calls and SMSs, bypass billing, steal money from mobile accounts, or affect mobile network communications even in developed countries.

USSD and SMS as means of communication have long been known as susceptible to attack and have many published vulnerabilities. Exploiting these vulnerabilities enables attackers to commit fraud and steal funds from unsuspecting victims, who in in most cases are unaware their account is being compromised or hacked.

This document surveys telecom vulnerabilities and their impact on digital financial services, both on the end user's side and the service provider's side. This document helps DFS providers understand the telecom vulnerability situation and create mitigation strategies to safeguard their clients.

2 IMPACT OF TELECOM VULNERABILITIES ON DFS

Telecom vulnerabilities enable criminals to perform various attacks that result in fraud to steal digital money; many of these attacks involve the attacker masquerading as the DFS provider to fraud the end-user or the attacker masquerading as the end-user to fraud the DFS provider. In all these cases, the attacker uses telecom vulnerabilities to pass authentication and perform actions on compromised accounts. For example:

2.1 Over the counter cash fraud

In this example, a fraudster walks up to a DFS agent (for example a seven-eleven branch) and requests cash withdrawal from his account. The fraudster provides the victim's account number to the agent, when the agent initiates the transaction, an SMS verification code is sent to the victim, however, this verification SMS is intercepted by the fraudster, and used to complete the fraud and steal the money.

2.2 Account takeover

In this example, a fraudster uses USSD to takeover an account that does not belong to him. To perform this attack, the fraudster first needs to spoof his victim's phone number and dial the USSD code (this can be done by over the air interception, explained further in Section 7). Once the fraudster initiates the USSD session with the DFS provider spoofing the victim's phone number they can change the PIN code and add another phone number to the account. Once done, the fraudster performs another USSD session, this time with the new phone number they added and uses the new PIN to login to the account and transfer the money out.

2.3 Social engineering

There are many ways of social engineering, in this example; the fraudster uses USSD to perform social engineering that misleads the victim to give away the account number and PIN. To perform this attack, the fraudster impersonates the DFS provider and sends a USSD message to the victim telling him that there is a pending money transfer for his account, and in order to receive it the victim enters his account number and PIN in the USSD dialog. Once done, the attacker now has the victim's account number and PIN and can take over the victim's account.

3 TELECOM VULNERABILITIES AND ATTACK SURFACES

Telecom vulnerabilities can be exploited through two attack surfaces, the SS7 network and the cellular air interface:

- The SS7 network is a legacy signalling network interconnecting **all cellular operators in the world,** the SS7 protocol[1] that is used for signalling has been around since the 1980's, and the latest move to Diameter protocol[2] (for 4G-LTE networks) did not solve any of the basic vulnerabilities found in SS7.
- The cellular air interface (the radio frequency communication between the cell phone and the cellular network) has been a major attack surface since the inception of cellular communications. Interception of these radio communications enable intelligence collection and espionage capabilities without the requirement that the perpetrator have access to the cellular network. Despite the evolution to newer generations of cellular networks (3G/4G) with stronger security measures, most off-the-air interception systems have successfully overcome these measures. Furthermore, even when 2G air interface encryption is easily decrypted and open-source software to crack the encryption is available; many 2G networks remain active.

4 COMMON TYPES OF TELECOM ATTACKS

TABLE 1: Common types of telecom attacks

ATTACK	DESCRIPTION	IMPACT ON DFS
Spam	Routing a short message to the Mobile Terminating device has a cost, charged to the sender. An attacker can send bulk SMS messages, bypassing the correct route, and hence evading billing. Another option is to spoof various SMS parameters, such as sender ID, or bypass a control system to send directly SMS to victims.	Massive sending of SMS and calls, with the goal of stealing personal data, or gain financial benefits using toll numbers.
Spoofing	Identifiers (addresses, names and subsystem numbers) used at various levels of SS7 and Diameter are not authenticated and may be spoofed by malicious actors.	Billing evade, in the case where the telecom operator is also the DFS provider and the currency used in credits (trading top-ups, not e-money). An attacker can top-up a sim card with another subscriber's identity and evade payment
Location tracking	An attacker can locate a target subscriber based on MSISDN. As mobile networks need to efficiently route messages to subscribers, the home network knows where to send messages to contact any given subscriber. In some cases, the attacker does not even need to send messages, since passive eavesdropping may reveal the target location. Obtaining subscriber's visited location is also a prerequisite for further attacks such as intercept.	Obtain the approximate location of a given victim. This information is used for social engineering to fool the user into giving up DFS account credentials.
Subscriber fraud	An attacker can tamper with subscriber's profile, or send signalling messages to trigger malicious charging, with the objective to benefit from a service while evading billing.	Objectives can be: To get or steal prepaid voice, SMS or data credits, and convert them into mobile money or goods/services. To alter charging, e.g. overbill another subscriber or simply evade it (applies to DFS in the case the telecom operator is also the DFS provider) To abuse mobile money services based on MAP USSD
Intercept	An attacker can alter current subscriber's location and profile in order to receive mobile terminating and/or mobile originating calls, SMS, or data traffic. This attack allows eavesdropping victim's communications, or may involve a full man-in-the-middle with alteration of communication. Access to signalling interface, allows an attacker to organize efficient local interception attacks based on fake antennas.	SMS is commonly used for second factor authentication (2FA), attackers may also eavesdrop SMS in part of a larger attack, to circumvent 2FA.
Denial of Service (DoS)	An attacker can cause a denial of service to the whole network, or to a set of subscribers, or even to a single targeted subscriber. Mobility offers functions to remove a subscriber from a specific geographical zone, and an attacker can use it to deny a service to a specific user.	Typical high-level impact is a regional network equipment reboot, which would discard all currently attached subscriber's contexts. As it is repeatable at will, it can cause persistent service unavailability.
Infiltration Attacks	An attacker can abuse interconnect to obtain access to otherwise inaccessible systems. User data is tunneled when traversing the mobile core network. Misconfigurations may allow attackers to get illegal access to part of the mobile core network. Attackers may also get access to mobile core network systems via mobile data or operational interfaces, which may lead to other attacks.	Unauthorized access to mobile core network elements. Typical impacts include personal data theft, or access to other sensitive assets such as other Packet Data Networks.
Routing Attacks	Interconnect based on packet networks make use of routing (a process of selecting a path for traffic in a network), and hence may be sensitive to routing hijack attacks.	Due to the lack of integrity checks and encryption, an attacker may eavesdrop or alter interconnect traffic.

5 THE COMMONALITY OF TELECOM ATTACKS

According to research conducted by ENISA,[3] 39 electronic communication providers across the European Union (EU) were surveyed on the commonality and frequency of telecom attacks. More than 80% of the surveyed telecom operators in the EU responded they have detected or encountered some attacks, and about 25% reported encountering a substantial number of attacks, as seen in the following chart. However, at this point, the low number of reported attacks can be affiliated to the lack of detection mechanisms in place within the telecom operators, a fact shown in Figure 2.

According to the SIT workstream survey, over 70% of the telecom regulators and telecom operators surveyed have no clue if their networks are under telecom attacks.

The telecoms that detected attacks identified them in the categories shown below. It is visible that attacks directly associated to DFS fraud, such as spoofing, SMS interception, and subscriber fraud take a dominant percentage in the chart.

FIGURE 1: Frequency of telecom attacks in the EU (survey)

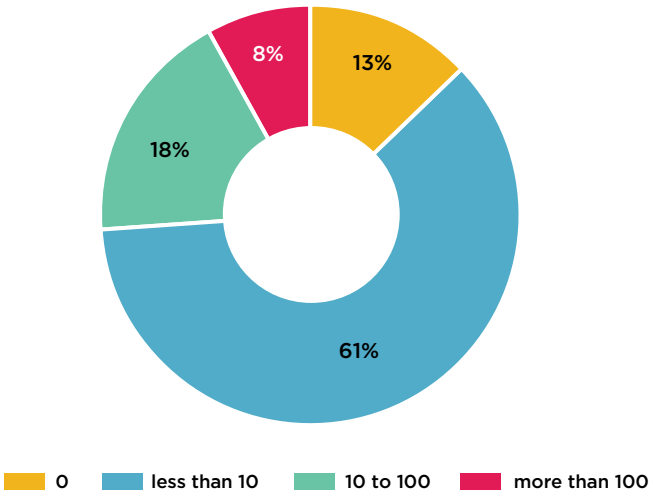
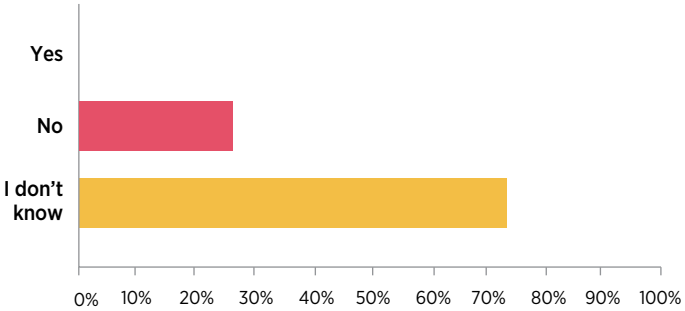


FIGURE 2 Awareness to telecom attacks in the developing world (survey)



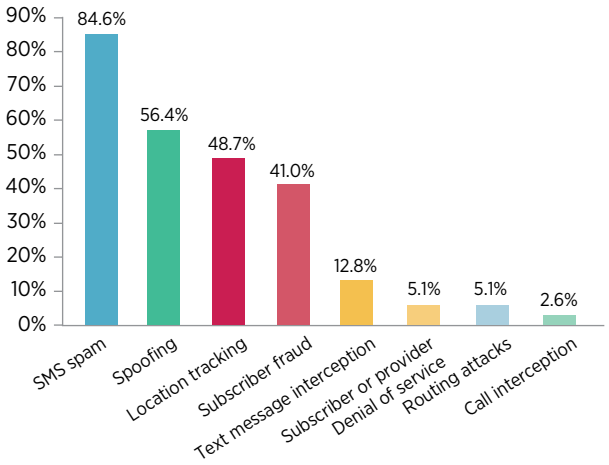
6 THE CHALLENGE

Protection of these two attack surfaces is considered to be exclusively in the cellular operators' domain, i.e. if the operator implements measures to protect itself, all of the subscribers that use the network will be protected. However:

- Most cellular operators have not yet protected their networks against these attacks even though the GSMA and ITU (global telecommunication governing bodies) have issued guidelines[5] on how to defend against such attacks.
- Operators that did comply with these recommendations, in most cases only implemented these guidelines[6] partially, maintaining part of the vulnerabilities in their networks.
- Network operators cannot protect against most of the air interface vulnerabilities, even more so when the subscriber is roaming.

The challenge therefore remains, how can a DFS provider or client defend themselves from cellular attacks without relying on the mobile operators to solve this issue?

FIGURE 3: Types of telecom attacks in the EU (survey)



7 MISCONCEPTION: IS IT NOT HARD TO ATTACK THE TELCO? GOVERNMENTS DO THAT

This misconception is common among CISO's and cyber security officers in enterprises today. The barriers for entry have dropped significantly, and today, every hacker with ~$500 in to spare can exploit cellular vulnerabilities.

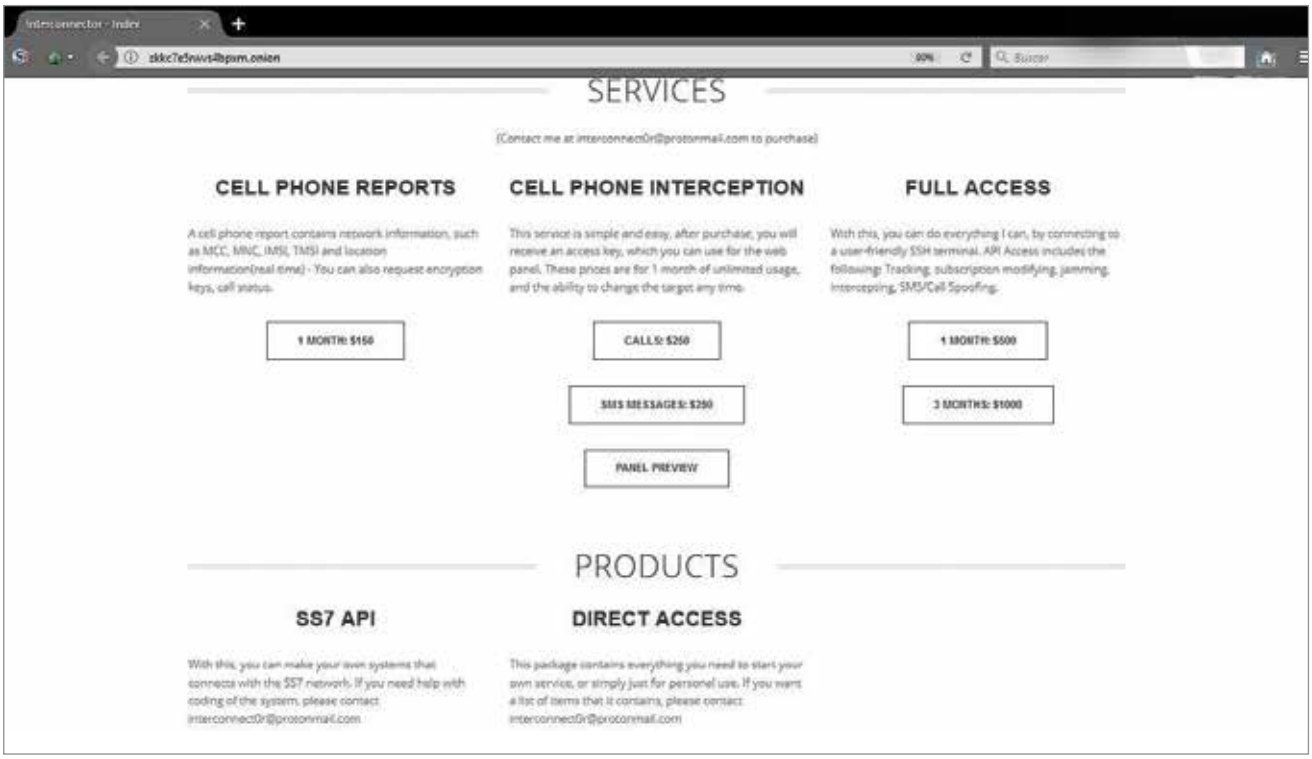
For Example: Using home brewed cellular off-the-air Man-In-The-Middle (MITM) system an attacker can intercept cellular communications in their proximity. Since the encryption can be cracked,[6] all of the calls, SMS and http traffic from/to the intercepted device can be decrypted. Today, creating a basic MITM system like one below in figure 4, requires ~600$ worth of hardware that can be purchased on eBay and open-source software from the internet, nothing more.

Another example to show the relative ease of performing cellular attacks is SS7 network access. The SS7 network used to be considered a "walled-garden" which could only be accessed by licensed mobile operators. Today with the spread of bulk-SMS providers, Internet of Things (IoT) and location-based services, other non-licensed entities have gained access to the SS7 network.

Consequently, more businesses and individual with direct access to the network and intermediaries are selling their access on the dark web. For $150–$2500, a hacker can gain unauthorized access to the SS7 network and exploit cellular vulnerabilities without requiring any infrastructure at all.

FIGURE 4: A rudimentary MITM interception system based on commercial HW and open-source SW

FIGURE 5: A dark web site selling SS7 access



8 THE CELLULAR ATTACK KILL CHAIN

In order to gain access to sensitive data such as banking credentials and execute attacks such as online account-takeover (ATO) the attacker needs to obtain information essential to performing the attacks. Table 2 below illustrates how an attacker can obtain the information required to execute every step in the kill chain by leveraging the cellular attacks surfaces:

9 EXAMPLES OF ATTACKS ON DFS INFRASTRUCTURE

9.1 SMS OTP interception

SMS One Time Password (OTP) is the most popular method today for identification strengthening of authentication processes. The vast majority of DFS providers use SMS OTP today worldwide. Using SS7 or Over-The-Air Man-In-The-Middle (OTA-MITM), SMS interception, An OTPs obtained from the intercepted SMS can be used maliciously to gain unlawful access to users' accounts. An attacker can use the intercepted OTP to recover passwords / PIN codes to accounts or combined with a USSD attack (described below) switch the phone number associated to an account. Here is an example of OTP interception and use for unlawful access to an online account:

TABLE 2: Telecom attacks and the kill chain

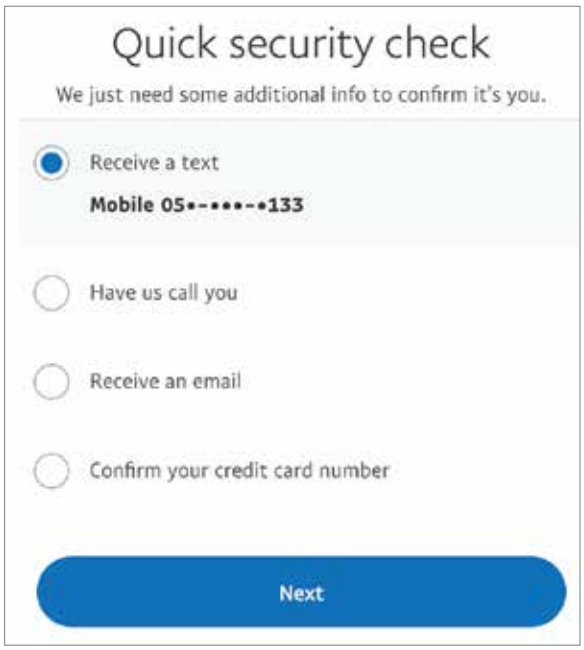
STAGE	TELECOM ATTACK SURFACE	SS7 ATTACK SURFACE	MITM ATTACK SURFACE
Information gathering	Victim's phone number	Social engineering	Social engineering
	Victim's IMSI	SS7 query (must obtain TMSI first)	IMSI catching (of all phones in the vicinity)
Location leak	Track the victim's location	SS7 query	Triangulation
Data leak	Intercept calls and SMS	Roam (using UL[7]) the victim to intercept incoming SMS Reroute the victim's calls using Call-forwarding to intercept incoming calls Modify the victim's profile in the HLR/ VLR to intercept outgoing calls and SMS (via the billing mechanism)	Downgrade the cellular RF link to 2G or 3G and obtain the encryption keys (various methods), this will result in both incoming and outgoing call and SMS interception.
	Intercept USSD transactions —acquire mobile banking account credentials	Phish the victim's mobile banking credentials using social engineering—see elaboration in figure 6	Intercept the victim's credentials from an existing USSD transaction performed by the victim
	Intercept the mobile data channel and perform MITM	Reroute the GTP tunnel of the subscriber in order to connect to the internet via the attacker's POP	Provide GPRS/EDGE/UMTS support to the mobile device and tunnel the mobile data connection through the system
Cyber attack	Credentials to online accounts (bank / email / etc.)	Use extracted USSD credentials to mobile money account. Use intercepted OTP SMS to login to online account.	
	Malware implant on the mobile device	Implant malware on the phone by exploiting a browser vulnerability (inserting an iframe with a link to an infection website inside a requested web page)	

a) **Step 1: "I forgot my password"**
The attacker enters the login portal and initiates the "restore password" flow

FIGURE 6: Initiate the "password recovery" flow

b) **Step 2: Opt to receive an SMS OTP for authentication**
The attacker enables an SS7 / OTA-MITM interception on the victim and selects the "send me an SMS OTP" option in the "recover password" flow:

FIGURE 7: Select the option of SMS OTP for authentication

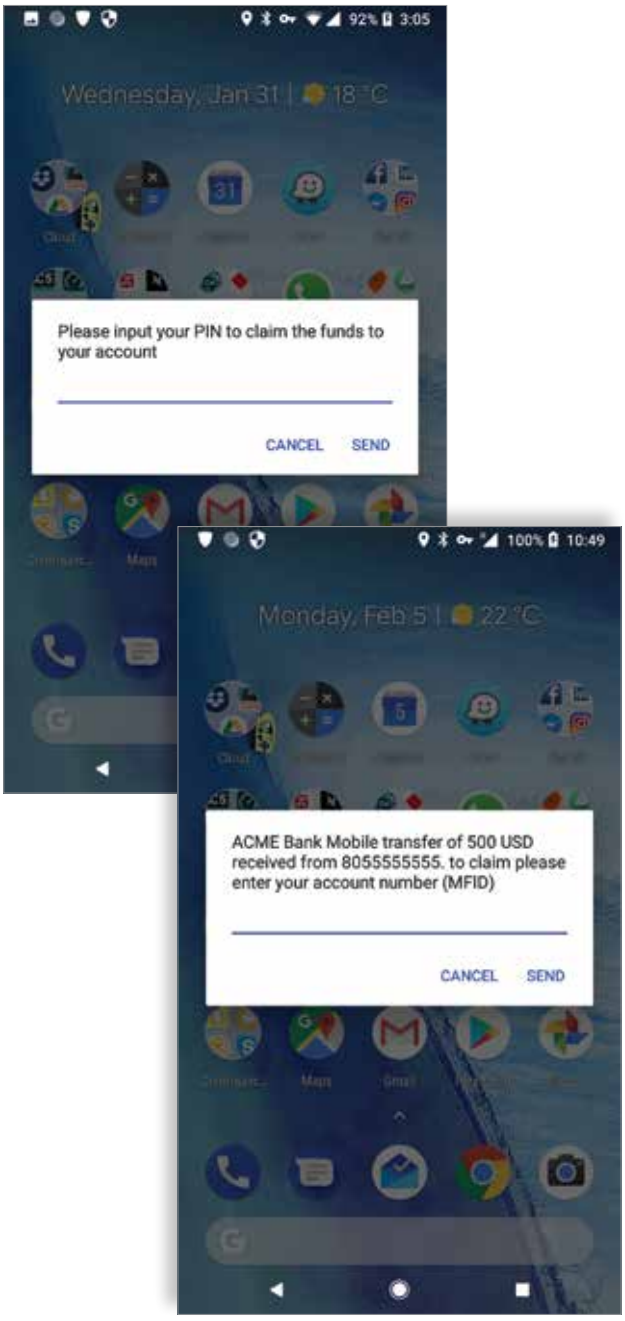


c) **Step 3: Use intercepted OTP SMS and gain access to the account**
In this step, the attacker uses the code sent via the SMS OTP. Since the victim does not receive the same SMS, thus is completely unaware of the attack taking place. Once the DFS provider's online system verifies the code the attacker typed, it lets the attacker login to the victim's account and transfer funds.

9.2 Social engineering of sensitive credentials using USSD

Unstructured Supplementary Service Data (USSD) is used for, online banking and other financially sensitive applications. Due to the high level of assumed trust by the users (when receiving USSD messages), the simplest attack to execute and scale an attack is using USSD to send a fraudulent message to the user spoofing the identity of the financial service provider, luring the user to divulge sensitive information such as account number and PIN code. For example, to phish these credentials, the attacker sends a phishing USSD message: Such as in figure 8 below.

FIGURE 8: Using USSD to socially engineer the user



Since there is no identification in the USSD message, and the user is used to having these messages from the network, trust is achieved, and the user divulges their account number and PIN. From there on, the attacker logs into the account and transfers the funds out.

9.3 Denial of service attacks

Using SS7 an attacker can cause Denial of Service (DoS) for selected subscribers or cause a network wide outage. There are various ways to create a DoS attack, for example: sending an Update Location message with an out-of-network serving address will block all incoming calls and SMS from reaching the subscriber; deleting a subscriber record from the serving VLR[8] will cause a DoS for a given subscriber until the record is re-inserted to the VLR. Performing each attack in scale (automatically for a range of IMSIs) can cause a network wide outage. However, in most cases, since these SS7 DoS attacks are not affecting the radio network, performing an outgoing transaction such as placing a call or sending an SMS will reverse the effects of the DoS almost immediately.

9.4 SIM card swap

Another way to takeover accounts is by performing a "SIM swap". An example of this attack is the case that the attacker social engineers the mobile carrier to issue them a SIM card belonging to the victim, by impersonating the victim at a point of service, and claiming that they have lost the original SIM card. If successful, they have obtained a cloned SIM. Once in possession of the cloned SIM, the attacker accesses the DFS provider's USSD menu and resets the PIN of the account. The attacker uses the cloned SIM to receive the OTP SMS and confirms the new PIN. From there the attacker has essentially taken over, can log in to the account and transfers the funds out.

For Example: Airtel Money account wiped clean by the same tricksters.[9] They called him on the pretext that they wanted to assist him with sim card registration and upgrade to fourth generation (4G) technology. In the course of the conversation, they asked him to dial *102#, the sim swap code. The next thing he realized he could not receive or make calls and his Airtel Money account was drained.

9.5 SIM card recycle

SIM card recycle is not an SS7 attack, but rather a lack of due care and due diligence by the DFS provider that gives an unauthorized person access to funds belonging to other people.

The SIM recycle scenario is as follows:

- Person A is issued a prepaid SIM card and opens a DFS account using the associated phone number.
- After a few months of usage, Person A stops topping-up the prepaid SIM card, meanwhile, Person A still has a positive balance on this DFS account associated with the phone number.
- After a dormancy period usually (1-6 months) of no usage and topping-up the SIM, the network operator cancels the SIM and will no longer be active, effectively disconnecting Person A from the DFS account (which may still have funds).
- Person B is issued a new prepaid SIM card by the network operator which has Person A's phone number (that's the recycle action)
- Person B can now access Person A's DFS account and use whichever funds remained in the A's account.

10 MITIGATION STRATEGIES FOR MOBILE OPERATORS

The SS7 attack surface is the domain of the mobile operator, global telecom organizations such as ITU and GSMA have noticed the problem and issued guidelines for mobile operators to mitigate these attacks, these guidelines are covered in several documents. The GSMA RIFS sub-group authored a range of SS7 and Diameter signalling security related documents in response to the attacks described above, which tackle different aspects of the signalling security problem. Those documents are GSMA internal and accessible to members only, therefore, no exact reference is given and companies that have access can find those documents in the GSMA internal tool easily with the given information below. We will provide here a snapshot on what industrial standards exist and describe on high-level what they offer in form of practical mitigation.

GSMA members can access these documents here: https://www.gsma.com/newsroom/gsmadocuments/technical-documents/

10.1 FS.11: SS7 interconnect security monitoring guidelines

This document describes how to monitor SS7 traffic for potential attacks. The first step in improving signalling related security is to evaluate, what state the network is in. The main question is, is it under attack, what kind of attacks. In this document, mobile operators can find strategies on how to effectively monitor traffic, how long, how to classify incoming MAP messages that are arriving on the interconnection interface. It lists mitiga-

tion strategies for many SS7 attacks on 2G/3G network. Based on the filtering rules found in this document an operator can determine if a message that arrives at the interconnection interface is legitimate, prohibited, unauthorized, suspicious or otherwise "strange".

10.2 FS.07 SS7 and SIGTRAN network security

This document provides substantial background how to handle SS7 messages on the edge of the network. It describes the whole SS7 stack, while putting emphasis on the MAP protocol level, where attacks are most common. It provides security analysis for SS7 and SIGTRAN. It lists a set of countermeasures for many SS7 attacks, and recommendations on how they can be deployed. FS. 07 also contains details on how to configure an SS7 firewall or an edge node to stop unauthorized messages and attacks from reaching the core network, for all MAP v2/3 messages and provides countermeasures for the currently known SS7 attacks.

10.3 IR.82 security SS7 implementation on SS7 network guidelines

This document outlines general security measures for SS7 security, which include for example SMS specific security measures and many SS7 stack related security measures. It should be seen as a toolbox for operators, as not every measure mentioned in this document can be deployed in every network.

10.4 IR.88 LTE and EPC roaming guidelines

This document outlines LTE interconnect (roaming) security measures. It is the LTE counterpart to the IR.82. It contains a security toolbox for Diameter, it covers aspects like routing attacks, DoS, location tracking and other types of diameter-based interconnection attacks on the SCTP, GTP and interface specific recommendation e.g. S6a, S9, S8. It also tackles legacy interworking, SMS security and charging and policy related security aspects.

10.5 Mitigations in GSMA documents vs common telecom attacks

TABLE 3: Coverage of mitigation strategies in GSMA documents vs common SS7/Diameter attacks

Attack	FS.11 (2/3G)	FS.07 (2/3G)	IR.82 (2/3G)	IR.88 (4G)
Spam	✘	✓	✓	✘
Spoofing	✓	✓	✓	✘
Location tracking	✓	✓	✓	✓
Subscriber fraud	✘	✓	✓	✓
Intercept	✘	✓	✘	✘
Denial of Service (DoS)	✓	✓	✓	✘
Infiltration attacks	✓	✓	✓	✓
Routing attacks	✘	✓	✓	✘

11 IMPLEMENTATION OF MITIGATION AMONG MOBILE OPERATORS

Mobile operators have not really addressed the issue of SS7 telecom vulnerabilities. This is demonstrated by the ENISA survey in the EU and the Security Infrastructure and Trust workstream survey by the ITU within the developing world. According to ENISA's survey most telecom operators only addressed this issue by implementing SMS home routing[10] and performing some filtering[11] on signalling nodes. Only about a quarter of the telecom operators have implemented any of the mitigation strategies mentioned in Section 11 above. In the developing world the majority of the telecom regulators and telecom operators surveyed did not know about these mitigation strategies, and for those who knew, the implementation rate was very low (below 10%).

The reason for this low implementation rate is simple, implementing strong mitigation strategies are cost inhibiting for the telecom operator. About 75% of the surveyed operators in the EU replied that cost is the inhibiting factor in implementation, that and the lack of regulation mandating it.

FIGURE 9: Implementation of mitigation in mobile operators within the EU

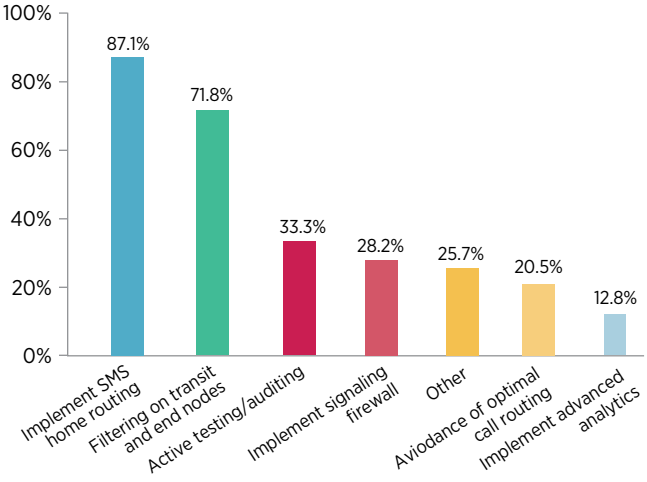
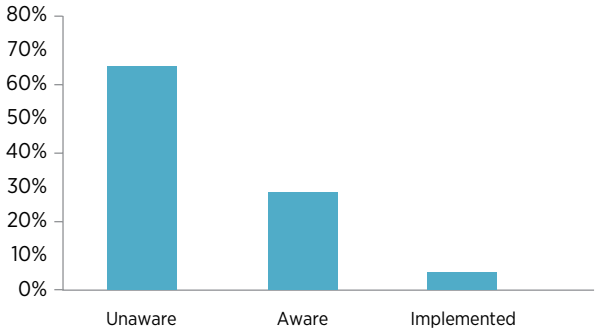


FIGURE 10: Mitigation implementation in the developing world



12 MITIGATION STRATEGIES FOR DFS PROVIDERS

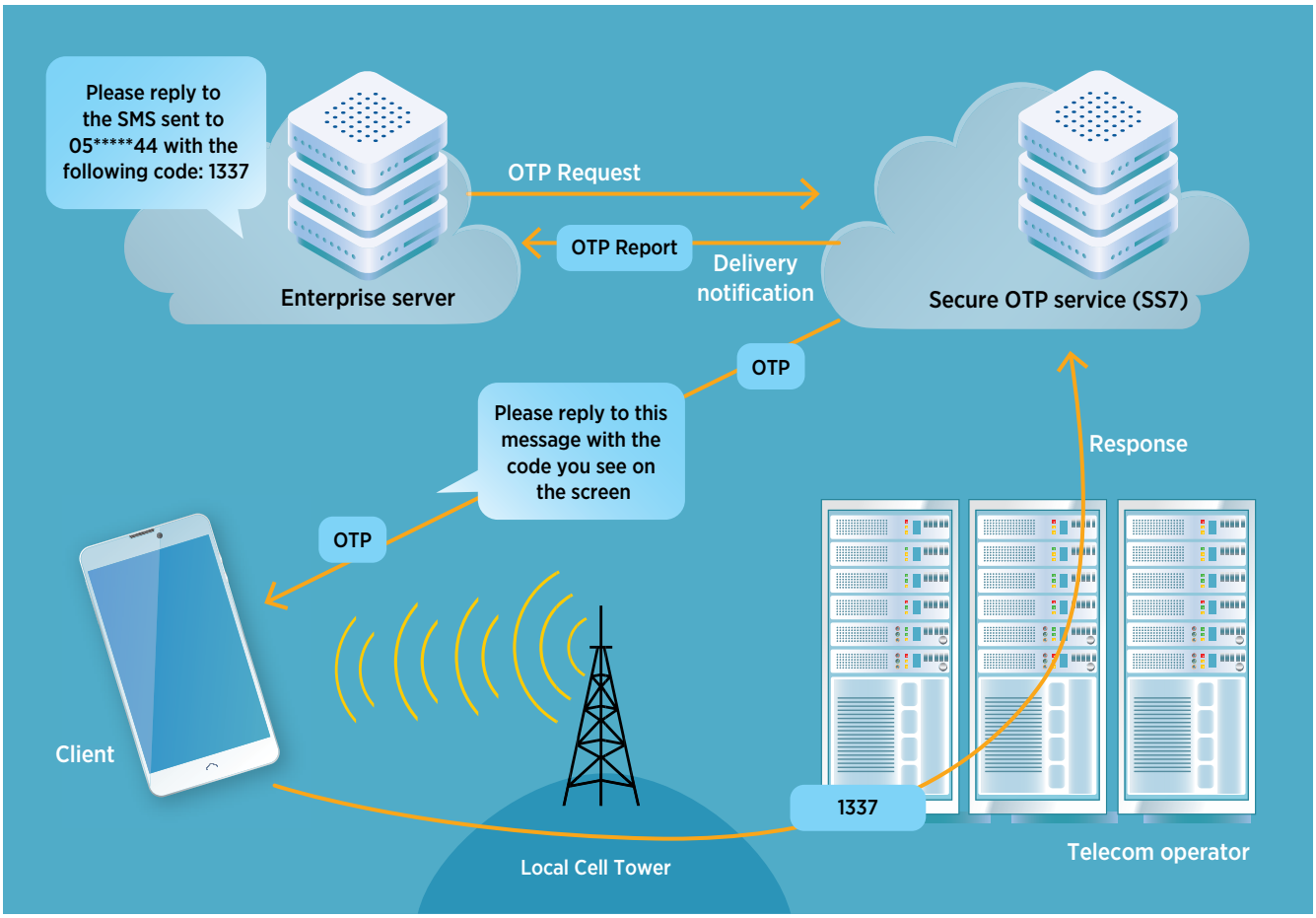
The first and foremost the DFS provider can do to avoid these attacks is implement another out-of-band authentication outside the telecom ecosystem, this is possible for clients that use smartphones and access the DFS via the smartphone app. DFS providers should implement best of breed authentication and encryption mechanisms.

However, since many DFS users do not own a smartphone and access the DFS via USSD or SMS. In that case, although the recommendations and the strategies described above mitigate most attacks mentioned in this paper, the majority of cellular operators in the world did not implement the GSMA published guidelines. This creates a situation for the DFS provider that suffers fraud due to vulnerabilities they cannot close or mitigate. However, using SS7 connectivity the DFS provider can implement mitigation strategies for the attacks above. Here are some examples of mitigation strategies that can be used requiring SS7 connectivity, but not requiring any investment from the mobile operator.

12.1 Detecting and mitigating account take over using intercepted OTP SMS

In order to detect and mitigate this attack, a different approach to SMS OTP needs to be taken. The DFS provider should make the authentication flow bidirectional, that is receive the OTP from the user, not send it. This requires displaying the OTP code in a view resource (e.g. webpage) and sending a SMS to the user to reply the code they see in the view resource. This flow allows the DFS provider, given SS7 access to determine if the reply SMS originated from the legitimate user or from an attacker. This is done by looking at the SCCP metadata from the reply SMS and verifying the Global Title (GT) it came from as legitimate and matching the user's location and home network. The following illustration describes the process:

FIGURE 11: Detection and mitigation of SMS interception



12.2 Detecting and mitigating social engineering attacks with MT-USSD

Once the attacker solicits the account number and PIN from the victim, they will attempt to use it with another phone and register the new phone to the account in order to transfer funds. Alternatively, use the account number and PIN to withdraw funds at an ATM or convenience store or kiosk (e.g. 7-Eleven).

Once the DFS Provider receives the transaction request, before authorizing it the DFS provider needs to ascertain the following:

a) The location of the account holder's phone is indeed near the ATM or kiosk where the transaction is taking place (if this is an ATM transaction).

b) Provide the IMSI and IMEI of the phone preforming the transaction in order to check with the cellular carrier if the owner of the IMSI and phone is the account holder.

c) Verify with 2-way SecureOTP[12] to the original phone number to verify the legitimacy of the transaction.

12.3 Detecting and mitigating interception of MO-USSD transactions

Once the fraudster intercepts the account Number and PIN from the victim they will attempt to use it. The attacker has two main ways to use the intercepted credentials:

a) During the MITM session, while the victim's SIM is cloned in the MITM system, the attacker can initiate MO-USSD session from the MITM system.

b) After the MITM session the attacker will attempt to use it with another phone and register the new phone to the account in order to transfer funds (just like in the scenario above).

We will detail how to detect the first scenario since the second is the same as above. Once the DFS Provider receives the transaction request, before authorizing it the DFS provider needs to ascertain the following:

a) Check if the IMEI of the device performing the transaction matches the IMEI of the account holder's phone (an MITM system may clone the SIM with a different IMEI).

b) Compare the location of the phone preforming the current transaction to the last reported location of the phone (last in/out SMS or call), since once under the MITM system the attacked phone changes its network location abruptly.

12.4 Detecting and mitigating unauthorized SIM card swap

Once the attacker is in possession of the new SIM, they perform the transaction to reset the PIN code using OTP SMS. Once the DFS provider receives the transaction request, before authorizing it the DFS provider needs to ascertain the following:

a) Check if the IMSI associated with the phone number has changed, this is an indication of SIM swap.

b) If there is an indication of a SIM swap, check the IMEI of the phone holding the SIM. If the IMEI has also changed, there is a high probability of SIM swap. In that case the DFS provider should block the account until performing account verification procedures, for example, via a voice call or an agent.

c) Systems and procedures to detect suspicious SIM swap behavior can be implemented. These rely on *inter alia.*

Regulatory rules on SIM swaps, including:

a) Standardization by regulators of SIM swap rules amongst MNOs/MVNOs by the regulator, including SIM swaps leading to porting of numbers to other MNOs/MVNOs.

b) Identification to an MNO/MVNO or its agents of persons requesting new SIMs including an affidavit signed by the subscriber and a passport photograph of the subscriber where the replacement is to be done by a proxy.[13]

c) Where SIM replacement is carried out by proxy, the MNO/MVNO or its agents must capture a facial image of the proxy which must be kept for twelve (12) months.[14]

d) Rules that a SIM should be replaceable only if it is faulty, damaged, stolen, lost, obsolete (but eligible for replacement or an upgrade), and any other reasonable legitimate reason or condition necessitating a SIM replacement.[15]

Internal rules on SIM swaps by MNOs/MVNOs including:[16]

a) 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.

b) A general 2-4 hour holding time from the time of a SIM card request to providing the new SIM card to the requestor.

c) Challenge questions posed to the SIM swap requestor, including value of last prepaid voucher recharge and/or numbers called regularly, or name of person who paid the last bill if a post-paid account.

d) Linking bank 2FA systems used by banks/PSPs for undertaking (new) payment beneficiary verification via SMS and/or push USSD OTP, to SIM/phone number databases housed at MNOs. Linking the two data-

bases will allow velocity checks to be undertaken by the bank/PSP that will check and flag whether SIM swap request for a number linked to the true account owner are suspiciously close in time to a request at the bank/PSP for adding a new (possibly fraudulent) payment beneficiary.

12.5 Detecting, preventing and mitigating SIM card recycle

Once there is inactivity in a DFS account, start monitoring the IMSI associated with the account phone number, once the SIM is deactivated the mobile operator will not reply correctly to these queries (one query a day is sufficient).

When the SIM is recycled, the mobile operator will report a new IMSI for the account phone number, the DFS provider should block the account until the identity if the new person holding the SIM card is verified as the account holder.

12.6 Embedding data within the user's phone for authentication

DFS providers can work with device manufacturers and MNOs to embed a hard to spoof identifier within the device software, this identifier (which should be cryptographic to prevent spoofing) needs to be integrated in all communications between the DFS provider and the user's phone to authenticate the user and phone.

12.7 Regulatory activities

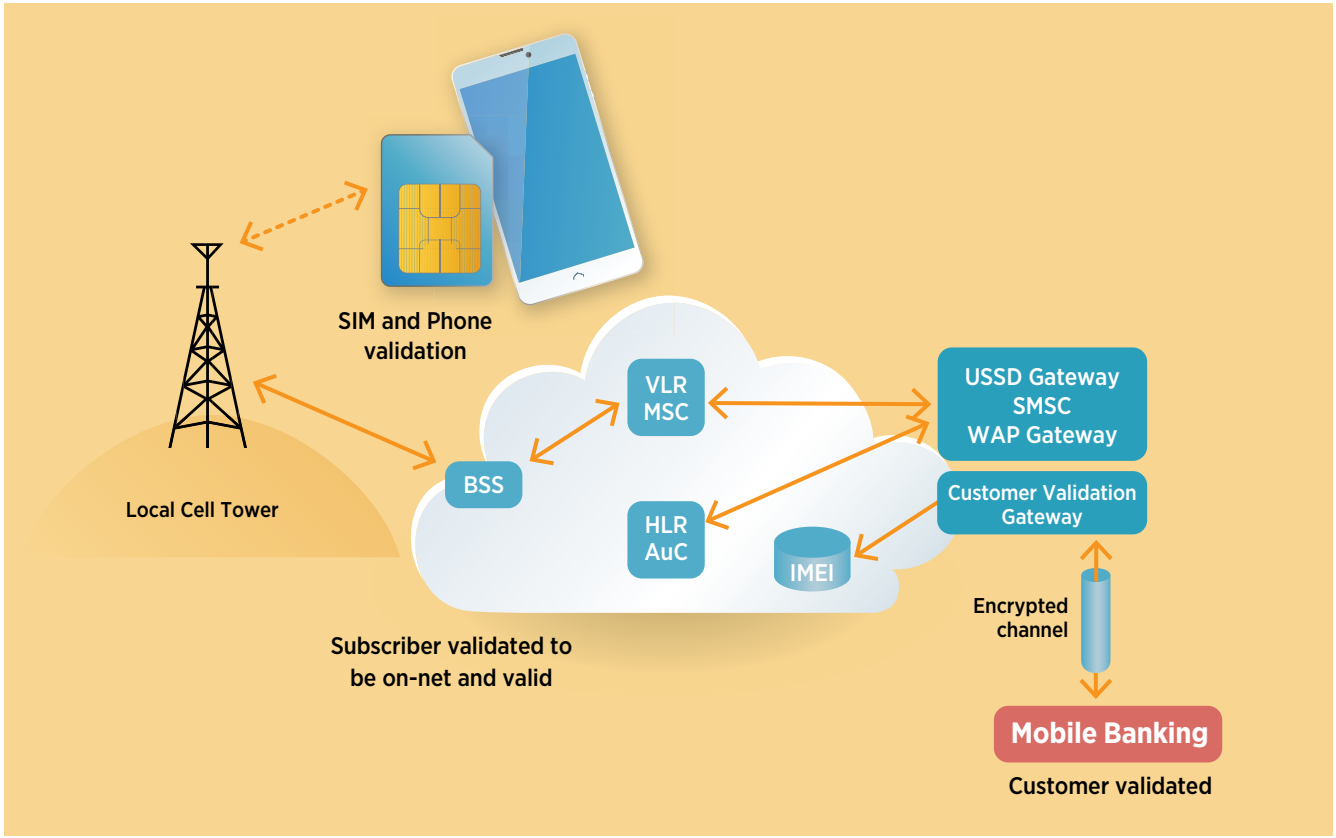
Regulators with remit over DFS may establish procedures and principles for detecting, preventing, reporting, and mitigating SS7 and related attacks. They may also establish procedures that licensees may need implement to prevent SIM swaps.

Regulatory coordination between these regulators is key, so as to assign specific and joint roles and responsibilities. This should take the form of a Memorandum Of Understanding (MOU) between the parties. An extract from a model MOU between a telecommunications regulator and a central bank that contains language outlining these responsibilities is shown in Annex B.

The MOU includes *inter alia* the need to assign individual and shared technical responsibilities relating to infrastructure and related security issues that may impact the DFS ecosystem to each of these regulators, including reporting lines and actions relating to intrusions. The telecommunications regulator in particular should also undertake continuous testing in conjunction with its licensees to detect IMSI catchers. A joint working committee between these two regulators that meets monthly to discuss DFS-related issues and any security threats or incidents is also envisaged in the MOU.

An IMSI validation gateway can be used to validate to DFSPs and banks that the real, registered customer is using the system via USSD.

FIGURE 12: An IMSI validation gateway



13 CONCLUSIONS AND RECOMMENDATIONS

It can be concluded that:

a. The DFS providers, telecom operators and the telecom regulators are mostly unaware of the mitigation strategies that they can employ to detect and prevent SS7 attacks.

b. The implementation of mitigation measures is low mainly due lack of adequate regulation and prohibitive cost (on the telecom side).

c. Attacks exploiting SS7 vulnerabilities to steal funds are easy to perform and not the sole property of government agencies.

d. Mitigation countermeasures both for DFS providers and for mobile operators are readily available commercial products; given the proper regulation, the DFS providers and telecoms can implement such mitigation countermeasures.

e. Because DFS contracts today place all the responsibility for fraud on the end-user, and the DFS providers are not required to indemnify the end-users in case of fraud, there is no incentive for DFS providers to invest any resources into solving this problem.

f. The same apply for telecom operators, since the financial damage due to financial fraud stops at the DFS provider, the telecom is not liable for any damage, thus suffers no losses. Hence has no incentive to invest resources to solve this problem.

g. Telecommunication authorities and central banks generally do not meet or interact regularly enough, or at all, to have contemporaneous insights into DFS-related security threats and intrusions.

h. DFS ecosystem participants and regulators do not meet or interact regularly enough, or at all, in a neutral, collegial environment to be able to share and have contemporaneous insights into DFS-related security threats and intrusions.

In order to address the above-mentioned issues, the Working Group recommends the following measures:

a. **Education for telecom and financial services regulators on SS7 vulnerabilities and impact to DFS**—telecom and financial regulators around the world needs to be aware of these risks and most importantly be aware that there are available solutions to mitigate these risks.

b. **Regulation and legal framework to include measures for signalling security and reporting of such incidents**—work towards financial and telecom regulators passing regulation to make it mandatory for DFS providers and telcos to implement countermeasures and to provide reports on any security-related breaches and incidents.

c. **Telecom regulators to establish baseline security measures for each category (3G/4G/5G)**—Telecom regulators are encouraged to establish baseline security measures for each category (3G/4G/5G) which should be implemented by telecom operators to ensure a more secure interconnection environment.

d. **Regulatory coordination**—A bilateral Memorandum of Understanding (MOU) related DFS should be in place between the telecommunications regulator and the central bank. The MOU should include modalities around the creation of a Joint Working Committee on DFS security and risk-related matters. A sample MOU is included at Annex B as a template that can be considered.

e. **Industry-regulator coordination**—Forums should be created where all commercial actors in the DFS ecosystem meet or interact regularly in a neutral environment with DFS-focused regulators where security-related issues can be freely discussed without providing any sensitive or competitive information.

f. **Intra-Industry coordination**—Forums should be created where all commercial actors in the DFS ecosystem meet or interact regularly in a neutral environment where security-related issues can be freely discussed without providing any sensitive or competitive information or undertaking potentially collusive actions.

g. **Incentivize the industry**—create incentive programs with industry to promote the development of countermeasures in the telco-DFS anti-fraud field.

h. **Incentivize the operators and providers**—create regulation that passes the financial damage from DFS fraud to the DFS providers and to the telcos, creating a financial incentive for action on their part.

ANNEX A

Technical description of SS7 and diameter

A.1 THE SS7 PROTOCOL STACK

Signalling System No. 7 (SS7) is a set of telephony signalling protocols developed in 1975, which is used to set up and tear down most of the world's public switched telephone network (PSTN) telephone calls. It also performs number translation, local number portability, prepaid billing, Short Message Service (SMS), and other mass market services.

In North America it is often referred to as CCSS7, abbreviated for Common Channel Signalling System 7. In the United Kingdom, it is called C7 (CCITT number 7), number 7 and CCIS7 (Common Channel Interoffice Signalling 7). In Germany, it is often called ZZK-7 (Zentraler ZeichengabeKanal Nummer 7).

The only international SS7 protocol is defined by ITU-T's Q.700-series recommendations in 1988. Of the many national variants of the SS7 protocols, most are based on variants of the international protocol as standardized by ANSI and ETSI. National variants with striking characteristics are the Chinese and Japanese (TTC) national variants.

The Internet Engineering Task Force (IETF) has defined the SIGTRAN protocol suite that implements levels 2, 3, and 4 protocols compatible with SS7. Sometimes also called Pseudo SS7, it is layered on the Stream Control Transmission Protocol (SCTP) transport mechanism.

The SS7 protocol stack may be partially mapped to the OSI Model of a packetized digital protocol stack. OSI layers 1 to 3 are provided by the Message Transfer Part (MTP) and the Signalling Connection Control Part (SCCP) of the SS7 protocol (together referred to as the Network Service Part (NSP)); for circuit related signalling, such as the BT IUP, Telephone User Part (TUP), or the ISDN User Part (ISUP), the User Part provides layer 7. Currently there are no protocol components that provide OSI layers 4 through 6. The Transaction Capabilities Application Part (TCAP) is the primary SCCP User in the Core Network, using SCCP in connectionless mode. SCCP in connection-oriented mode provides transport layer for air interface protocols such as BSSAP and RANAP. TCAP provides transaction capabilities to its Users (TC-Users), such as the Mobile Application Part, the Intelligent Network Application Part and the CAMEL Application Part.

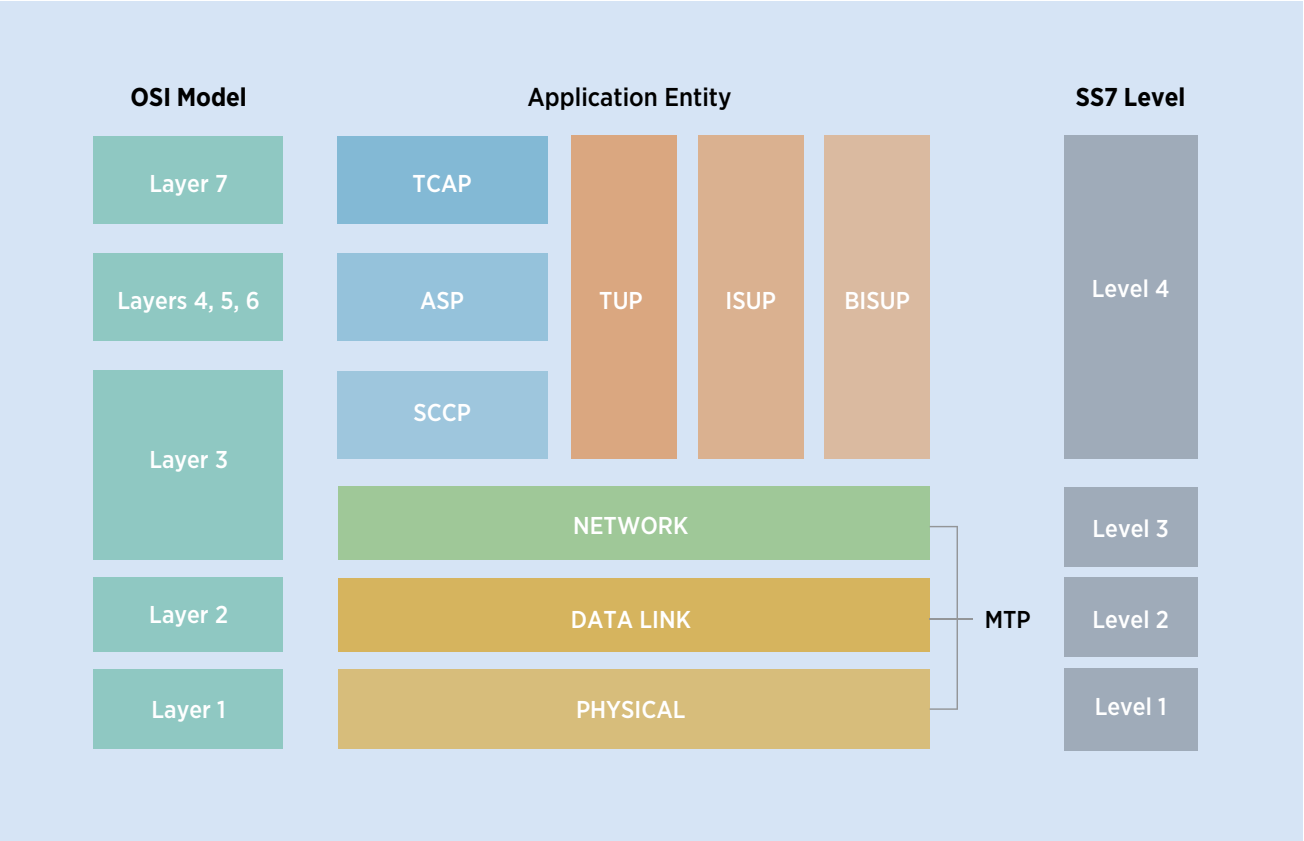
The Message Transfer Part (MTP) covers a portion of the functions of the OSI network layer including: network interface, information transfer, message handling and routing to the higher levels. Signalling Connection Control Part (SCCP) is at functional Level 4. Together with MTP Level 3 it is called the Network Service Part (NSP). SCCP completes the functions of the OSI network layer: end-to-end addressing and routing, connectionless messages (UDTs), and management services for users of the Network Service Part (NSP). Telephone User Part (TUP) is a link-by-link signalling system used to connect calls. ISUP is the key user part, providing a circuit-based protocol to establish, maintain, and end the connections for calls. Transaction Capabilities Application Part (TCAP) is used to create database queries and invoke advanced network functionality, or links to Intelligent Network Application Part (INAP) for intelligent networks, or Mobile Application Part (MAP) for mobile services.

A.2 THE DIAMETER PROTOCOL STACK

The diameter protocol is used to communicate between components in the System Architecture Evolution (SAE). SAE is the core network architecture of 3GPP's LTE wireless communication standard. SAE is the evolution of the GPRS Core Network, with some differences:

- simplified architecture
- all-IP Network (AIPN)
- support for higher throughput and lower latency radio access networks (RANs)
- support for, and mobility between, multiple heterogeneous access networks, including E-UTRA (LTE

FIGURE A.1: The SS7 Protocol stack



and LTE Advanced air interface), 3GPP legacy systems (for example GERAN or UTRAN, air interfaces of GPRS and UMTS respectively), but also non-3GPP systems (for example WIFI, WiMAX or CDMA2000)

The main component of the SAE architecture is the Evolved Packet Core (EPC), also known as SAE Core. The EPC will serve as the equivalent of GPRS networks (via the Mobility Management Entity, Serving Gateway and PDN Gateway subcomponents).

The Non-Access Stratum (NAS) protocols form the highest stratum of the control plane between the user equipment (UE) and MME. [3] NAS protocols support the mobility of the UE and the session management procedures to establish and maintain IP connectivity between the UE and a PDN GW. They define the rules for a mapping between parameters during inter-system mobility with 3G networks or non-3GPP access networks. They also provide the NAS security by integrity protection and ciphering of NAS signalling messages. EPS provides the subscriber with a "ready-to-use" IP connectivity and an "always-on" experience by linking between mobility management and session management procedures during the UE attach procedure.

Complete NAS transactions consist of specific sequences of elementary procedures with EPS Mobility Management (EMM) and EPS Session Management (ESM) protocols

A.3 EPC PROTOCOL STACK

A.3.1 MME (Mobility Management Entity) protocols

The MME protocol stack consists of:

- S1-MME stack to support S1-MME interface with eNodeB
- S11 stack to support S11 interface with Serving Gateway

MME supports the S1 interface with eNodeB. The integrated S1 MME interface stack consists of IP, SCTP, S1AP.

- SCTP (Stream Control Transmission Protocol) is a common transport protocol that uses the services of Internet Protocol (IP) to provide a reliable datagram delivery service to the adaptation modules, such as the S1AP. SCTP provides reliable and sequenced delivery on top of the existing IP framework. The main features provided by SCTP are:
  i) Association set up: An association is a connection that is set up between two endpoints for data transfer, much like a TCP connection. A SCTP association can have multiple addresses at each end.
  ii) Reliable Data Delivery: Delivers sequenced data in a stream (Elimination of head-of-line blocking):

SCTP ensures the sequenced delivery of data with multiple unidirectional streams, without blocking the chunks of data in other direction.

- S1AP (S1 Application Part) is the signalling service between E-UTRAN and the Evolved Packet Core (EPC) that fulfills the S1 Interface functions such as SAE Bearer management functions, Initial context transfer function, Mobility functions for UE, Paging, Reset functionality, NAS signalling transport function, Error reporting, UE context release function, Status transfer.

MME supports S11 interface with Serving Gateway. The integrated S11 interface stack consists of IP, UDP, eGTP-C.

A.3.2 SGW (Serving Gateway) protocols

The SGW consists of:

- S11 control plane stack to support S11 interface with MME
- S5/S8 control and data plane stacks to support S5/S8 interface with PGW
- S1 data plane stack to support S1 user plane interface with eNodeB
- S4 data plane stack to support S4 user plane interface between RNC of UMTS and SGW of eNodeB
- Sxa: since 3GPP Rel.14, the Sx interface and the associated PFCP protocol was added to the PGW, allowing for the Control User Plane Separation between PGW-C and PGW-U.
- SGW supports S11 interface with MME and S5/S8 interface with PGW. The integrated control plane stack for these interfaces consists of IP, UDP, eGTP-C.

SGW supports the S1-U interface with eNodeB and S5/S8 data plane interface with PGW. The integrated data plane stack for these interfaces consists of IP, UDP, eGTP-U.

A.3.3 PGW (Packet Data Network Gateway) protocols

Main interfaces supported by the P-GW are:

- S5/S8: this interface is defined between S-GW and P-GW. It is named S5 when the S-GW and the P-GW are located in the same network (non-roaming scenario) and S8 when the S-GW is located in the visited network and the P-GW in the home network (roaming scenario). eGTP-C and GTP-U protocols are used in the S5/S8 interface.
- Gz: this interface is used by the P-GW to communicate with the Offline Charging System (OFCS), mainly to send the Charging Data Records (CDRs) of the post-paid users via FTP.
- Gy: this interface is used by the P-GW to communicate with the Online Charging System (OCS). The P-GW informs the charging system about pre-paid users payload in real time. Diameter protocol is used in the Gy interface.
- Gx: this interface is used by the P-GW to communicate with the Policy and Charging Rules Function (PCRF) in order to handle Policy and Charging Rules (PCC) rules. These rules contain charging related information as well as Quality of Service (QoS) parameters that will be used in the bearer establishment. Diameter protocol is used in the Gx interface.
- SGi: this interface is defined between the P-GW and external networks, for example, Internet access, corporate access, etc.
- Sxb: since 3GPP Rel.14, the Sx interface and the associated PFCP protocol was added to the PGW, allowing for the Control User Plane Separation between PGW-C and PGW-U.

A.4 SUPPORT OF VOICE SERVICES AND SMS

The EPC is a packet-only core network. It does not have a circuit-switched domain, which is traditionally used for phone calls and SMS.

A.4.1 3GPP specified solutions for voice

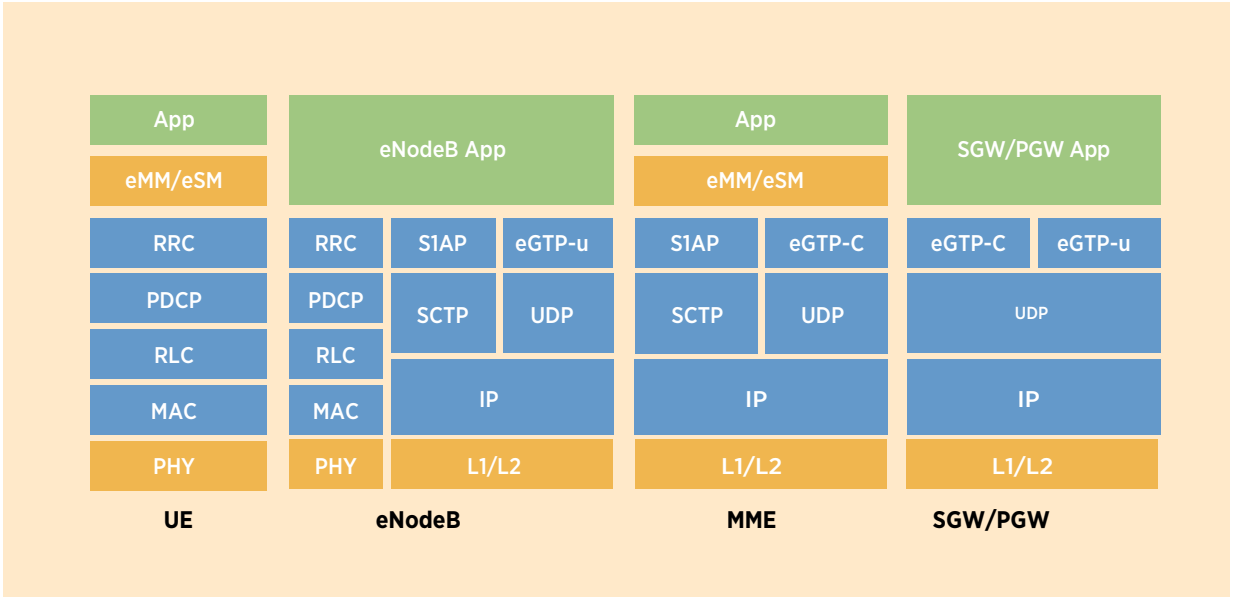
- IMS: A solution for IMS Voice over IP was specified in Rel-7.
- Circuit-Switched fallback (CSFB): in order to make or receive calls, the UE changes its radio access technology from LTE to a 2G/3G technology that supports circuit-switched services. This feature requires 2G/3G coverage. A new interface (called SGs) between the MME and the MSC is required. This feature was developed in Rel-8.

A.4.2 3GPP specified solutions for SMS

- IMS: A solution for SMS over IP was specified in Rel-7.
- SMS over SGs: this solution requires the SGs interface introduced during the work on CSFB. SMS are delivered in the Non-Access Stratum over LTE. There is no inter-system change for sending or receiving SMS. This feature was specified in Rel-8.
- SMS over SGd: this solution requires the SGd Diameter interface at the MME and delivers SMS in the Non-Access Stratum over LTE, without requiring the fully signalling neither the legacy MSC doing CSFB, nor the overhead associated with the IMS signalling and the associated EPC bearer management.

CSFB and SMS over SGs are seen as interim solutions, the long term being IMS.

FIGURE A.2: LTE (Diameter) protocol stack



ANNEX B

Template for a model MOU between a telecommunications regulator and central bank related to DFS security

B.1 BASIS OF THE MOU

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.

B.2 AREAS OF COOPERATION AND COOPERATION STRATEGIES

GENERAL PROVISIONS

B.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.

B.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;

i) Consultations on amendments to existing laws, guidelines, by-laws, or regulations where these may relate to DFS;

j) Consultations on the need for any new laws, guidelines, by-laws, or regulations where these may relate to DFS;

k) Use of technical expertise;

l) Management and operation of DFS infrastructure;

m) Availability of, and fair access to, MNO communication channels by DFSPs;

n) Availability of, and fair access to, any MNO data that can legally be shared with DFSPs or other parties;

o) Development and enforcement of minimum technical and operational standards;

p) Identification, mitigation, and expeditious handling and containment of all security issues and incidents;

q) Participation where necessary in the development of RMFs related to DFS;

r) Anti-money laundering, counter terrorism financing, and fraud;

s) Consumer protection generally;

t) Monitoring of systems and networks for security breaches and intrusions where these may affect DFS, and the reporting of any breaches and intrusions relating to DFS provision to the other Authority;

u) Mutually support the other Authority's activities in relation to DFS and adjacent matters;

v) Mutual and expeditious notification to the other of any issues, processes, and events that may affect the operation of DFS in (the country); and

w) Any other strategy relating to the scope of this MOU deemed necessary and appropriate by the Authorities;

NATIONAL TELECOMMUNICATIONS AUTHORITY-DESIGNATED ROLES

B.2.3 The NATIONAL TELECOMMUNICATIONS REGULATOR hall undertakes continuous monitoring of the licensed frequencies operated by the MNOs so as to ensure that no unauthorized radio frequency devices are being used on these frequencies to, inter alia, capture customer information and to disrupt MNO communications with their customers.
This monitoring may be undertaken jointly between the NATIONAL TELECOMMUNICATIONS REGULATOR and the MNOs as may be necessary. Any breaches and intrusions that may have an effect on the operation and financial security of DFS in (the country) shall be expeditiously reported by the NATIONAL TELECOMMUNICATIONS REGULATOR to the CENTRAL BANK.

B.2.4 The NATIONAL TELECOMMUNICATIONS REGULATOR will operate through its mandate of oversight and supervision to ensure that their licensees offer their services to DFSPs:

a) At a high technical level;

b) At a high security level;

c) At a high availability level in ensuring uninterrupted communications and/or data transfer for customers;

d) In an effective and affordable manner;

e) In a fair and equitable manner;

f) Not in a manner that may amount to abuse of their licensed access to and provision of scarce telecommunications resources to the detriment of other entities reliant on these resources;

g) Transparently;

h) Without exercising any price, access, and Quality of Service differentiation between DFSPs and for any other entities reliant on these resources;

i) Without delaying the transfer and the delivery of any service messages;

j) Without violating any intellectual property rights;

k) Whilst ensuring the availability of network access in accordance with applicable standards;

l) In a manner that may amount to anti-competitive behaviour; and

m) Where the licensees are MNOs, to validate and ensure that only verified and authorized persons are able to have access to—or provide, as the case may be —customer SIM cards;

n) Undertake, as may be required, continuous testing, intrusion filtering and monitoring of their core networks, BTS infrastructure and licensed mobile phone frequency bands to ensure that there is no unauthorized access, disruption or use.

B.2.5 Tests and monitoring that may be required and which relate to specific issues identified in Section 2.4 above shall include, but not be limited to, those for:

a) Unauthorized access to and use of any Signalling System 7 (SS7)-based core components of the MNO's infrastructure;

b) Use of any SS7 components of the MNO's infrastructure by any party where that use may be designed to undertake unauthorized or fraudulent activities;

c) Unauthorized access to and use of any LTE-based core components of the MNO's infrastructure;

d) Detection, as far as may be technically possible, of unauthorized radio frequency devices operated by unauthorized parties that may be designed to disrupt the MNOs licensed activities and/or to gain unauthorized access to customer handsets, SIM cards, customer access rights to MNO and DFS facilities, and customer data.

B.2.6 The NATIONAL TELECOMMUNICATIONS REGULATOR shall also ensure that its licensees and any other entities under its supervision:

a) Provide to the NATIONAL TELECOMMUNICATIONS REGULATOR reports on penetration tests that relate to the security of their systems. These reports must include any remedial action taken, if applicable;

b) Provide to the NATIONAL TELECOMMUNICATIONS REGULATOR reports on incidents that relate to authorized access to their systems and data; These reports must include any actual and potential data losses and breaches of consumer data protection measures, and any remedial action taken;

c) Expeditiously implement the most recent international technical and security standards;

d) Allow DFS end users to choose and fully access any of the available DFSPs, without any restrictions, discrimination, or preferential treatment among them.

CENTRAL BANK-DESIGNATED ROLES

B.2.7 The CENTRAL BANK shall undertake continuous monitoring of its supervised entities.

B.2.8 The CENTRAL BANK will operate through its mandate of oversight and supervision to ensure that their licensees and entities under their supervision:

a) Offer their services to DFSPs:
   i) At a high technical level;
   ii) At a high security level;
   iii) At a high availability level in ensuring uninterrupted communications and/or data transfer for customers;
   iv) In an effective and affordable manner;
   v) In a fair and equitable manner;
   vi) Not in a manner that may amount to abuse of their license or authorization to operate to the detriment of other entities reliant on these resources.
   vii) Transparently;
   viii) Without exercising any price, access, and Quality of Service differentiation between DFSPs;
   ix) Without delaying the transfer and the delivery of any service messages;
   x) Without violating any intellectual property rights
   xi) Whilst ensuring the availability of service access in accordance with applicable standards;

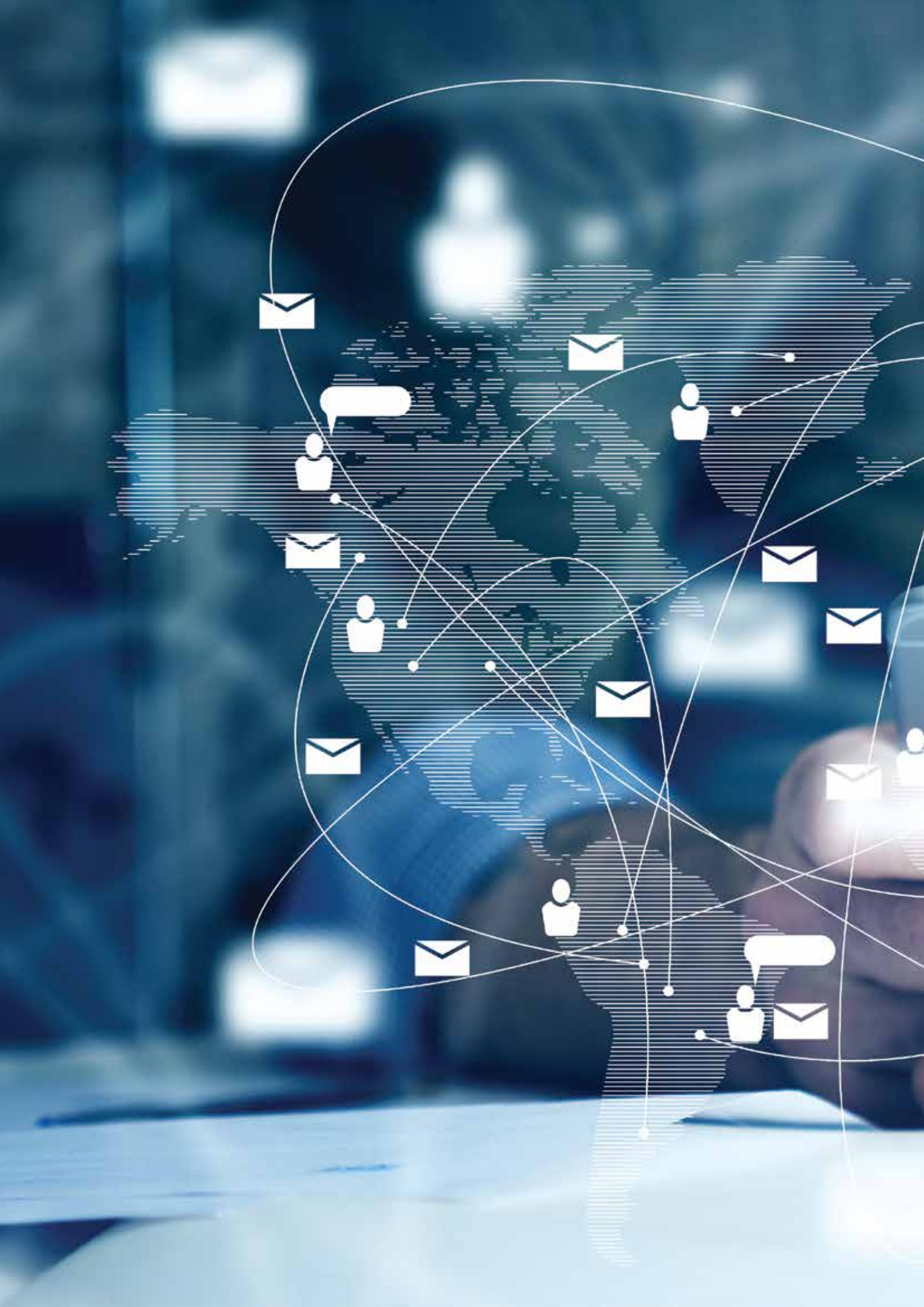
b) Do not act in a manner that may amount to anti-competitive behaviour.

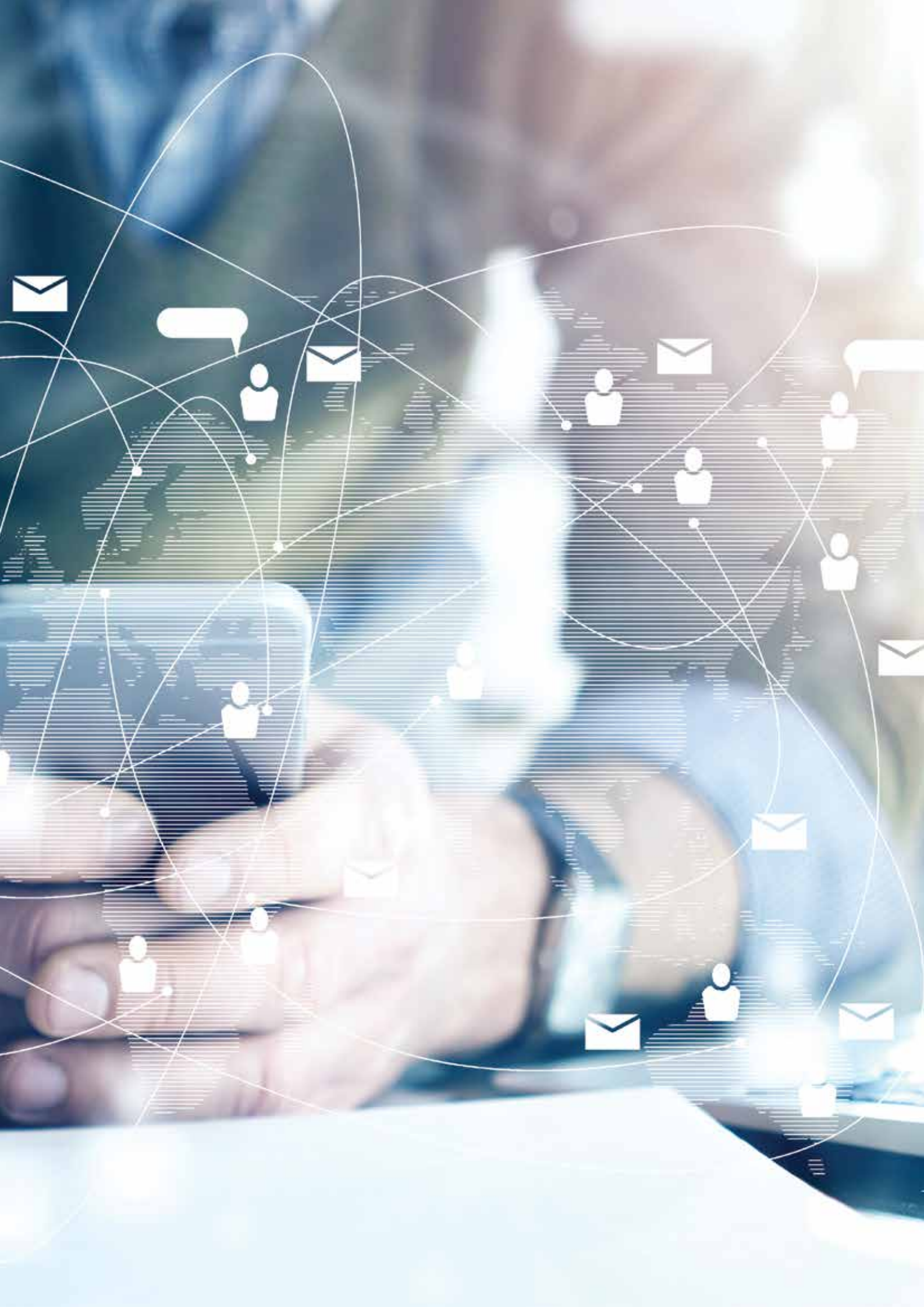
c) Undertake, as may be required, continuous testing, intrusion filtering and monitoring of their infrastructure to ensure that there is no unauthorized access, disruption or use; and expeditiously:
   i. Provide to the CENTRAL BANK reports on penetration tests that relate to the security of their systems. These reports must include any remedial action taken if applicable.
   ii. Provide to the CENTRAL BANK reports on incidents that relate to authorized access to their systems and data. These reports must include any actual and potential data losses and breaches of consumer data protection measures, and any remedial action taken.
   iii. Implement the most recent international technical and security standards;

d) Allow DFS consumers to choose any of the available DFSPs, without any restrictions, discrimination, or preferential treatment among them.

Endnotes

1. A diagram of the SS7 protocol stack can be found in Annex A
2. A diagram of the Diameter protocol stack can be found in Annex A
3. ENISA research result can be found at: https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g/at_download/fullReport.
4. Reference: https://www.gsma.com/newsroom/gsmadocuments/technical-documents/
5. A fact derived from recent audits performed on more than two dozen cellular networks by Vaulto.
6. In 2010, Dunkelman, Keller and Shamir published a new attack that allows an adversary to recover a full A5/3 key by related-key attack. The time and space complexities of the attack are low enough that the authors carried out the attack in two hours on an Intel Core 2 Duo desktop computer even using the optimized reference KASUMI implementation.
7. Update Location—an SS7 operation causing the victim's home network to believe they have roamed to another network
8. Visitor Location Register
9. https://mwnation.com/be-alert-mobile-money-fraudsters-on-the-loose/
10. SMS home routing prevents the real IMSI of a subscriber to be sent in every inbound SMS signalling, however with other types of signalling attacks the IMSI can be extracted from the HLR of the telco.
11. Filtering on signalling nodes prevents, in theory, access from unverified addresses. However, this filtering is only effective if configured correctly and maintained properly.
12. SecureOTP - OTP SMS send bi-directional and secured from interception
13. Nigerian Communications Commission (2017) Guidelines on SIM Replacement, available at https://www.ncc.gov.ng/docman-main/legal-regulatory/guidelines/733-guidelines-on-sim-replacement/file
14. Nigerian Communications Commission (2017) Guidelines on SIM Replacement, available at https://www.ncc.gov.ng/docman-main/legal-regulatory/guidelines/733-guidelines-on-sim-replacement/file
15. Nigerian Communications Commission (2017) Guidelines on SIM Replacement, available at https://www.ncc.gov.ng/docman-main/legal-regulatory/guidelines/733-guidelines-on-sim-replacement/file
16. These may be a result of SIM swap guidelines issued by a regulator.





International Telecommunication Union
Place des Nations, CH-1211
Geneva 20, Switzerland