Key Recommendations for Digital Financial Services security

Key Recommendations for Digital Financial Services security

The guidelines in Annex 1 to 5 are proposed for adoption

Summary of the guidelines

1. **Recommendations for regulators to mitigate SS7 vulnerabilities:** recommendations for DFS regulators and mobile network operators to mitigate the effects of SS7 vulnerabilities on digital financial services security.

2. **Security recommendations to protect against DFS SIM risks and SIM swap fraud**: guidance and recommendations for regulators and providers to mitigate SIM vulnerabilities like SIM swaps, SIM recycling, and attacks on SIMs like binary over the air attacks.

3. **Mobile Application Security Best practices:** best practices for mobile financial services application security that DFS regulators can adopt as guidelines.

4. **Template for a Model MOU between a Telecommunications Regulator and Central Bank on Digital Financial Services Security:** includes clauses that address the security of DFS that regulators should consider for adoption or incorporate into existing MOUs.

5. DFS consumer competency framework: The DFS Consumer Competency Framework provides guidance to policymakers, national regulators and DFS providers when developing consumer awareness and literacy programmes as part of the DFS/financial inclusion strategy.

See details for documents mentioned in 1-4 in the Annex.

Annex 1: Recommendations for regulators to mitigate SS7 vulnerabilities

1 Recommendations for regulators to mitigate SS7 vulnerabilities

The USSD and SMS communication channels with which the end-user communicates with the DFS provider rely on the legacy Signaling System 7 protocol which has for long been "broken" and with many published vulnerabilities, some over 20 years old, which enables attackers to commit fraud, compromise DFS and steal funds through account takeovers, DFS interception, denial of service attacks etc.

The SS7 Vulnerabilities and Mitigation Measures for DFS Transactions contain details on the recommendations for DFS regulators and mobile network operators to mitigate SS7 vulnerabilities. These recommendations are summarized below.

1.1 Regulatory guidance to address vulnerabilities due to SS7

a) **Regulatory coordination: -** a bilateral Memorandum of Understanding (MOU) related DFS should be in place between the telecommunications regulator and the Central Bank on SS7. A sample MOU is included at Annex B of the Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions. The MOU should include modalities around the creation of a Joint Working Committee on DFS security and risk-related matters that address SS7.

b) **Incentivize the industry** - create incentive programs with industry to promote the development of countermeasures in the Telcom-DFS anti-fraud field.

c) **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.

d) **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 the risks and most importantly be aware that there are available solutions to mitigate these risks.

e) **IMSI validation gateway**: An IMSI validation gateway can be used to validate to DFSPs and banks that the real, registered customer is using the system via USSD for DFSPs to detect USSD interception.

f) **Telecom regulators to establish baseline security measures for each category (2G/3G/4G/5G)** - Telecom regulators are encouraged to establish baseline security measures for each category (2G/3G/4G/5G) which should be implemented by telecom operators to ensure a more secure interconnection environment.

g) **Mobile Network operators and DFS operators should consider adopting controls in section 1.2 and 1.3 below.**

1.2 MNO controls to address DFS vulnerabilities due to SS7

a) **Secure GSM ciphers for radio network traffic**: The mobile operator should ensure the use of secure radio encryption between users' devices and base stations.

b) **Session time out:** use session timeout for USSD and STK to reduce success man in the middle attacks.

c) **USSD PIN masking:** Deploy USSD PIN masking whenever possible.

d) **Secure and monitor core network traffic**: Use a TLS v1.2 or higher to secure the connection between the SMSC GW, USSD GW, and the DFS application server.

e) **Limit access to traces and logs**: Ensure there is an auditable process in place to review access to traces and logs on interfaces that use inherently insecure protocols. USSD PINs should not be logged in the event data records.

f) **SMS filtering**: Remote attackers rely on mobile networks to deliver binary SMS to and from victim phones. Mobile operators should implement blocking the ability to send and receive binary messages like OTA SMS. Such SMS should only be allowed from whitelisted sources.

g) **SMS home routing:** This is the barring of all outgoing and incoming SMS except those routed through the home network hosts. OTA messages with STK coding from home subscribers should be restricted to only be sent to/by the MNO platform—and not to other subscribers.

1.3 DFS provider controls to address DFS vulnerabilities due to SS7

DFS operators should consider adopting the following controls to mitigate SS7 risks**.**

a) **Session time out:** use session timeout for USSD and STK to reduce success man in the middle attacks, OTP messages for DFS should also have a session time out.

b) **Transaction limits for insecure channels:** Set transaction limits for customer withdrawals and transfers through insecure channels like USSD.

c) **User education:** DFS users should be educated on how to engage securely with digital financial services including impacts of using rooted devices, connecting to public Wi-Fi, installing unverified applications etc.

d) **Bidirectional OTP SMS flow**: The DFS provider should make the authentication flow bidirectional, that is receive the OTP from the user, not send it.

e) **Detecting and mitigating social engineering attacks with MT-USSD and interception of USSD** by verifying using secureOTP, location validation, IMSI and IMEI validation

Annex 2: Security recommendations to protect against DFS SIM risks and SIM swap fraud.

2 Best practices for regulators to protect DFS against SIM risks

ITU-T X.1456: Security guidelines for digital financial service (DFS) applications based on unstructured supplementary service data (USSD) and subscriber identification module tool kit (STK) contains details on the recommendations on mitigating SIM vulnerabilities.

2.1 SIM vulnerabilities

Financial institutions have adopted digital means and are continuing to avail financial products on mobile based application like Unstructured Supplementary Services (USSD) and STK banking, which makes financial services available anywhere, anytime through strings of interactions via Unstructured Supplementary Service Data (USSD), Short Messaging Service (SMS), internet. The interactions between the mobile user and the network are authenticated with the SIM card. However, there has been increased fraud risks on SIMs due to threats arising from notably SIM swaps, SIM jacker attacks and SIM recycling and number porting.

2.1.1 SIM swap fraud

SIM swap fraud has become a common tactic used to takeover accounts. In a SIM swap fraud, a telecom provider is tricked into issuing a replacement of a victim's SIM to a fraudster allowing them to take over a DFS accounts that relies on the SMS one time password (OTP) or USSD for authentication.

2.1.2 SIM recycling risks

SIM recycling risks is related to reliance on the phone numbers, Mobile Station Integrated Services Digital Network (MSISDN) as the primary DFS account numbers. Telco providers reassign phone numbers that are dormant or deemed to have churned (not used within specific period). The reassignment of the phone number may effectively lead to an account takeover of the DFS wallet associated with the number if the DFS provider is not aware of the change of ownership.

2.1.3 Binary Over the Air attack (SIM jacker)

The SIM jacker attack exploits a vulnerability in a SIM Card library called the S@T browser. A specially formatted binary text message is sent to the victim handset, which contains a set of commands to be executed by the S@T Browser environment in the SIM card. The commands can instruct the handset to exfiltrate this information, force the mobile device to initiate a USSD request, make a phone call, or send a message.

3 Recommendations for regulators and providers to protect DFS against SIM risks

3.1 Regulatory guidance to mitigate against SIM risks (SIM swap, SIM cloning, SIM recycling and binary over the air attacks).

a. **Regulatory coordination: -** a bilateral Memorandum of Understanding (MOU) related DFS should be in place between the telecommunications regulator and the Central Bank on SIM swaps. A sample MOU is included at Annex B of the Technical report on SS7 vulnerabilities and mitigation measures for digital financial services transactions

b. **Mobile network operators should consider adopting the following controls to mitigate SIM risks and fraud in section 2.1 below.**

3.2 Mobile network operator controls to mitigate SIM risks and fraud

i. 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.

ii. 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.

iii. MNOs should notify DFS providers on swapped SIMs, ported and recycled numbers.

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.

3.3 DFS operators controls to mitigate SIM risks and fraud

xi. **Real time IMSI/ICCID detection**: DFS and Payment Service Providers should be able to detect real-time whenever a SIM card associated with DFS services is swapped or replaced. Further verification before authorizing any transaction or account changes with new SIM should be required.

xii. **Real time device change detection:** Device authentication to improve endpoint security by tracking the IMEI's of the devices used to access financial services. In this way, an account that changes devices can be flagged by the DFS operator

xiii. **Encourage use of secure DFS access:** Avail the customers the option to opt-out of the USSD or STK channels for financial transactions, especially those that can access the DFS using an app.

The measures recommended above could also be adopted as regulations by DFS regulators.

Annex 3: Template for a Model MOU between a Telecommunications Regulator and Central Bank on Digital Financial Services Security:

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;

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;

3 National Telecommunications Regulator-Designated roles

The National Telecommunications Regulator shall undertake continuous monitoring of the licensed frequencies operated by the MNOs 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.

3.1 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.

3.2 Tests and monitoring that may be required and which relate to specific issues identified in Section 3.1 above shall include, but not be limited to, those for:

a) Unauthorized access to and use of any Signaling 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.

3.3 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.

4 Central Bank-designated roles

4.1 The Central Bank shall undertake continuous monitoring of its supervised entities.

4.2 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.

Annex 4: Mobile Application security best practices.

The template for application security proposes best practices that Digital Financial Services regulators which could be included in an app security policy document by DFS providers. The template strictly considers the mobile application on the device unless stated otherwise, and subsections describing recommendations deal with various aspects of the operation or underlying policy relating to the mobile application. The focus is primarily on Android applications given their large market share, though many recommendations are applicable across mobile operating systems. This template is extracted from Appendix 1 of **ITU-T Recommendation X.1150 : Security assurance framework for digital financial services**

1 Template For Mobile Application Security Best Practices

In this section, we summarize the recommendations as a starting point for regulators or application security examiners to perform security assessments. The template strictly considers the mobile application on the device unless stated otherwise, and subsections describing recommendations deal with various aspects of the operation or underlying policy relating the mobile application. The focus is primarily on Android applications given their large market share, though many recommendations are applicable across mobile operating systems. Privacy is also an important factor to consider, but these recommendations focus on security.

1.1 Device and Application Integrity

i. The safest devices for performing financial transactions on are ones that have not been "jailbroken" or "rooted", as it can be difficult or impossible to assess the security of the underlying operating system when it has been replaced or exploited. Applications should thus use the mobile platform services to determine that they and the underlying platform have not been modified.
ii. Remove any extraneous code that might have been added to the application during development, such as features that are not designed for the device platforms that the app is to be deployed upon or developer/debug features to reduce the attack surface of the deployed production code.
iii. On the server-side, determine whether the app is running in a high integrity state through signature validation or hashing over the app or certain program function blocks.

1.2 Communication Security and Certificate Handling

i. Apps should be making use of standardized cryptographic libraries and for communication with back-end services, should use end-to-end encryption with standardized protocols, specifically transport layer security (TLS). The minimum recommended version of TLS that should be used is version
ii. TLS certificates should not be expired and should present strong cipher suites, specifically AES-128 encryption and SHA-256 for hashing. Authenticated encryption modes of operation such as Galois/Counter mode (GCM) are encouraged.
iii. Limit the lifetime of issued certificates to 825 days in accordance with the CA/Browser Forum best practices.
iv. Assure the trustworthiness of the certificate authority and consider a contingency plan for if the CA is no longer trusted.
v. Ensure the configuration of TLS is performed in a secure fashion and avoid misconfiguration issues that could result in failure to authenticate or poor algorithm selection.
vi. Certificate pinning should prevent replacement of certificates where it refers to the process of associating a host with their expected public key certificate or public key. Once a certificate or

public key is known or seen for a host, the certificate or public key is associated or 'pinned' to the host.

vii. Client devices shall ensure that they correctly validate server certificates

1.3 User Authentication

i. PINs and passwords should not be easily guessable and weak credentials should be disallowed; however, users should not be forced to change passwords on a regular basis.

ii. Multi-factor authentication before performing financial or other sensitive functions should be strongly encouraged. A phishing-resistant form of multi factor authentication [b-ITU-T X.1277] [b-ITU-T X.1278] should be used.

iii. Smartphone authenticator apps should be used for sending one-time passwords rather than SMS due to the possibility of SS7 hijacking and other insecurities.

iv. If biometric information is used for authentication, it shall be stored with appropriate security measures such as encrypted in the Android Keystore or with the use of trusted hardware.

1.4 Secure Data Handling

i. Mobile devices should securely store confidential information.

ii. Trusted hardware should be used for the storage of sensitive information if it is available on client smartphones.

iii. Avoid storing information in external storage and if it is done, ensure that strong input validation is performed prior to using this data.

iv. Delete confidential data from caches and memory after it is used and avoid general exposure of information (e.g., placing the secret key on the stack). Assure the clean-up of memory prior to the application exiting.

v. Restrict data shared with other applications through fine-grained permissions. Minimize the number of permissions requested by the app and ensure that the permissions correlate to functionality required for the app to work.

vi. Do not hard-code sensitive information such as passwords or keys into the application source code.

vii. Validate any input coming from the client that is to be stored in databases to avoid SQL injection attacks.

1.5 Secure Application Development

i. Develop applications according to industry-accepted secure coding practices and standards.

ii. Assure a means of securely updating applications and assure that all dependent libraries and modules are secure; provide updates for these when required.

iii. Have code independently assessed and tested by internal or external code review teams