ITUPublications

International Telecommunication Union
Standardization Sector

ITU-T Technical Report

(05/2026)

Technical Report ITU-T DFS-2026

Digital financial services security recommendations

Technical Report ITU-T DFS-2026

Digital financial services security recommendations

Summary

This ITU-T Technical Report presents a set of recommendations to strengthen the security of digital financial services (DFS). It addresses vulnerabilities arising from Signalling System No. 7 (SS7) and related cross-protocol signalling risks involving newer network technologies, and outlines regulatory, operational and technical measures for mobile network operators and DFS providers to mitigate fraud, interception, account takeover and other threats. The report also covers SIM-related risks, including SIM swap fraud, SIM recycling and binary over-the-air attacks, and provides best practices for regulators, operators and providers to reduce these exposures. In addition, it includes a model memorandum of understanding to support coordination between telecommunications regulators and central banks, as well as a template of mobile application security best practices for securing DFS applications. Overall, the report emphasizes coordinated action across regulators, telecom operators, financial service providers and other stakeholders to improve resilience, protect consumers and sustain trust in digital financial ecosystems.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Table of Contents

Contents

Page

Technical Report ITU-T DFS -2026

Digital financial services security recommendations

The guidelines in Annexes 1 to 5 are proposed for adoption.

1 Summary of the guidelines

a) **Recommendations for regulators to mitigate SS7 vulnerabilities:** Recommendations for DFS regulators and mobile network operators to mitigate the impact of SS7 vulnerabilities on the security of digital financial services.

b) **Security recommendations to protect against DFS SIM risks and SIM swap fraud:** Guidance for regulators and DFS providers on mitigating SIM-related vulnerabilities, including SIM swap fraud, SIM recycling, and binary over-the-air attacks.

c) **Mobile application security best practices:** Best practices for securing mobile financial services applications that DFS regulators may adopt as guidelines.

d) **Template for a model MoU between a telecommunications regulator and central bank on digital financial services security:** Model clauses addressing DFS security that regulators may adopt or incorporate into existing memoranda of understanding.

e) DFS consumer competency framework: The DFS Consumer Competency Framework provides guidance to policymakers, national regulators, and DFS providers in developing consumer awareness and financial literacy programmes as part of a DFS or financial inclusion strategy.

See the annexes for details on the documents listed in items 1 to 4.

Annex 1: Recommendations for regulators to mitigate SS7 vulnerabilities

1 Introduction

The unstructured supplementary service data (USSD) and short message service (SMS) communication channels employed by end users to communicate with the digital financial services (DFS) provider rely on the legacy Signalling System No. 7 (SS7) protocol, which has for long been "broken". SS7 possesses many well-known vulnerabilities, some over 20 years old, which enable attackers to commit fraud, compromise DFS and steal funds through account takeovers, DFS interception, denial-of-service attacks, etc.

These risks are further amplified by multi-protocol and cross-generational signalling attacks, where vulnerabilities in SS7 are exploited to affect modern signalling protocols (e.g. Diameter and session initiation protocol/IP multimedia subsystem (SIP/IMS)) used in long term evolution (LTE) and voice over LTE (VoLTE) environments. DFS security controls must therefore address not only SS7 in isolation, but also its interaction with newer signalling technologies.

Guidelines, such as [b-ITU-T QSTR-SS7-DFS], focus on SS7 vulnerabilities and mitigation measures for DFS transactions [b-ITU-T QSTR-SS7-DFS]. However, consistent with the scope of [b-ITU-T Q.3066], this guidelines document also addresses DFS-relevant risks arising from interworking between SS7 and newer signalling protocols such as Diameter and SIP/IMS. A full signalling security asset inventory is not replicated here; instead, this document provides a DFS-focused mapping to the most relevant assets, interfaces and fraud scenarios to preserve readability for regulators and DFS providers.

A concrete example of cross-protocol risk would be an attacker using SS7 signalling (e.g. SendRoutingInfo or ProvideSubscriberInfo) to obtain a DFS subscriber's international mobile subscriber identity (IMSI), current serving network, or location data. This legacy-derived information can then be used to craft targeted Diameter or SIP/IMS requests such as fraudulent authentication vectors, manipulated routing, or session hijacking that affect the subscriber's DFS sessions in fourth generation (4G)/VoLTE environments. Such multi-protocol attack chains underscore the need for cross-protocol consistency checks and correlated detection across signalling layers.

2 Regulatory guidance to address vulnerabilities due to SS7

Below is a list of key regulatory measures and recommendations designed to address vulnerabilities in DFS resulting from weaknesses in the SS7 signalling protocol:

a) **Regulatory coordination:** a DFS-related bilateral memorandum of understanding (MoU) addressing signalling-related security risks, including those arising from SS7, should be established between the telecommunication regulator and the central bank. A sample MoU is provided in Annex B of the ITU technical report on SS7 vulnerabilities and mitigation measures for DFS transactions [b-ITU-T QSTR-SS7-DFS].

b) **The telecommunication regulator should also oversee signalling security risks arising from SS7, Diameter, SIP/IMS, and interworking interfaces, including risks associated with cross-protocol and cross-generational signalling attacks impacting DFS services**: Traditional SS7 networks do not operate in isolation. They interwork with Diameter (used in 4G/LTE) and SIP/IMS (used for VoLTE and multimedia services) through interworking functions and gateway nodes. Attackers

can exploit these interworking points to carry out cross-protocol attacks that bypass controls deployed on only one signalling layer. For example, an attacker with access to SS7 can send a SendRoutingInfo or ProvideSubscriberInfo query to obtain a subscriber's IMSI, serving mobile switching centre (MSC), or location data, and then use that information to craft targeted Diameter messages (e.g. a fraudulent Insert-Subscriber-Data-Request or Authentication-Information-Request) in the 4G domain, potentially hijacking a DFS user's session or redirecting their traffic. Because the attack spans two protocol generations, monitoring only SS7 or only Diameter would fail to detect it.

The regulator should require mobile network operators (MNOs) to deploy cross-protocol correlation and anomaly detection at signalling interworking points, maintain audited filtering rules across SS7, Diameter, and SIP interfaces, and include cross-generational attack scenarios in periodic signalling security assessments and incident reporting obligations.

c) **Incentivize the industry:** create incentive programmes with industry to promote the development of countermeasures in the telecom-DFS anti-fraud field.

d) **Incentivize the operators and providers:** create regulation that passes the financial damage from DFS fraud to the DFS providers and to the telecommunication operators, creating a financial incentive for action.

e) **Education for telecommunication and financial services regulators on SS7 vulnerabilities and impact on DFS:** telecommunication and financial regulators around the world need to be aware of the risks and, most importantly, be aware that there are available solutions to mitigate these risks. This awareness should include an understanding of signalling threat models, detection methods and mitigation principles, including those applicable to multi-protocol and cross-generational signalling attacks affecting DFS.

f) **IMSI validation gateway**: an IMSI validation gateway can be used by digital financial services providers (DFSPs) and banks to validate that the customer using the system is authentic and has been registered. This would allow DFSPs to detect USSD interception. However, the IMSI validation depends on the integrity of the underlying signalling path and should not be treated as standalone proof of user legitimacy. Its effectiveness requires trusted signalling validation controls to be in place, and it should be used in conjunction with other authentication factors.

g) **Telecommunication regulators to establish baseline security measures for each category (3G/4G/5G):** telecommunication regulators are encouraged to establish baseline security measures for each category (3G/4G/5G), which should be implemented by telecommunication operators to ensure a more secure interconnection environment. Baseline measures should include signalling threat detection and mitigation capabilities for interfaces supporting DFS services, including authentication of signalling messages and monitoring for anomalous signalling behaviour.

h) **Signalling security incident reporting and minimum security obligations**: regulators should establish mandatory signalling security incident reporting requirements for mobile network operators and DFS providers. The legal and regulatory framework should define minimum security obligations, including obligations to detect, report, and remediate signalling-related security incidents affecting DFS services. These requirements should be periodically reviewed and updated in line with evolving threat landscapes.

i) **Governance of baseline measures, allow-lists, and filtering controls**: where baseline security measures, allow-lists, or signalling filtering controls are deployed, these should be subject to audited rule sets, formal change control procedures, periodic review, testing, and maintenance. Such controls are only effective when correctly configured and continuously updated to reflect changes in network topology, interconnection agreements, and threat intelligence.

j) Mobile network operators and DFS providers should consider adopting the controls described in sections 2.1 and 2.2**.**

2.1 Mobile Network Operator (MNO) controls to address DFS vulnerabilities due to SS7

The MNO controls below span four distinct control families, consistent with the mitigation framework in [b-ITU-T Q.3066]: (a) correct configuration and hardening of network elements (e.g. secure ciphers, Transport Layer Security (TLS), access controls); (b) authenticity validation of signalling messages (e.g. allow-lists, message origin verification); (c) heuristic mitigation and logic checks (e.g. detecting engineered message sequences and cross-protocol inconsistencies); and (d) blocking of anomalous signalling flows (e.g. rate-limiting, filtering). Controls in list item h) (i) and (iv) below are complementary radio and infrastructure protections; the remaining controls directly address operational hardening and signalling interconnection attack detection and mitigation.

a) **Secure GSM ciphers for radio network traffic**: the mobile operator should ensure the use of secure radio encryption between user devices and base stations. Note: this radio-layer protection is complementary and does not replace detection and mitigation controls at signalling interconnection points (SS7/Diameter)..

b) **Session time out:** use session timeout for USSD and SIM toolkit (STK) to reduce the number of successful man-in-the-middle attacks.

c) **USSD personal identification number (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 short message service centre (SMSC) gateway (GW), USSD GW, and the DFS application server. Note: TLS between gateways and the DFS application server is a complementary infrastructure protection; it does not address signalling-level threats at the interconnect boundary.

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 allow-listed 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.

h) **Signalling threat detection and mitigation:** mobile network operators should deploy signalling threat detection and mitigation mechanisms, such as signalling firewalls or equivalent controls, to protect DFS-relevant signalling interfaces. These mechanisms should include:

i) Detection of unauthenticated or unauthorized signalling messages;
ii) Enforcement of signalling-origination allow-lists;
iii) Monitoring and rate-limiting of signalling requests impacting USSD, SMS, subscriber identity, and location.
iv) Heuristic analysis to detect engineered discrepancies and logic anomalies in signalling message sequences, as described in [b-ITU-T Q.3066];
v) Anomaly detection based on traffic pattern monitoring to identify deviations from established baselines for signalling volume, frequency, and geographic origin;
vi) Cross-protocol consistency checks to verify that signalling data across SS7, Diameter, and SIP/IMS interfaces is mutually consistent and has not been manipulated through interworking boundaries.

2.2 DFS provider controls to address DFS vulnerabilities due to SS7

DFS providers should consider adopting the following controls to mitigate SS7 risks**:**

a) **Session time out:** use session timeout for USSD and STK to reduce the number of successful man-in-the-middle attacks.one time password (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 such as USSD.

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

d) **Bidirectional OTP SMS flow:** require DFS providers to implement a bidirectional OTP process in which the user supplies a one-time password (OTP) via a controlled input channel (for example, USSD, an in-app input, or a secure web form) rather than relying solely on OTP delivery by SMS. This measure reduces the likelihood of OTP interception over the SMS channel but remains dependent on signalling integrity and therefore must be combined with additional authentication factors; signalling-derived information must not be the sole basis for authentication decisions.

e) **Detecting and mitigating social engineering attacks with Mobile-Terminated USSD (MT-USSD) and interception of USSD** by verifying using secureOTP, location validation, IMSI and international mobile equipment identity (IMEI)validation: DFS providers should not rely solely on signalling-derived data (e.g. SMS delivery, USSD session initiation, location, IMSI, or IMEI for authentication or authorization decisions and should correlate such data with additional device, behavioural, or risk-based controls.

f) **Detection of Mobile-Originated USSD (MO-USSD) interception:** DFS providers should implement controls to detect interception of mobile-originated USSD sessions, including monitoring for anomalous session initiation patterns, unexpected USSD gateway substitution, and man-in-the-middle attack indicators in the USSD transaction flow.

g) **SIM swap detection:** DFS providers should implement SIM swap detection mechanisms using IMSI and IMEI change indicators. When a change in IMSI is detected for a subscriber number linked to a DFS account, and particularly when accompanied by a change in IMEI, the DFS provider should trigger enhanced verification or temporarily restrict high-value transactions pending further authentication.

h) **SIM recycle controls:** DFS providers should implement controls to detect and prevent unauthorized access to DFS accounts when a phone number is recycled by the MNO and assigned to a new subscriber. This should include procedures to detect dormant SIM/number reassignment and to require re-verification of the account holder before permitting continued DFS access on a recycled number.

i) **Device binding and hard-to-spoof device identifiers:** where feasible, DFS providers should implement stronger device-binding mechanisms or use hard-to-spoof device identifiers to reduce the effectiveness of account takeover attacks that rely on SIM swap or signalling manipulation. Device binding should be considered as an additional authentication layer alongside signalling-derived data.

3 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

3G	Third Generation (mobile network)
4G	Fourth Generation (mobile network)
5G	Fifth Generation (mobile network)
DFS	Digital Financial Services
DFSP	Digital Financial Services Provider
GSM	Global System for Mobile Communications
GW	Gateway
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
LTE	Long Term Evolution
MNO	Mobile Network Operator
MO-USSD	Mobile-Originated USSD
MoU	memorandum of understanding

MT-USSD	Mobile-Terminated USSD
OTA	Over-The-Air
OTP	One-Time Password
PIN	Personal Identification Number
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SMSC	Short Message Service Centre
SS7	Signalling System No. 7
STK	SIM Toolkit
TLS	Transport Layer Security
USSD	Unstructured Supplementary Service Data
VoLTE	Voice over LTE
Wi-Fi	Wireless Fidelity

4 Bibliography

[b-ITU-T QSTR-SS7-DFS] International Telecommunication Union – Telecommunication Standardization Sector (2019), *SS7 Vulnerabilities and Mitigation Measures for DFS Transactions*. Available at: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-PROTO-2019-PDF-E.pdf

[b-ITU-T Q.3066] Recommendation ITU-T Q.3066 (2026), *Principles for detection and mitigation of signalling attacks in telecommunication networks*. Available at: https://handle.itu.int/11.1002/1000/1668

Annex 2: Best practices for regulators to protect DFS against SIM risks

1 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.

1.1 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.

1.1.1 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.

1.1.2 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.

1.1.3 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.

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

2.1 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 2.2 below.

c. 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

2.2 Mobile network operator controls to mitigate SIM risks and fraud

a) Where SIM replacement is carried out by proxy, the MNO/MVNO or its agents must capture a biometric, facial image of the proxy which must be kept for a specified period.

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

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

d) **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).

e) **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.

f) **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

g) **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).

h) **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

i) **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.

2.3 DFS operators controls to mitigate SIM risks and fraud

a) **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.

b) **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

c) **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 Interpretation

Unless the context clearly indicates a contrary intention, the following definitions shall apply to all clauses in this MOU:

1.1 '**Anti-Money Laundering,'** often referred to as AML, relates to sets of procedures and policies implemented according to international standards to prevent money laundering, fraud and terrorist financing in a country.

1.2 **'Base Station,'** often also referred to as Base Transceiver Station (BTS), is a transmitter/receiver that relays information from a transmitting/receiving unit such as a mobile phone

1.3 '**Consumer Protection'** involves safeguarding consumers in the DFS ecosystem from financial and associated harm due to practices of providers. Consumer protection laws and regulations are generally and specifically designed to protect consumers against falsely described low quality and dangerous goods and services, fraud, abuse, errors and unfair trade and credit practices.

1.4 **'Core Network,'** also referred to as backbone network, is a part of the telecommunications network that facilitates exchange of information between different sub-networks. It offers services to end users who are connected to the core network through different access networks.**"Confidential Information"** means any information of whatever nature disclosed to or acquired by the Authorities in the course of implementing this MOU, including all exchanged information and trade secrets both verbal and written transmitted by any means whatsoever, to the extent that such

knowledge and information at the time of the disclosure or acquisition is not intended to be or part of public knowledge or literature.

1.5 **'Data Protection'** refers to the practices of enterprises to protect end user data, based either on internal policies or specific laws and regulations.

1.6 **'Digital Financial Services'** (DFS) include methods to electronically store and transfer funds; to make and receive payments; to borrow, save, insure and invest; and to manage a person's or enterprise's finances.

1.7 **'Digital Financial Service Providers' (DFSPs)** are supervised entities involved in providing DFS to end users.

1.8 **'Dispute Resolution'** refers to processes specified by a service provider or by the rules of a payment scheme or telecommunications network to resolve issues between end users and providers, between a customer (as an end user) and its counterparty, or between providers.

1.9 **'End user,**' means either a consumer or a business.

1.10 **'Financial Inclusion'** means the sustainable provision of affordable financial services that bring the poor into the formal economy.

1.11 **'LTE'** means Long term Evolution, a broadband mobile phone protocol.

1.12 **'Mobile Network Operator'** (MNO) is an enterprise which provides mobile phone services, including voice and data communication.

1.13 **'Mobile Phone Frequency Band'** are the groups of radio frequencies used by mobile networks to communicate with mobile phones.

1.14 **'Payment System'** refers to all payment-related activities, processes, mechanisms, infrastructure, institutions, and users in a country or a broader region such as a common economic area.

1.15 **'Provider'** is an entity that provides a digital financial service or associated telecommunications service to an end user.

1.16 **'Regulator'** – also an **'Authority'** - refers to a state or governmental entity that derives its power through national law and/or associated regulations to establish and enforce standards and practices. The **BOSS** and the **NCA** are examples of such entities.

1.17 **'Risk Management'** means practices that enterprises do to understand, detect, prevent, and manage various types of risks. This may involve provision of a risk management framework (RMF).

1.18 **'Signaling System 7' (SS7)** is an international standard that outlines the functions and protocol to be performed by a signaling system-network used in a mobile or fixed-line network. **'Subscriber Identity Module (SIM) Card'** is a smart card inside a mobile phone handset, carrying an identification number unique to the owner, storing personal data, and preventing full operation if removed.

3 Areas of cooperation and cooperation strategies general provisions

3.1 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.

3.2 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;

4 National Telecommunications Regulator-Designated roles

4.1 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.

4.2 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.

4.3 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.

4.4 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.

5 Central Bank-designated roles

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

5.2 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.

6 Joint Role: Consumer Protection

7 Joint Role: Anti Money Laundering

7.1 The CENTRAL BANK and NATIONAL TELECOMMUNICATIONS REGULATOR agree to cooperate on coordinating on the implementation of effective measures to combat the financing of terrorism, money laundering and fraud. This includes the following activities:

7.2 Facilitating the discovery of and actions against non-compliance or fraudulent practices by market participants and customers.

7.3 Conducting frequent capacity building and awareness programs on cyber-security and cyber resilience for market participants and customers respectively;

7.4 Ensuring the imposition of effective sanctions for non-compliance.

8 Coordination between the parties

8.1 The CENTRAL BANK and NATIONAL TELECOMMUNICATIONS REGULATOR agree to work together to promote a coordinated framework for the regulation and supervision of DFS. Such collaboration will include but not be limited to the following:

a) Establishing appropriate systems and clear procedures for the supervision of DFS;

b) Regulating and supervising providers to ensure DFS are provided in a safe, sound and sustainable manner that promotes financial inclusion;

c) Developing standards and guidelines as deemed necessary;

d) Implementing strategies and policies aimed at enhancing financial inclusion through DFS;

e) Inspecting DFS participants and providing technical expertise.

9 Nomination of Liaison Officers

9.1 The CENTRAL BANK and shall designate primary liaison officers to facilitate the exchange of information, handling of technical, operational and legal/regulatory issues, and implementation of the provisions of this MOU. The parties shall also designate alternative personnel that may be contacted and involved when primary personnel are unavailable.

10 Establishment of a Joint Working Committee

10.1 A Joint Working Committee (JWC) constituted by representatives of the CENTRAL BANK and NATIONAL TELECOMMUNICATIONS REGULATOR and as nominated by each Authority - shall be established pursuant to this MOU within sixty MOU ands of the signing of this MOU, and shall function on an on-going basis.

10.2 The JWC shall be constituted of not more than twelve (12) members, six (6) from each Authority. The nominated members shall possess the relevant technical, operational, and legal/regulatory skills necessary to achieve the goals and specific activities outlined in this MOU.

10.3 The JWC shall appoint a chairperson amongst its membership at its first meeting, and shall develop operational procedures for the JWC.

10.4 The chairpersonship of the JWC shall be on one year rotation basis between the Authorities.

10.5 Functions of the JWC

a) To manage and facilitate cooperation and consultation in respect of matters dealt with by each regulator in terms of this MOU;
b) To advise on the proper functioning of the MOU arrangements;
c) To propose, when necessary, any amendments or supplements to this MOU;
d) To determine the effect and mitigation of any breaches and intrusions of mobile networks that may have an effect on the proper operation and financial security of DFS.
e) To advise management of both the CENTRAL BANK and NATIONAL TELECOMMUNICATIONS REGULATOR on issues affecting DFS and adjacent issues, and make recommendations on how to deal with such issues. Such advice shall be with regard to, but not limited to, the following:
   i) Nature of potential regulatory overlap between the CENTRAL BANK and NATIONAL TELECOMMUNICATIONS REGULATOR in relation to DFS;
   ii) International approaches to issues of jurisdictional overlap between CENTRAL BANK and NATIONAL TELECOMMUNICATIONS REGULATOR;
   iii) Necessary amendments to any relevant or applicable law, guidelines, regulations, or any other legal or statutory instrument that may be required so as to allow either Authority to give effect to its statutory mandate for matters that fall within the scope of this MOU;
   iv) The need for any new law, guideline, by-law regulation, or any other legal or statutory instrument as the case may be, which may be required so as to allow either Authority to give effect to its statutory mandatefor matters that fall within the scope of this MOU;

v) Any issue related to, *inter alia*, security, service availability, risk management, pricing, and consumer protection for matters that fall within the scope of this MOU; and Any other related matters.

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