

ITU-T Technical Report

(05/2026)

Technical Report ITU-T DFS-SS7-2026

Recommendations to mitigate Signalling System No. 7 vulnerabilities in digital financial services



Technical Report ITU-T DFS-SS7-2026

Recommendations to mitigate Signalling System No. 7 vulnerabilities in digital financial services

Summary

This ITU-T Technical Report provides recommendations for enhancing the security of digital financial services by addressing vulnerabilities within Signalling System No. 7 (SS7). It examines the risks posed to financial transactions and customer data due to security flaws in SS7, a protocol widely used in global telecommunications. The report outlines technical measures, operational best practices, and policy guidelines aimed at mitigating these threats. Emphasis is placed on the importance of collaboration among telecom operators, regulators, and financial service providers to safeguard digital financial ecosystems and maintain public trust in digital transactions.

Keywords

Digital financial services, SS7, telecommunications security, Q.3066

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.

© ITU 2026

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Page

1	Introduction.....	1
2	Regulatory guidance to address vulnerabilities due to SS7.....	1
2.1	Mobile Network Operator (MNO) controls to address DFS vulnerabilities due to SS7.....	3
2.2	DFS provider controls to address DFS vulnerabilities due to SS7.....	4
3	Bibliography	5

Technical Report ITU-T DFS-SS7-2026

Recommendations to mitigate Signalling System No. 7 vulnerabilities in digital financial services

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 secure OTP, 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>
-