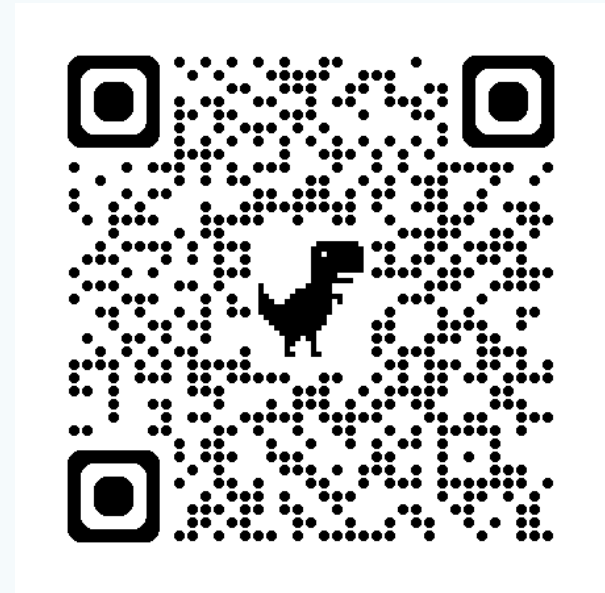


# DFS Security Recommendations for Regulators and Providers

---

Arnold Kibuuka, Project Officer, ITU

February 2025



<http://www.itu.int/go/dfssl>

## DFS Security Recommendations

1. [Security recommendations to protect against DFS SIM related risks](#)
2. [Recommendations to mitigate SS7 vulnerabilities](#)
3. [DFS Mobile application security Best practices](#) (From [ITU-T X.1150](#) )
4. [Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security](#)
5. [DFS consumer competency framework](#)

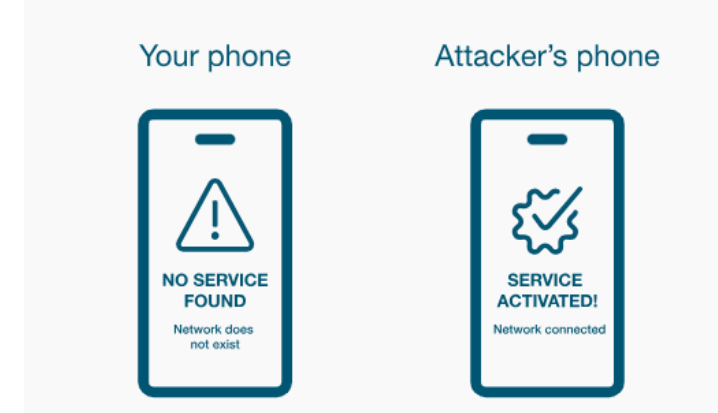
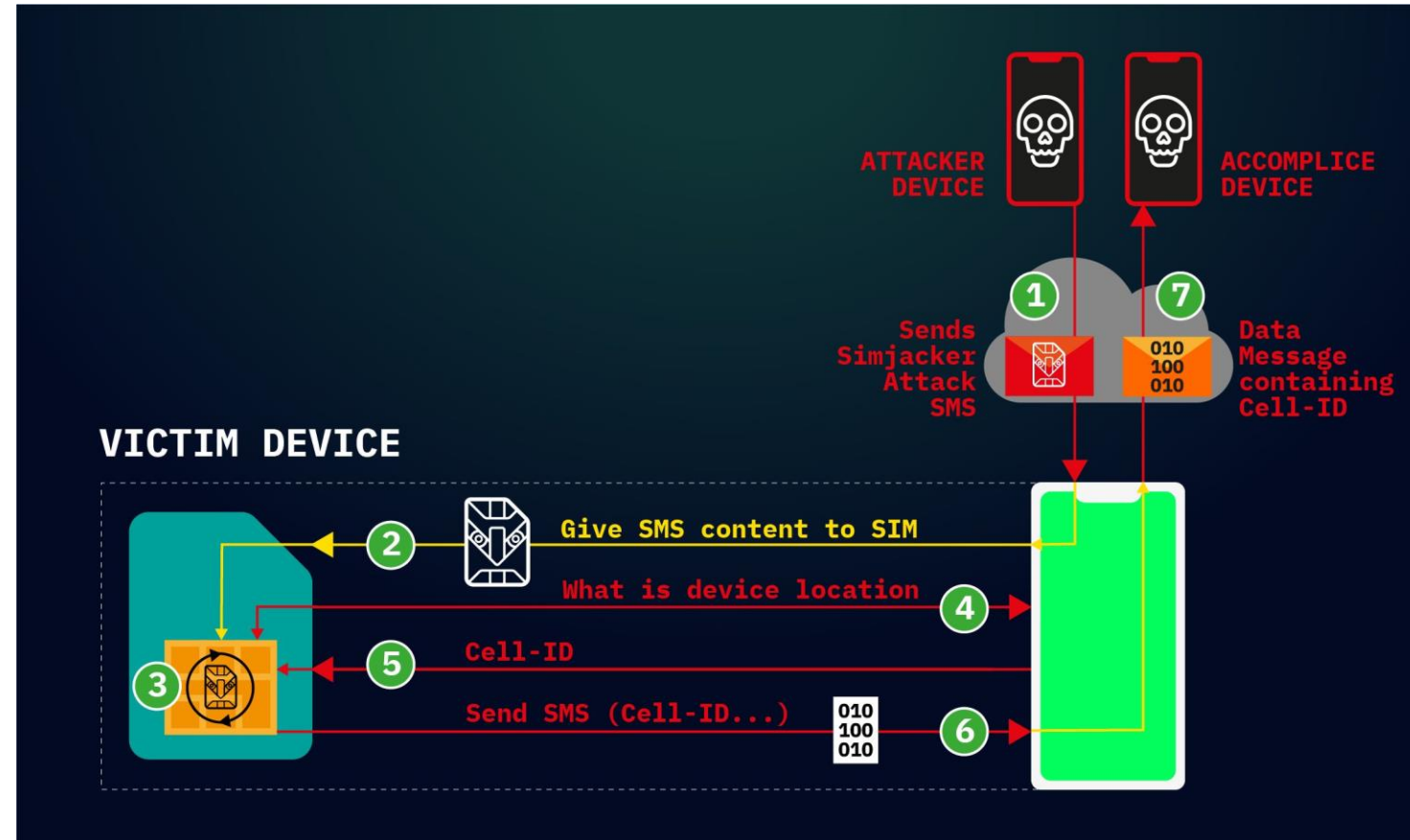
## **Regulatory Guidance to Mitigate SIM Risks**

## Poll Question

*Which of these SIM card-related security risks are you familiar with?*

## SIM Risks

- SIM cloning
- SIM swaps
- SIM Recycling
- Binary over the air attacks (Sim jacker and WIB browser attacks)





## Regulatory Guidance to Mitigate SIM Risks

- Regulatory coordination between telco and DFS regulator on SIM vulnerabilities.
  - e.g. An MOU between the DFS regulator and Telco regulator
- Standardization by regulators of SIM swap rules amongst MNOs/MVNOs
- Recommending security measures for DFS operators on SIM risks.



**Business Rules & Operational Processes for  
Implementation of the SIM Replacement Guidelines 2022**

# MOU between the Central Bank and Telco Regulator

- A bilateral MOU related DFS should be in place between the ICT and Financial regulators.
- responsibilities of the central bank and ICT regulator for security of DFS (SIM swap fraud, SS7, consumer protection etc.)
- modalities around the creation of a Joint Working Committee on DFS security and risk-related matters.

## **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:**

- DFS generally;
- Full and fair access to, security, and reliability of all components of DFS in (the country);
- Consumer Protection; and
- 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:**

- Exchange of any relevant information;
- Mutual capacity building;
- Investigation of any incident, issues and cases relating to the scope of this MOU;
- Joint or individual hearings, as needed;
- Use of common systems for DFS transaction monitoring
- Fostering competition and promoting a level playing field for all participants of a DFS ecosystem;
- Dispute resolution between providers, and between consumers as end users;
- Development, monitoring and enforcement of relevant provisions of respective laws, by-laws, guidelines, or regulations where these may relate to DFS;

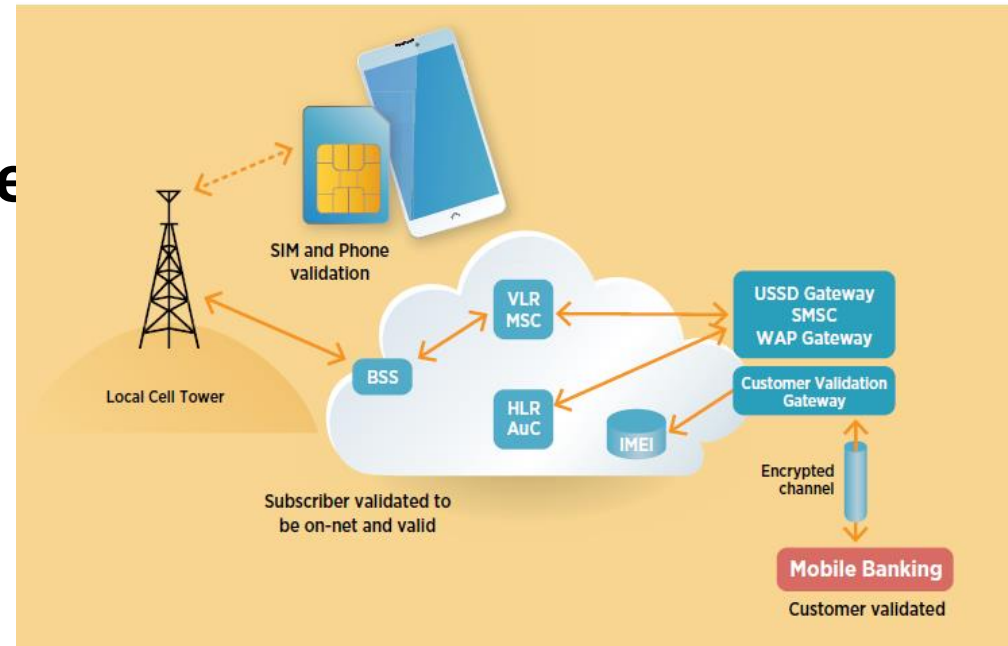


## **MNO Controls on SIM Swaps (SIM Swap Rules for MNOs and MVNOs)**

- the MNO/MVNO or its agents must capture a biometric, facial image of the proxy which must be kept for a specified period.
- MNOs should notify DFS providers on swapped SIMs, ported and recycled numbers.
- SIM swap notifications to users
- Biometric SIM swap verification
- Multifactor user validation before SIM swap
- Secure SIM data protection
- Holding time before activation of a swapped SIM
- Service support representatives training

## DFS Operators Controls to Mitigate SIM Swaps

- Real time IMSI/ICCID detection
- Real time device change detection – device to DFS account binding
- Encourage use of secure DFS access through apps.



### Category: PREMIUM

#### API Name

#### API Definition

Sim Swap API

API which allows a corporate customer to check if a given MSISDN has performed a SIM swap. Returns 'MSISDN', date of last SIM swap'

Authentication API

API which allows a corporate customer to use MTN Service to send OTPs . A customer is onboarded on the MTN instance and the OTP service is configurable to them

KYC Premium API

API allows a customer to check if the KYC info provided by its customers matches with that provided at Sim registration. Returns one or more actual customer details. This requires customer consent

## Guidance to Mitigate SS7 Threats

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

## Poll Question

SS7 (Signalling System No. 7) is a network protocol used by telecom companies. Vulnerabilities in SS7 can impact the security of Digital Financial Services (DFS).

*How familiar are you with SS7 and its potential impact on DFS?*

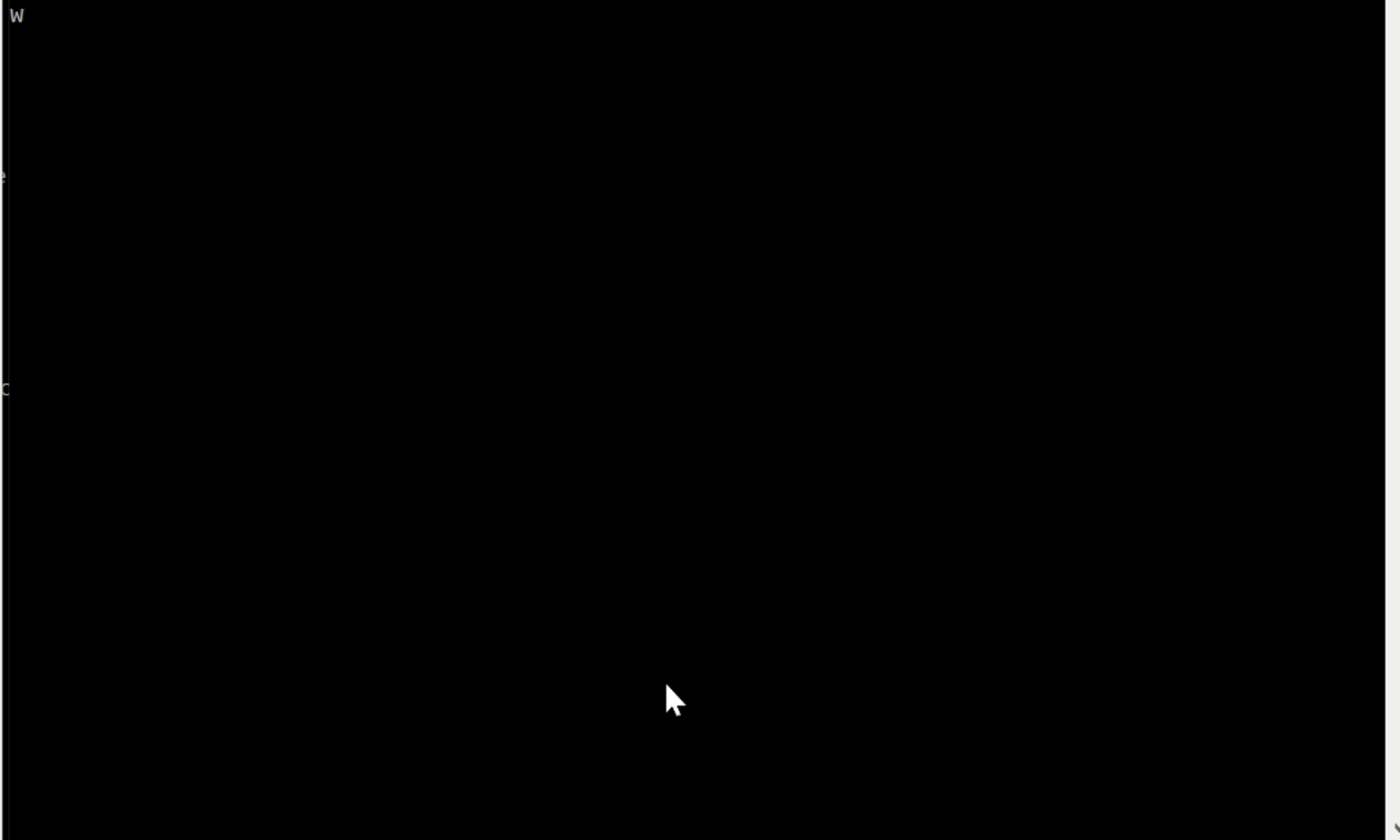


Next

or

Sign Up

```
assaf@DESKTOP-MCKINNK: /mnt/c/Work/Vaulto/Vaulto/tests
assaf@DESKTOP-MCKINNK:~$ cd /mnt/c/Work/Vaulto/Vaulto/tests/
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ clear
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ python demo_ul_sms_intercept.py 972502138133 ne
w
```



## Regulatory Guidance to Mitigate SS7 Risks

- Regulatory coordination between telco and DFS regulator on SS7 vulnerabilities.
- Incentivize the industry
- Education for telecom and financial services regulators on SS7 vulnerabilities and impact to DFS
- Telecom regulators to establish baseline security measures for each SS7 risk category
- IMSI validation gateway: An API that provides status of a number and real time country where client is located.

## Recommendations for MNO to Mitigate SS7 Risks

- SS7 interconnect security monitoring guidelines
- Session time out
- USSD PIN masking
- Secure and monitor core network traffic
- Limit access to traces and logs
- SMS filtering
- SMS home routing

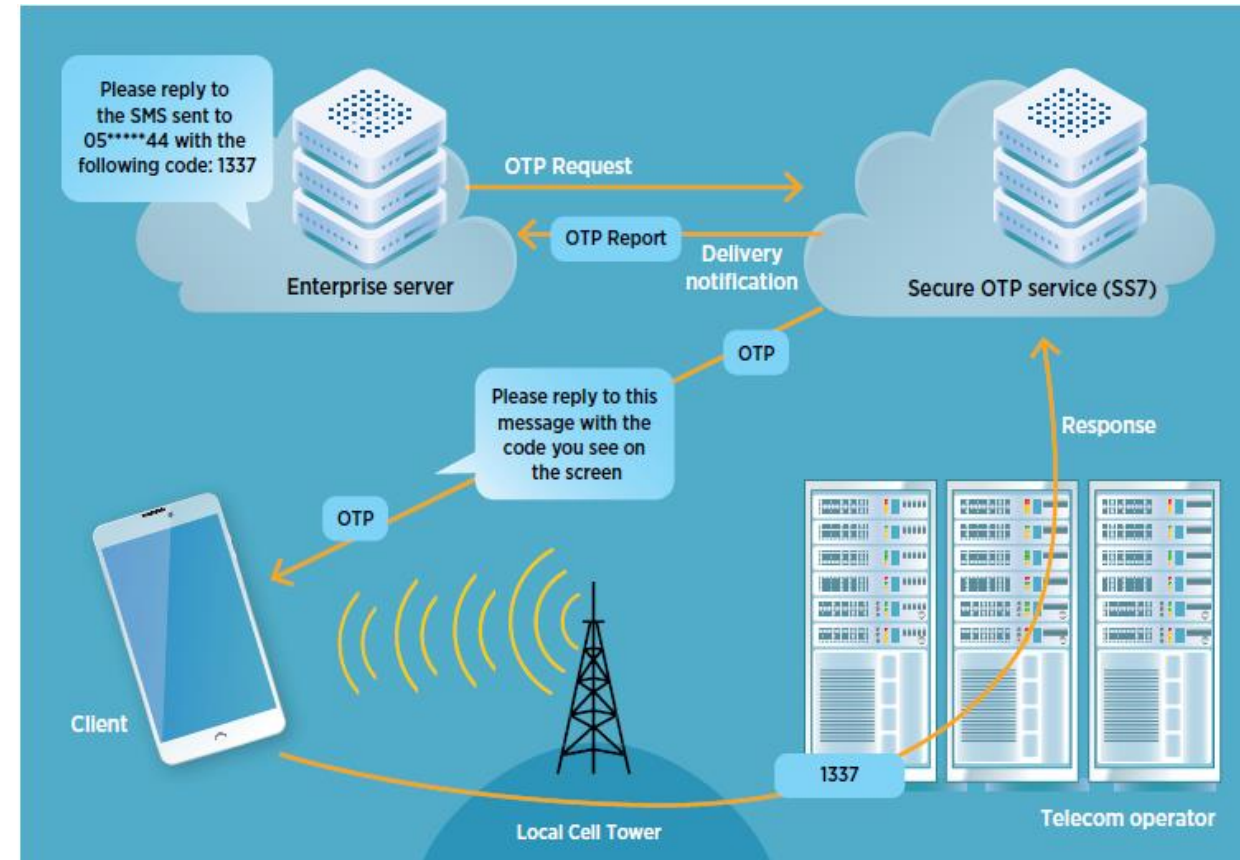
```

1 13:08:00.624000      1841      8744
> Frame 1: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits)
> Ethernet II, Src: Private_01:01:01 (01:01:01:01:01:01), Dst: MS-NLB-PhysSer
> Internet Protocol Version 4, Src: 1.1.1.1, Dst: 2.2.2.2
> Stream Control Transmission Protocol, Src Port: 2984 (2984), Dst Port: 2984
> MTP 2 User Adaptation Layer
> Message Transfer Part Level 3
> Signalling Connection Control Part
> Transaction Capabilities Application Part
v GSM Mobile Application
  v Component: invoke (1)
    v invoke
      invokeID: 1
      > opCode: localValue (0)
      > ussd-DataCodingScheme: 0f
      v ussd-String: aa180da682dd6c31192d36bbdd46
        USSD String: *140*0761241377#
      v msisdn: 917267415827f2
        1... .... = Extension: No Extension
        .001 .... = Nature of number: International Number (0x1)
        .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.1
      v E.164 number (MSISDN): 27761485722
        Country Code: South Africa (Republic of) (27)

```

## DFS Operator Controls to Mitigate SS7 Risks

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

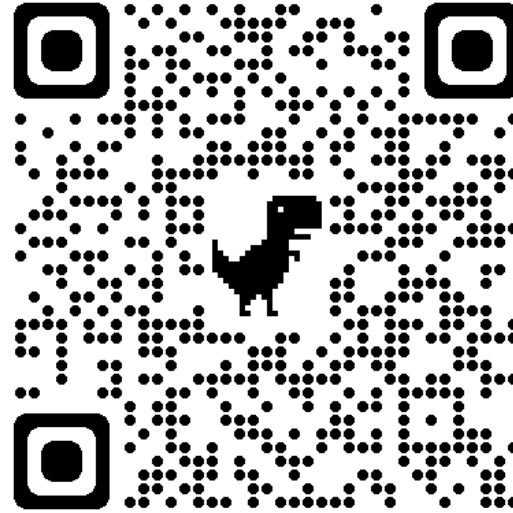




## ITU-T Study Group 11 Work on SS7

### Published Recommendations and Technical Reports:

- [ITU-T QSTR-SS7-DFS \(2019\)](#): SS7 vulnerabilities and mitigation measures for digital financial services transactions
- [ITU-T QSTR-USSD \(2021\)](#) Low resource requirement, quantum resistant, encryption of USSD messages for use in financial services
- [ITU-T Q.3062 \(2022\)](#): Signaling procedures and protocols for enabling interconnection between trustable network entities in support of existing and emerging networks
- [ITU-T Q.3063 \(2022\)](#): Signaling procedures of calling line identification authentication
- [Draft Q.TSCA](#): Requirements for issuing End-Entity and Certification Authority certificates for enabling trustable signaling interconnection between network entities.
- [Draft Q.DMSA](#): Principles for detection and mitigation of signaling attacks in security signaling gateway



<http://www.itu.int/go/dfssl>

**Contact:** [dfssecuritylab@itu.int](mailto:dfssecuritylab@itu.int)

**Thank you!**