

# ITU DFS Security Knowledge Sharing platform



# ITU Knowledge Sharing Platform for Digital Finance Security



## Team Library

ITU DFS Security Knowledge Sharing Platform



Collaborating & contributing to the Recommendation  
Edited 20d ago



DFS Security Assurance Framework  
Edited 20d ago



Mobile Payment Application Security Best Practices  
Edited 20d ago



SS7 Vulnerability Security Controls  
Edited 20d ago



SIM swap threats  
Edited 20d ago



MOU between Telco Reg & Central Bank for Security  
Edited 20d ago

## Objective

- Collaborate with ITU to keep up to date the DFS security assurance framework security controls and DFS security recommendations.
- Share experiences, challenges, and lessons learned from the implementation of security measures across various jurisdictions.
- Communicate directly with their peers on issues relating to security of digital financial services.

[Link: Knowledge Sharing Platform for Digital Finance Security \(itu.int\)](https://www.itu.int)

# Why?

## Collaborate

Collaborate with ITU to keep up to date the DFS security assurance framework security controls and DFS security recommendations.

## Share

Share experiences, challenges, and lessons learned from the implementation of security measures across various jurisdictions.

## Communicate

Communicate directly with their peers on issues relating to security of digital financial services.

# Who can contribute? DFS stakeholders



DFS regulators



DFS providers



Telco regulators



Telco providers

# The collaboration tools



discussions  
amongst  
members



Propose and  
discus &  
changes



Manages agreed  
changes and  
comments



<https://staging.itu.int/en/ITU-T/dfs/Pages/share-platform.aspx>



## Knowledge Sharing Platform for Digital Finance Security

YOU ARE HERE [ITU](#) > [HOME](#) > [ITU-T](#) > [DFS](#) > KNOWLEDGE SHARING PLATFORM FOR DIGITAL FINANCE SECURITY

SHARE    

The ITU Knowledge Sharing Platform for Digital Finance Security is designed to foster collaboration among regulators and other stakeholders in the development and implementation of security guidelines and best practices for Digital Financial Services (DFS).

The [WTS-20 Resolution 89](#) instructs the Director of the Telecommunication Standardization Bureau, in collaboration with the Directors of the other Bureaux to establish a platform or, where possible, connect to those already existing, for peer learning, dialogue and experience-sharing in digital financial services among countries and regions, regulators from the telecommunication and financial services sectors, industry experts and international and regional organizations; PP-22 Resolution 204 further instruct pertinent ITU-T study groups to participate in global initiatives aimed at enhancing the cybersecurity and resiliency of the digital finance ecosystem. This involves developing international standards and industry best practices to ensure a secure and robust digital financial landscape.

The ITU Knowledge Sharing Platform is a component of the [ITU DFS security lab](#), which provides resources for conducting security tests for Mobile payment applications as well as developer resources for Fast Identity Online (FIDO) implementation of strong consumer authentication.

### The Objectives of the Knowledge Sharing Platform are as follows:

- Collaborate with ITU to keep up to date the DFS security assurance framework security controls and DFS security recommendations.
- Share experiences, challenges, and lessons learned from the implementation of security measures across various jurisdictions.
- Communicate directly with their peers on issues relating to security of digital financial services.



← ↻ 🔒 https://app.gitbook.com/o/1yZjfc3b7W6BuwvveBBZ/home


Quick find **^K**

ITU DFS Security ...







- Collaborating & contribu...
- DFS Security Assurance ...
- Mobile Payment Applica...
- SS7 Vulnerability Securit...
- SIM swap threats
- MOU between Telco Re...

+ New Space

**ITU DFS Security Knowledge Sharing Platform**

 **Team Library**  
ITU DFS Security Knowledge Sharing Platform

☰ ☰

-  Collaborating & contributing to the Recommendation  
Edited 21d ago
-  DFS Security Assurance Framework  
Edited 20d ago
-  Mobile Payment Application Security Best Practices  
Edited 20d ago
-  SS7 Vulnerability Security Controls  
Edited 20d ago
-  SIM swap threats  
Edited 20d ago
-  MOU between Telco Reg & Central Bank for Security  
Edited 20d ago

**Invite your team** ✕

Invite team members to your organization to enjoy the best of GitBook.

[Invite teammates](#)



Adding a  
change  
request in  
Gitbook via  
slack  
channel

Quick find ^K

ITU DFS Securit...  
Collaborating & contri...  
DFS Security Assuran...  
Mobile Payment Appli...  
567 Vulnerability Sec...  
IM swap threats  
YOU between Telco ...  
New Space

Invite your team  
Invite team members to your organization to enjoy the best of GitBook.  
Invite teammates

Import content  
Templates

1

## DFS Security Assurance Framework

Change Requests History Customize Discussions Files Insights Integrations

DFS Security Assurance Framework

Table of contents

Security threats

Risk assessment methodology >

DFS security vulnerabilities, threats and mitigation Measures In order to systematical

Account and Session Hijacking

Attacks against systems and platforms

Code Exploitation Attacks

Data Misuse

Denial of Service Attacks

# Account and Session Hijacking

The general threat is the ability of an attacker to take control of an account or communication session. The vulnerabilities are manifested in different ways at the DFS provider and the MNO.

**Affected Entity: DFS Provider**

**Risk: Data exposure and modification**

- **Vulnerability:** Inadequate controls on dormant accounts
  - Control 1.1:** Set timeouts and auto logouts user sessions on DFS applications (logical sessions). Within the application, ensure support for password complexity (enforced by the server), set maximum unsuccessful login attempts, password history and reuse periods, account lock-out periods to a reasonably minimal value to minimize the potential for offline attack

# Contributing: Propose a change in slack

The image shows a dual-screen setup. The left screen displays a GitHub repository page for the 'DFS Security Assurance Framework'. The main heading is 'Attacks against systems and platforms'. The page content includes a table of contents, a description of the attacks, and a list of vulnerabilities and controls. The right screen shows a Slack workspace named 'ITU DFS security'. The channel is '#security-assurance-framework'. A message from 'dfssecuritylab' is visible, containing a link to the GitHub page and a suggestion to suggest changes. The Slack interface also shows a sidebar with channel lists and a profile section for 'dfssecuritylab'.

**Attacks against systems and platforms**

We characterize these attacks as those that a remote adversary can carry out to spy on or modify information without insider credentials or other privileged access.

**Affected entity: Mobile user**

**Risk: Spying and credentials stealing from user devices**

- Vulnerability:** Unverified malicious binary SMS SIM updates (SD: authentication)
  - Control 3.1:** Provide the mobile user with the ability to trust or distrust individual binary-based SMS messages. Doing so could prevent malicious updates to the SIM card
- Vulnerability:** Insecure transfer of customer credentials (SD: access control)
  - Control 3.2:** DFS providers should transmit the user authentication credentials securely over a different channel (out of band).

**Risk: Account access, compromise and denial of service**

- Vulnerability:** Exposure of Internal network to external adversaries (SD: access control)
  - Control 3.3:** Use Network Address Translation to limit external exposure of DFS IP address and routing information.

**Affected entity: DFS Provider**

**Risk: Account access, compromise, and denial of service**

- Vulnerability:** Insufficient protection of internal systems against external adversaries (SD: access control)
  - Control 3.4:** Avoid direct access by external systems to the DFS backend systems by

**Slack Channel: #security-assurance-framework**

This is the very beginning of the #security-assurance-framework channel  
You created this channel yesterday. Add description

dfssecuritylab 1:53 PM  
joined #security-assurance-framework along with A Kibuuka.

https://itu.gitbook.io/dfs-security-assurance-framework/dfs-security-vulnerabilities[...]-in-order-to-systematical/attacks-against-systems-and-platforms | suggest ...

itu.gitbook.io  
Attacks against systems and platforms...

Schedule for later



