Digital Financial Services Security Clinic

Addressing security risks to digital finance ecosystem

DFS Security lab

Vijay Mauree
Programme Coordinator, ITU

Introduction

Financial Inclusion Global Initiative (FIGI)

Global Goal – UFA 2020

FIGI 3X3X3

Implementation Principles, Recommendations, Guidelines

PAFI Guiding Principles + ITU DFS Focus Group Recommendations + Level One Design Principles

BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

BILL & MELINDA GATES foundation

International Standards

www.figi.itu.int/figi-resources/dfs-security-lab/

FIGI Security Infrastructure & Trust Working Group

SIT WG workstreams

Working Group Reports

Security Workstream

Address DFS application security, telecom infrastructure security issues, consumer authentication and cybersecurity risk management.

Trust Workstream

Address unlicensed digital investment schemes, digital skills for users, and innovations and risks that AI and big data pose when used in financial inclusion.

Quality of Service Workstream

Develop methodology for measurement of key performance indicators (KPIs) for QoS and QoE for DFS

Distributed Ledger Technologies Workstream

Use of distributed ledger technology to secure digital financial services transactions.

www.figi.itu.int/figi-resources/dfs-security-lab/

Problem statement

No common approach for regulators, developers and DFS providers to test DFS mobile apps in a complex mobile ecosystem in order to provide/verify the level of assurance on security.

DFS application systemic vulnerabilities

Systemic vulnerabilities include those that can impact integrity and confidentiality of the transactions, for instance:

- The security communication protocols used (strength of ciphers).
- Secure user authentication
- Security checks on certificates
- Can the application be executed on rooted devices?
- Is consumer data privacy preserved?
- Is the source code properly obfuscated?

The DFS security lab provides a common methodology to conduct security audit for mobile DFS apps and address systemic vulnerabilities.

DFS security lab objectives

Collaborate with DFS regulators and DFS providers to enhance the cybersecurity strategy for DFS and security assurance of the DFS ecosystem by implementing the recommendations in:

1. DFS Security Assurance Framework
2. Security testing for USSD and STK based DFS applications
3. Security audit of various DFS applications
4. DFS security audit guideline

See https://figi.itu.int/figi-resources/working-groups/

DFS security lab objectives

The reports contain the following specific guidelines that may be adopted by regulators.

1. Recommendations to mitigate SS7 vulnerabilities
2. Model Memorandum of Understanding between a Telecommunications Regulator and a Central Bank Related to Security for Digital Financial Services
3. Recommendations for securing mobile payment apps
4. Recommendations for operators and regulators for SIM card risks such as SIM swap fraud and SIM card recycling

See *https://figi.itu.int/figi-resources/working-groups/*

DFS Security Lab Components

Security testing for **USSD** and **STK**

Developer resources for strong authentication using **Fast Identity Online** (**FIDO)**

Security audit of **Android** DFS apps using **OWASP** Mobile Top 10 Risks.

DFS Security Lab Objectives

Collaboration with DFS regulators on security

Perform DFS **security audits** of DFS Apps

Encourage adoption of **international standards on DFS security**

Organise **security clinics**

Assist DFS regulators to evaluate the **cyber preparedness** for DFS ecosystem

Knowledge sharing on threats to security of DFS apps

FIDO Developer Resources

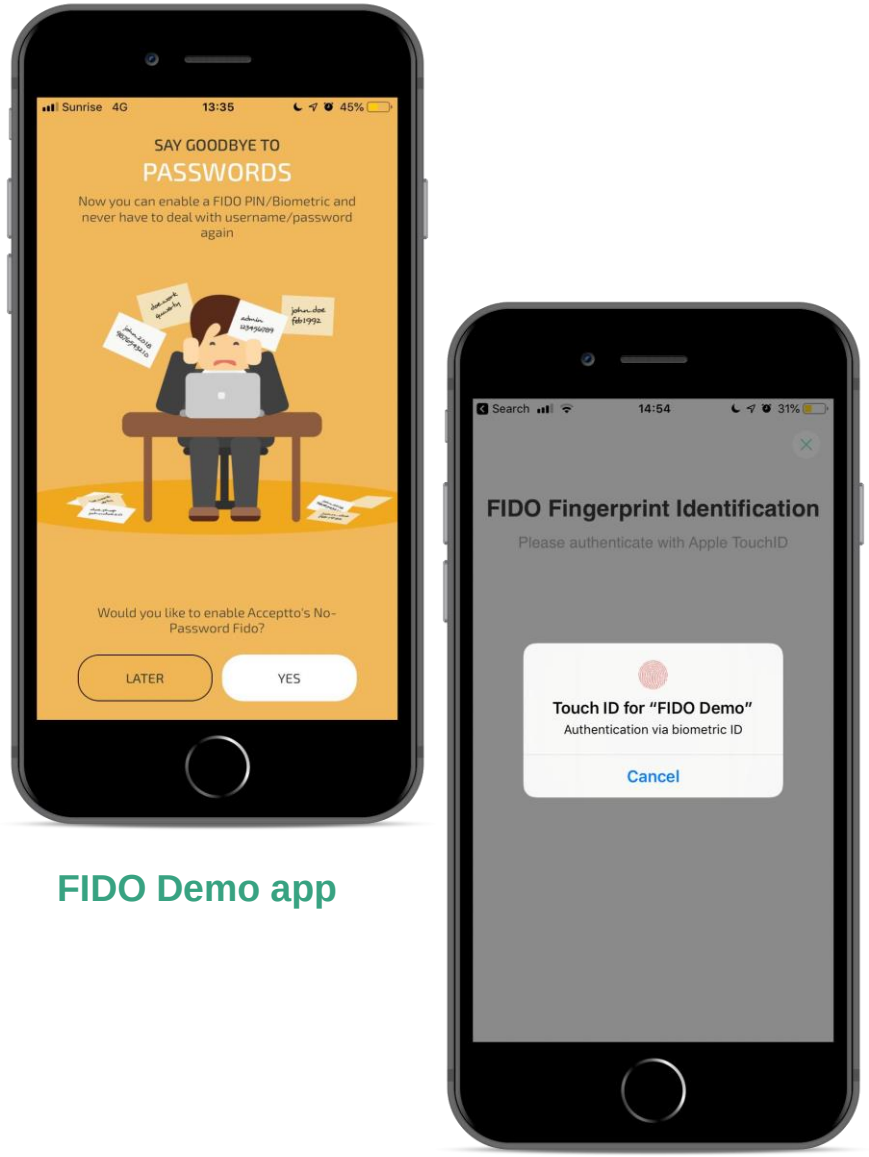
FIDO (Fast ID Online) is a set of technology-agnostic security specifications for strong authentication (passwordless authentication).

ITU Resources for developers

i. Step-by-step guide for deploying FIDO UAF on a native app

ii. FIDO UAF compliant server to test FIDO UAF authentication

iii. Sample Android and iOS FIDO demo client app to show user registration, deregistration, and transaction authentication.

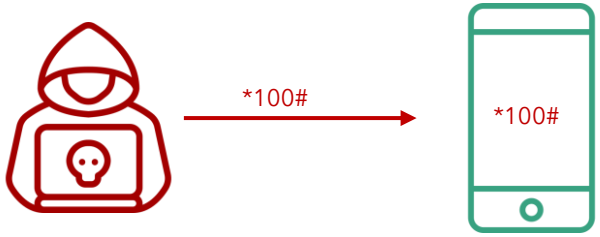


FIDO Demo app

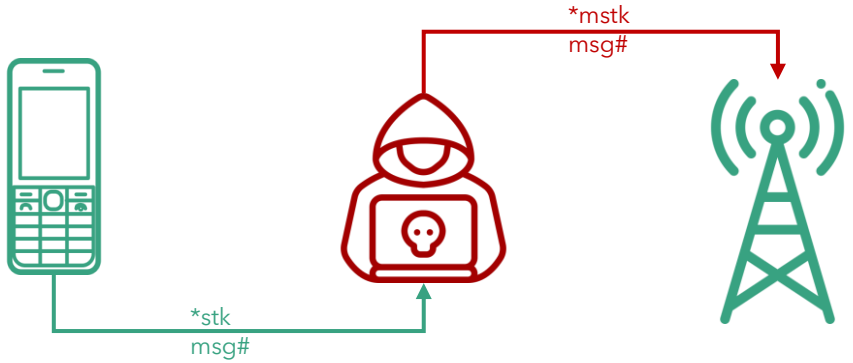
USSD & STK tests

a. **SIM Swap** and **SIM cloning**

b. susceptibility to **binary OTA attacks** (SIM jacker, WIB attacks)



c. **remote USSD** execution attacks



d. **man-in-the-middle attacks** on STK based DFS applications

Android app security tests

Risks	Security test
M1 Improper Platform Usage	Check misuse of platform features or failing to use platform security controls provided
M2 Insecure Data Storage	Check that malware and other apps do not have access to DFS sensitive information
M3 Insecure Communication	Check that communication channels are encrypted
M4 Insecure Authentication	Authentication cannot easily be bypassed
M5 Insufficient Cryptography	Check crypto algorithms used
M8 Code Tampering	Check whether it is possible to modify the code
M9 Reverse engineering	Decompile source code

What ITU needs to test DFS applications

USSD and STK Tests

- 2 SIM cards of the networks to be tested.
- Active DFS account on each SIM card.
- DFS Wallet PINs
- Prepaid mobile credit on SIM cards – SIM cards must have mobile roaming enabled for Switzerland
- Include USSD codes for each of the DFS providers.
- DFS Credit on DFS Wallets (approximately $10 to be used for testing)

Android application tests

in addition to the above requirements, Android apps (apk file) must be shared, or links to download the apps from the Play Store.

Collaboration with regulators

1. Adoption of FIGI security recommendations for telecommunications, mobile payment applications and managing risks and vulnerabilities
2. Adoption of the Security Assurance Framework and Audit Guidelines for DFS
3. Establish minimum security guidelines for the security of mobile payment applications through the adoption of FIGI's technical guidelines for the security of mobile payment applications
4. Evaluate the security of mobile payment applications used in the region.
5. Organize regional safety clinics with a focus on the implementation of FIGI security recommendations

DFS Security Lab

Get in touch

dfssecuritylab@itu.int

https://figi.itu.int/figi-resources/dfs-security-lab/

www.itu.int