ITU DFS Security Lab

Arnold Kibuuka, Project Officer, ITU

09 December 2021

FIGI Security Infrastructure & Trust Working Group

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

Security, Infrastructure & Trust Working Group 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

There is not a 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 Security Lab

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.

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

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

DFS Security Lab Objectives

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services security assurance framework

REPORT OF SECURITY WORKSTREAM

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Security testing for USSD and STK based Digital Financial Services applications

REPORT OF SECURITY WORKSTREAM

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services security audit guideline

REPORT OF SECURITY WORKSTREAM

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Security audit of various DFS applications

REPORT OF THE SECURITY WORKSTREAM

Collaborate with DFS regulators and DFS providers to implement recommendations:

- DFS Security Assurance Framework
- methodology for testing of USSD and STK based DFS applications.
- Security audit of various Android apps
- DFS Security Audit Guidelines.

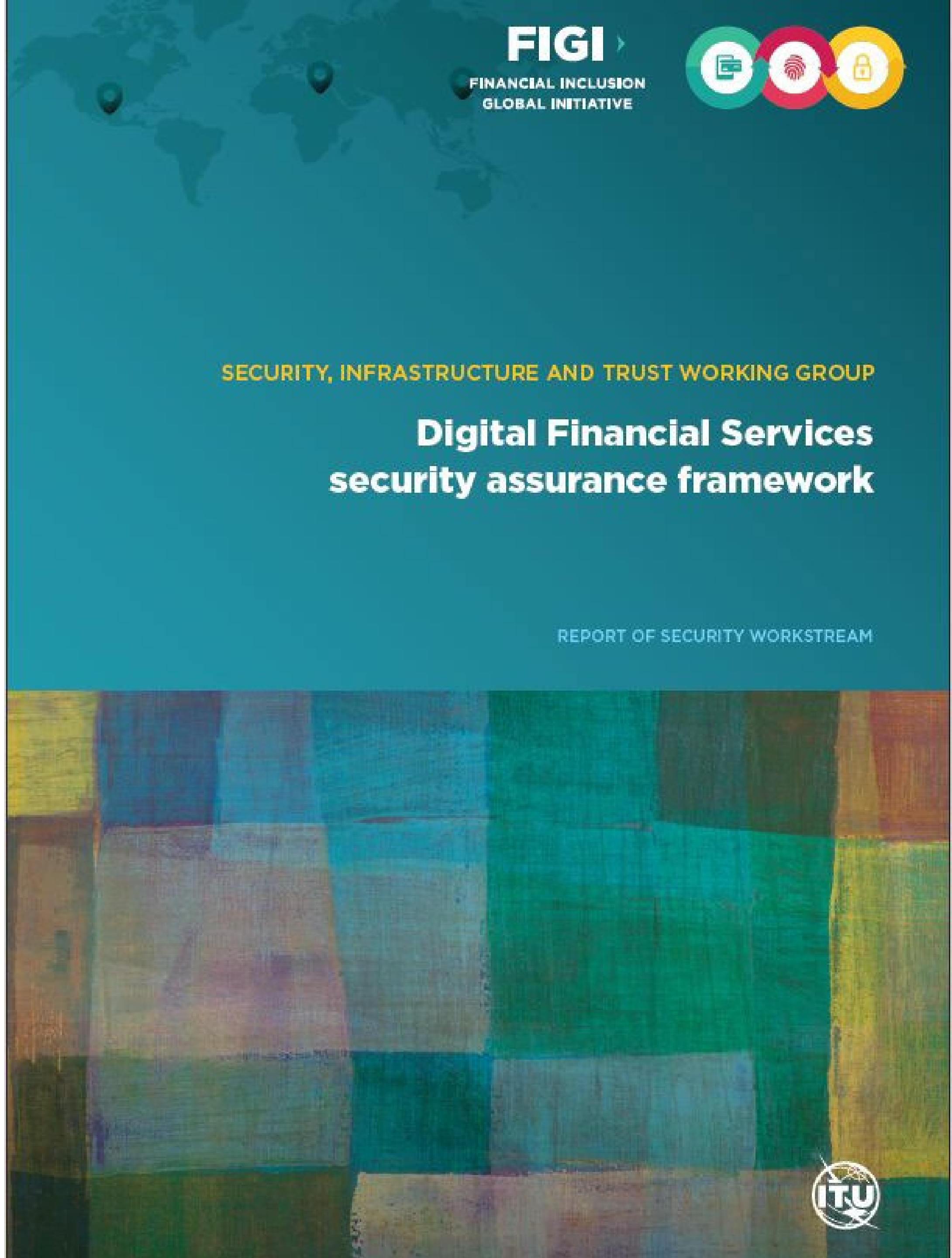
See https://figi.itu.int/figi-resources/working-groups/

DFS Security Assurance Framework

DFS ecosystem vulnerable to variety of threats due to:

- Interconnectedness of system entities
- Extended security boundaries due to reliance on numerous parties
- Mobile ecosystem itself is increasingly complex – devices, OSes

Difficult for stakeholders in DFS ecosystem to manage the interdependencies of the security threats within the DFS value chain and keep up with the new vulnerabilities and risks.



FIGI

FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services security assurance framework

REPORT OF SECURITY WORKSTREAM

ITU

Principles & Components

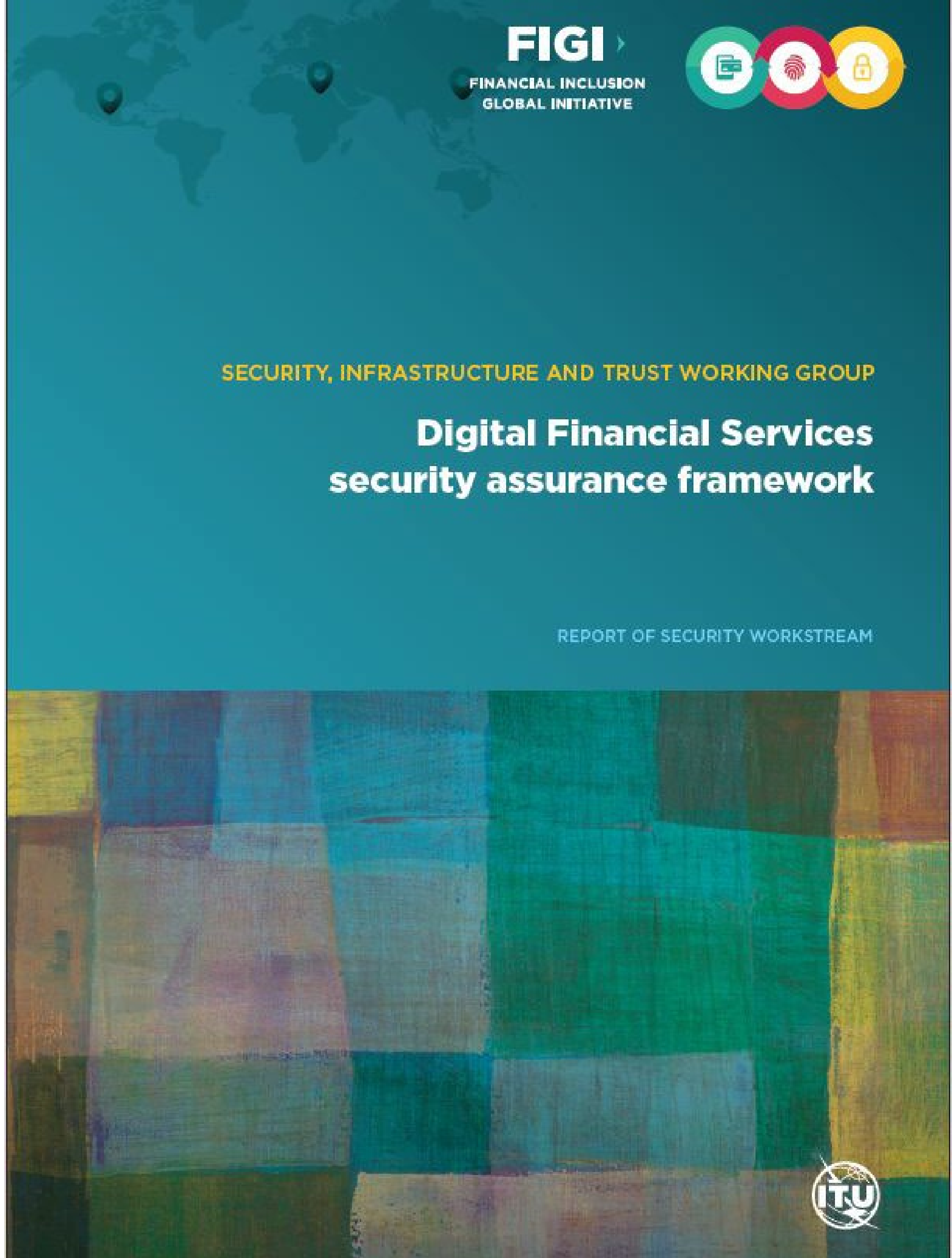
Draws on principles from several standards:

- ISO/IEC 27000 security management systems standards, PCI/DSS v3.2, NIST 800-53, OWASP top-10 vulnerabilities, GSMA application security best practices

Contains the following components:

- Assessment of threats and vulnerabilities to underlying infrastructure, DFS applications, services, network operators, third-party providers
- Identification of vulnerabilities enabling the threats
- Security control measures and the x.805 security dimension they represent (117 controls identified)
- *Mobile payment app security guideline for DFS regulators*

Living document and will evolve over time



FIGI

FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

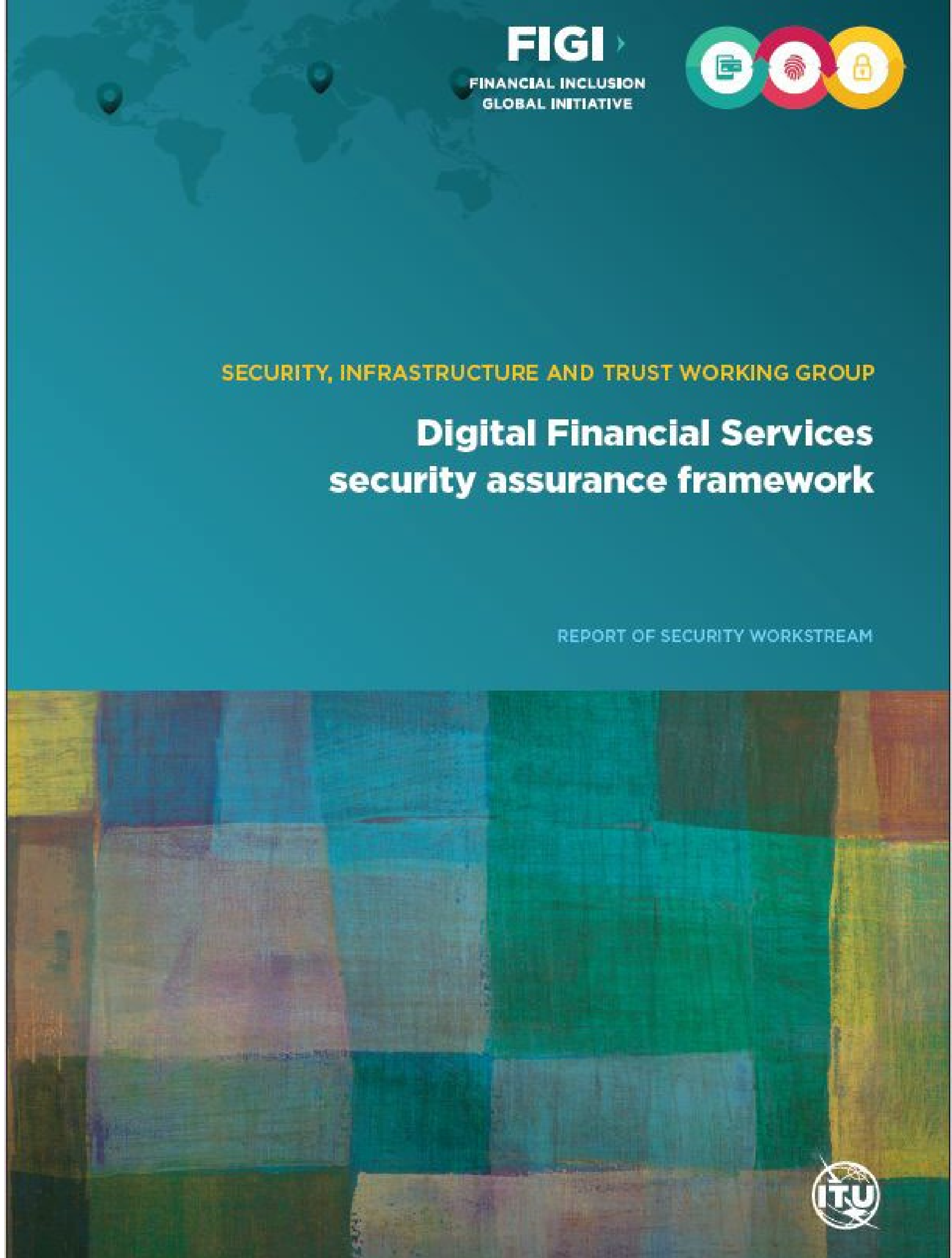
Digital Financial Services security assurance framework

REPORT OF SECURITY WORKSTREAM

ITU

Mobile Payment App Security Best Practices

- Draws upon GSMA study on mobile money best practices, ENISA smartphone security development guidelines, State Bank of Pakistan mobile payment applications security framework
- Template can be used as input to an app security policy by DFS providers to provide minimum security baselines for app developers and DFS providers as well as setting criteria for verifying compliance of apps
- Template considerations:
  1. device and application integrity.
  2. communication security and certificate handling.
  3. user authentication.
  4. secure data handling.
  5. secure application development.



FIGI
FINANCIAL INCLUSION
GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services
security assurance framework

REPORT OF SECURITY WORKSTREAM

ITU

FIGI

FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services security audit guideline

REPORT OF SECURITY WORKSTREAM

ITU

DFS Audit guideline

- Builds on the DFS security assurance framework to give guidance for auditing/assessing whether security controls are implemented.
- The purpose of the guideline is to assess whether basic controls as well as policies and procedures are in place to give some assurance on the security of DFS services.
- In the Deming cycle:- PCDA, monitor and review involves assessing and measuring security performance of DFS assets against security checklist.
- The DFS security audit questions/checklist is categorized into six different groups: *Access control, Authentication, Availability, Network security, Fraud detection , Privacy and confidentiality*

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

FIGI

FINANCIAL INCLUSION GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services security audit guideline

REPORT OF SECURITY WORKSTREAM

ITU

DFS Audit guideline

- The DFS provider needs to have a policy on please
- The DFS security audit questions/checklist is categorized into six different groups:
  - *Access control*
  - *Authentication*
  - *Availability*
  - *Network security*
  - *Fraud detection*
  - *Privacy and confidentiality*

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

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.

FIDO Developer Resources

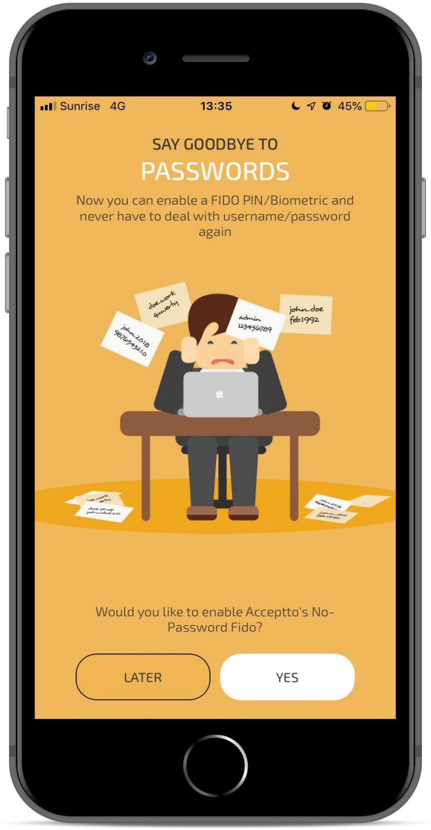
FIDO (Fast ID Online) is a set of technology-agnostic security specifications for strong authentication (passwordless authentication).

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.



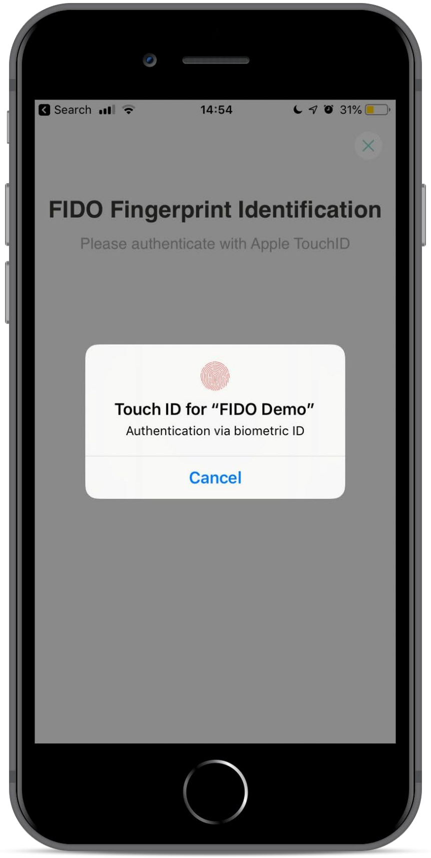
Sunrise 4G 13:35 45%

SAY GOODBYE TO
PASSWORDS

Now you can enable a FIDO PIN/Biometric and never have to deal with username/password again

Would you like to enable Acceptto's No-Password Fido?

LATER YES



Search 14:54 31%

FIDO Fingerprint Identification

Please authenticate with Apple TouchID

Touch ID for "FIDO Demo"

Authentication via biometric ID

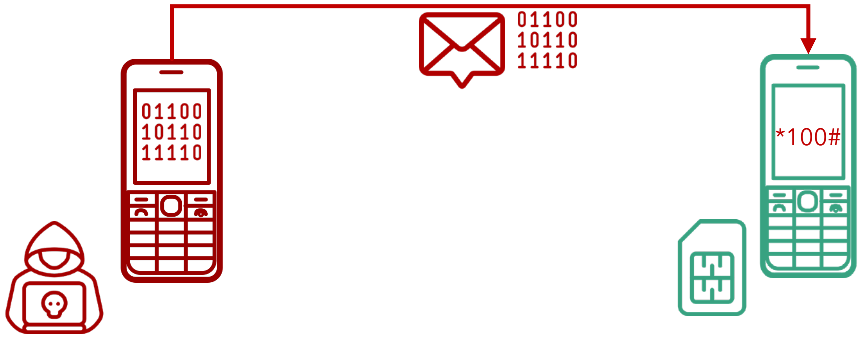
Cancel

FIDO Demo app

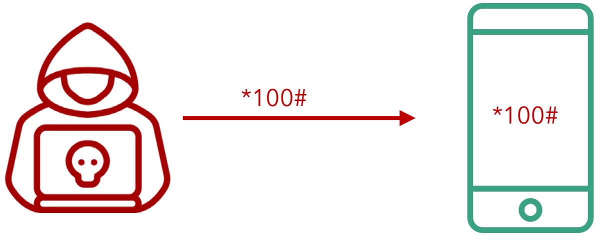
www.figi.itu.int/figi-resources/dfs-security-lab/

USSD & STK tests

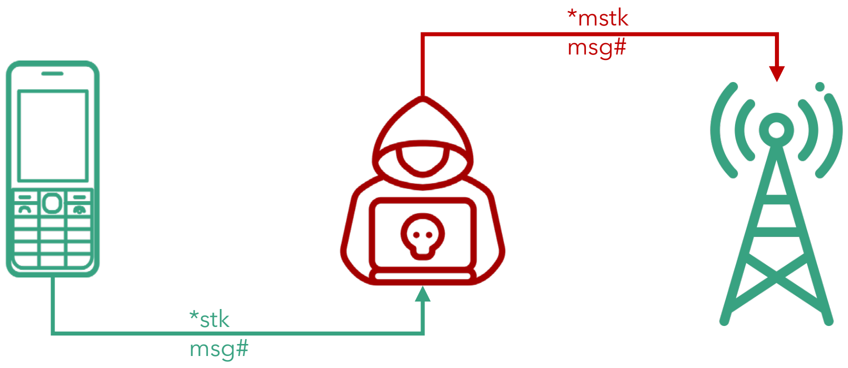
a. **SIM Swap** and **SIM cloning**



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 the Lab needs for testing DFS apps

USSD and STK tests

- 2 SIM cards for the MNO networks to be tested.
- Active DFS account on each SIM

Android app testing

- 2 accounts used for the Android app.
- Links to the Android DFS apps

Areas of collaboration with DFS Regulators and Providers

1. Implement security recommendations from FIGI
2. Adoption of DFS security assurance framework and audit guidelines
3. Establish minimum security baselines for mobile payment application security
4. Conduct mobile payment application security audit
5. Assess the cyberresilience of the DFS ecosystem
6. DFS Security Clinics on:
   a. Security assurance framework for DFS
   b. Application security threats and vulnerabilities to USSD, STK, Android.
   c. DFS telecom infrastructure vulnerabilities (SS7 vulnerabilities and mitigation measures).
   d. Knowledge transfer on setting up the DFS Security Lab.

Questions

Get in touch

dfssecuritylab@itu.int

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