ITUWebinars

Emerging technology for connectivity

Accelerating digital transformation in LDCs, LLDCs and SIDS

ITU Digital Financial Services Security Lab

Arnold Kibuuka, ITU

8 July 2021
10:00 – 11:00 AM, CEST

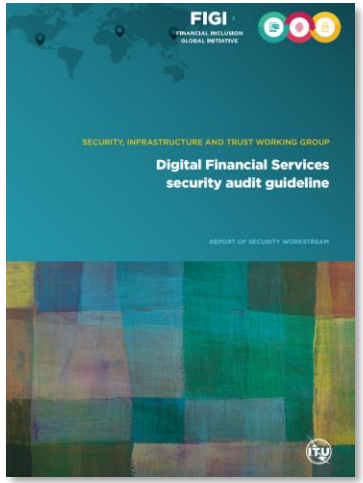
DFS Security Lab

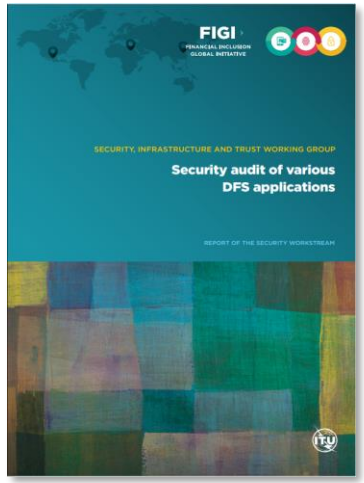
There is not a common approach for regulators, developers and DFS providers to test DFS mobile apps in a complex mobile ecosystem in order to provide/verify the level of assurance on security.

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

DFS Security Lab

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 the DFS Security Assurance Framework, methodology for testing of USSD, STK and Android apps and DFS Security Audit Guidelines.





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

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 Components

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

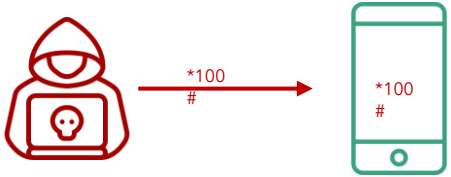
Developer resources for strong authentication using **FIDO**

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

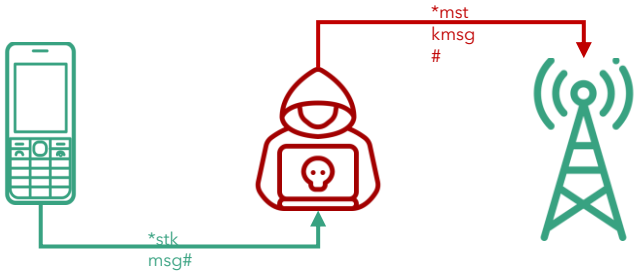
USSD & STK Security Tests

a. **SIM Swap** and **SIM clone** testing

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



c. Testing **remote USSD** execution attacks



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

Android DFS security tests
(based OWASP Mobile Top 10 Risks)

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

Get in touch

dfssecuritylab@itu.int

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

ITUWebinars

Emerging technology for connectivity

Accelerating digital transformation in LDCs, LLDCs and SIDS

5 -19 July

Mobile payment apps

Testing for vulnerabilities using the OWASP Mobile Top Ten

Philippe Oechslin, Objectif Sécurité

philippe.oechslin@objectif-securite.ch

Executive summary

- Developed method for testing DFS apps on Android
  - 18 tests organized according to OWASP mobile top ten
- Tested 3 applications
  - Payment applications
- They all have different ways of not implementing the best practices!
  - No critical issue detected

1 Introduction

- DFS: Applications used for payment and money transfer without the need of having a bank account

- OWASP: The Open Web Application Security Project
  www.owasp.org
  - A collaborative, non-for-profit foundation that works to improve the security of web applications
  - Also works on security of mobile applications

- OWASP Mobile Top Ten
  - OWASP project that aims to identify and document the top ten vulnerabilities of mobile applications

2 The tests

- Our tests are organized according to the subjects of the OWASP Mobile Top Ten:
    - M1 Improper Platform Usage
    - M2 Insecure Data Storage
    - M3 Insecure Communication
    - M4 Insecure Authentication
    - M5 Insufficient Cryptography
    - M6 *Insecure Authorization*
    - M7 *Client Code Quality*
    - M8 Code Tampering
    - M9 Reverse Engineering
    - M10 *Extraneous Functionality*
- M6, M7, M10 out of scope because they would need access to the source code or require collaboration with the editor

M1 Improper Platform Usage

The application should make correct use of the features of the platform (phone's operating system)

- Allow cloud backup,
- debugging,
- install location,
- dangerous permissions

M2 Insecure Data Storage

Data should be stored in a way that limits the risks in case of loss or compromise of the phone

- Use of external storage
- Disabling screenshots

M3 Insecure Communication

Protect against eavesdropping and manipulation of traffic

- Use of HTTPS
- Only accept trusted certificates
- Only accept a specified certificate
- App manifest should not allow clear text traffic

M4 Insecure Authentication

Prevent unauthorized access to the application

- Request pin/fingerprint before accessing sensitive information
- Inactivity timeout
- Handling of new fingerprints

M5: Insufficient Cryptography

Cryptography can only protect confidentiality and integrity of data if correctly implemented

- Do not use unsafe crypto primitives (e.g. MD5, SHA-1, RC4, DES, 3DES, Blowfish, ECB)
- Configure HTTPS according to best practices

M8: Code Tampering

Prevent an attacker from tampering the code on the telephone

- Refuse to run on a rooted device

M9 Reverse engineering

Prevent attackers from analyzing the logic of the application

- Obfuscate the code

3. Results

- Three applications have been tested with the same method
- Only failed tests are described below

3.1 App1

Payment app, backed by a bank account, credit card or prepaid

- ✗ Has permission to write to external storage external storage and, if it did, that this data is sensible.
- ✗ Uses the weak crypto (MD5 and SHA-1, ECB), probably not for critical data
- ✗ Interception of data shows names, phone numbers and amounts in clear inside HTTPS connection
- ✗ Runs on rooted devices

3.2 App2

App2 is provided by a mobile network operator that provides digital financial services in areas in which they operate across Africa

- Sends some traffic in clear text (not sensitive data)
- Does not require a PIN or fingerprint every time, PUK can be accessed
- Uses the weak crypto (SHA-1, random number generator), probably not for critical data

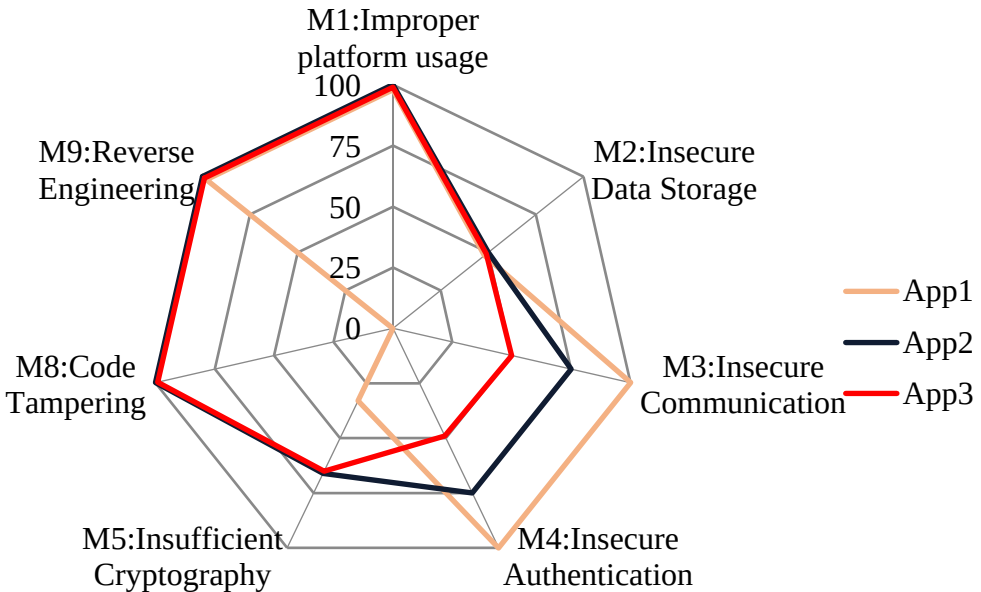
3.3 App3

App3 is also provided a mobile operator and in several countries across Africa and Asia. The app makes it possible for users to send money to contacts, pay for goods and services

- ✗ Screenshot is not disabled when running
- ✗ Trusts the certificates trusted by the phone (enables interception)
- ✗ Requires permission to send clear text traffic
- ✗ Does not require a PIN or fingerprint every time, balance can be accessed
- ✗ Uses the weak crypto (MD5, SHA-1, random number generator), probably not for critical data

Summary of results

- No critical vulnerabilities were detected but
  - App1 has no application-level encryption
  - App2 displays PUK without requiring PIN



4 Conclusions

- The tests allow an independent evaluation of the security of DFS apps
- Done locally, without access to code or server
- Detects missing best practices
- Detailed analysis of impact would require collaboration of the provider
- Provider could do more for security and transparency
  - Open source their applications
  - Offer Bug bounty programmes

ITUWebinars

Emerging technology for connectivity

Accelerating digital transformation in LDCs, LLDCs and SIDS

Blockchain and Cybersecurity challenges and opportunities for emerging economies

Blockchain for financial inclusion

By Suzana Maranhão Moreno, BNDES

8 July 2021

10:00 – 11:00 am, CEST

DLT/Blockchain

An option to generate TRUST

Relevant Factors for not having a Banking Account

1

MAJOR
Not enough money / too expensive

2

Family member already has account

Too far away

Lack of necessary documentation

Refs:
http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf
https://www.worldbank.org/content/dam/Worldbank/Research/GlobalFindex/PDF/N2Unbanked.pdf
https://www-forbes-com.cdn.ampproject.org/c/s/www.forbes.com/sites/yayafanusie/2021/01/01/stop-saying-you-want-to-bank-the-unbanked/amp/

1 Can DLT help to make financial services cheaper?

Digitalization many times leads to more affordable services. DLT is a technology to that, enabling some new possibilities and permissionless innovation.

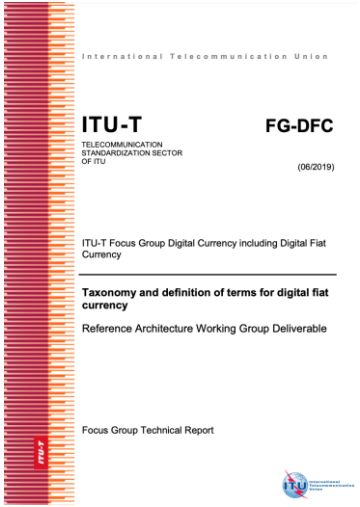
Payments

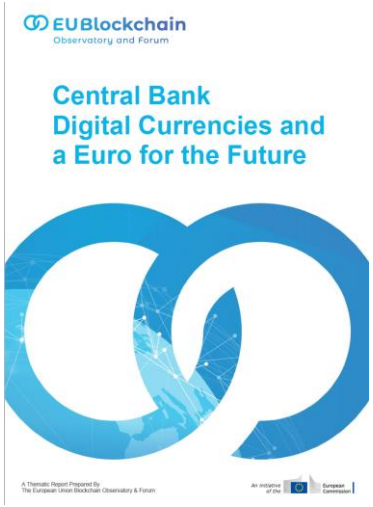
Remittance

Stablecoin

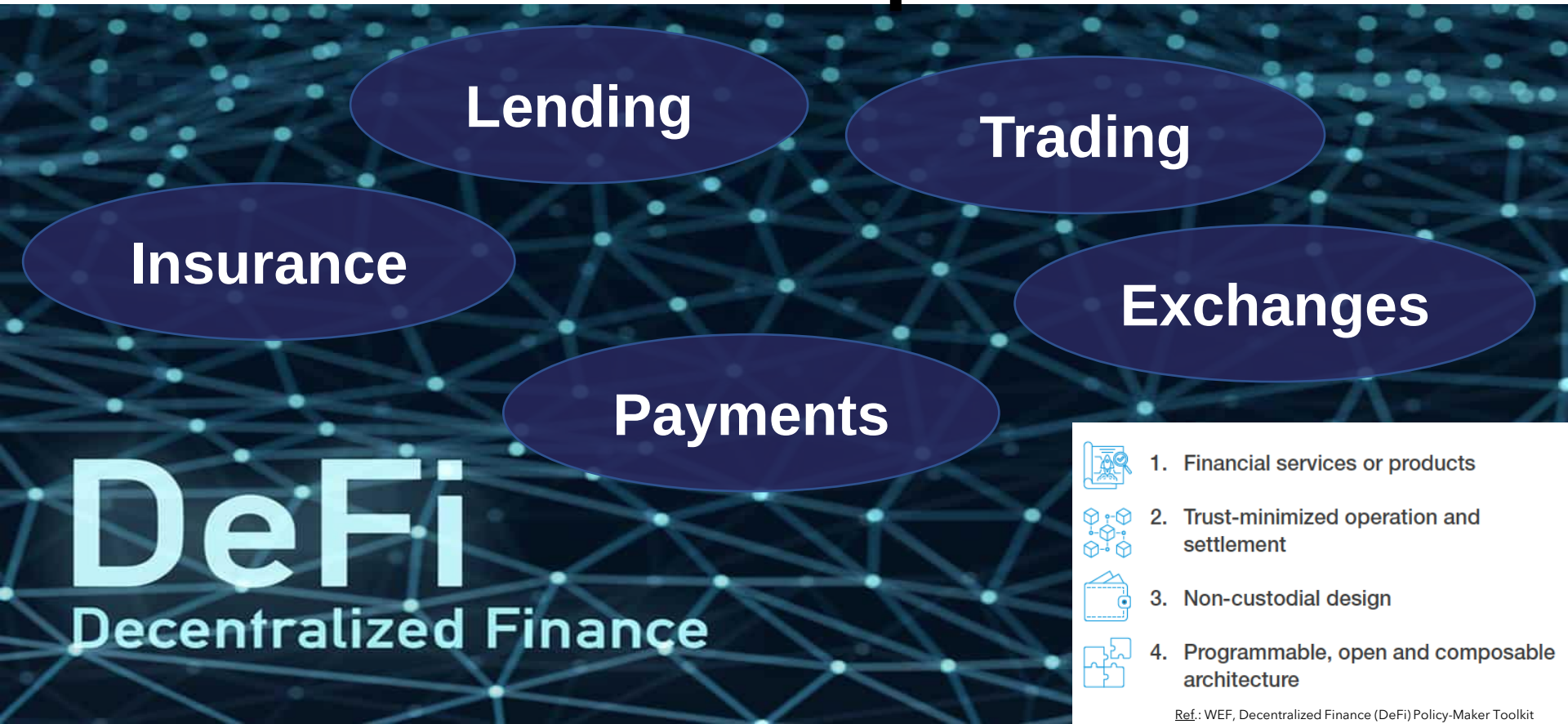
CBDC

DeFi





1 Can DLT help to make financial services cheaper?



1. Financial services or products
2. Trust-minimized operation and settlement
3. Non-custodial design
4. Programmable, open and composable architecture

Ref.: WEF, Decentralized Finance (DeFi) Policy-Maker Toolkit

1 Can DLT increase aid to vulnerable people?

Technology may help to increase the trust and transparency of social projects, leaded by private or public sector.

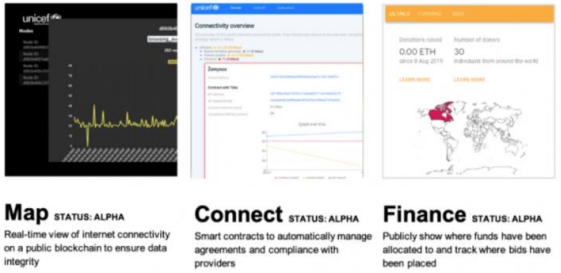
follow the money

hyper-transparency

compliance by design

programmable money

giga | unicef for every child | ITU



From Hyperledger Global Forum:

Transparency -> Accountability -> Empathy -> Action

1 Can DLT help to create market opportunities to vulnerable people?

Technology may enable new business models, data ownership and new relationships based on trust.

Farmers with data ownership in supply chain

Recycling activities more transparent and valuable

Relevant Factors for not having a Banking Account

1

MAJOR
Not enough money / too expensive

2

Family member already has account

Too far away

Lack of necessary documentation

Refs:
http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf
https://www.worldbank.org/content/dam/Worldbank/Research/GlobalFindex/PDF/N2Unbanked.pdf
https://www-forbes-com.cdn.ampproject.org/c/s/www.forbes.com/sites/yayafanusie/2021/01/01/stop-saying-you-want-to-bank-the-unbanked/amp/

2 Can DLT help to deal with the lack of documentation?

DID, VC, SSI

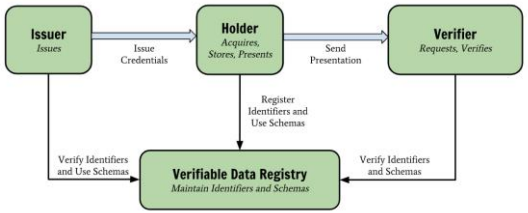


Figure 1 The roles and information flows forming the basis for this specification.

Id + verifiable credit history

kiva protocol

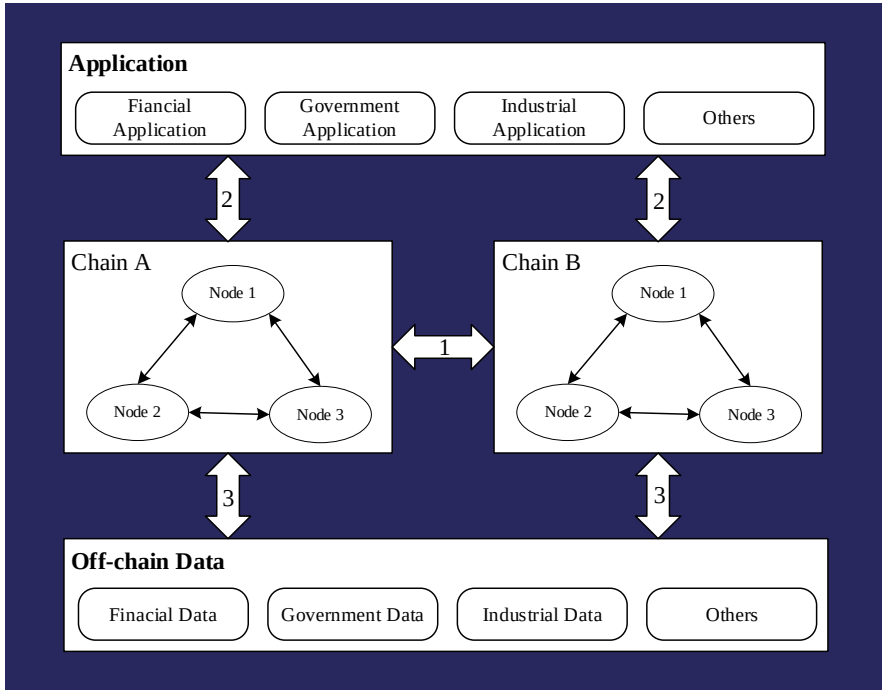
Web of Certifiers – open ecosystem of certifiers and conditions

WEB OF CERTIFIERS

DEFI FOR GOOD

Refs:
https://www.w3.org/TR/did-core/
https://www.w3.org/TR/vc-data-model/
https://www.kiva.org/
https://www.igi-global.com/chapter/a-survey-of-kycaml-for-cryptocurrencies-transactions/261722
https://www.defi-for-good.com/

ITU-T DLT Technical Interoperability Framework



Refs:
ITU DLT Meet-ups - https://www.itu.int/en/ITU-T/webinars/Pages/dlt.aspx (see first episode)
SG16/Q22 H.DLT-TFI - Technical Framework for distributed ledger technology (DLT) Interoperability

Lacchain and Brazilian Blockchain Network

111
#Nodes

LACCHAIN

15
#Countries

58
#Entities with Nodes

Focus on Inclusion
https://www.lacchain.net/

Foster innovation for public interest applications, with special emphasis on enabling trust for anti-fraud and pro-transparency measures.
(aligned with Brazilian Digital Government Strategy 2020-2022)

GOVERNANCE

NETWORK

SERVICES

ITUWebinars

Emerging technology for connectivity

Accelerating digital transformation in LDCs, LLDCs and SIDS

5 -19 July

By Suzana Maranhão Moreno, BNDES
suzana@bndes.gov.br