FIGI Security Clinic

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

DFS Security Assurance Framework

Vijay Mauree & Kevin Butler

4-5 December 2019
#financialinclusion

Sponsored by

BILL & MELINDA GATES foundation

Organized by

Committee on Payments and Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

Motivation

- Digital technology has spurred financial access to millions
  - 55% of account owners in high-income economies and 30% of account owners in developing world economies have made at least one direct payment using a mobile money account, a mobile phone, or the Internet
- The digital financial services (DFS) ecosystem is uniquely vulnerable to a variety of security threats
  - Interconnectedness of system entities
  - Extended security boundaries due to reliance on numerous parties
  - Mobile ecosystem itself is increasingly complex – devices, OSes
- Questions:
  - What are the security threats and control measures (mitigations) for stakeholders within the DFS ecosystem?
  - Main focus - Telecom infrastructure, application and device Security

Goals

- The DFS Security Assurance Framework aims to bridge the knowledge gap and recommends a structured methodology for risk management
- Main goals
  - Enhance customer trust and confidence in DFS
  - Clarify roles and responsibilities for each stakeholder in the ecosystem
  - Identify security threats and vulnerabilities within the ecosystem
  - Establish security controls to provide end-to-end security
  - Strengthen management practices with respect to security risk management in a manner that is inclusive to all shareholders

Intended Audience

- The security assurance framework provides an overview of security threats and vulnerabilities facing DFS service providers
  - **Banks and non-banks providing mobile money services**
  - **Mobile network operators**
  - Customers
  - Payment system providers
  - Merchants
  - **Technology services/third party providers**
- Regulators (telecom authorities, banking and payments regulators) can use the framework for establishing security baselines for DFS providers

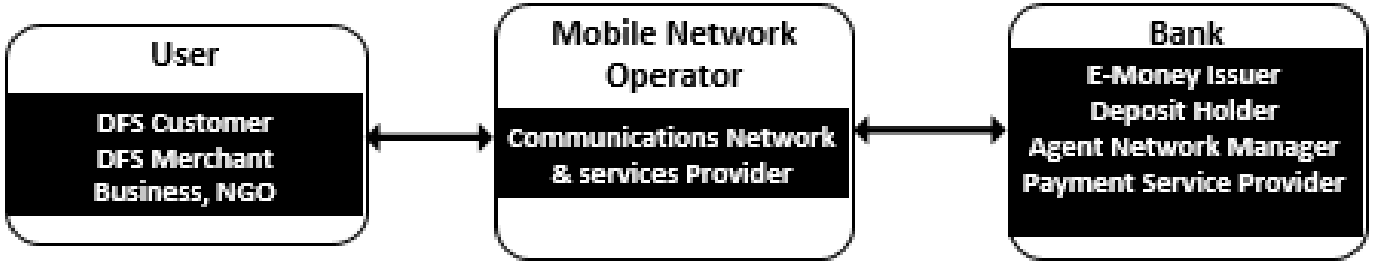
Introductory Concepts

- **Vulnerability:** a weakness in a system that can be exploited by an adversary
- **Threat:** the specific means by which a vulnerability is exploited
- **Risk:** the consequences of a threat being successfully deployed

- ITU-T Recommendation X.805 provides a foundation for the document, with eight *security dimensions* to address security:
  - Access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability, privacy

DFS Provider Business Models

- **Bank-led:** bank performs key financial roles and leverages a mobile network operator for communication with users



User

DFS Customer
DFS Merchant
Business, NGO

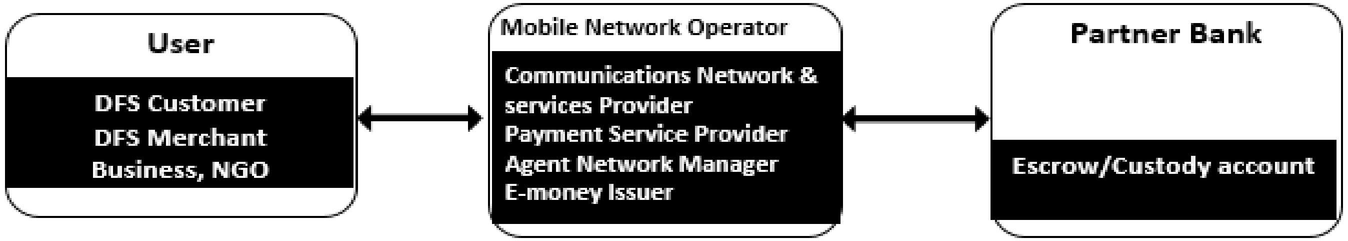
Mobile Network Operator

Communications Network & services Provider

Bank

E-Money Issuer
Deposit Holder
Agent Network Manager
Payment Service Provider

- **MNO-led:** MNO not only provides communication but also the bulk of financial roles, manages DFS agent network



User

DFS Customer
DFS Merchant
Business, NGO

Mobile Network Operator

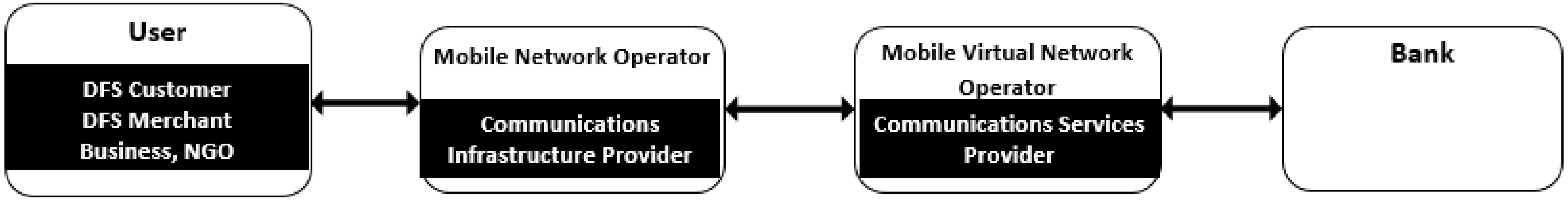
Communications Network & services Provider
Payment Service Provider
Agent Network Manager
E-money Issuer

Partner Bank

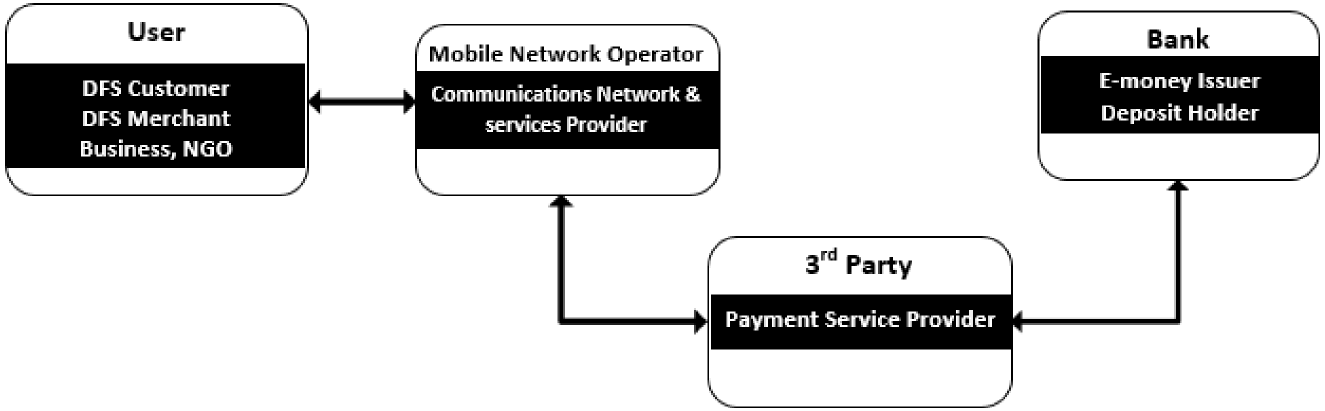
Escrow/Custody account

DFS Provider Business Models (2)

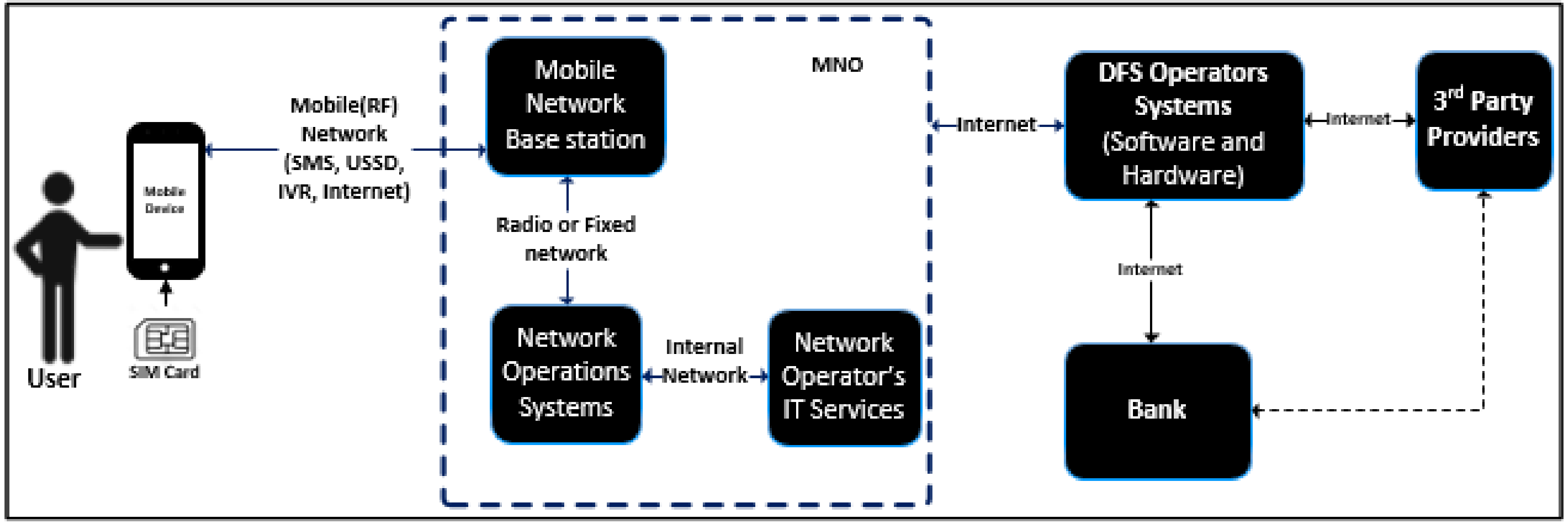
- **MVNO-led:** MVNO provides telecommunication services using MNO infrastructure, DFS provided with a bank or independently


User
DFS Customer
DFS Merchant
Business, NGO
Mobile Network Operator
Communications Infrastructure Provider
Mobile Virtual Network Operator
Communications Services Provider
Bank

- Hybrid: Critical roles are shared between bank and MNO, third parties provide additional services (e.g., PSP, agent network)

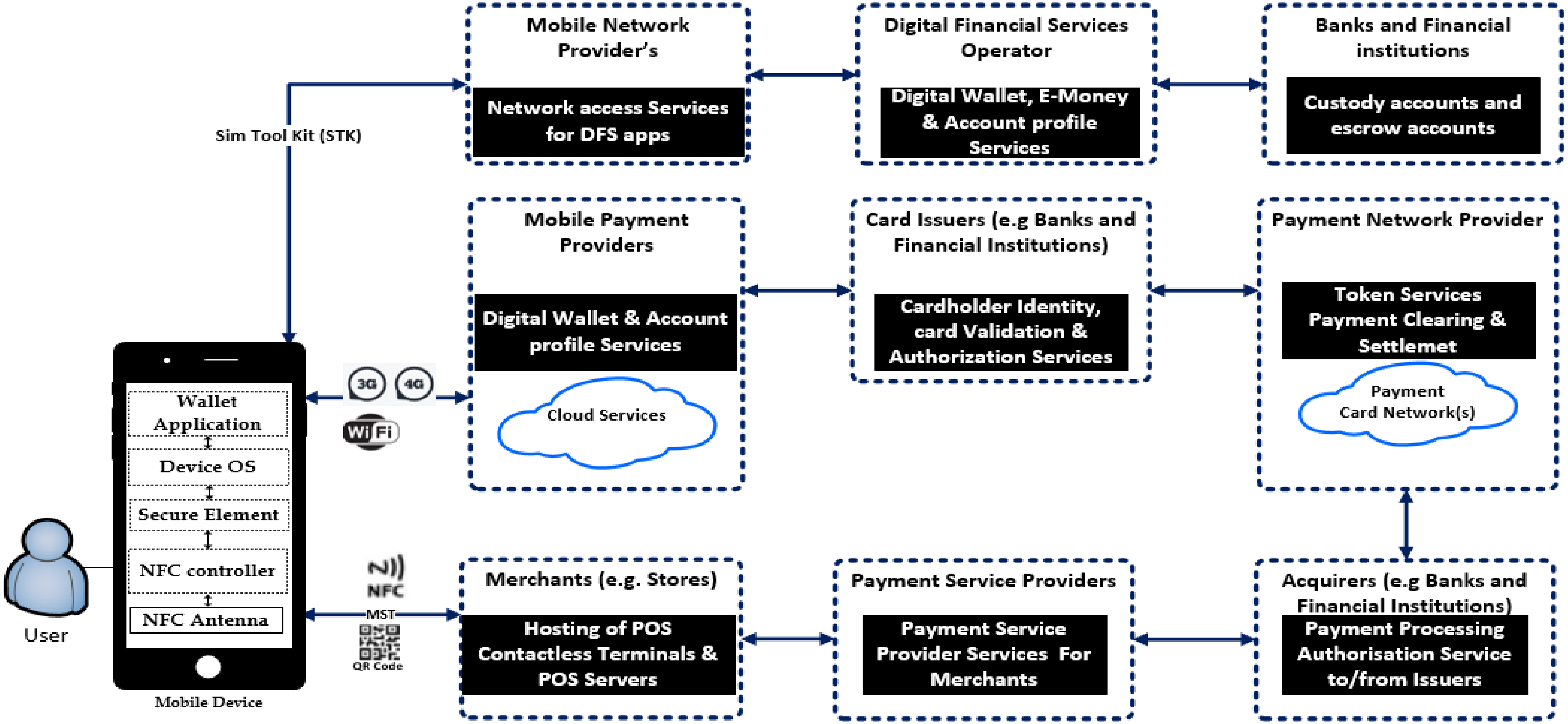


Elements of DFS Ecosystem


User
Mobile Device
SIM Card
Mobile(RF) Network (SMS, USSD, IVR, Internet)
MNO
Mobile Network Base station
Radio or Fixed network
Network Operations Systems
Internal Network
Network Operator's IT Services
Internet
DFS Operators Systems (Software and Hardware)
Internet
3rd Party Providers
Internet
Bank

- **User** is target audience for DFS, uses mobile money application on a mobile device to access the DFS ecosystem
- **MNO** provides communication infrastructure from wireless link through the provider network
- **DFS provider** handles application component, interfaces with payment systems and third-party providers

Digital Wallet DFS Ecosystem



Mobile Network Provider's

Network access Services for DFS apps

Digital Financial Services Operator

Digital Wallet, E-Money & Account profile Services

Banks and Financial institutions

Custody accounts and escrow accounts

Sim Tool Kit (STK)

Mobile Payment Providers

Digital Wallet & Account profile Services

Cloud Services

Card Issuers (e.g Banks and Financial Institutions)

Cardholder Identity, card Validation & Authorization Services

Payment Network Provider

Token Services Payment Clearing & Settlemet

Payment Card Network(s)

3G

4G

WiFi

Wallet Application

Device OS

Secure Element

NFC controller

NFC Antenna

Mobile Device

User

NFC

MST

QR Code

Merchants (e.g. Stores)

Hosting of POS Contactless Terminals & POS Servers

Payment Service Providers

Payment Service Provider Services For Merchants

Acquirers (e.g Banks and Financial Institutions)

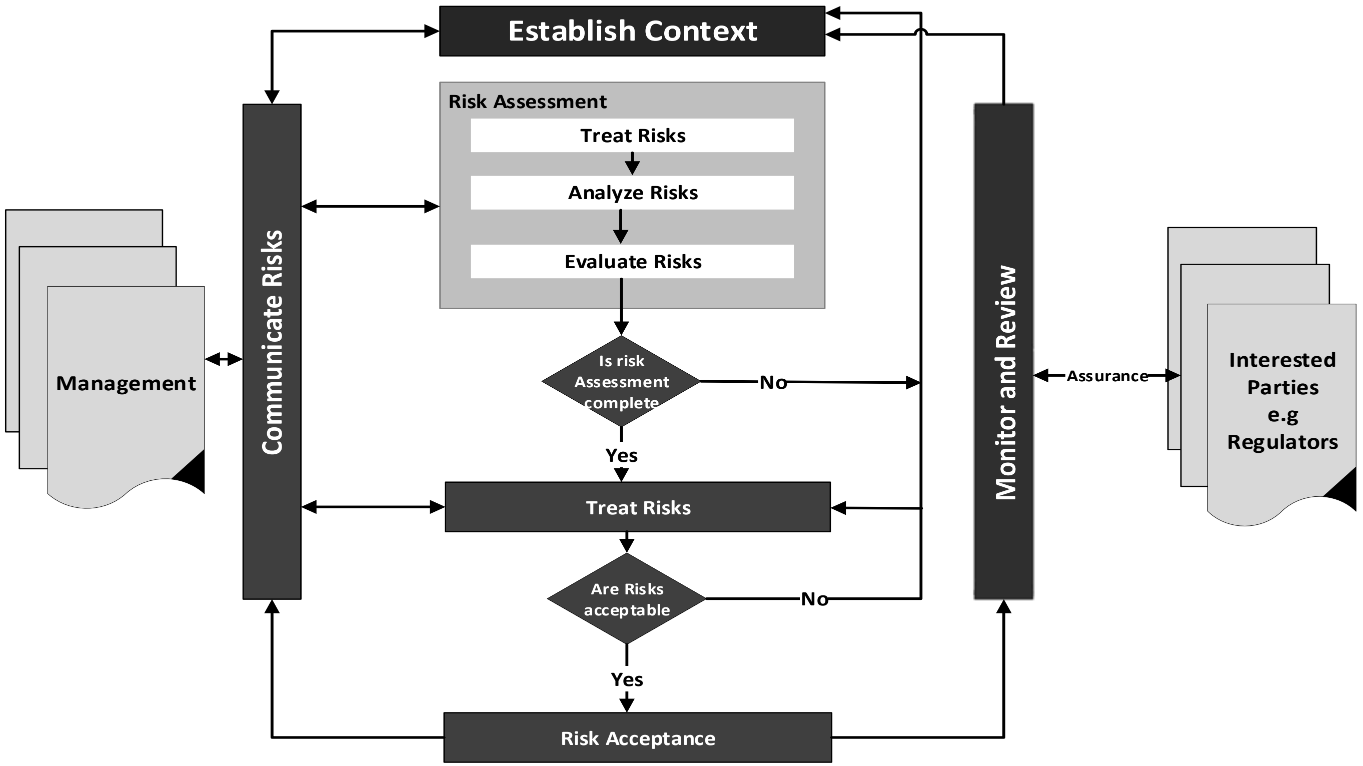
Payment Processing Authorisation Service to/from Issuers

Adopted from ENISAWP2016

Components of the Framework

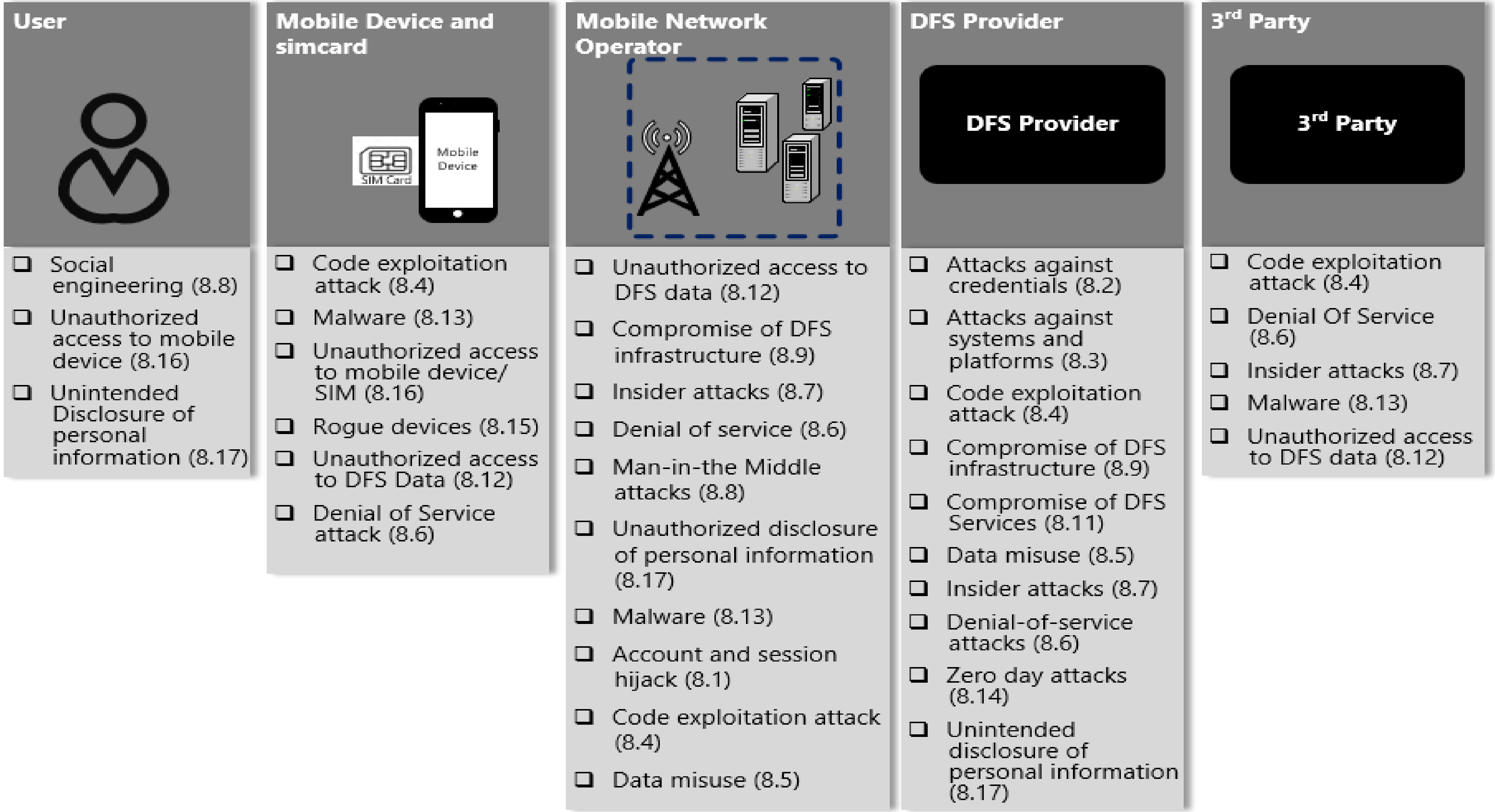
- Draws on principles from ISO/IEC 27000 security management systems standards, PCI/DSS v3.2, PA-DSS, NIST 800-53, CIS controls version 7, OWASP top-10 vulnerabilities, GSMA application security best practices
- Contains the following components:
  - A security risk management methodology based on ISO/IEC 27005 – (Section 7 of the report).
  - Assessment of threats and vulnerabilities to the underlying infrastructure of the mobile network operator and DFS provider, DFS applications, services, network operations and third-party providers involved in the ecosystem for DFS delivery.
  - Security control measures for the threats and vulnerabilities - 117 security controls measures are outlined in Section 8 of the report.

Risk Assessment Methodology



- Based on Deming cycle of Plan, Do, Check, Act (PDCA) phases
- Monitoring and review depend on the stakeholder
  - E.g., regulator reviewing controls, audits by providers
- Context necessary for effective risk assessment/evaluation/analysis

Summary: DFS Ecosystem Threats



User

- □ Social engineering (8.8)
- □ Unauthorized access to mobile device (8.16)
- □ Unintended Disclosure of personal information (8.17)

Mobile Device and simcard

- □ Code exploitation attack (8.4)
- □ Malware (8.13)
- □ Unauthorized access to mobile device/ SIM (8.16)
- □ Rogue devices (8.15)
- □ Unauthorized access to DFS Data (8.12)
- □ Denial of Service attack (8.6)

Mobile Network Operator

- □ Unauthorized access to DFS data (8.12)
- □ Compromise of DFS infrastructure (8.9)
- □ Insider attacks (8.7)
- □ Denial of service (8.6)
- □ Man-in-the Middle attacks (8.8)
- □ Unauthorized disclosure of personal information (8.17)
- □ Malware (8.13)
- □ Account and session hijack (8.1)
- □ Code exploitation attack (8.4)
- □ Data misuse (8.5)

DFS Provider

- □ Attacks against credentials (8.2)
- □ Attacks against systems and platforms (8.3)
- □ Code exploitation attack (8.4)
- □ Compromise of DFS infrastructure (8.9)
- □ Compromise of DFS Services (8.11)
- □ Data misuse (8.5)
- □ Insider attacks (8.7)
- □ Denial-of-service attacks (8.6)
- □ Zero day attacks (8.14)
- □ Unintended disclosure of personal information (8.17)

3rd Party

- □ Code exploitation attack (8.4)
- □ Denial Of Service (8.6)
- □ Insider attacks (8.7)
- □ Malware (8.13)
- □ Unauthorized access to DFS data (8.12)

Threats Based on Apps/Digital Wallets

- **Mobile payment application/device:** similar to previous slide
- **Merchant:** OS malware, QR code compromise, MITM attacks against POS terminals, relay attacks
- **Acquirers:** payment system compromise, network and system infrastructure compromise
- **Payment Service Provider:** payment gateway compromise, software vulnerabilities in POS terminals, network compromise, design/implementation flaws in POS systems and gateways
- **Issuer:** payment processing system compromise, network and infrastructure compromise
- For framework, we consider merchants, acquirers, payment service providers, issuers to be third-party providers: other FIGI work covers mitigations for these entities

Threat: Denial of Service Attacks

- DoS as an example of the standardized threats we consider (Section 8.7 in the Security Assurance Framework document)
- Characterized as attacks designed to prevent services within the DFS ecosystem from being offered
- Affected entities: MNO, DFS provider

Threat: Denial of Service Attacks (2)

- ***Risks*** at the **MNO:**
  - Inability to perform transaction due to a service outage
  - Transaction failure due to high delays
- ***Vulnerability:***
  - Network failure due to insufficient network capacity or to maintenance or design (*security dimension:* availability)
- ***Controls:***
  - **C22:** The mobile network operator should take steps to ensure network high network availability to allow access to DFS services through USSD, SMS and Internet.
  - **C23:** The MNO should perform technical capacity tests simulating different transactions based on customer numbers, expected growth, expected number of transactions and expected peak periods to ensure continued system performance.

Threat: Denial of Service Attacks (3)

- ***Risks*** at the **DFS Provider:**
  - Inability to perform transaction due to a service outage
  - Transaction failure due to high delays
  - Unauthorized access to user data
- ***Vulnerabilities:***
  - Network failure due to insufficient network capacity or to maintenance or design (*SD:* availability)
  - Lack of monitoring of network traffic and individual network packets (*SD:* availability, communication security)
  - Enabling unnecessary services (*SD:* data confidentiality)

Threat: Denial of Service Attacks (3)

- ***Controls:***
  - **C24:** The DFS provider should protect against network attacks by use of firewalls and traffic filters, and protect against DFS infrastructure threats by challenging suspicious traffic through network admission techniques and mechanisms such as CAPTCHAs.
  - **C25:** Inbound internet traffic should be limited and continuously monitored.
  - **C26:** Set restrictive firewall rules by default, use ports whitelisting, use packet filters, and continuously monitor access to whitelisted/permitted ports and IP's.

Template for Application Security Best Practices

- General best practices for a mobile money smartphone application security framework
- 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
- Considerations: device and application integrity, communication security and certificate handling, user authentication, secure data handling, secure application development
- More details in tomorrow’s session

Summary

- Security Assurance Framework is designed to provide guidance to stakeholders within the DFS ecosystem
- Not designed to be static: is a living document where security advice will evolve as new access technologies, vulnerabilities, and threats are discovered
- Culmination of a year and a half long effort to characterize threats

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

Thank You