DFS Security Assurance Framework

Arnold Kibuuka, Project Officer, ITU

http://www.itu.int/go/dfssl

January 2025

Outline

1. DFS Security Assurance Framework
2. DFS Business Models
3. DFS Ecosystem Elements
4. Security Risk Management Process
5. Threats, Vulnerabilities & Security Controls
6. Mobile Payment App Security Best Practices
7. Summary

DFS Security Assurance Framework

- DFS ecosystem vulnerable to variety of threats:
  - 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.


ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation
ITU-T X.1150 (03/2024)

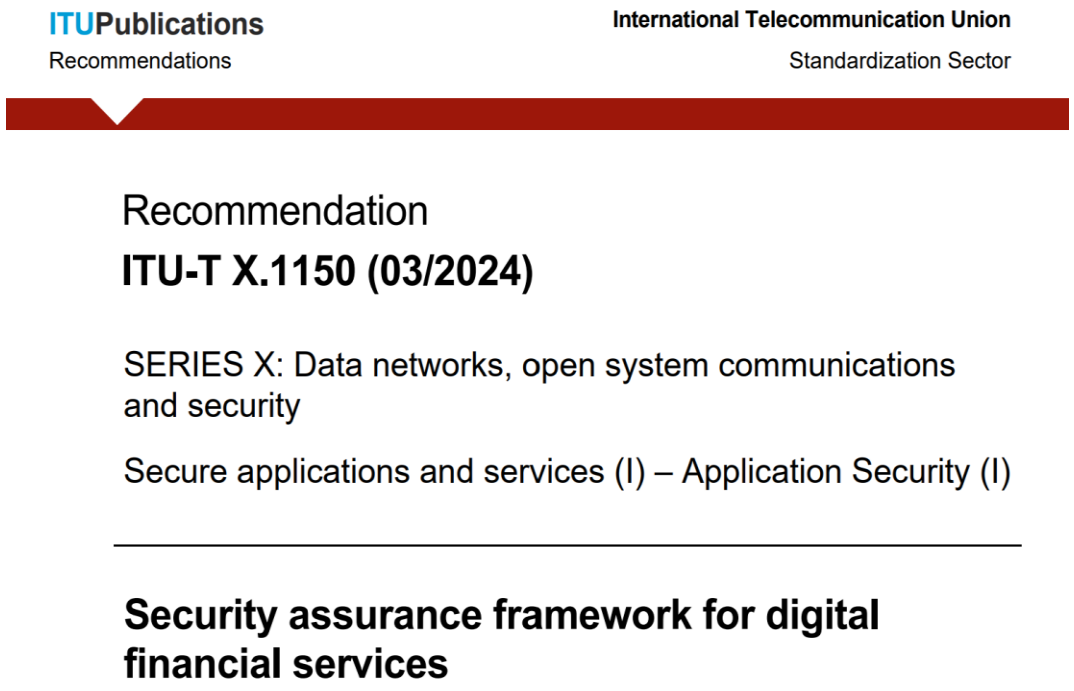
SERIES X: Data networks, open system communications and security

Secure applications and services (I) – Application Security (I)

Security assurance framework for digital financial services

DFS Security Assurance Framework

- 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:
  - Security risk assessment based on ISO/IEC 27005
  - Identifies common threats and vulnerabilities to underlying infrastructure, DFS applications, services, network operators, third-party providers
  - Security control measures and the x.805 security dimension they represent (117 controls identified)
  - Mobile application security best practices for DFS applications
  - The Security assurance is an international standard: Rec. ITU-T X.1150


ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation
ITU-T X.1150 (03/2024)

SERIES X: Data networks, open system communications and security

Secure applications and services (I) – Application Security (I)

Security assurance framework for digital financial services

How can the DFS security assurance and audit guidelines can be used?

- Identify security threats and vulnerabilities within the ecosystem
- Define security controls to mitigate the risks
- Strengthen security risk management.
- The **audit guideline** is for DFS regulators & providers to assess whether DFS controls in place

http://www.itu.int/go/dfssl

Introductory Concepts

ITU-T Rec. X.805

ITU-T Recommendation X.805 provides a foundation for the document, with eight security dimensions to address security:

1. access control,
2. authentication,
3. non-repudiation,
4. data confidentiality,
5. communication security,
6. data integrity,
7. availability,
8. privacy

Vulnerability

A weakness in a system that can be exploited by an adversary/hacker

Threat

the specific means by which a vulnerability is exploited

Risk

the consequences of a threat being successfully deployed

Control

A *safeguard* or *countermeasure* prescribed to *protect* the **confidentiality**, **integrity**, and **availability** of information systems and assets to meet a set of defined security requirements.

DFS Business Models

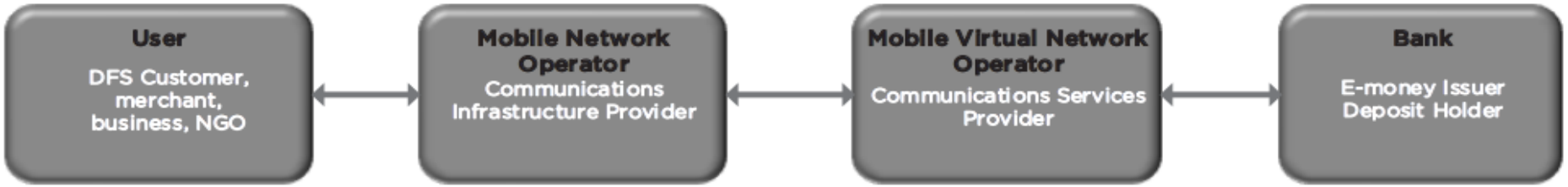
Bank Led

Bank performs key financial roles and leverages a mobile network operator for communication with users

MNO Led

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

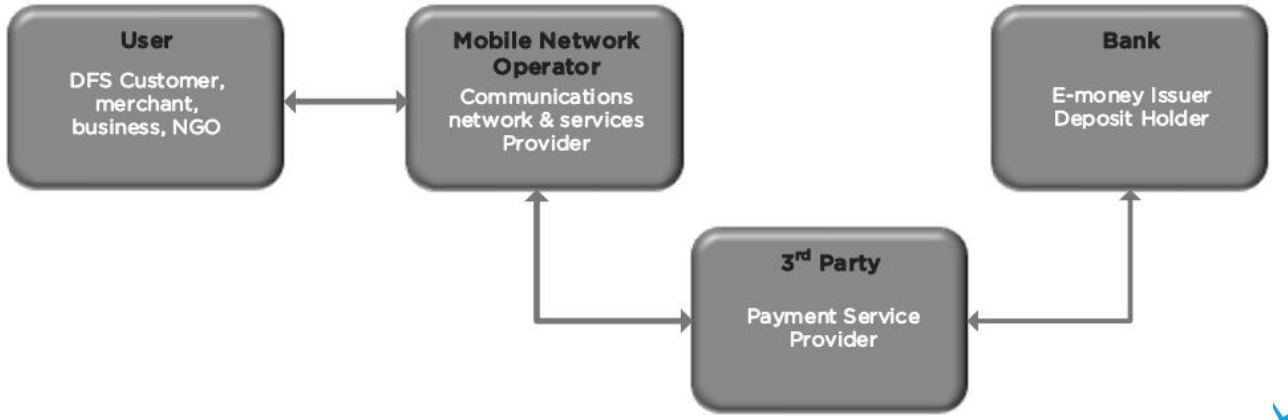
MVNO Led



MVNO provides telecommunication services using MNO infrastructure, DFS provided with a bank or independently

Hybrid

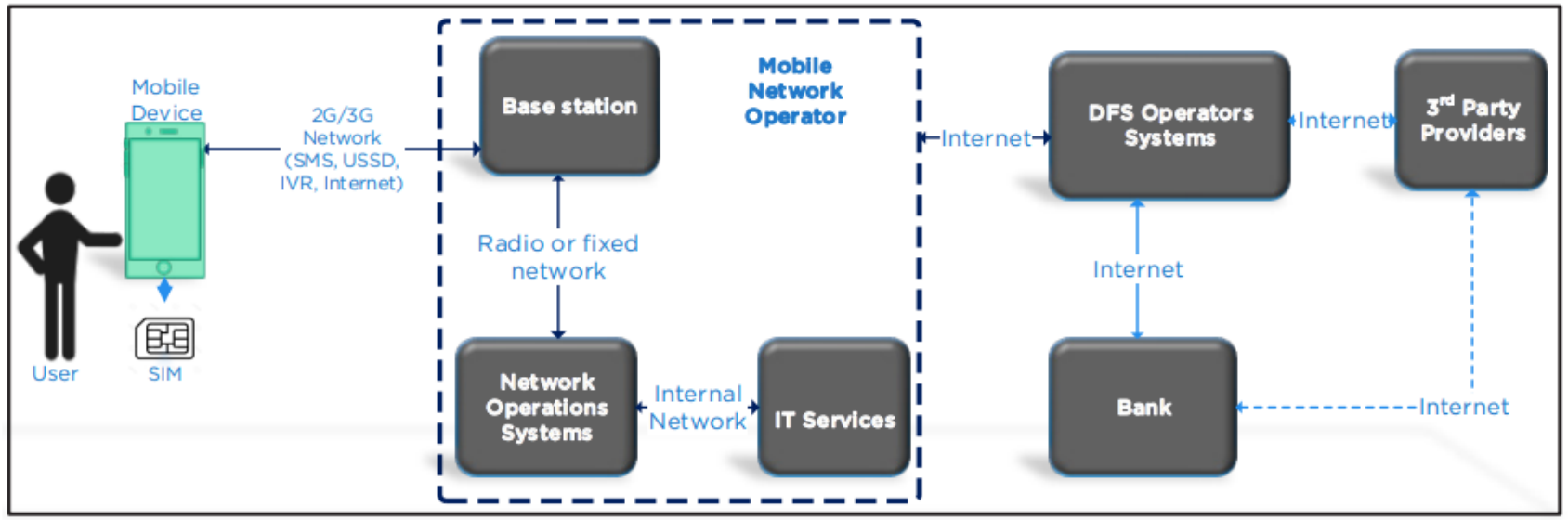
Critical roles are shared between bank and MNO, third parties provide additional services (e.g., PSP, agent network)



Which of these is the most common business model in your country?

DFS Ecosystem Elements

Elements of a DFS Ecosystem



User

is target audience for DFS, uses mobile money application on a mobile device to access the DFS ecosystem

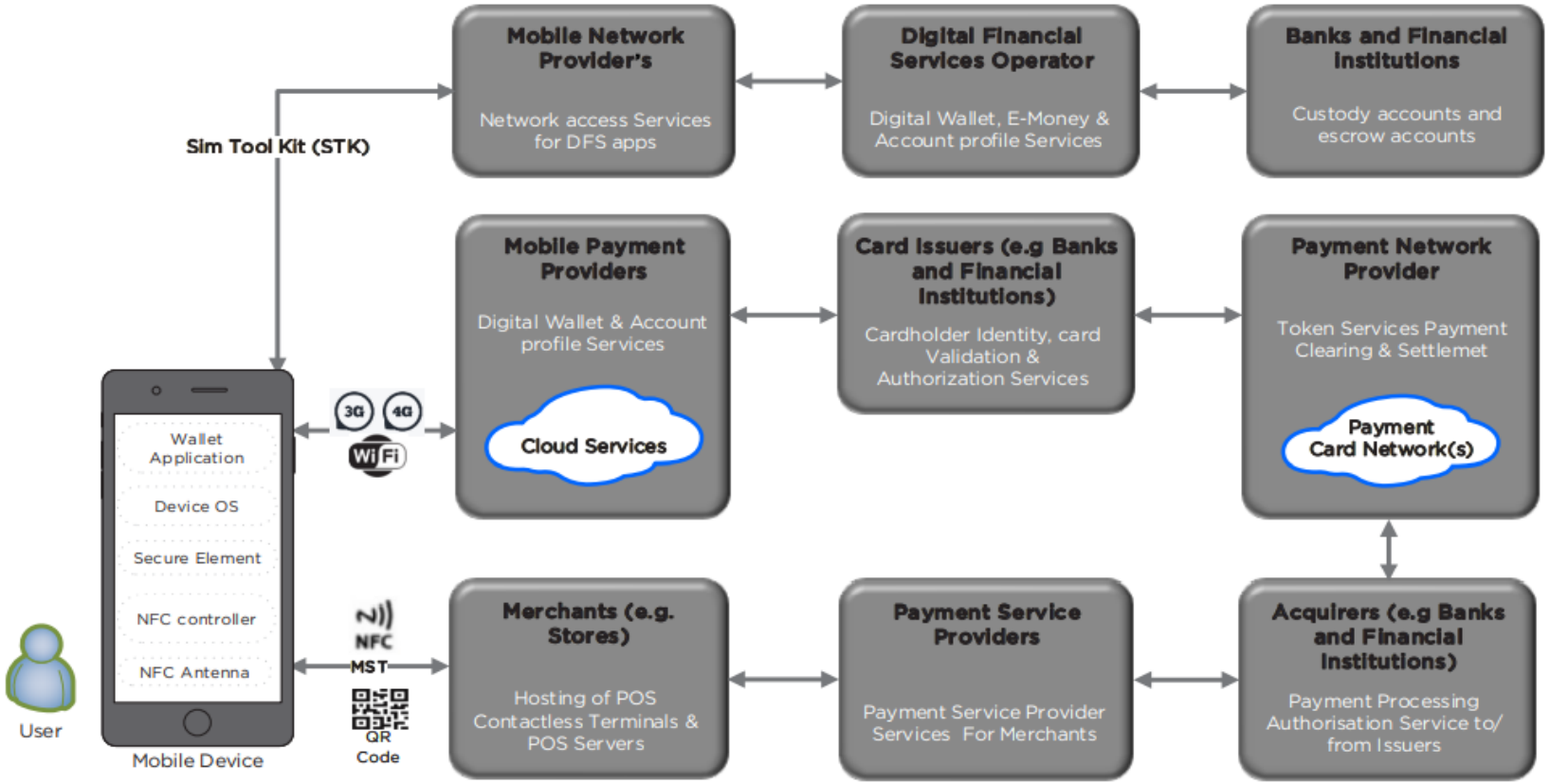
MNO

provides communication infrastructure from wireless link through the provider network

DFS Provider

application component, interfaces with payment systems and third-party providers.

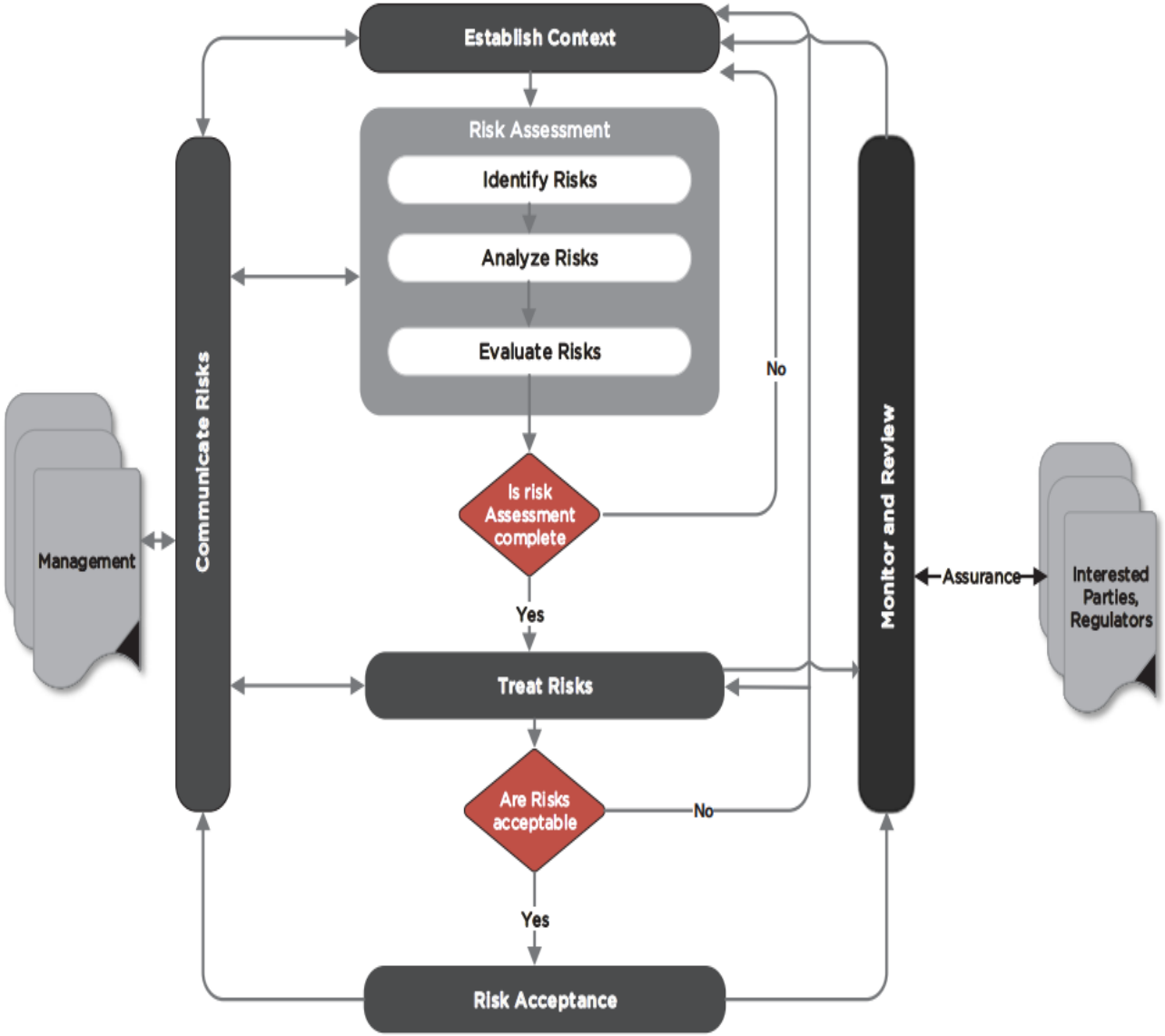
Digital Wallet DFS Ecosystem



Security Risk Management Process

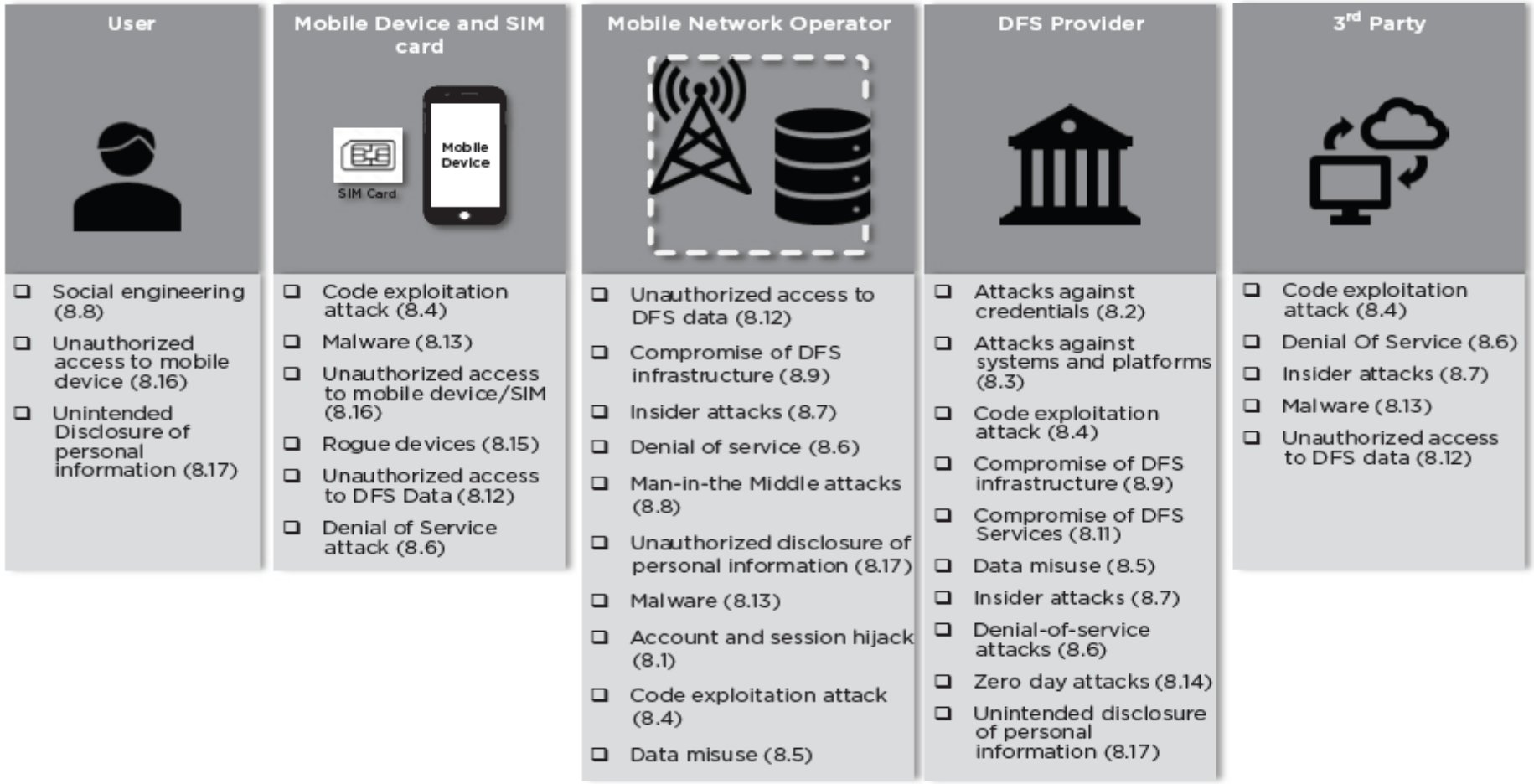
Risk Assessment Methodology

- Based on Deming cycle of Plan, Do, Check, Act (PDCA) phases of the ISO 27001 – information security management
- Monitoring and review depend on the stakeholder (e.g., regulator reviewing controls, internal audits or new service)
- Context with inputs from Senior Management necessary for effective risk assessment/evaluation/analysis
- **Information Security Management System** based on ISO 27001 describing the risk treatment plans and security controls implemented for each threat and vulnerability is the main output of this phase



Threats, Vulnerabilities and Security Controls

DFS Ecosystem Threats



Example 1: Threat 8.1 Account and Session Hijacking

Source: DFS security assurance framework

13.8 Threat: Man-in-the-middle and social engineering attacks

These two types of attacks are grouped together because they both involve an adversary actively interposing themselves into communication or interaction (e.g., between a user and device or MNO, or a communication interposition between parties). Table 9 summarizes the risks and vulnerabilities and controls for mobile users, MNO, DFS providers and third-party providers.

Table 9 – Summary of risks and vulnerabilities and controls for mobile user, MNO, DFS providers and third-party providers

Affected entity	Risks and vulnerabilities	Controls requirements
Mobile user	The risk of ***data exposure and modification*** is due to the following vulnerabilities:	
	– Unverified and unsigned applications (SD: privacy, data integrity)	**C35**: Critical focus should be on guiding the customer to access and download DFS applications through official application release channels to mitigate the risk of running malware-infected apps.
	– Unverified inputs such as unsolicited SMS messages, in-app advertisements, or e-mails (SD: data integrity)	**C36**: MNOs and DFS providers should undertake active customer awareness campaigns to educate consumers and internal staff about malicious messages, phishing attacks, and spoofing.
	– Insufficiently protected credentials (SD: access control)	**C37**: MNOs and DFS providers should mask user passwords and PINs, actively educate customers on shoulder surfing and safe PIN/password usage to avoid shoulder surfing and writing down of passwords.
MNO	The risk of ***unauthorized access to user data*** is due to the following vulnerability: – Weak over-the-air encryption (SD: communication security)	**C38**: MNOs should discontinue the use of A5/0, A5/1, and A5/2 GSM encryption ciphers. Closely monitor results from the security and cryptographic community regarding the feasibility and ease of compromising A5/3 and A5/4 and begin considering stronger ciphers. Have a deployment strategy ready for these newer ciphers.
	The risk of ***user impersonation*** is due to the following vulnerability: – Weak calling line identification filtering (SD: communication security)	**C39**: MNOs should do CLI analysis for calls/SMS to detect calls and SMS that may be spoofed to appear like DFS provider calls.

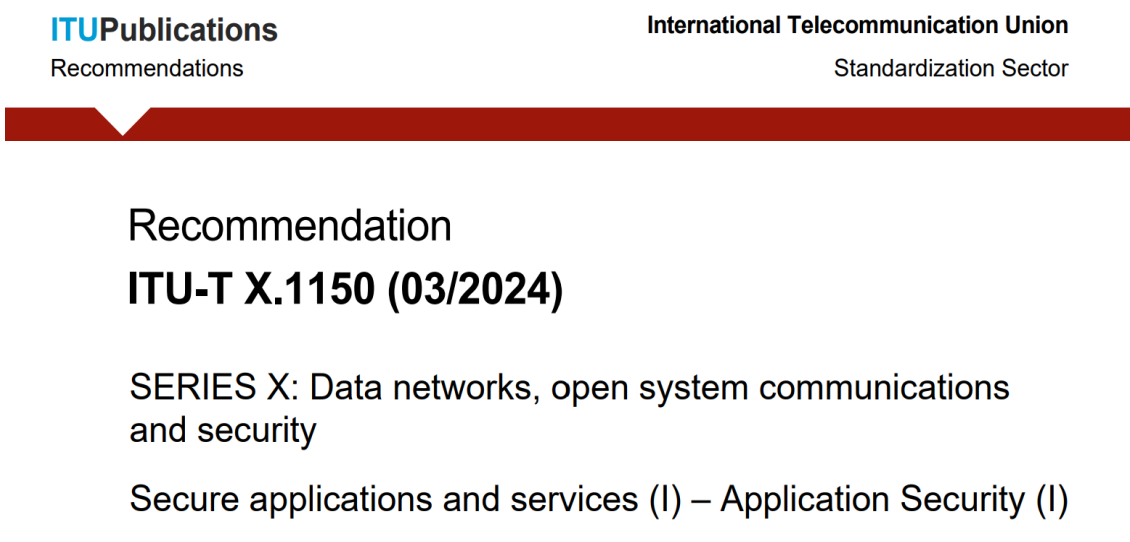
Mobile Payment App Security Best Practices (Appendix 1)

- 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.

Summary

- Identify the threats and vulnerabilities for different DFS stakeholder types.
- Adopt a risk management process
- Implement Information Security Management System (ISMS) based on ISO 27001
- Establish minimum security baselines for app security development address systemic vulnerabilities
- Conduct periodic security audit of DFS providers and/or security audit of DFS applications

- **Aimed at DFS regulators and providers**


ITUPublications
Recommendations

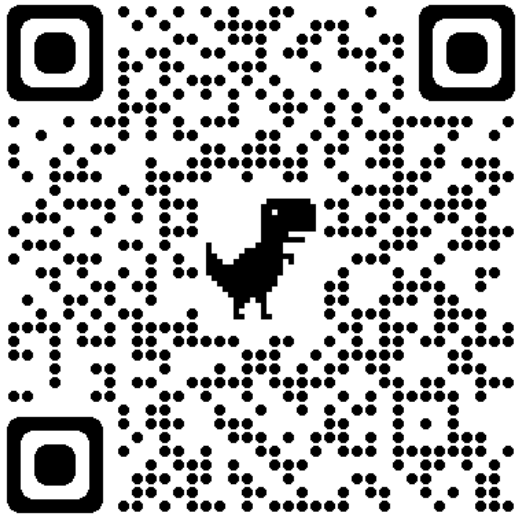
International Telecommunication Union
Standardization Sector

Recommendation
ITU-T X.1150 (03/2024)

SERIES X: Data networks, open system communications and security

Secure applications and services (I) – Application Security (I)

Security assurance framework for digital financial services



http://www.itu.int/go/dfssl

Contact: dfssecuritylab@itu.int

Thank you!