Digital Financial Services Security Clinic

Addressing security risks to digital finance ecosystem

DFS Security Assurance Framework

Vijay Mauree
Programme Coordinator, ITU

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

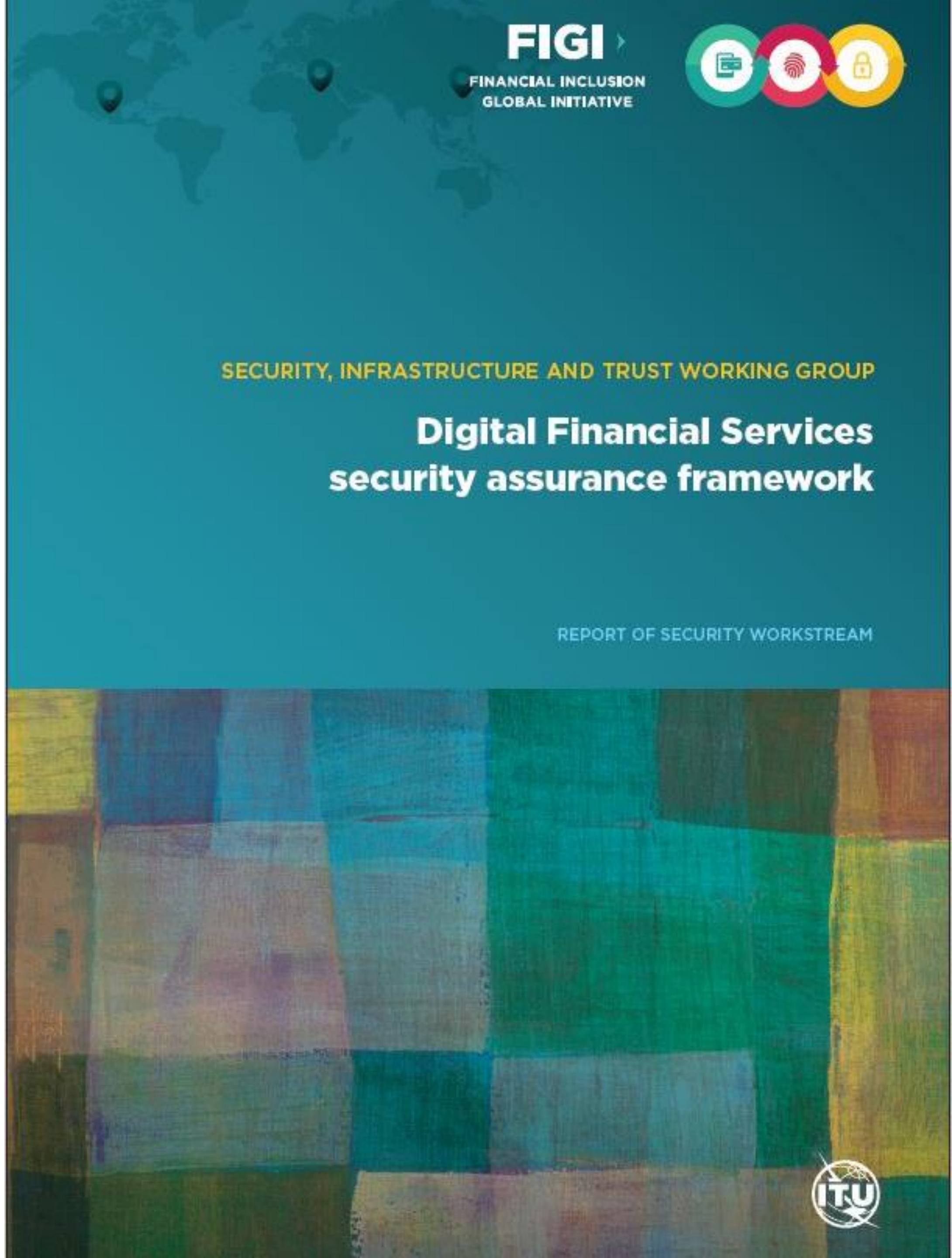
Download the report

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**.**



FIGI
FINANCIAL INCLUSION
GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services
security assurance framework

REPORT OF SECURITY WORKSTREAM

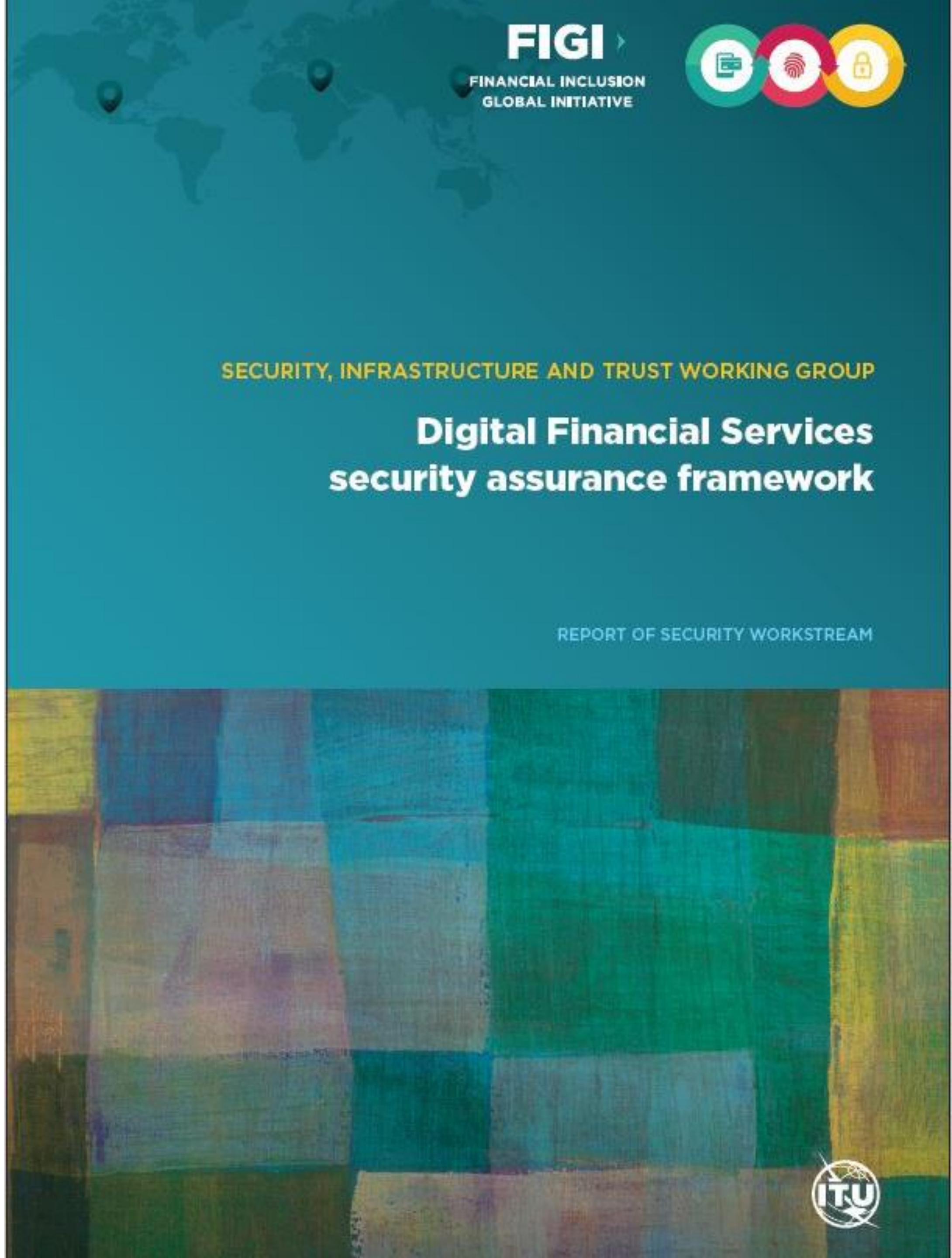
Report summary

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

Living document and will evolve over time Aimed at DFS ecosystem regulators & providers



FIGI
FINANCIAL INCLUSION
GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services
security assurance framework

REPORT OF SECURITY WORKSTREAM

ITU

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

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

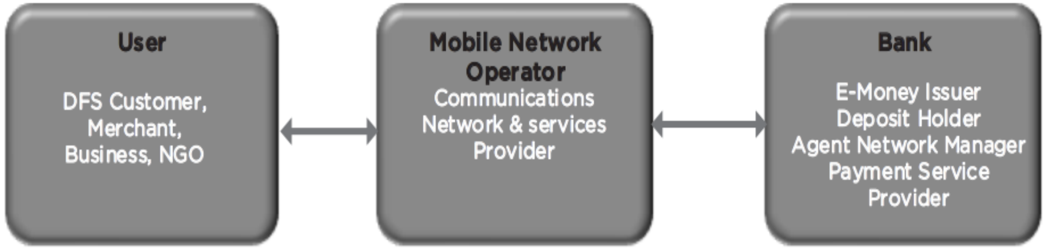
Control:

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

DFS Business Models

Bank led



User

DFS Customer, Merchant, Business, NGO

Mobile Network Operator

Communications Network & services Provider

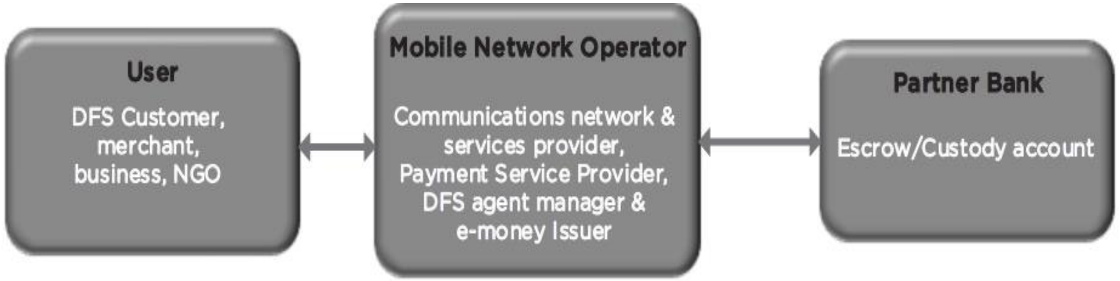
Bank

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

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



User

DFS Customer, merchant, business, NGO

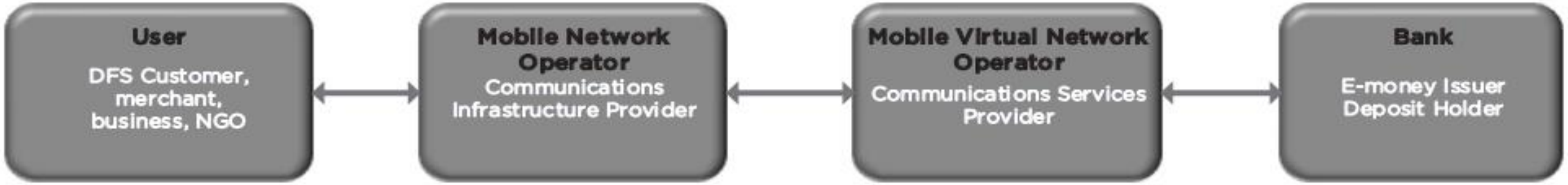
Mobile Network Operator

Communications network & services provider,
Payment Service Provider,
DFS agent manager & e-money Issuer

Partner Bank

Escrow/Custody account

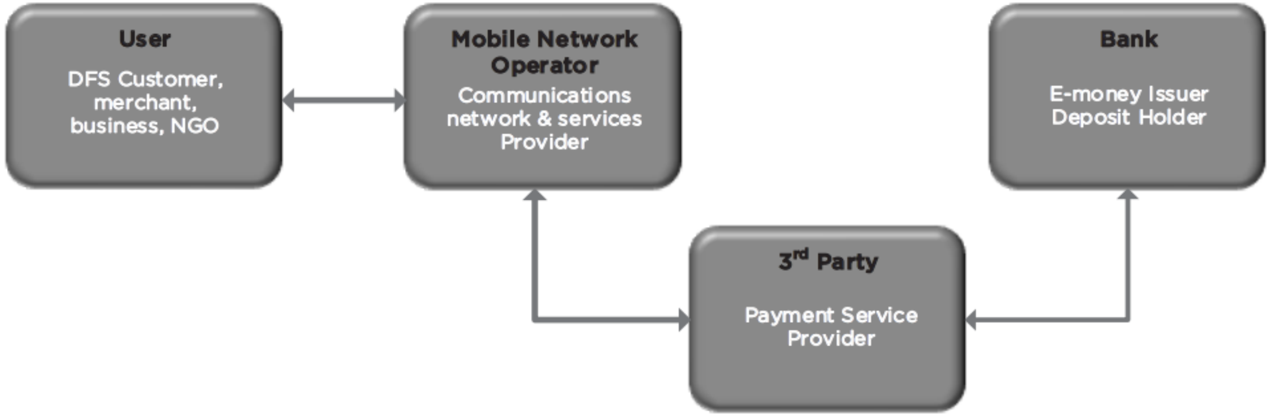
MVNO led


User
DFS Customer, merchant, business, NGO
Mobile Network Operator
Communications Infrastructure Provider
Mobile Virtual Network Operator
Communications Services Provider
Bank
E-money Issuer
Deposit Holder

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)

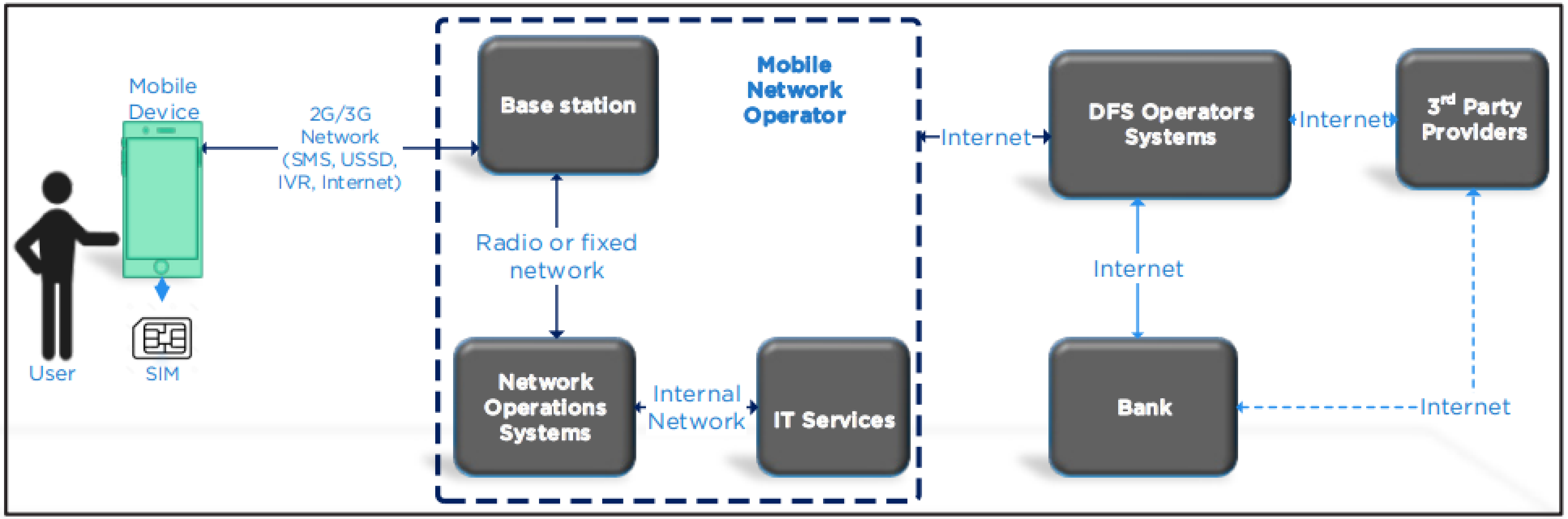


?

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

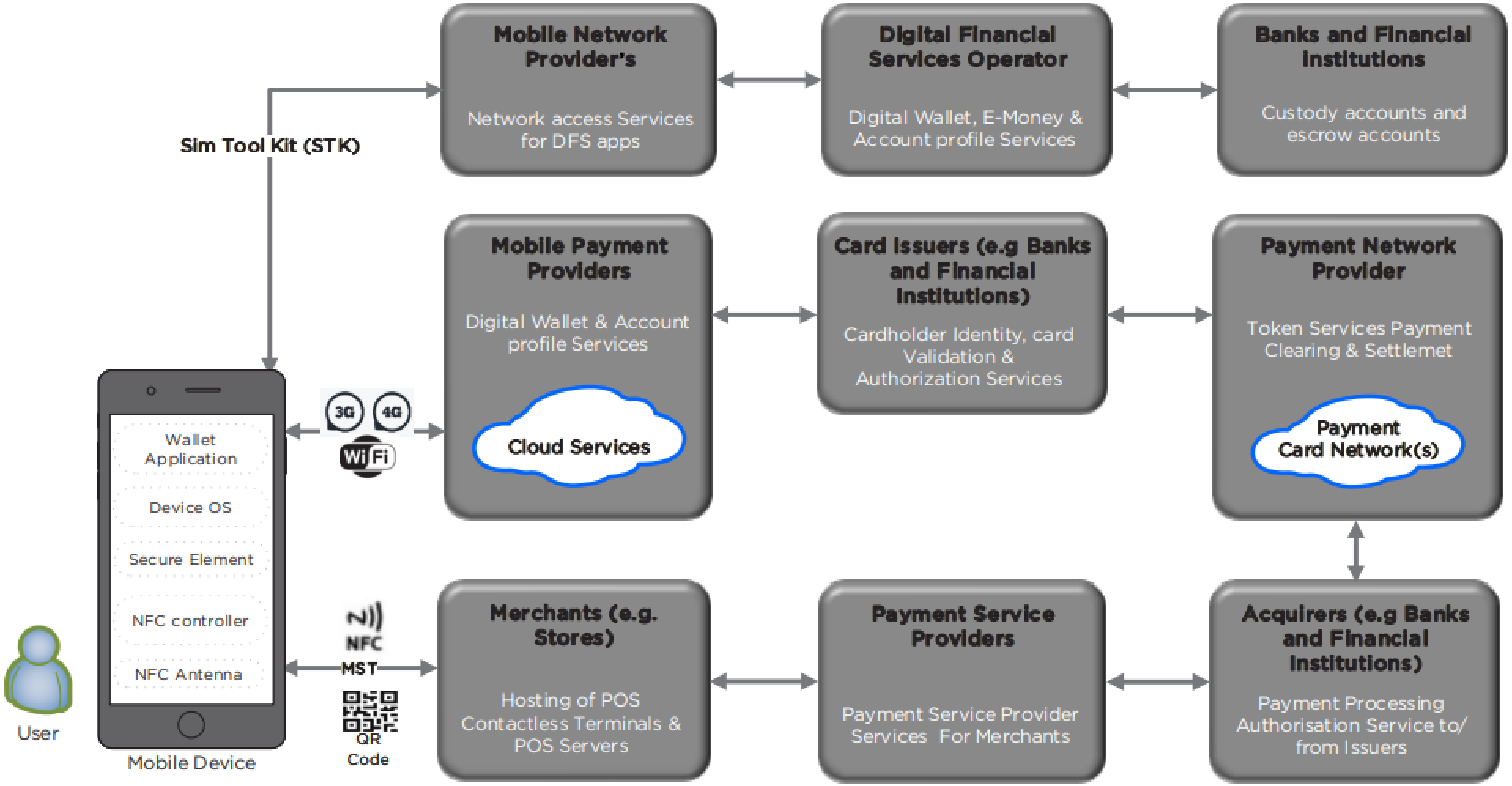
MNO

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

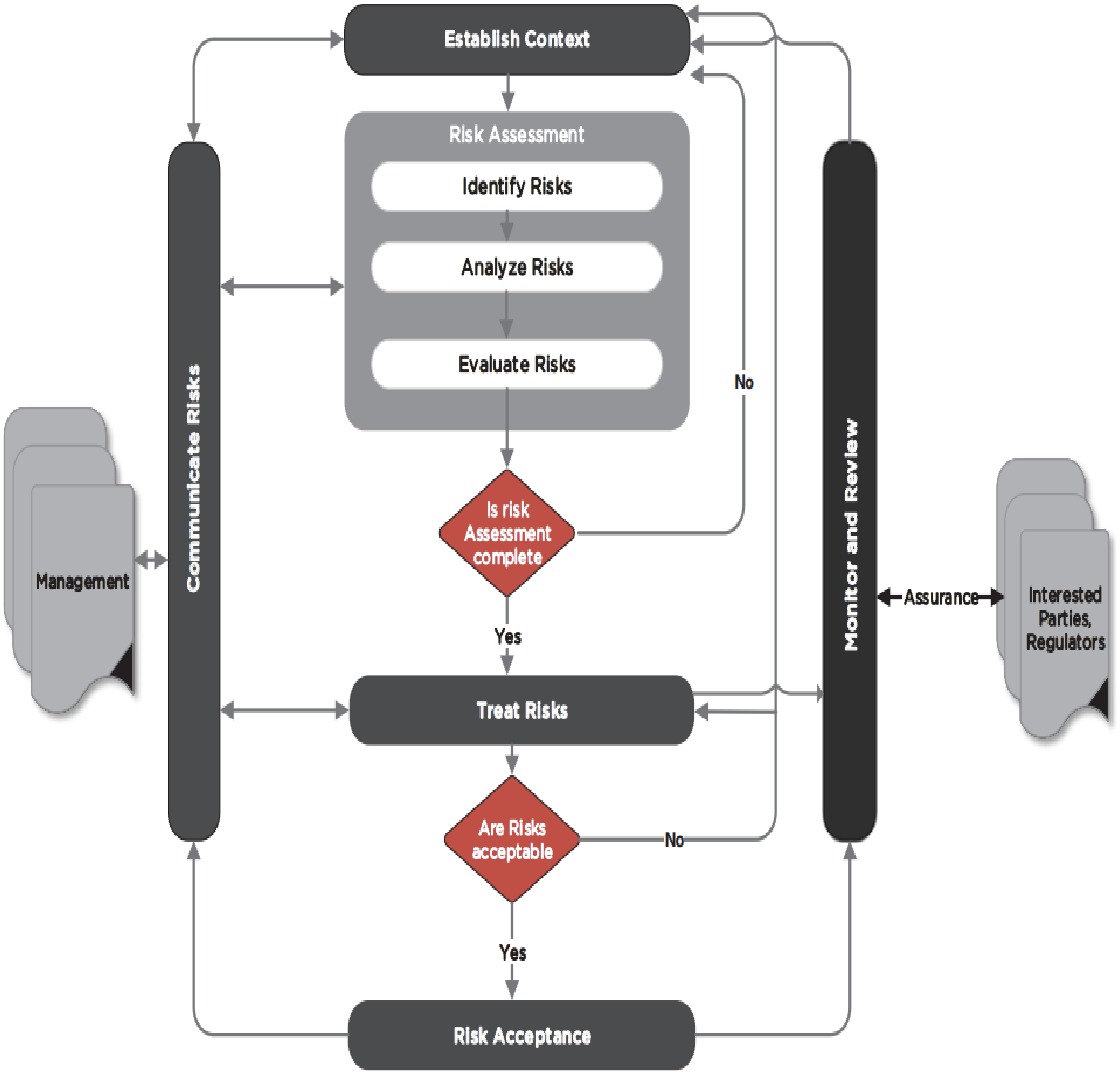

Mobile Network Provider's
Network access Services for DFS apps
Digital Financial Services Operator
Digital Wallet, E-Money & Account profile Services
Banks and Financial Institutions
Custody accounts and escrow accounts
Sim Tool Kit (STK)
Mobile Payment Providers
Digital Wallet & Account profile Services
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
User
Mobile Device
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

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

Security risk management process

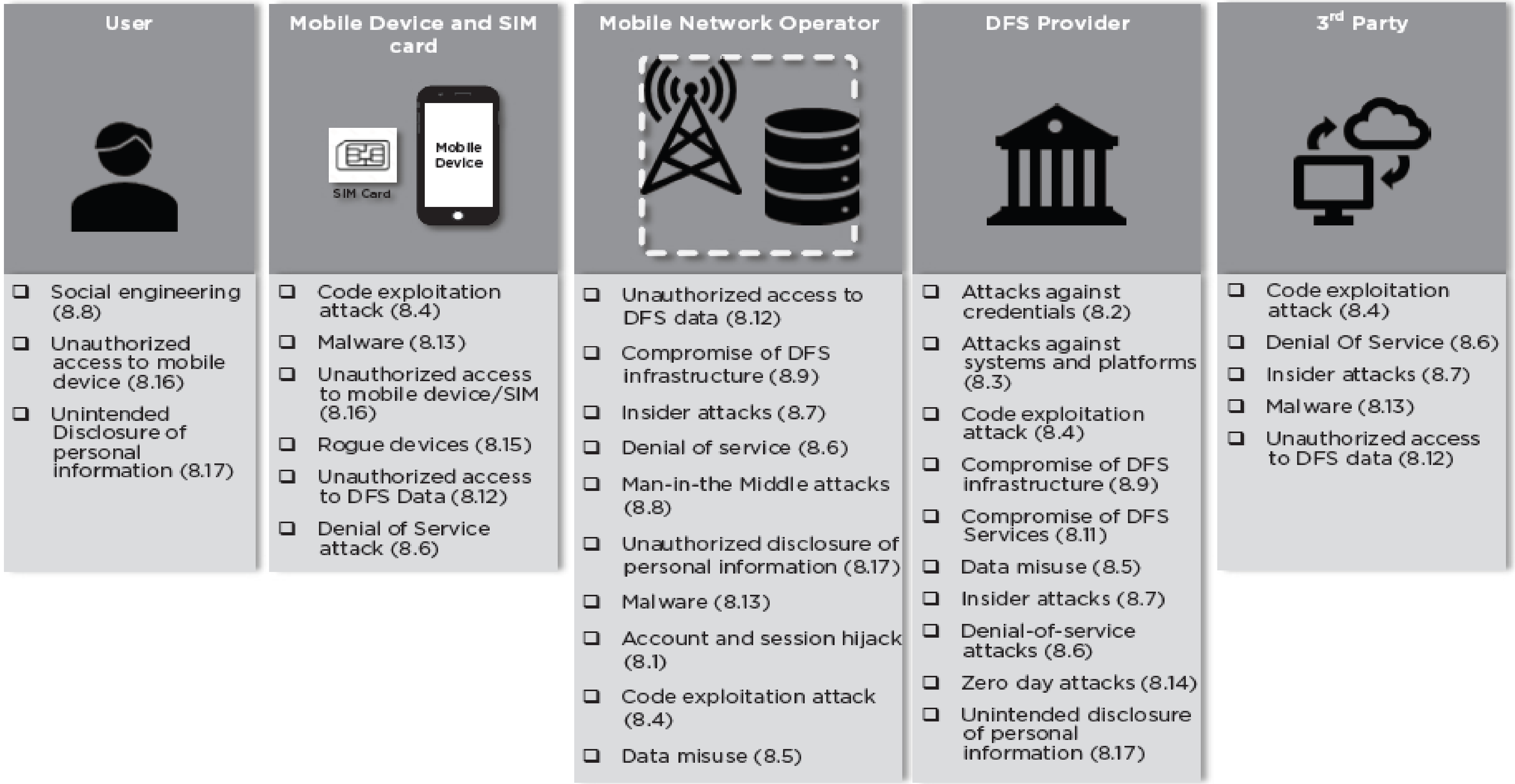
Risk Assessment methodology

- 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


SIM Card
Mobile Device

User

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

Mobile Device and SIM card

- ❑ 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 to DFS based on digital wallets

Mobile payment application/device

like previous slide

Merchant

- OS malware,
- QR code compromise,
- MITM attacks against POS terminals,
- relay attacks

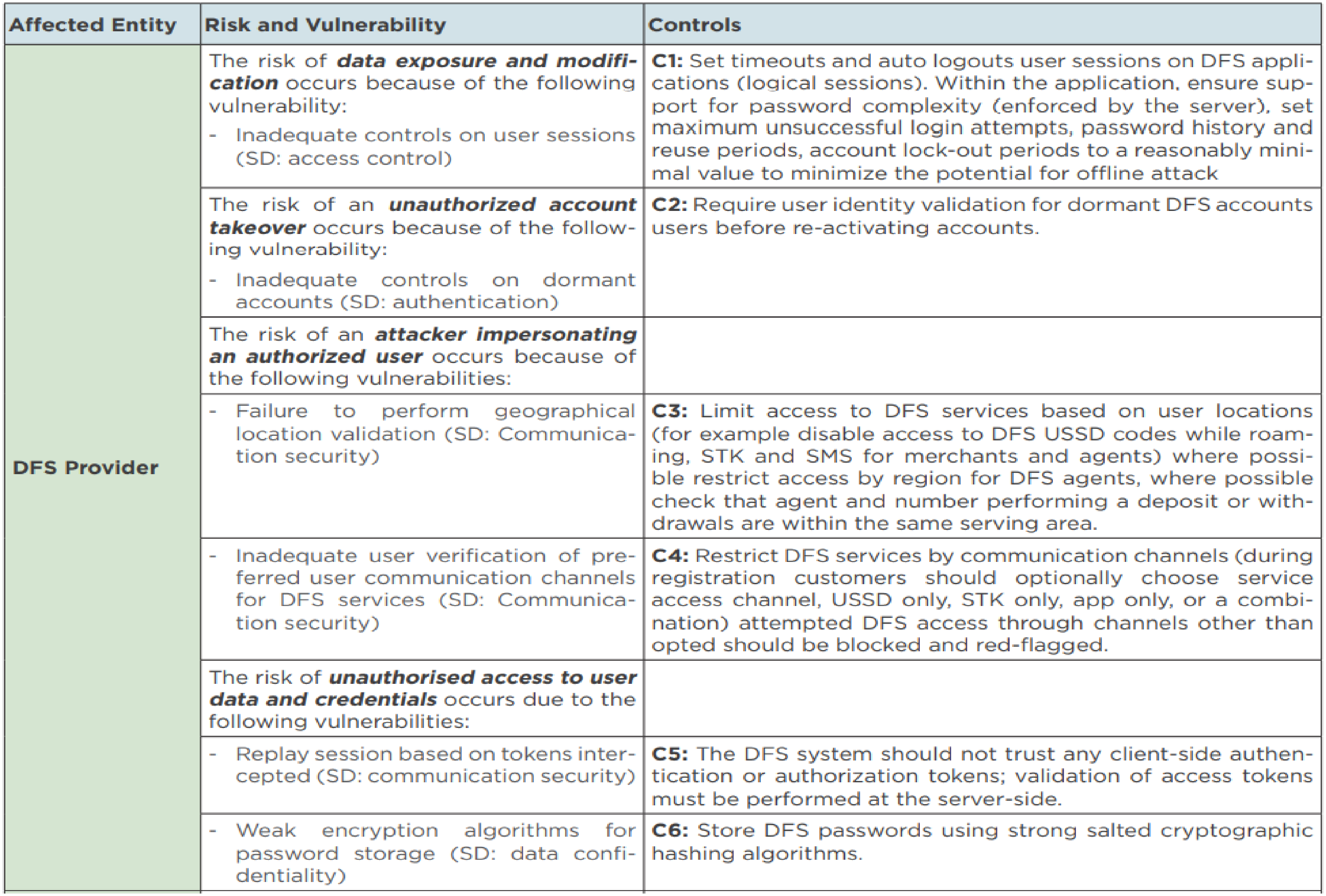
Acquirers & Issuers

- 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

Example 1: Threat 8.1 Account and session hijacking



Affected Entity	Risk and Vulnerability	Controls
DFS Provider	The risk of ***data exposure and modification*** occurs because of the following vulnerability: - Inadequate controls on user sessions (SD: access control)	**C1:** Set timeouts and auto logouts user sessions on DFS applications (logical sessions). Within the application, ensure support for password complexity (enforced by the server), set maximum unsuccessful login attempts, password history and reuse periods, account lock-out periods to a reasonably minimal value to minimize the potential for offline attack
	The risk of an ***unauthorized account takeover*** occurs because of the following vulnerability: - Inadequate controls on dormant accounts (SD: authentication)	**C2:** Require user identity validation for dormant DFS accounts users before re-activating accounts.
	The risk of an ***attacker impersonating an authorized user*** occurs because of the following vulnerabilities:	
	- Failure to perform geographical location validation (SD: Communication security)	**C3:** Limit access to DFS services based on user locations (for example disable access to DFS USSD codes while roaming, STK and SMS for merchants and agents) where possible restrict access by region for DFS agents, where possible check that agent and number performing a deposit or withdrawals are within the same serving area.
	- Inadequate user verification of preferred user communication channels for DFS services (SD: Communication security)	**C4:** Restrict DFS services by communication channels (during registration customers should optionally choose service access channel, USSD only, STK only, app only, or a combination) attempted DFS access through channels other than opted should be blocked and red-flagged.
	The risk of ***unauthorised access to user data and credentials*** occurs due to the following vulnerabilities:	
	- Replay session based on tokens intercepted (SD: communication security)	**C5:** The DFS system should not trust any client-side authentication or authorization tokens; validation of access tokens must be performed at the server-side.
	- Weak encryption algorithms for password storage (SD: data confidentiality)	**C6:** Store DFS passwords using strong salted cryptographic hashing algorithms.

Extracted from: DFS security assurance framework

Threat: Denial of service attack (section 8.7)

Risks at DFS provider

- Inability to perform transaction due to a service outage
- Transaction failure due to high delays
- Unauthorized access to user data

Vulnerability

- 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)

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.

Mobile Payment App Security Best Practices

Mobile Payment App Security Best Practices (Section 9)

- 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:
  - i. device and application integrity.
  - ii. communication security and certificate handling.
  - iii. user authentication.
  - iv. secure data handling.
  - v. secure application development.

Device and Application Integrity

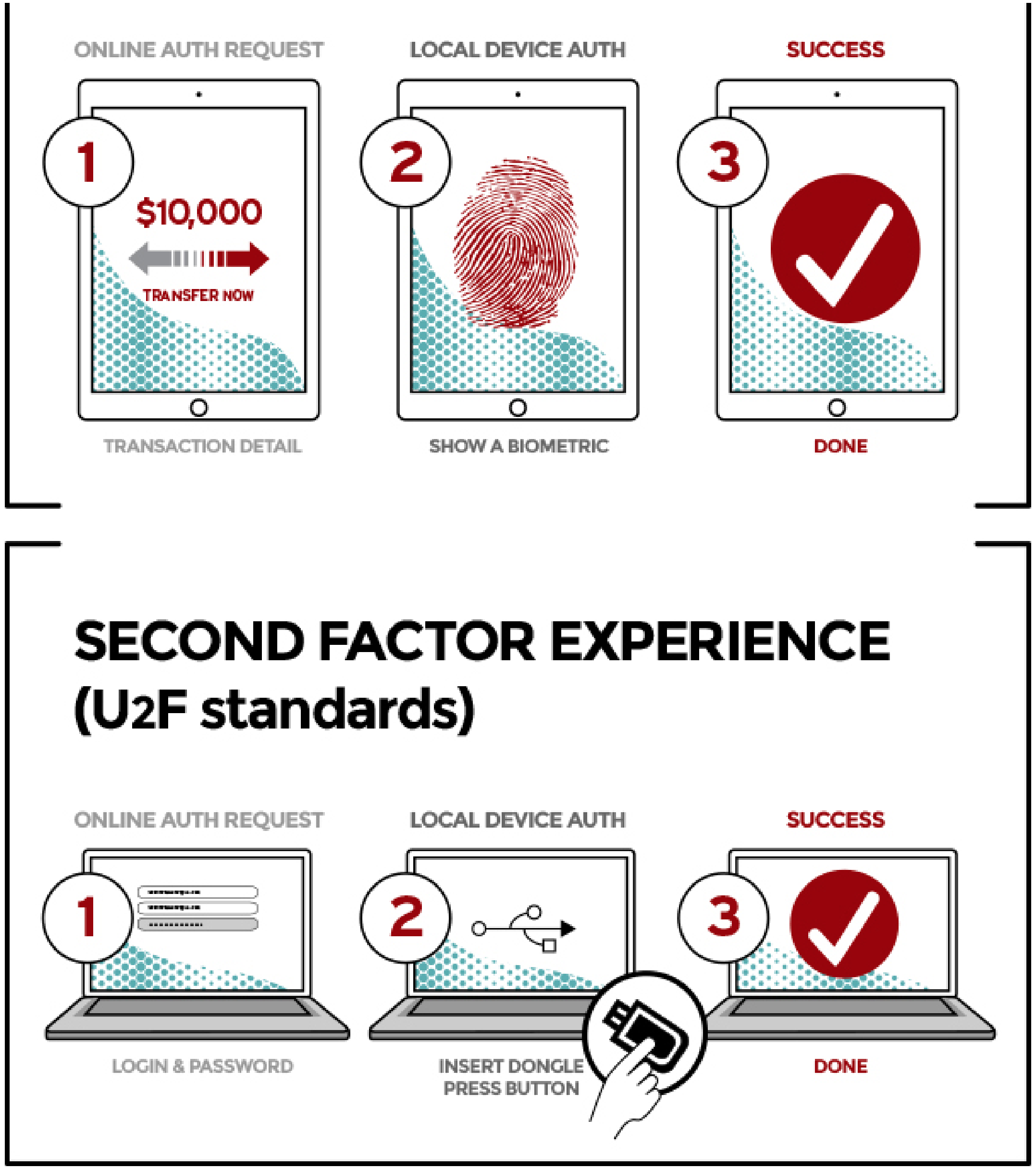
- Applications should thus use the mobile platform services to determine that they and the underlying platform have not been modified
- Remove any extraneous code that might have been added to the application during development
- On the server-side, determine whether the app is running in a high integrity state

Communication Security and Certificate Handling

- Apps should be making use of standardized cryptographic libraries
- TLS certificates should not be expired and should present strong cipher suites.
- Limit the lifetime of issued certificates to 825 days in accordance with the CA
- Assure the trustworthiness of the certificate authority and consider a contingency plan for if the CA is no longer trusted
- Ensure the configuration of TLS is performed in a secure fashion and avoid misconfiguration issues
- Certificate pinning is recommended to prevent replacement of certificates
- Client devices must ensure that they correctly validate server certificates

User Authentication

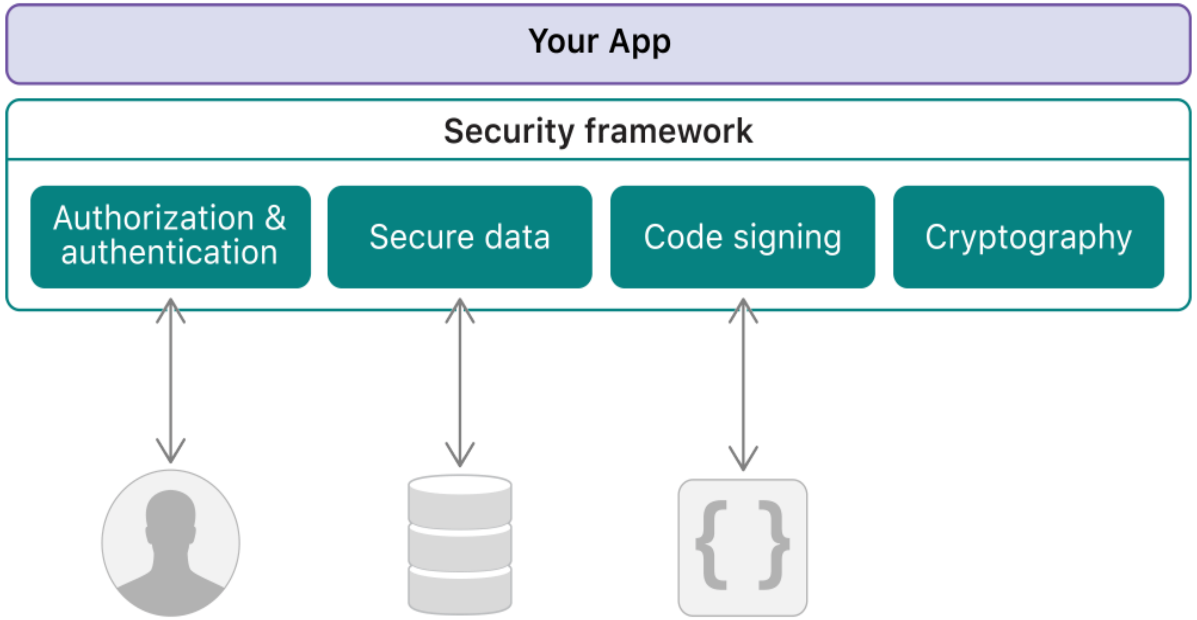
- PINs and passwords should not be easily guessable and weak credentials should be disallowed (Mobile Apps Password Policy).
- Multi-factor authentication before performing financial or other sensitive functions is strongly encouraged.
- Smartphone authenticator apps should be used for sending one-time passwords rather than SMS
- Assure the trustworthiness of the certificate authority and consider a contingency plan for if the CA is no longer trusted
- Biometric information is used for authentication, it must be stored with appropriate security measures



Source: FIDO

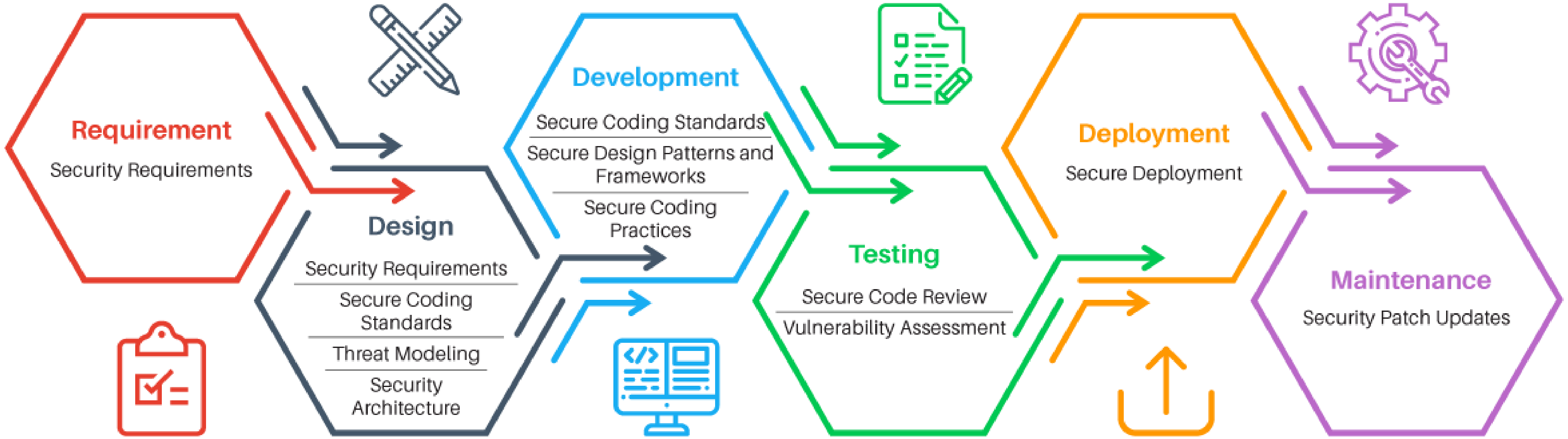
Secure Data Handling

- Mobile devices should securely store confidential information
- Trusted hardware should be used for the storage of sensitive information - If available on client device.
- Avoid storing information in external storage
- Delete confidential data from caches and memory after it is used
- Restrict data shared with other applications through fine-grained permissions
- Do not hard-code sensitive information such as passwords or keys
- Validate any input coming from the client that is to be stored in databases



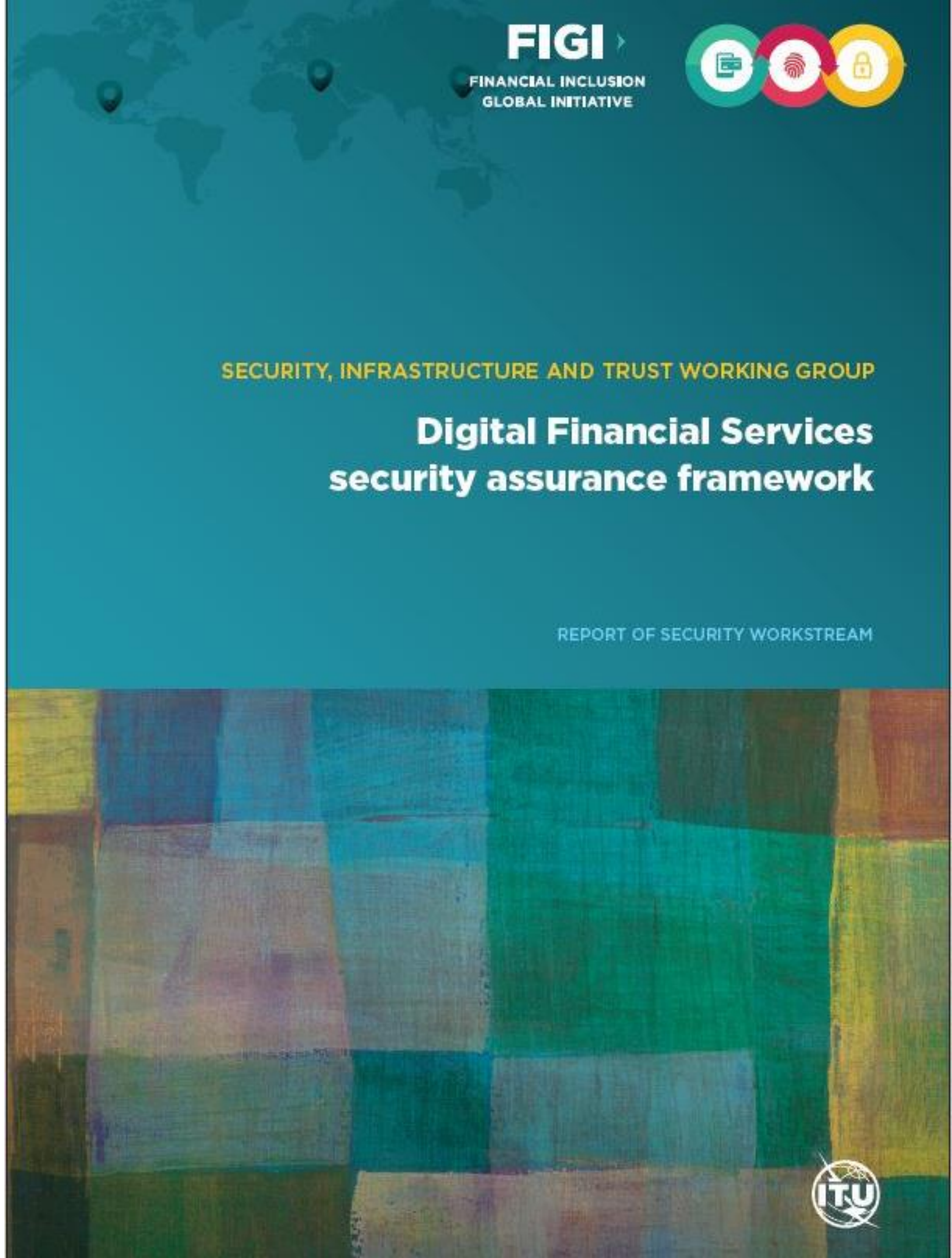
Secure Application Development

- Develop according industry-accepted secure coding practices and standards
- Assure a means of securely updating applications.
- Have code independently assessed and tested by internal or external code review teams.



Recommendations for regulators

- Identify the threats and vulnerabilities for different DFS stakeholder types.
- Adopt a risk management process
- Recommend an Information Security Management System (ISMS) based on ISO 27001 for DFS providers
- 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



FIGI

FINANCIAL INCLUSION
GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services
security assurance framework

REPORT OF SECURITY WORKSTREAM

ITU

Device and Application Integrity

- Applications should thus use the mobile platform services to determine that they and the underlying platform have not been modified
- Remove any extraneous code that might have been added to the application during development
- On the server-side, determine whether the app is running in a high integrity state

Communication Security and Certificate Handling

- Apps should be making use of standardised cryptographic libraries
- TLS certificates should not be expired and should present strong cipher suites.
- Limit the lifetime of issued certificates to 825 days in accordance with the CA
- Assure the trustworthiness of the certificate authority and consider a contingency plan for if the CA is no longer trusted
- Ensure the configuration of TLS is performed in a secure fashion and avoid misconfiguration issues
- Certificate pinning is recommended to prevent replacement of certificates
- Client devices must ensure that they correctly validate server certificates

User Authentication

- PINs and passwords should not be easily guessable and weak credentials should be disallowed (Mobile Apps Password Policy).
- Multi-factor authentication before performing financial or other sensitive functions is strongly encouraged.
- Smartphone authenticator apps should be used for sending one-time passwords rather than SMS
- Assure the trustworthiness of the certificate authority and consider a contingency plan for if the CA is no longer trusted
- Biometric information is used for authentication, it must be stored with appropriate security measures

Mobile Apps Password Policy (Example)

Client-side Policy

- *The user's mobile application password shall never be stored persistently on the device.*
- *The user's mobile application password shall have a minimum length of 8 characters.*
- *Mobile application password should kept in working storage (main memory and overwrite when app goes to background).*
- *Users have to provide the mobile application password again every time the app comes back to foreground.*
- *By default, any already persistently stored data to which the application-level encryption was applied shall be deleted after 20 unsuccessful attempts to provide the correct mobile application password.*

Service side Policy

- *The user's mobile application password has to have minimum length, upper-case and lower-case characters, numbers and special characters as defined by the configured policy.*
- *The number of unsuccessful attempts to provide the correct password before data will be deleted shall be enforced as configured by the customer.*

Secure Data Handling

- Mobile devices should securely store confidential information
- Trusted hardware should be used for the storage of sensitive information - If available on client device.
- Avoid storing information in external storage
- Delete confidential data from caches and memory after it is used
- Restrict data shared with other applications through fine-grained permissions
- Do not hard-code sensitive information such as passwords or keys
- Validate any input coming from the client that is to be stored in databases

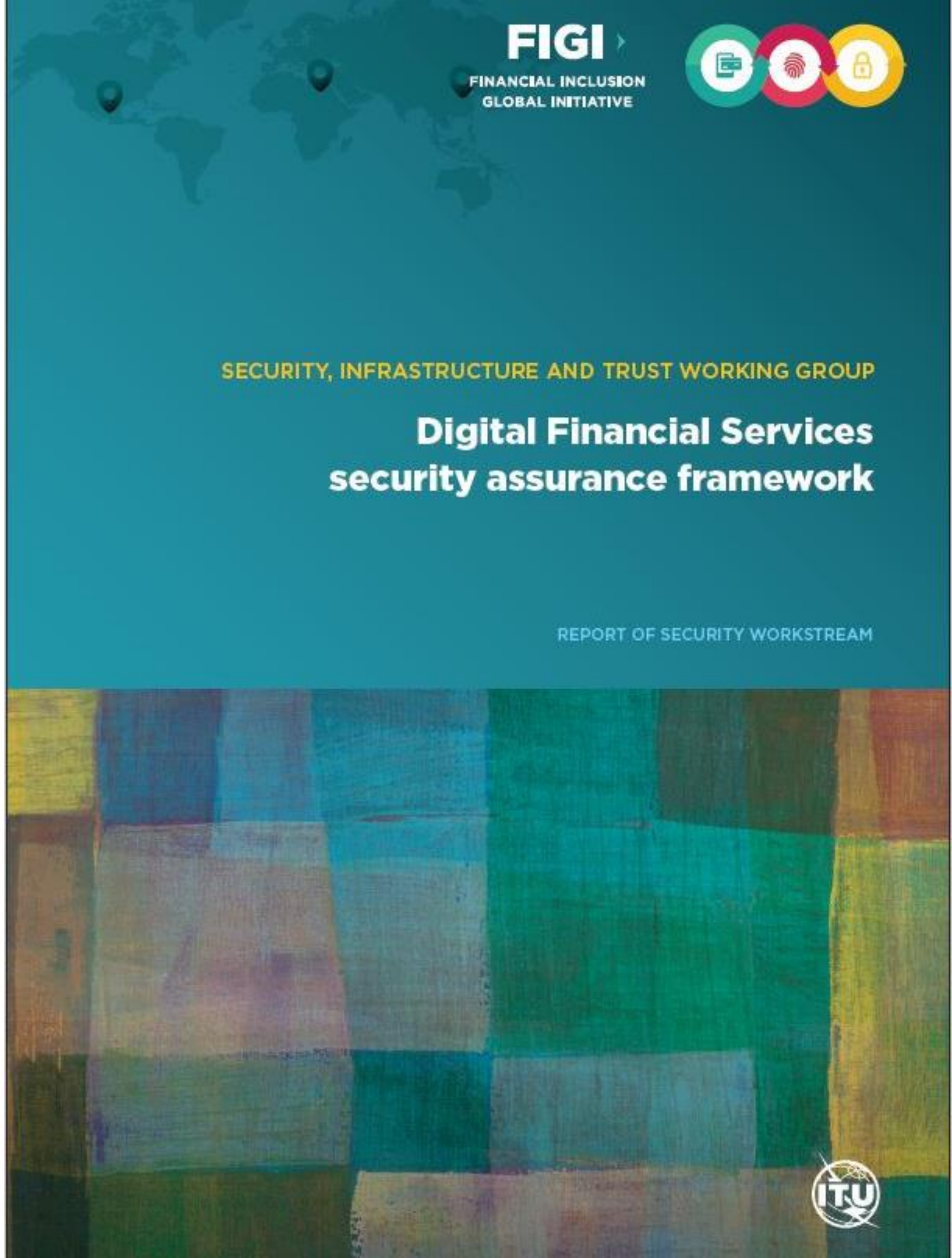
Secure Application Development

- Develop according industry-accepted secure coding practices and standards
- Assure a means of securely updating applications.
- Have code independently assessed and tested by internal or external code review teams.

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



FIGI

FINANCIAL INCLUSION
GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

**Digital Financial Services
security assurance framework**

REPORT OF SECURITY WORKSTREAM

ITU

Questions

Contact: dfssecuritylab@itu.int

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