ITUEvents

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

FIGI Symposium

22-24 January 2019
Cairo, Egypt

#financialinclusion

Hosted by

NTRA National Telecom Regulatory Authority الجهاز القومي لتنظيم الاتصالات

Sponsored by

BILL & MELINDA GATES foundation

Organized by

Committee on Payments and Market Infrastructures

BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

Security Assurance Framework

Vijay Mauree & Kevin Butler

Vijay.Mauree@itu.int

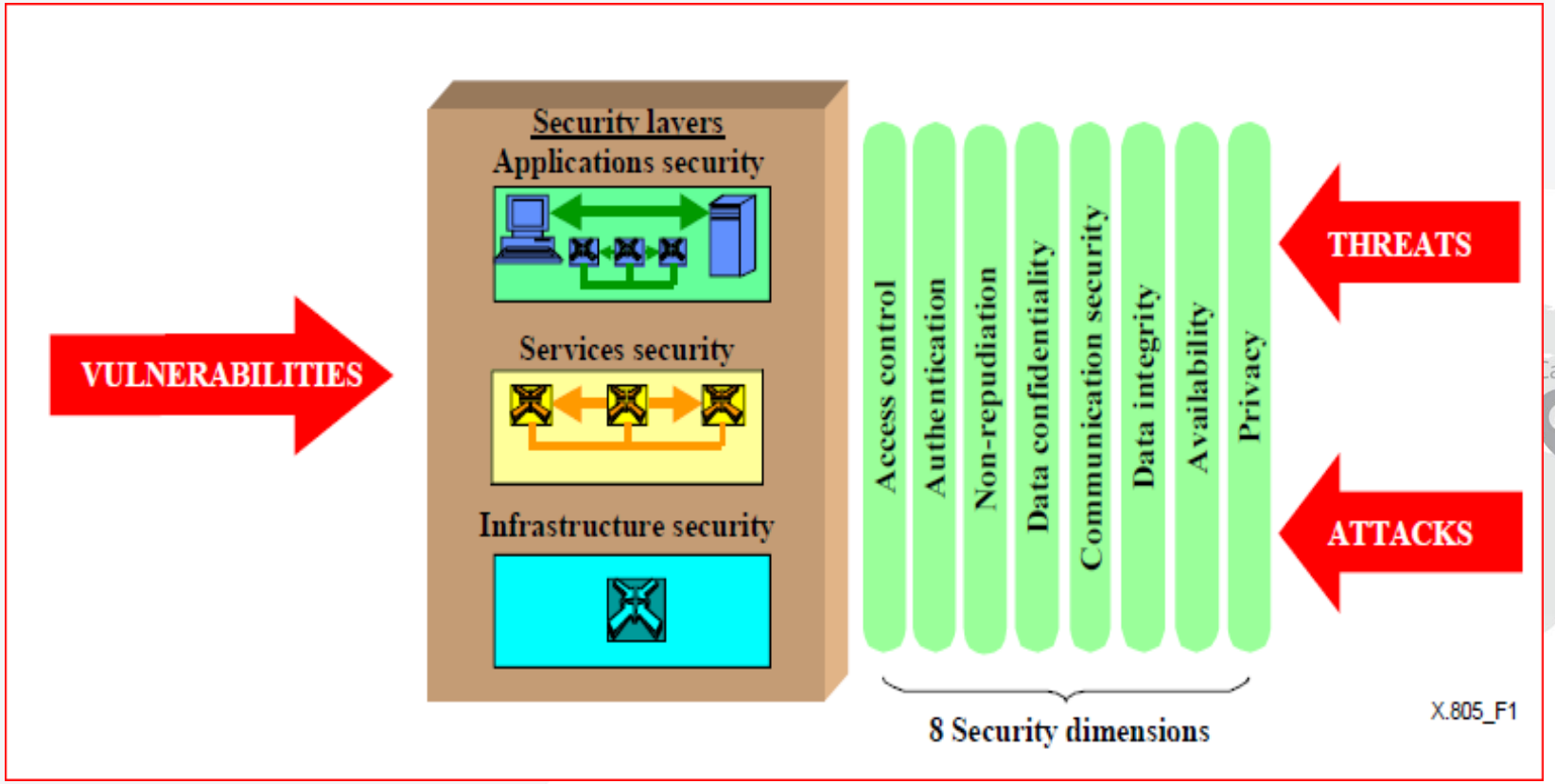
DFS Security Assurance Framework

Objectives

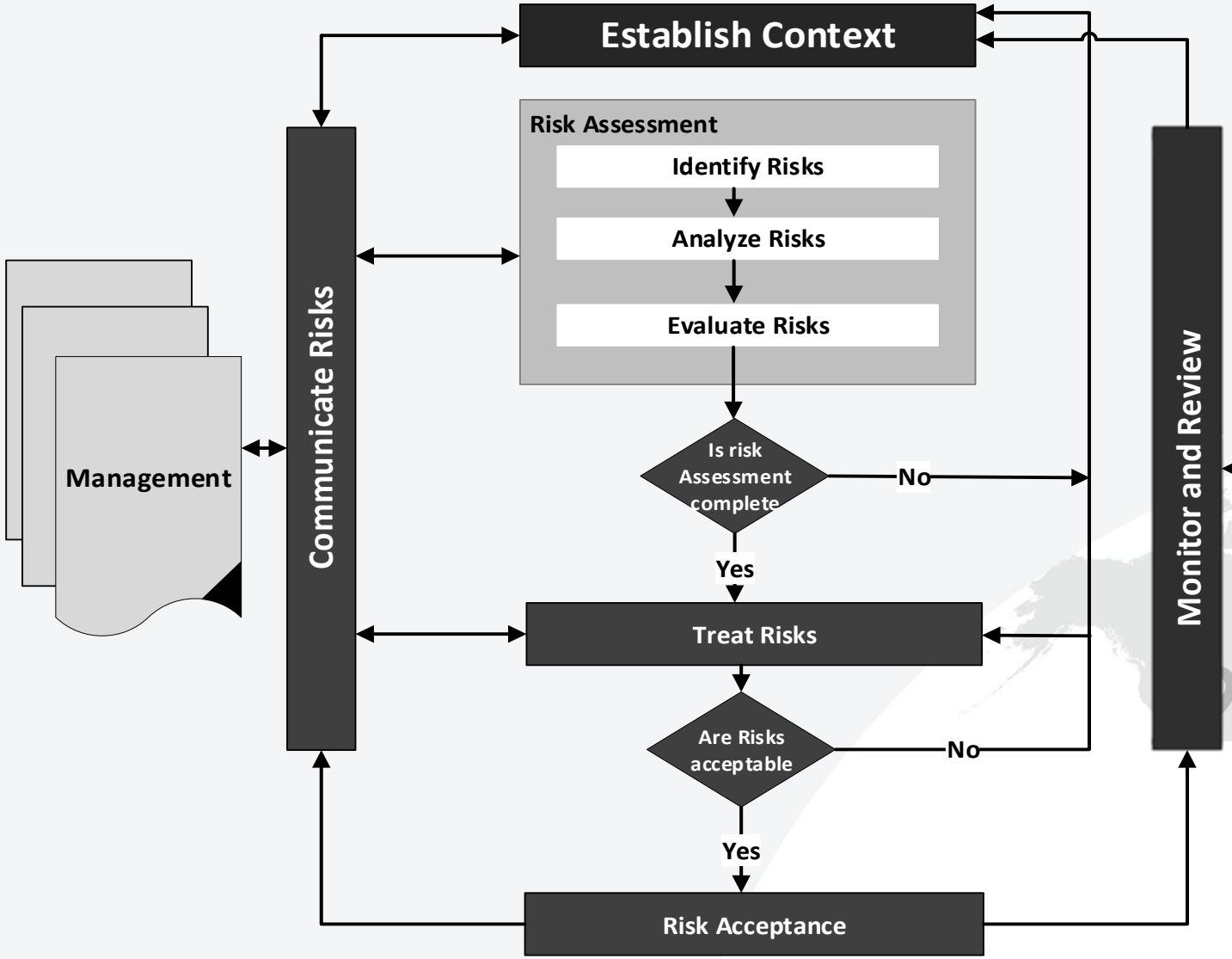
- ❑ Risk Assessment Framework – ISO 27001
- ❑ Identify DFS Security Threats and Vulnerabilities
- ❑ Propose Mitigation Measures to Security Threats (ITU-T Recommendation X.805)
- ❑ Develop Guidelines For a DFS Security Audit

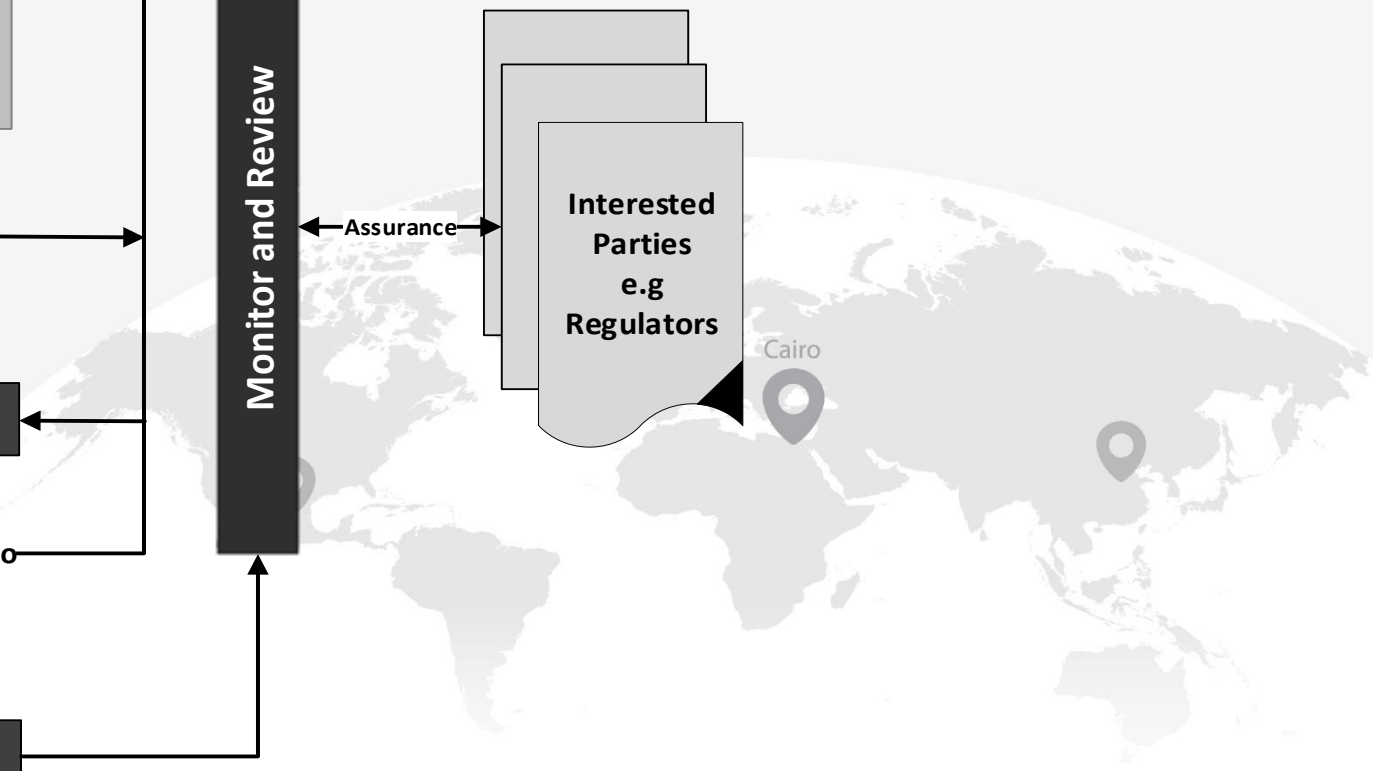
The ITU-T Recommendation X.805

Considers 8 '*security dimensions*' to address network security.



Risk Assessment Framework





Risk Assessment Framework

Risk Identification

- ❑Identify DFS assets
- ❑Identify associated vulnerabilities
- ❑Identify threats
- ❑Identify Existing controls
- ❑Identify consequences

Risk Analysis

- ❑Assessment of consequences
- ❑Likelihood and impact of occurrence
- ❑Define inherent risks
- ❑Definition of rsidual risks

Risk Evaluation

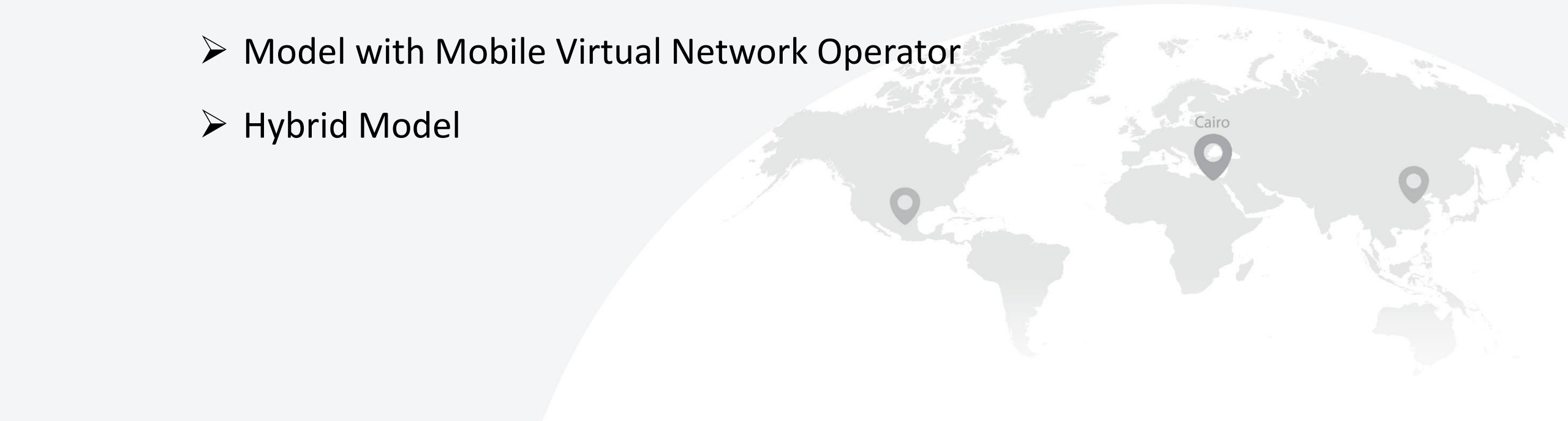
- ❑Identify controls implemented to reduce vulnerability
- ❑Evaluate effectiveness of existing controls
- ❑Define Risk Impact

Approach

- ISO 27001 – Risk Management Methodology used for risk assessment framework
- Elements of the DFS ecosystem analysed for threats and vulnerabilities based on type of communication channel, model and application
- ITU-T Recommendation X.805 security architecture used for categorising the security controls and related measures

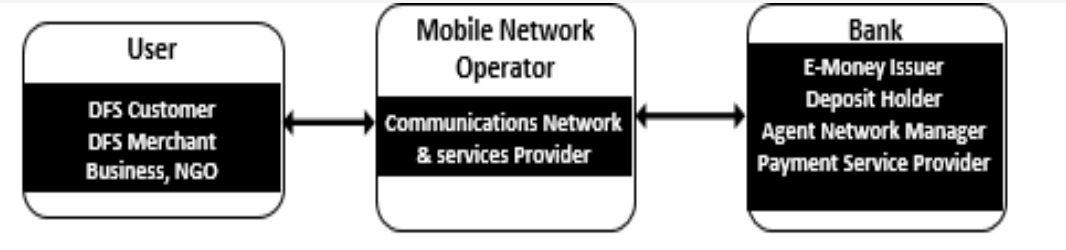
DFS Business Models

- Four types of models
  - Bank Led Business Model
  - MNO Led Business Model
  - Model with Mobile Virtual Network Operator
  - Hybrid Model



DFS Business Models

- **Bank led**



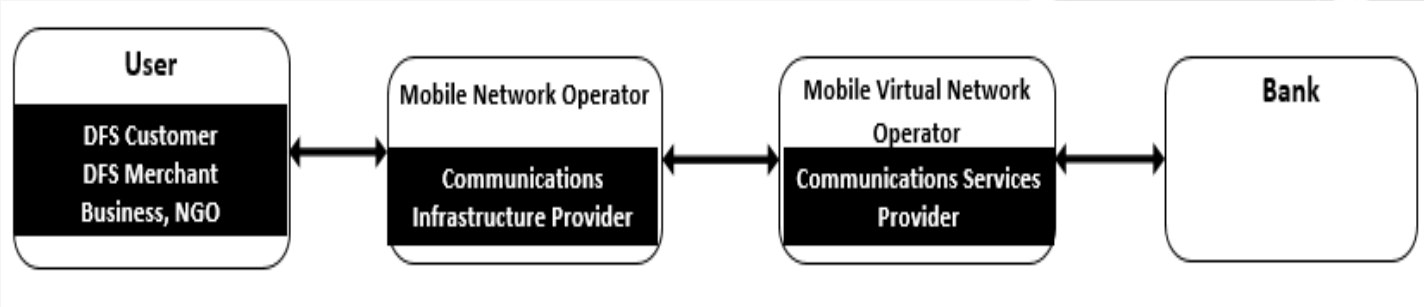
- **MNO Led**

Most Common DFS Business Models

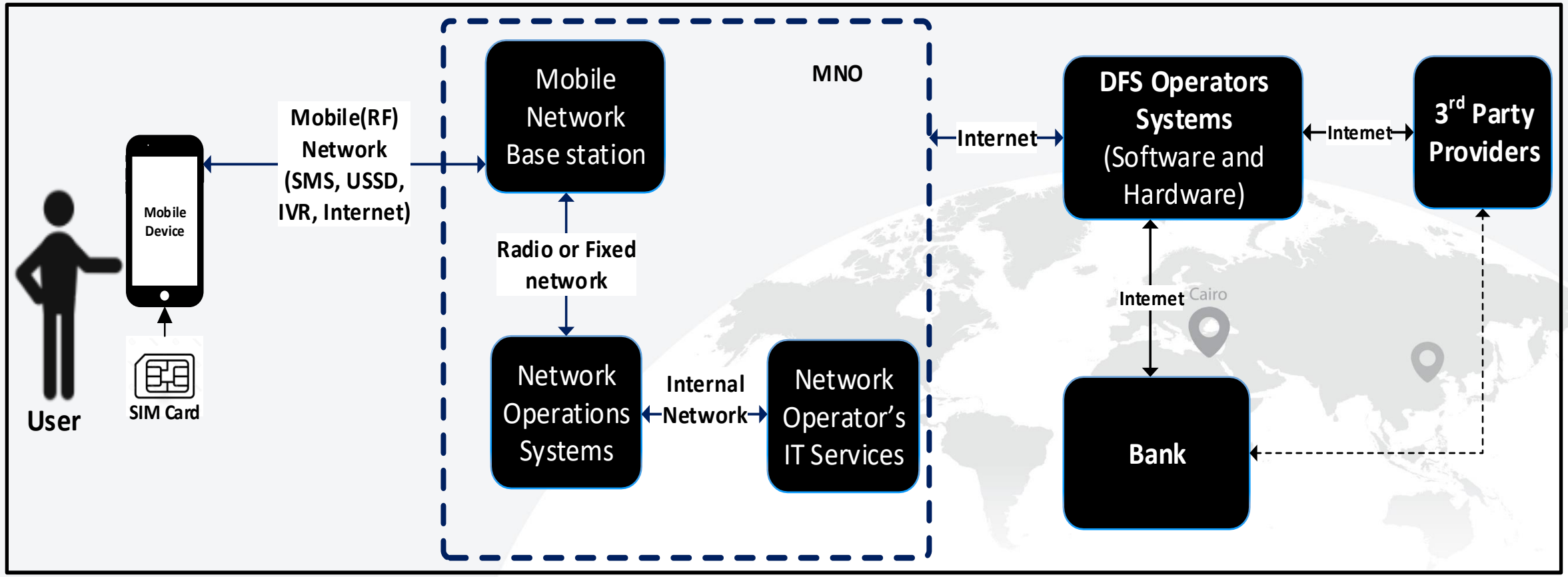
FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

➢ Model with Mobile Virtual Network Operator

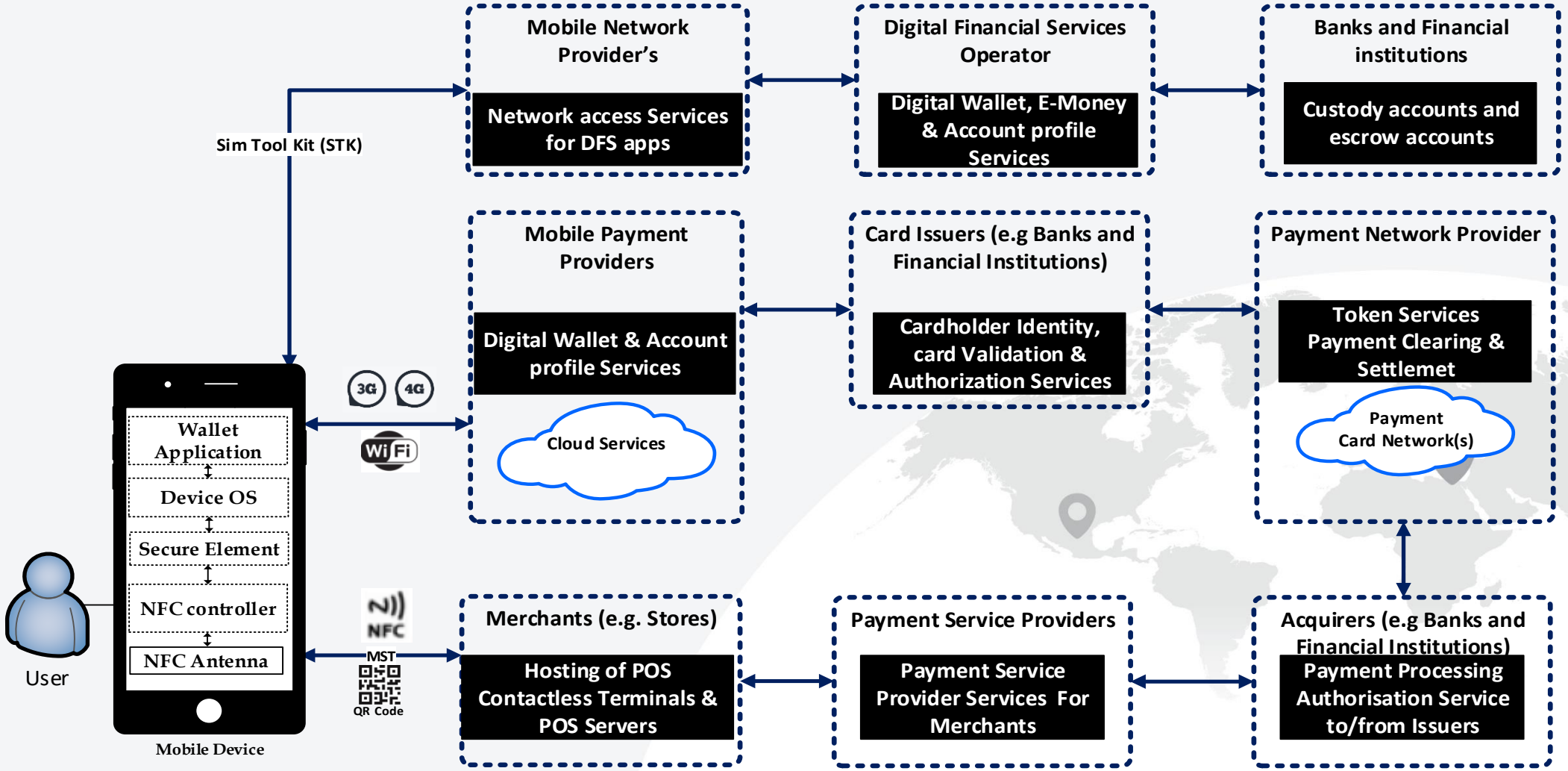
➢ Hybrid Model



Elements of a DFS ecosystem using USSD, SMS, IVR, STK and NSDT



Mobile payment applications and digital wallets



Adopted from ENISA

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

The DFS Threats

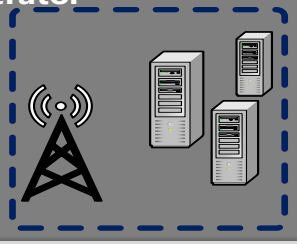
User

- Social engineering
- Unauthorized access to mobile device
- Disclosure of personal infromation

Mobile Device and simcard

- Code exploitation attack
- Malware
- Unauthorized access to mobile device/ SIM
- Rogue devices
- Unauthorized access to DFS Data
- Denial of Service attack

Mobile Network Operator



- Signaling and control channel attacks
- Compromise of MNO infrastructure
- Compromise of MNO Services
- Insider attacks
- Denial-of-service attacks
- Man-in-the Middle attacks
- Unauthorized disclosure of personal information
- Malware
- Account and session hijack
- Code exploitation attack
- Data misuse
- Malware

DFS Provider

DFS Provider

- Attacks against credentials
- Attacks against systems and platforms
- Code exploitation attack
- Compromise of DFS infrastructure
- Compromise of DFS Services
- Data misuse
- Insider attacks
- Denial-of-service attacks
- Zero day attacks
- Unintended disclosure of personal information

3rd Party

3rd Party

- Code exploitation attack
- DOS
- Insider attacks
- Malware
- Unauthorised access to DFS data

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

Security Assurance Framework Controls

Kevin Butler

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

Controls

- Use X.805 security dimensions as a way of classifying the vulnerabilities that arise from the threats
- Categorize the controls in terms of generalized threats: allows coalescing of threats common across multiple stakeholders to simplify discussion
- Risks, vulnerabilities, and threats discussed relative to the given stakeholder

Example Threat:
Account and Session Hijacking

- General threat: ability of an attacker to take control of an account or a communication session

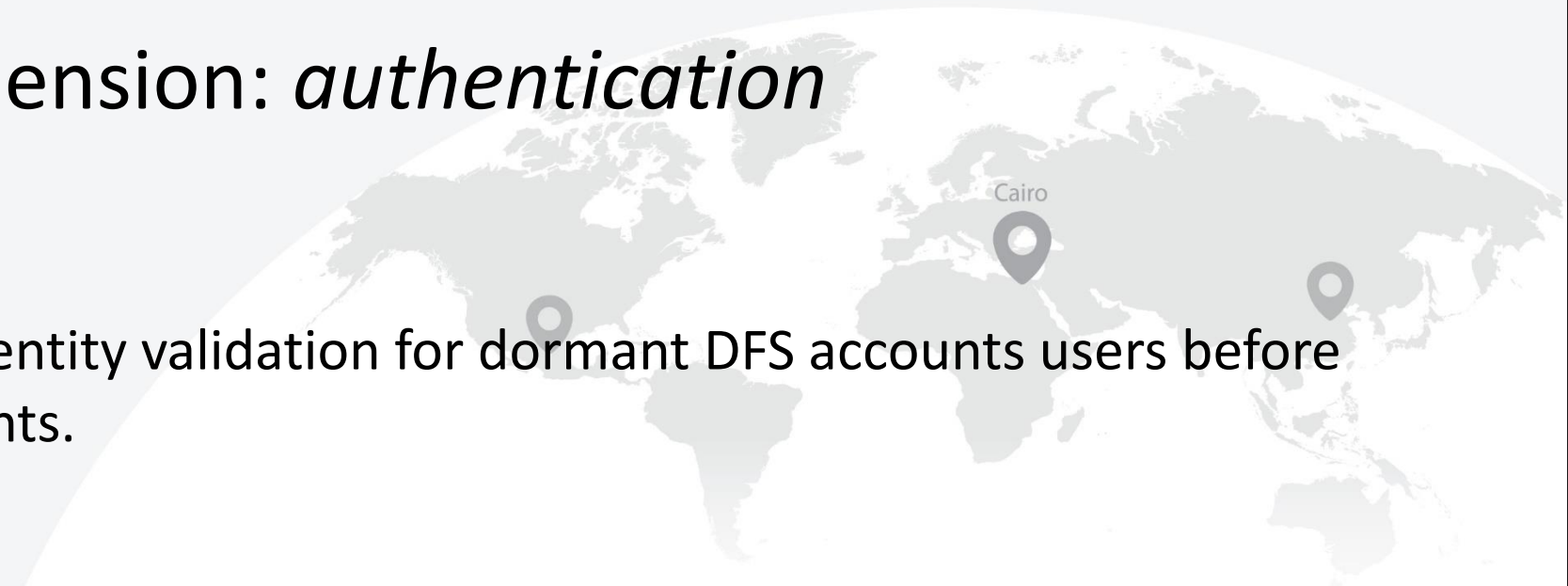
- Affected entities (DFS stakeholders): DFS Provider, MNO

Example Threat: Account and Session Hijacking

- At the DFS provider:
  - Risk: *data exposure and modification*
  - Vulnerability: *Use of credentials to elevate access*
    - Security dimension: *access control*
  - Controls:
    - **C1:** Set user session timeouts and auto logouts for access to DFS applications (logical sessions). Within the application, ensure support for password complexity (enforced by the server), set unsuccessful login attempts, password history and reuse periods, account lock-out periods to a reasonable minimal value in order to minimize the potential for offline attack.

Example Threat:
Account and Session Hijacking

- At the DFS provider (continued):
  - Risk: *unauthorized account takeover*
  - Vulnerability: *Inadequate controls on dormant accounts*
    - Security dimension: *authentication*
  - Controls:
    - **C2:** Require user identity validation for dormant DFS accounts users before re-activating accounts.



Example Threat: Account and Session Hijacking

- At the DFS provider (continued):
  - Risk: *attacker impersonating an authorized user*
  - Vulnerabilities:
    - *Lack of geographic location validation* (security dimension: *communication security*)
    - *Lack of verification on preferred user communication channels for DFS services* (security dimension: *communication security*)

Example Threat:
Account and Session Hijacking

- Controls:
  - **C3:** Limit access to DFS services based on user locations (for example while roaming disable access to DFS USSD codes, 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.
  - **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.

Example Threat: Account and Session Hijacking

- At the DFS provider (continued):
  - Risk: *unauthorized access to user data and credentials*
  - Vulnerabilities:
    - *Replay session based on intercepted tokens* (Security dimension: *communication security*)
    - *Weak encryption algorithms for password storage* (security dimension: *data confidentiality*)

Example Threat:
Account and Session Hijacking

- Controls:
  - **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.
  - **C6:** Store DFS passwords using strong salted cryptographic hashing algorithms.

Example Threat:
Account and Session Hijacking

- At the MNO:
  - Risk: *impersonation of authorised users*
  - Vulnerability: *Session timeouts not specified for DFS services*
    - Security dimension: *communication security*
  - Controls:
    - **C7:** Add session timeouts for USSD, SMS, application and web access to DFS services.

Example Threat: Account and Session Hijacking

- At the MNO (continued):
  - Risk: *unauthorised access to user data and credentials*
  - Vulnerability: *User credentials for DFS application are sent in inherently insecure ways like SMS or through agent*
    - Security dimension: *data confidentiality*

Example Threat:
Account and Session Hijacking

❑ Controls:

- ❑ **C8:** Where possible DFS users should set their own passwords at registration and these should be encrypted throughout the transmission to the DFS system. Where first time credentials are sent to the users, ensure DFS application credentials are sent to users directly without third-parties/agents. Users should then be required to set new passwords after first time logon.

Threats Currently Covered in Framework

- Account and Session Hijacking
  - Discussed above
- Attacks against Credentials
  - Threats designed to steal or tamper with credentials for users of DFS systems or mobile devices
- Attacks against Systems and Platforms
  - Attacks a remote adversary can carry out to spy on or modify information without insider access
- Code Exploitation Attacks
  - Threats aimed at the code comprising DFS applications
- Data Misuse Attacks
  - Relating to the mishandling of sensitive customer data

Threats Not Yet Enumerated

Compromise of DFS infrastructure	Denial of service
Compromise of DFS services	Insider Attacks
Man-in-the-middle attacks	Rogue devices
Signalling and control-channel attacks	SIM attacks
Unauthorized access to DFS data	Social engineering attacks
Unauthorized access to mobile devices	Zero-day attacks
Unintended disclosure of personal information	

FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

Thank You