

Security assurance framework for digital financial services (ITU-T X.1150)

24 April 2024

Heung Youl YOUM, Professor/PhD

Soonchunhyang University, Korea (Republic of)

Chair, ITU-T SG17

NOTE – This presentation is based on ITU-T X.1150 and drafting was supported by Mr. Junhyung Park, SCH University, Korea.

Security assurance framework for digital financial services

X.1150 (ex. X.saf-dfs)

Title

- Security assurance framework for digital financial services

Editors

- Prof. Heung Youl YOUM
- Mr. Junhyung Park
- MS. Sungchae Park

History

- Base line text published from ITU FIGI (Apr 2021)
- New Work Item Proposal (Aug 2021)
- TAP Determined (Sep 2023)
- **TAP Approval (March 2024)**

Provides an overview of the security threats and vulnerabilities facing the stakeholders in DFS ecosystem.

▪ Draft Recommendation ITU-T X.1150 (X.saf-dfs)↵

▪ Security assurance framework for digital financial services↵

▪ Summary↵

Digital financial service (DFS) involves a complex ecosystem with the participation of different stakeholders such as banks, DFS providers, mobile network operators (MNOs), DFS platform providers, regulators, agents, merchants, payment service providers, device manufacturers, application developers, token service providers, original equipment manufacturers (OEMs), and clients. The interconnectedness of these entities and reliance on several parties in the ecosystem extends the security boundaries beyond the DFS provider to customers, network providers, mobile phone manufacturer, and other third-party providers in the ecosystem.↵

A DFS security assurance framework identifies the security threats and vulnerabilities facing the applicable DFS stakeholders. Regulators including telecom authorities, banking, and payment regulators could also make use of the DFS security assurance framework to establish security.↵

This Recommendation describes a DFS security assurance framework which provides a systematic security risk management process to assess threats and vulnerabilities and identifies appropriate security controls to be implemented by the DFS stakeholders. Threats related to merchants, payment service providers and other financial services organizations and the specific mitigations for addressing the threats that they face are out of scope for this Recommendation.↵

The DFS security assurance framework consists of the following components:↵

- a) A security risk management process based on [b-ISO/IEC 27005].↵
- b) 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.↵
- c) Mitigation strategies based on the outcome of (b) above. The mitigation measures identify 119 security controls requirements for security threats which are outlined in clause 13 of this Recommendation.↵

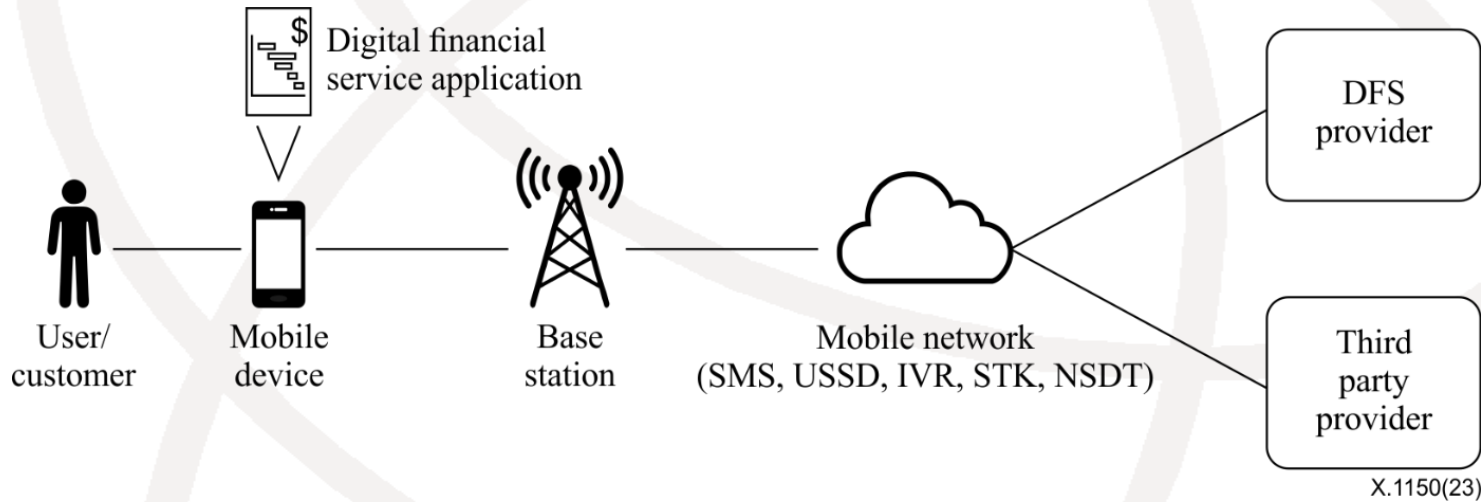
↵

▪ Keywords↵

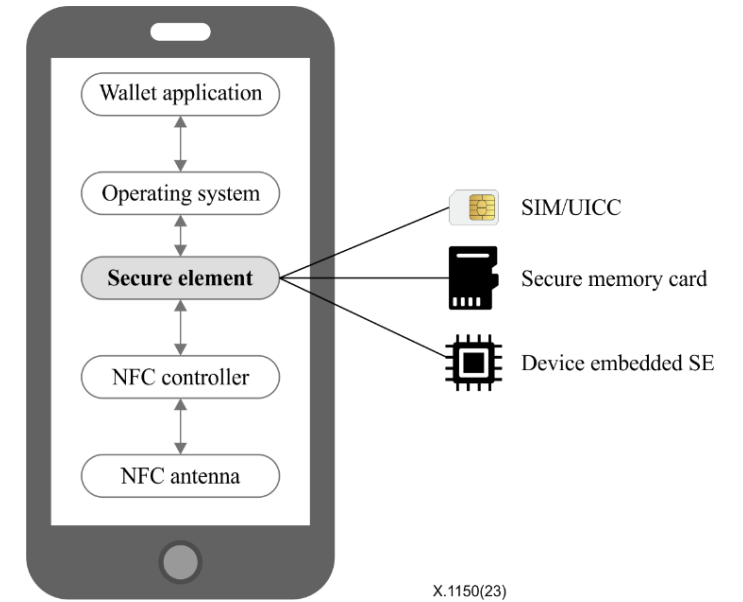
Business model, controls, digital financial services, security assurance, threats.↵

↵

Major elements of the DFS Ecosystem



Mobile device components



Source: ITU-T X.1150

Security assurance framework for digital financial services

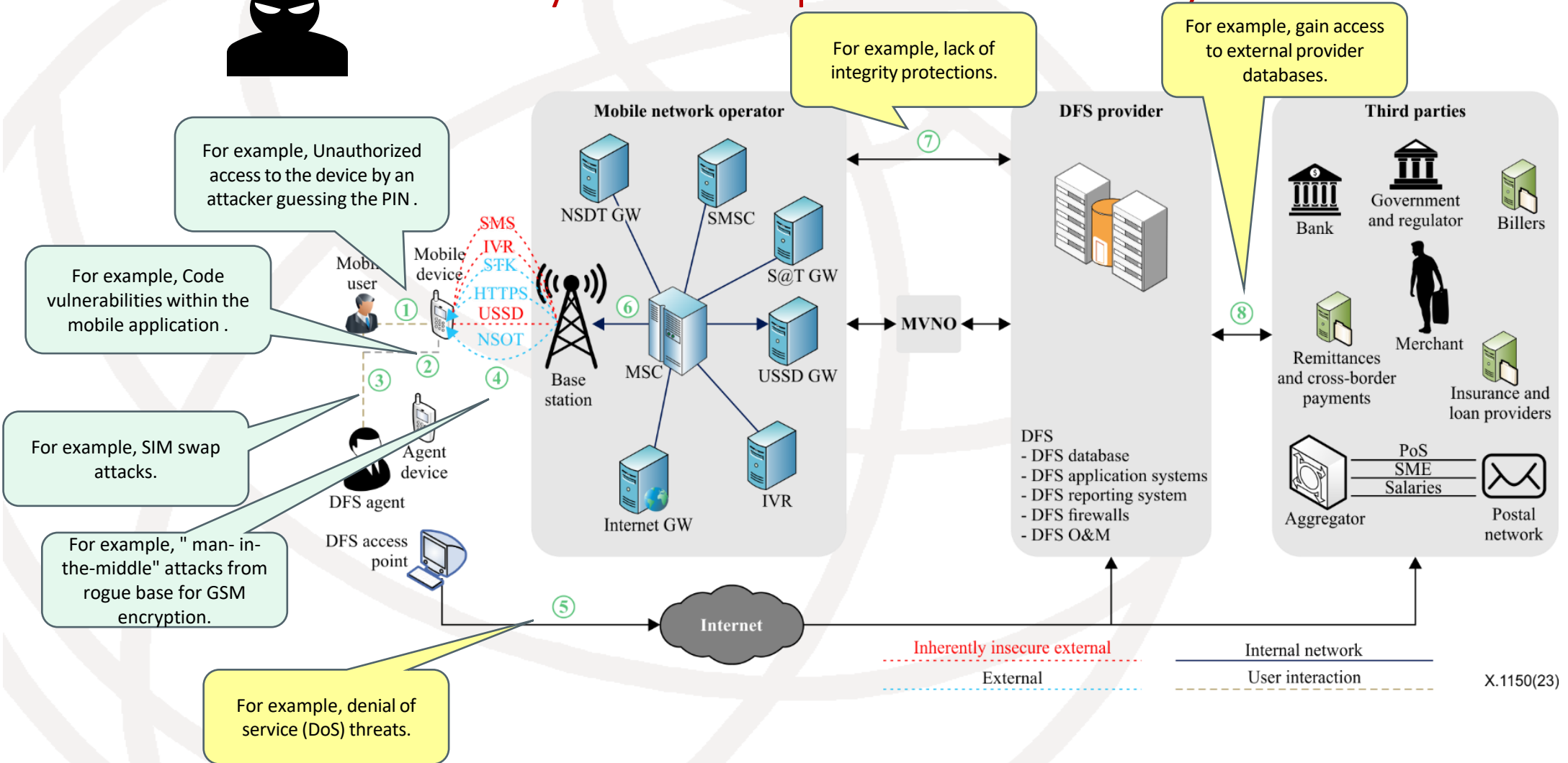
DFS Ecosystem - stakeholders

Element	Characteristic	Example
User	<ul style="list-style-type: none"> The target audience for a DFS service, who makes use of a mobile money application to interact with the service. 	Customers
Mobile Devices	<ul style="list-style-type: none"> The mobile device provides a platform for deploying a mobile money application It is the main channel through which the user 	Smartphone, Feature phone, Mobile terminal
Mobile Network	<ul style="list-style-type: none"> The carrier network provides transit connectivity for information originating at the user's devices. It is comprised of different nodes that enable communication to external providers and to DFS providers 	USSD, IVR, STK, SMS
DFS Provider	<ul style="list-style-type: none"> The DFS provider interfaces the application contents originating in mobile operator networks with the back-end financial providers and is used for administering the customers' information in a secure fashion, and allowing for services. 	Bank, Card company, securities company
3 rd party	<ul style="list-style-type: none"> 3rd party allows for the interfacing between carrier-based mobile money systems and provide the basis for connecting with back-end financial networks such as the banking infrastructure 	Fintech company, Payment company

Source: ITU-T X.1150

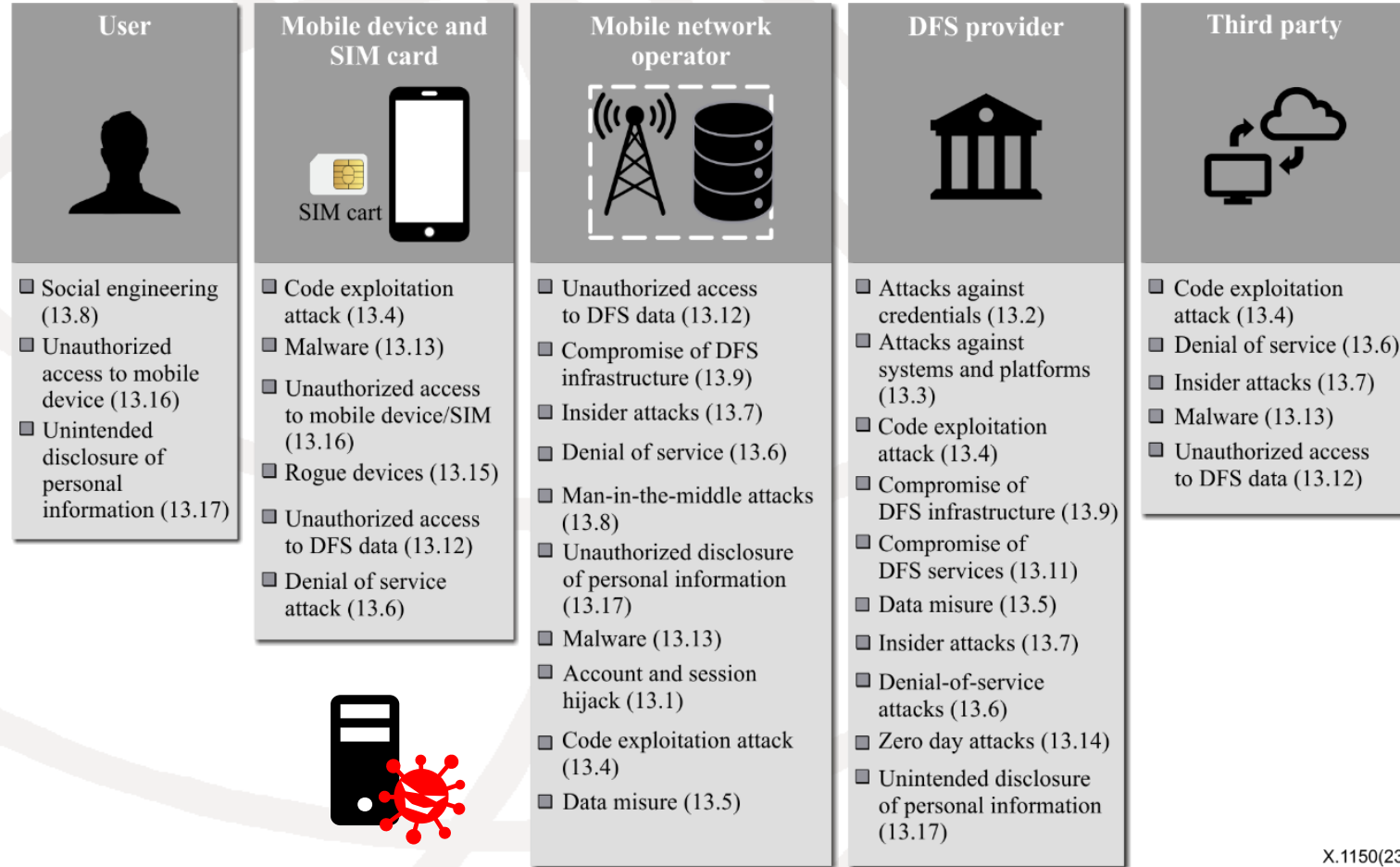
Security assurance framework for digital financial services

Ecosystems to map threats and security controls



Security assurance framework for digital financial services

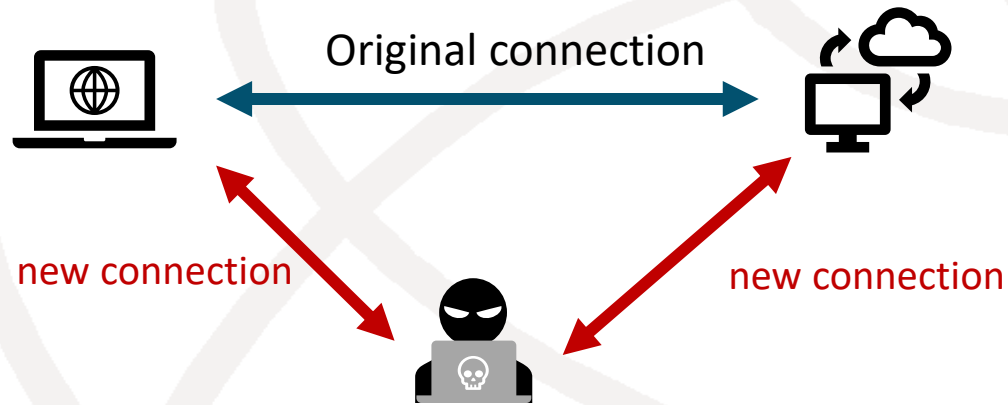
Typical Security threats



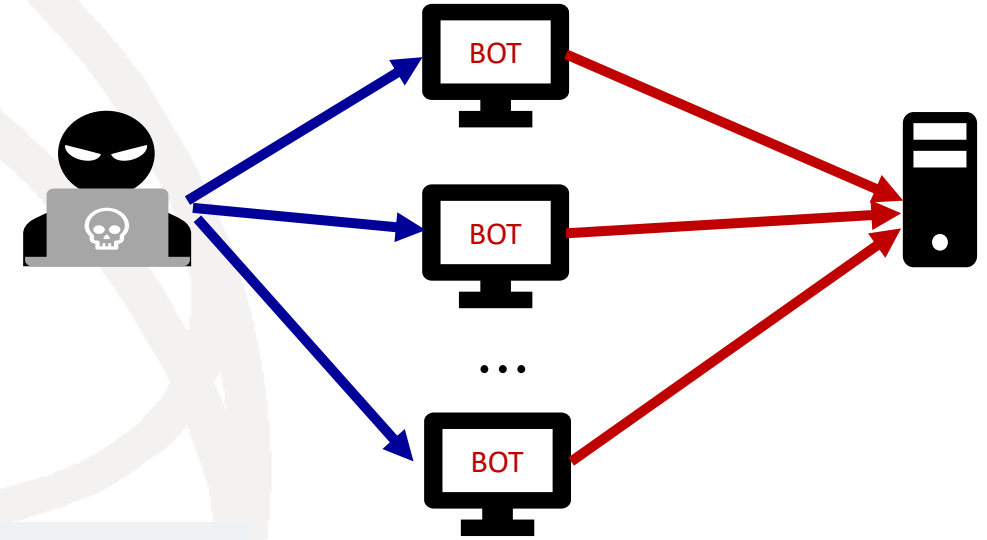
X.1150(23)

Typical attacks for DFS services

Man-in-the middle attacks



DDoS attacks



Insider attacks



(Source: Fortinet)

Security assurance framework for digital financial services

Security controls



Element	Threat	Control
User	Social engineering	Customer to access and download DFS applications through official application release channels to mitigate the risk of running malware-infected apps.
	Unauthorized access to mobile device	Mobile devices should automatically lock after a period of inactivity, forcing device authentication to be performed to unlock the device before it is used for DFS transactions.
	Unintended disclosure of personal information	DFS providers should ensure that customer data in production environments is not used in test environments unless anonymized according to best practices.
Mobile Devices	Code exploitation attack	Ensure that security libraries offered by the operating system are correctly designed and implemented and that the cipher suites they support are sufficiently strong.
	Malware	Deploy security software products on all mobile devices, including antivirus, antispymware, and software authentication products to protect systems from current and evolving malicious software threats.
	Unauthorized access to mobile device/SIM	Mobile devices should automatically lock after a period of inactivity, forcing device authentication to be performed to unlock the device before it is used for DFS transactions.
	Rogue devices	MNOs should monitor devices used to connect to or otherwise access the DFS system to ensure that such devices have the latest patches, updated antivirus software, are scanned for rootkits and key loggers, and do not support network extenders.
	Unauthorized access to DFS data	Ensure all sensitive consumer data such as PINs and passwords are securely stored with strong encryption with- in the internal network and while at rest to mitigate internal threats against this data.
	Denial of Service attack	MNOs should take steps to ensure network high network availability to allow access to DFS services through USSD, SMS, and the Internet.

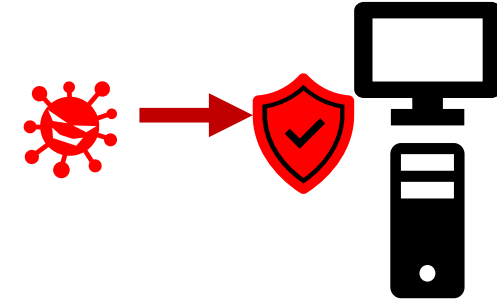
Source: ITU-T X.1150

Typical security controls for DFS services

Device authentication



Anti-virus, anti-malware products



DDoS mitigation solution






(Source: Imperva)

Security assurance framework for digital financial services



Security controls

Element	Threat	Control
Mobile Network Operator	Unauthorized access to DFS data	Ensure all sensitive consumer data such as PINs and passwords are securely stored with strong encryption with- in the internal network and while at rest to mitigate internal threats against this data.
	Compromise of DFS infrastructure	Use multi-factor or multi-model authentication for access to DFS accounts.  ★★★
	Insider attacks	Limit, control, and monitor physical access to sensitive physical DFS infrastructure.
	Denial of service attack	MNOs should take steps to ensure network high network availability to allow access to DFS services through USSD, SMS, and the Internet.
	Man-in-the-Middle attacks	MNOs should do CLI analysis for calls/SMS to detect calls and SMS that may be spoofed to appear like DFS provider calls.
	Unauthorized disclosure of personal information	DFS providers should ensure that customer data in production environments is not used in test environments unless anonymized according to best practices.
	Malware 	Deploy security software products on all mobile devices, including antivirus, antispysware, and software authentication products to protect systems from current and evolving malicious software threats. 
	Account and session hijacking	Add session timeouts for USSD, SMS, application, and web access to DFS services.
	Code exploitation attack	Ensure that security libraries offered by the operating system are correctly designed and implemented and that the cipher suites they support are sufficiently strong.
	Data misuse	Ensure all sensitive consumer data such as PINs and passwords are encrypted, when traversing the network and while the data is at rest.

Security assurance framework for digital financial services



Security controls

Element	Threat	Control
DFS Provider	Attack against credentials	Enforce a maximum number of login attempts to DFS accounts for back-end users, merchants, agents and DFS customers on DFS systems (database, OS, application).
	Attack against system and platforms	Avoid direct access by external systems to the DFS back- end systems by setting up a DMZ that logically separates the DFS system from all other internal and external systems.
	Code exploitation attack	Ensure that security libraries offered by the operating system are correctly designed and implemented and that the cipher suites they support are sufficiently strong.
	Compromise of DFS infrastructure	Use multi-factor or multi-model authentication for access to DFS accounts.
	Compromise of DFS services	Use strong multi-factor authentication for user and third party provider access to DFS systems.
	Data misuse	Ensure all sensitive consumer data such as PINs and passwords are encrypted, when traversing the network and while the data is at rest.
	Insider attacks	Limit, control, and monitor physical access to sensitive physical DFS infrastructure.
	Denial of service attacks	Inbound internet traffic should be limited and continuously monitored.
	Zero day attack	MNOs along with DFS providers and payment services providers should patch systems to the latest versions provided by the vendor to defend against attacks that have been developed from older vulnerabilities.
Unintended disclosure of personal information	DFS providers should ensure that customer data in production environments is not used in test environments unless anonymized according to best practices. Conversely, test data should not be migrated to the product.	



Source: ITU-T X.1150

Security assurance framework for digital financial services



Security controls

Element	Threat	Control
3 rd party	Code exploitation attack	Ensure that security libraries offered by the operating system are correctly designed and implemented and that the cipher suites they support are sufficiently strong.
	Denial of service attack	Inbound internet traffic should be limited and continuously monitored.
	Insider attacks	Limit, control, and monitor physical access to sensitive physical DFS infrastructure.
	Malware	Deploy security software products on all mobile devices, including antivirus, antispysware, and software authentication products to protect systems from current and evolving malicious software threats.
	Unauthorized access to DFS data	DFS Providers/Merchants should consistently dispose of old devices.

Security assurance framework for digital financial services

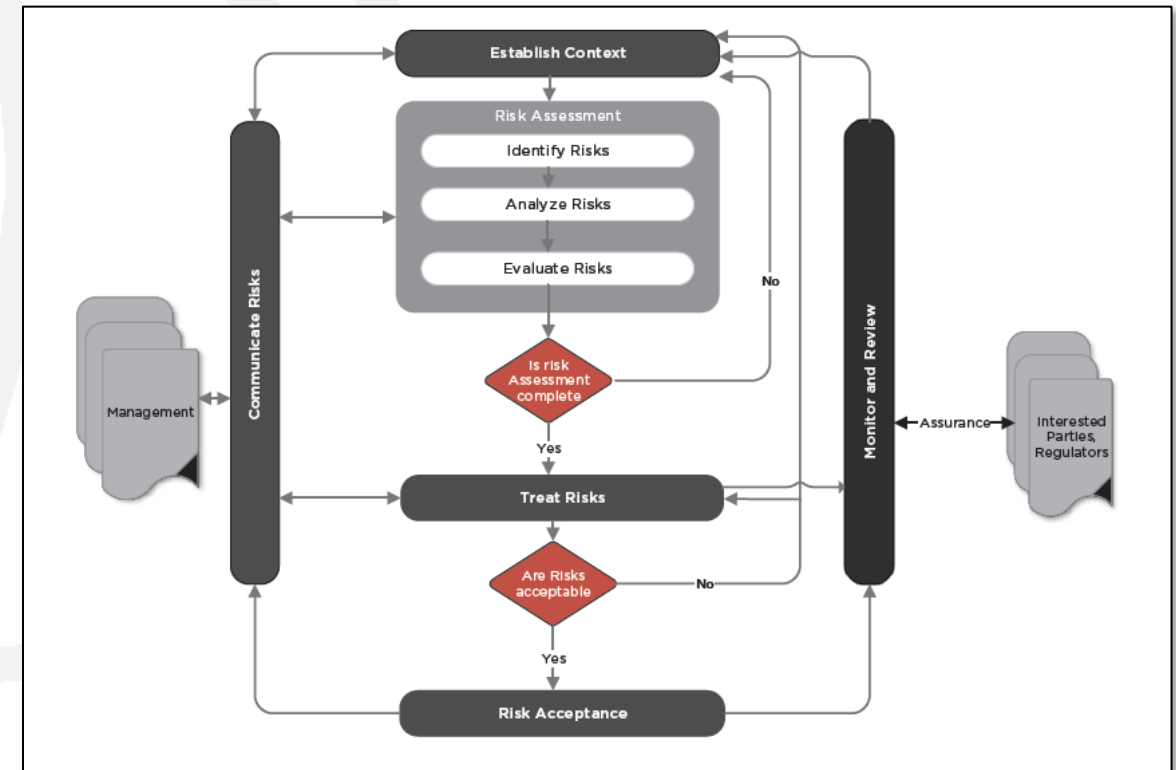
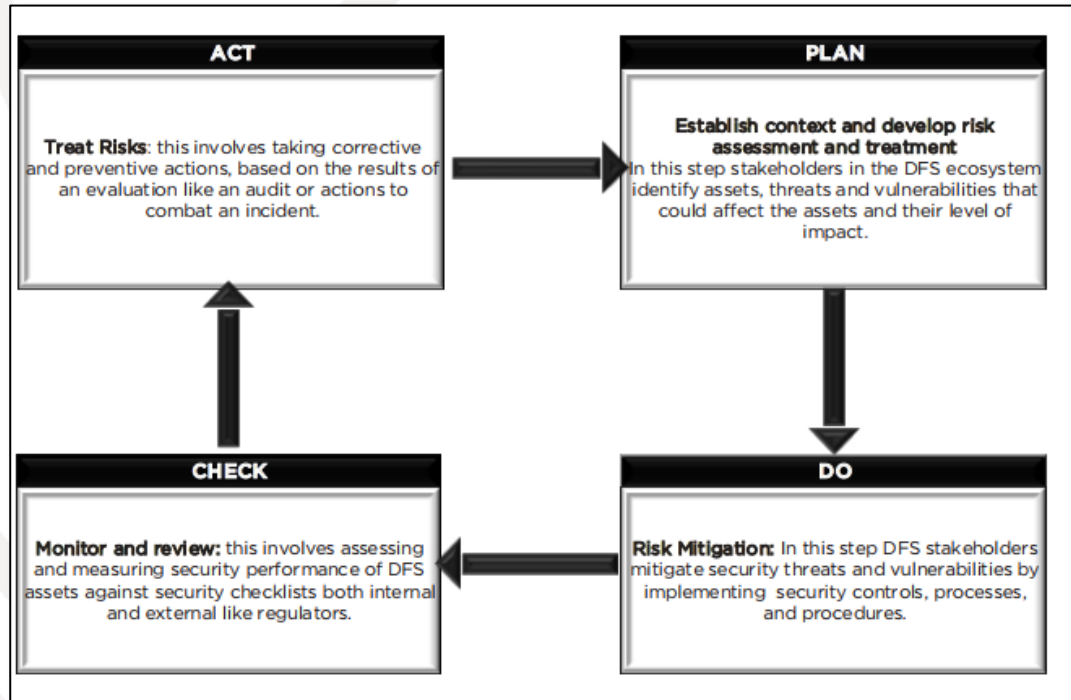
DFS Security assurance framework

- DFS security assurance framework follows similar principle from:
 - **ISO/IEC 27000**
 - Payment Card Industry Data Security Standard(PCI-DSS) v 3.2
 - Payment Application Data Security Standard(PA-DSS)
 - **NIST 800-53**
 - Technical guidelines from Centre for Internet Security(CIS) controls V.7
 - OWSAP
- DFS security assurance framework consist of the following components:
 - **A security risk assessment based on ISO/IEC 27005 (Clause 12)**
 - Assessment of threat and vulnerabilities to the underlying stakeholders in DFS ecosystem.
 - Mitigation strategies based on the outcome of assessment of threats and vulnerabilities
- **DFS security assurance framework identifies:**
 - **The various security threat to DFS assets**
 - **The related vulnerabilities that can be exploited by these threats**
 - **Security controls**

Security assurance framework for digital financial services

Security risk management process

- In order to ensure a security model that is sustainable and continuously improves DFS security, this framework uses PDCA.
- Each figure shows PDCA step and high-level risk management process plan based on the PDCA.



Security assurance framework for digital financial services

DFS Security incident management

- Often even after relevant controls have been applied security incidents do occur, especially in financial services where attackers have a financial motive to evade systems, this causes system disruption, alteration or disclosure of data.
- Organizations and stakeholders offering and involved in digital financial services need to develop the right procedures, reporting, data collection, management responsibilities, legal protocols, and communications strategies that will allow the organization to successfully understand, manage, and recover from security incidents
- A security incident management plan defines consistent procedures to be followed for orderly, quick and effective reporting, response analysis, investigation and recovery from security incidents that compromise any of the ten security dimensions.

DFS Security incident management

No	DFS Security incident management
1	Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management
2	Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution
3	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles
4	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification
5	Assemble and maintain information on third party contact information to be used to report a security incident, such as law enforcement, relevant government departments, vendors and device manufactures
6	Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities
7	Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real-world threats. Exercises should test communication channels, decision-making, and incident responder's technical capabilities using tools and data available to them
8	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures
9	Establish a disaster recovery system to prevent business disruption incidents such as natural disaster or cyber attacks to DFS systems
10	Respond to security incidents using a (SOAR) platform which collects threat-related data and automates threat responses

Source: ITU-T X.1150

Conclusion

- DFS is an industry that handles sensitive information along with customer and corporate assets.
- Due to the nature of the DFS industry, if a cyber threat occurs, it can cause great damage, so security must be considered a top priority.
- An assurance framework in X.1150 should be used to identify security threats that may occur in DFS and to establish controls for them.
- Monitor new cyber threats and find ways to respond to them should be conducted.
- Providing security and privacy assurance is critical for Fintech services.
- Using standardized method for incident management and risk assessment are important to provide the interoperable Fintech service.

A large, faint, light gray globe graphic is centered in the background of the slide, composed of several overlapping curved lines representing latitude and longitude.

Thank you for your attention