Implementing the DFS security assurance framework and security audit for DFS.

November 2021

Mobile Network Operator

Communication Security

Synopsis: Telecom operators are concerned with providing secure communication for DFS transactions.

The DFS Security audit guideline can be used to:

- Identify some of common risks & vulnerabilities to communication security and controls to mitigate them.

The DFS audit guideline can assist to:

- Assess/audit/evaluate whether sufficient controls are in place?

DFS providers, DFS providers, 3PP

Data protection, transaction integrity, application security

Synopsis: Banks are generally concerned with whether DFS providers are adequately protecting consumer's financial data and transactions.

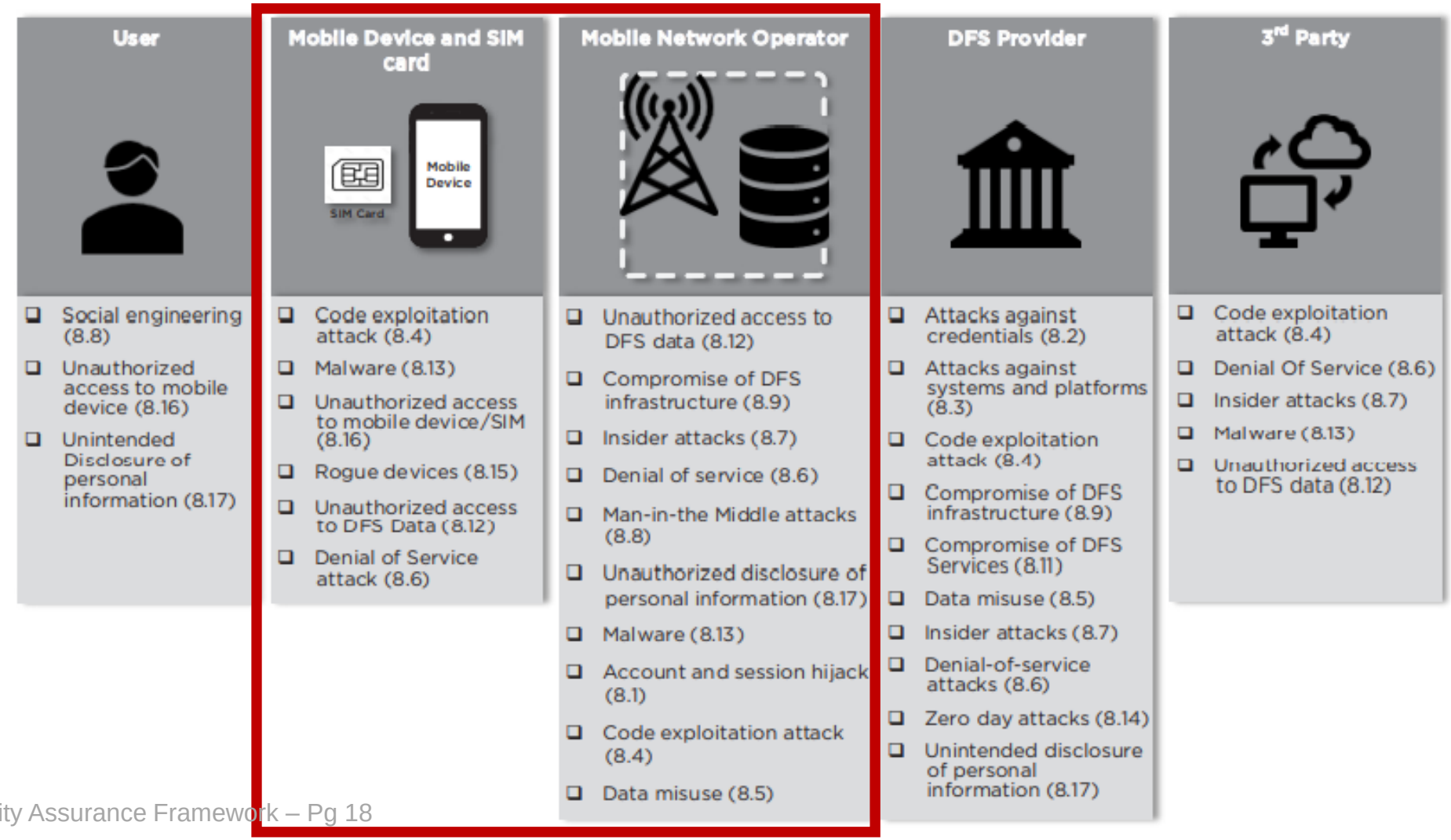
The DFS security assurance framework can be used to:

- Identify controls to adopt to protect digital financial services data, transactions and applications from attacks

The DFS audit guideline can assist to:

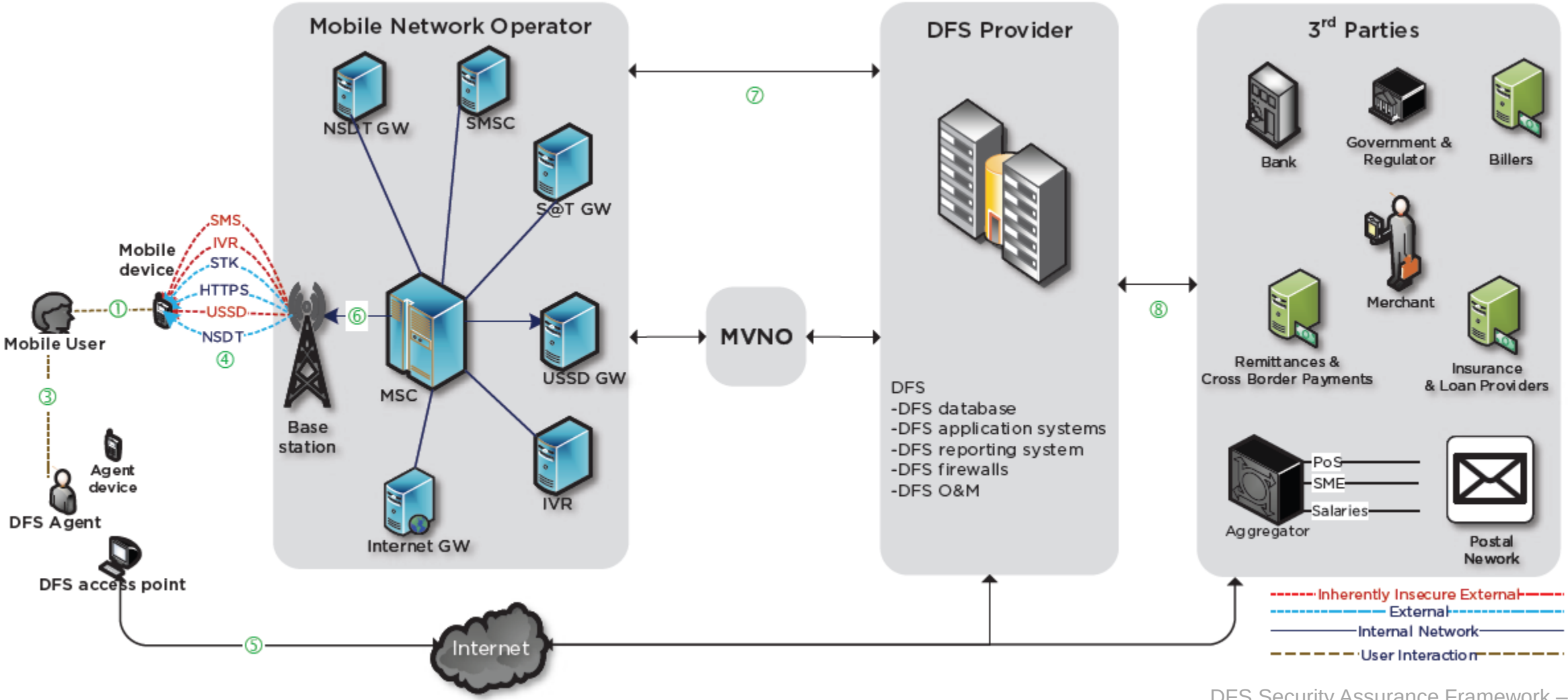
- Assess/audit/evaluate whether sufficient controls are in place
  - audit checklist/questions.
  - relevant policies and procedures

Common risks & vulnerabilities to communication security



Common risks & vulnerabilities to communication security

Figure 14 - Mapping of threats to security controls



DFS Security Assurance Framework – Page 26

Common risks & vulnerabilities to communication security

8.1 Threat: Account and Session Hijacking

The general threat here is the ability of an attacker to take control of an account or communication session. The vulnerabilities are manifested in different ways at the DFS provider and the MNO.

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 confi-	**C6:** Store DFS passwords using strong salted cryptographic hashing algorithms.
MNO	The risk of ***Impersonation of authorised users*** occurs because of the following vulnerability: - Session timeouts not specified for DFS services	**C7:** Add session timeouts for USSD, SMS, application, and web access to DFS services.
	The risk of ***unauthorized access to user data and credentials*** occurs due to the following vulnerability: - User credentials for DFS application are sent in inherently insecure ways like SMS or through agents (SD: data	**C8:** Where possible, DFS users should set their own passwords at registration and they 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 the first-time login

DFS Security Assurance Framework – Page 35

Common risks & vulnerabilities to communication security

Affected entity	Risks and vulnerabilities	Controls
MNO	The risk of ***unauthorized access to user data*** is due to the following vulnerability: - Weak over-the-air encryption (SD: communication security)	**C38:** 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.

Affected Entity	Risks and vulnerabilities	Controls
MNO	The risk of ***interception of DFS data in transit*** occurs because of the following vulnerabilities:	**C70**: Ensure all sensitive consumer data such as PINs and passwords are securely stored with strong encryption within the internal network and while at rest to mitigate internal threats against this data.
	- Inherent SS7 security weakness[6] (SD: Communication Security)	**C71:** Use firewalls to detect and limit attacks based on SS7 security flaws.
	- Interception of MO-USSD transactions (SD: Communication Security)	**C72:** Check if the IMEI of the device performing the transaction matches the registered IMEI of the account holder's phone (a MITM system may clone the SIM with a different IMEI)
	- Unprotected sensitive traffic and weak encryption practices (SD: Communication Security)	**C73:** Monitor user velocity by comparing the location of the phone used to perform transactions to the last reported location of the phone (last in/out SMS or call).
		C74: MNO's should enforce the use of the Personal Unlocking Key (PUK) on the SIM card for additional security in case the mobile device is lost or stolen.
		C75: Control and monitor the use of MSC MAP tracing and protocol analysers on USSD, SMS infrastructure to internal limit access to plain text SMS and USSD traffic in transit
		C76: Use 2-way SecureOTP to the original phone number to verify the legitimacy of the transaction[7]
		C77: Employ strong cryptography practices to assure confidentiality and integrity of data as it enters the DFS provider network and as it is processed and stored within this environment.
		C78: Limit number of DFS sessions per user. Allow a single session per user at a time irrespective of the access channel (STK, USSD, or https); a DFS user account should not be accessible using multiple channels simultaneously.
		C79: The mobile operator should deploy SS7 and diameter signalling security controls specified by the GSMA (FS.11, FS.07, IR.82, and IR.88) to limit threats due to SS7 attacks[8]

Mobile Network Operator

Communication Security

Synopsis: Telecom operators are concerned with providing secure communication for DFS transactions.

The DFS Security audit guideline can be used to:

- Identify some of common risks & vulnerabilities to communication security and controls to mitigate them.

The DFS audit guideline can assist to:

- Assess/audit/evaluate whether sufficient controls are in place?

DFS audit guideline page 15

Assessing controls on communication security:

Impacted DFS Entity	Group	Risk and vulnerability	Control	Security audit question	Applicable policy or procedure
MNO	Network security	- Weak over-the-air encryption (SD: communication security)	C38: 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.	Has the use of known weak ciphers been discontinued? Has the deployment been prepared for new ciphers?	Communications security: Information transfer
MNO	Fraud detection	- 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.	Are there mechanisms to detect SMS and ca spoofing? E.g., CLI analysis?	Communications security: Information transfer
MNO	Network Security	- Inherent SS7 security weakness[iii] (SD: Communication Security)	C70: Ensure all sensitive consumer data such as PINs and passwords are securely stored with strong encryption algorithms within the internal network and while at rest to mitigate internal threats against this data.	Are the encryption algorithms and keys used are strong enough to protect customer PINs and data?	Cryptography - Cryptographic controls
MNO	Network Security	- Inherent SS7 security weakness[iii] (SD: Communication Security)	C71: Use firewalls to detect and limit attacks based on SS7 security flaws.	Does the MNO have a firewall in place to detect and protect against external SS7 base attacks? For example (firewall protection against subscriber traffic interception, unauthorized USSD and SM use)	Communications security - Network security management
MNO	Access control	- Interception of MO-USSD transactions (SD: Communication Security)	C72: Check if the IMEI of the device performing the transaction matches the registered IMEI of the account holder's phone (a MITM system may clone the SIM with a different IMEI)	Is the DFS provider performing real time device validation before transaction processing?	Access control Policy - System and application access control
MNO	Network security	- Unprotected sensitive traffic and weak encryption practices (SD: Communication Security)	C73: Monitor user velocity by comparing the location of the phone used to perform transactions to the last reported location of the phone (last in/out SMS or call).	Is the DFS provider performing user transaction geo-velocity checks before transaction processing?	Access control Policy - System and application access control
MNO	Network Security	- Unprotected sensitive traffic and weak encryption practices (SD: Communication Security)	C74: MNO's should enforce the use of the Personal Unlocking Key (PUK) on the SIM card for additional security in case the mobile device is lost or stolen.	Does the MNO enforce use of the Personal Unlock Key on SIM cards to reduce the risk associated with stolen SIMs that are used for DFS?	Communications security - Information transfer

DFS audit guideline:
Page 22

Assessing controls on communication security:

4.5.1 Are all devices used to connect to DFS systems scanned for threats and checked for the latest software patches?
4.5.2 Are code changes tested and approved before moving it into production? For example, user and internal acceptance certificates that show that the code was tested.
4.5.3 Are encryption keys were changed from default at installation? Are default SNMP strings changed?
4.5.4 Are the clocks within the DFS ecosystem synchronized?
4.5.5 Are the DFS systems patched against known vulnerabilities?
4.5.6 Are the DFS systems updated to the latest versions to protect against new threats?
4.5.7 Are the encryption algorithms and keys used are strong enough to protect customer PINs and data?
4.5.8 Are the firewall rules adequately configured? e.g. port whitelisting, packet filtering
4.5.9 Are there adequate protections against network attacks like firewalls and traffic filters with proper configurations?
4.5.10 Are there logical boundaries that limit access to the DFS systems from all other systems? (For example, are other unauthorized internal users logically and/physically limited on the network from accessing DFS processing systems)
4.5.11 Are there operational controls to detect threats associated with APIs? Are there controls in place to detect rouge/malicious APIs?

4.5.16 Does the MNO enforce use of the Personal Unlock Key on SIM cards to reduce the risk associated with stolen SIMs that are used for DFS?
4.5.17 Does the MNO have a firewall in place to detect and protect against external SS7 based attacks? For example (firewall protection against subscriber traffic interception, unauthorized USSD and SM use)
4.5.18 Does the MNO operator have controls in place to limit access to MAP tracing and use of protocol analysers on the internal network? (SMS and USSD messages are transmitted in plain text in the MAP protocol)
4.5.19 Has MNO implemented the SS7 and diameter signaling controls to protect against SS7 vulnerabilities?
4.5.20 Has the use of known weak ciphers been discontinued? Has the deployment been prepared for new ciphers?
4.5.21 Is the DFS provider performing input validation checks?
4.5.22 Is the DFS provider performing user transaction geo-velocity checks before transaction processing?
4.5.23 Is there adequate monitoring of traffic for internet facing DFS applications?
4.5.24 Is there regular penetration testing of the DFS systems?
4.5.25 Is TLS encryption used secure? i.e., v.12 or higher (July 2020) Does the app use latest versions of TLS? Does the app use any deprecated TLS version?
4.5.26 Is transaction validation performed using secure OTP?

DFS providers, DFS providers, 3PP

Data protection, transaction integrity, application security

Synopsis: Banks are generally concerned with whether DFS providers are adequately protecting consumer's financial data and transactions.

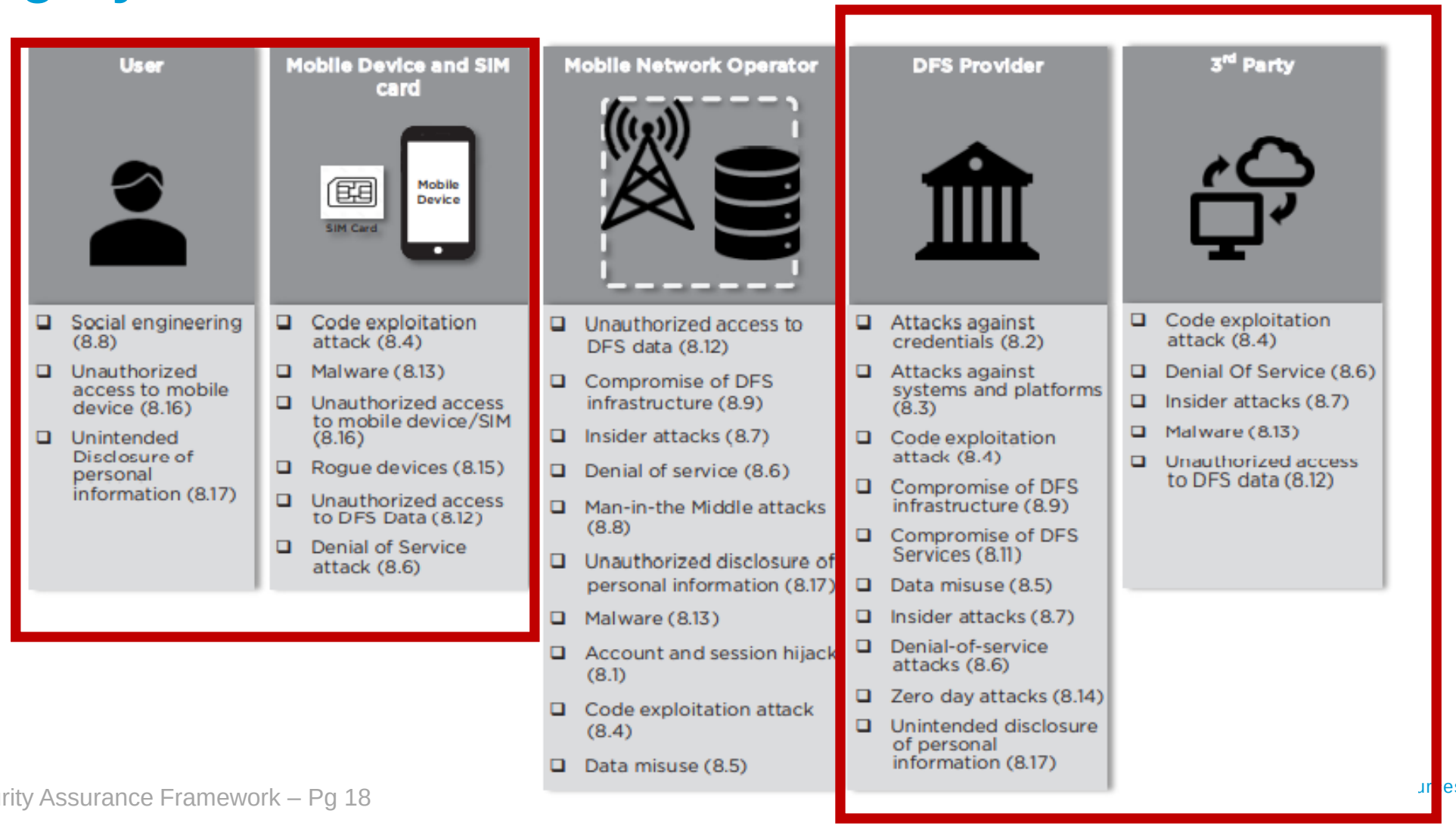
The DFS security assurance framework can be used to:

- Identify controls to adopt to protect digital financial services data, transactions and applications from attacks

The DFS audit guideline can assist to:

- Assess/audit/evaluate whether sufficient controls are in place?
  - Provides an appropriate audit checklist.
  - Identifies an appropriate se

Common risks & vulnerabilities to application security & data integrity



Thank you!