FIGI

FINANCIAL INCLUSION
GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services security audit guideline

REPORT OF SECURITY WORKSTREAM

Security, Infrastructure and Trust Working Group

Digital Financial Services security audit guideline

03/2021

DISCLAIMER

The Financial Inclusion Global Initiative (FIGI) is a three-year program implemented in partnership by the World Bank Group (WBG), the Committee on Payments and Market Infrastructures (CPMI), and the International Telecommunication Union (ITU) funded by the Bill & Melinda Gates Foundation (BMGF) to support and accelerate the implementation of country-led reform actions to meet national financial inclusion targets, and ultimately the global 'Universal Financial Access 2020' goal. FIGI funds national implementations in three countries – China, Egypt and Mexico; supports working groups to tackle three sets of outstanding challenges for reaching universal financial access: (1) the Electronic Payment Acceptance Working Group (led by the WBG), (2) The Digital ID for Financial Services Working Group (led by the WBG), and (3) The Security, Infrastructure and Trust Working Group (led by the ITU); and hosts three annual symposia to gather national authorities, the private sector, and the engaged public on relevant topics and to share emerging insights from the working groups and country programs.

This report is a product of the FIGI Security, Infrastructure and Trust Working Group, led by the International Telecommunication Union.

The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Financial Inclusion Global Initiative partners including the Committee on Payments and Market Infrastructures, the Bill & Melinda Gates Foundation, the International Telecommunication Union, or the World Bank (including its Board of Executive Directors or the governments they represent). The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted; the names of proprietary products are distinguished by initial capital letters. The FIGI partners do not guarantee the accuracy of the data included in this work. The boundaries, colours, denominations, and other information shown on any map in this work do not imply any judgment on the part of the FIGI partners concerning the legal status of any country, territory, city or area or of its authorities or the endorsement or acceptance of such boundaries.

© ITU 2021
Some rights reserved. This work is licensed to the public through a Creative Commons Attribution-Non-Commercial-Share Alike 3.0 IGO license (CC BY-NC-SA 3.0 IGO).
Under the terms of this licence, you may copy, redistribute and adapt the work for non-commercial purposes, provided the work is appropriately cited. In any use of this work, there should be no suggestion that ITU or other FIGI partners endorse any specific organization, products or services. The unauthorized use of the ITU and other FIGI partners' names or logos is not permitted. If you adapt the work, then you must license your work under the same or equivalent Creative Commons licence. If you create a translation of this work, you should add the following disclaimer along with the suggested citation: "This translation was not created by the International Telecommunication Union (ITU). ITU is not responsible for the content or accuracy of this translation. The original English edition shall be the binding and authentic edition". For more information, please visit https://creativecommons.org/licenses/by-nc-sa/3.0/igo/

About this report

This report was written by Kevin Butler, University of Florida. The author would like to thank Vijay Mauree and Arnold Kibuuka, ITU and Rehan Masood, State Bank of Pakistan for their guidance and assistance in the report's review and edits. The author would also like to thank the FIGI Security Infrastructure and Trust working group members for their contributions and comments.

If you would like to provide any additional information, please contact Vijay Mauree at tsbfigisit@itu.int.

Contents

Acronyms

API	Application Programming Interface
DFS	Digital Financial Services
DMZ	Demilitarized Zone
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
MD	Message Digest
MFA	Multi-Factor Authentication
MNO	Mobile Network Operator
MSISDN	Mobile Station International Subscriber Directory Number
NTP	Network Time Protocol
OTP	One Time Password
PKI	Public Key Infrastructure
POS	Point of Sale
RBAC	Role Based Access Control
SD	Security Dimension
SHA	Secure Hash Algorithms
SE	Secure Element - A formally certified, tamper-resistant, stand-alone integrated circuit often referred to as a "chip" as defined by the European Payments Council or other recognized standards authority.
SIM	Subscriber Identity Module
SMS	Short Messaging Service
STK	SIM Toolkit
XML	Extensible Markup Language
USSD	Unstructured Supplementary Service Data

Digital Financial Services security audit guideline

1 INTRODUCTION

The Digital Financial Services (DFS) Security Audit Guidelines complements the *DFS Security Assurance Framework* [1], to help stakeholders determine and identify security control deficiencies within the DFS infrastructure. The guidelines are based on the DFS Security Assurance Framework which provides a systematic security risk management process for identifying threats and vulnerabilities. The DFS Security Assurance Framework also proposes security control measures that should be implemented by the DFS provider, mobile network operator, and other third parties within the ecosystem.

In a DFS application, a deficiency in any one of the controls increases the likelihood of a breach of privacy, access to DFS data, confidentiality, user authentication and authorisation, DFS service availability, fraud (internal and external) network security. The audit checklist can be used by DFS regulators, providers, and operators in assessing whether the controls in the DFS Security Assurance Framework are present and functioning as intended.

2 DFS SECURITY AUDIT GUIDELINE

The DFS security audit guidelines are categorised into six different groups that a regulator, internal/external application security auditor, mobile network operator, or DFS provider can use to assess the implemented DFS security assurance control measures. Each group provides a series of questions that the auditor can use as a checklist for the security audit of the DFS infrastructure.

DFS Security audit Guidelines are categorised into the following groups:

i) Access control

Audit guidelines in this group assess whether sufficient selective restrictions on appropriate access to DFS associated systems, services, resources, and controls are in place to guarantee protection against unauthorized use of network resources.

ii) Authentication

Audit guidelines in this group assess a DFS application's capability to verify the authenticity of the users.

iii) Availability

Audit guidelines in this group assess the DFS infrastructure and application for reliability and ability to grant timely access to authorised DFS users. The application and infrastructure are validated for resistance to denial-of-service attacks.

iv) Fraud detection

Audit guidelines in this group to assess the controls in place within the DFS systems to detect intentional and unlawful interception by internal or external entities to obtain customer personal data and steal customer funds from a DFS system.

v) Network security

Audit guidelines in this group assess the controls in place to protect the underlying network infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure. These can also be used to test whether information only flows between authorized endpoints without being diverted or intercepted.

vi) Privacy and confidentiality

Audit guidelines in this group assess the controls in place to protect DFS participants/user's data from unauthorised disclosure, including data protection that might be derived from observing network activity.

The DFS security audit guideline is structured in the format below:

Impacted DFS Entity	**Group**	**Risk and Vulnerability**	**Control**	**Security audit question**	**Applicable policy or procedure**

The table above shows the DFS security risks and vulnerabilities, the DFS entities affected by those risks, controls to mitigate the risks, the security audit question an auditor would ask and the respective policy and procedure.

- The "*Impacted DFS entity*" lists the entity affected by the risk and vulnerability within the DFS ecosystem.
- The "*Risk and vulnerability*" column **outlines** the threats that an entity within the DFS ecosystem will face based on the eight security dimensions (SD).
- The "control" column lists the DFS **controls** for each of the DFS entities within the ecosystem.
- The "*Security audit question*" column **outlines** the auditor's question for compliance checking of the specific control.
- The "*Applicable policy or procedure*" column suggests the applicable policy or procedure documents that guide the day-to-day actions and strategies of a particular entity based on ISO/IEC 27001- Information Security Management [2].

The structure table above is elaborated in section 3 and includes the detailed audit checklist for all the security controls in DFS security assurance framework. The table outlines the various security checks that need to be undertaken at the DFS provider and mobile network operator level to verify compliance. This table can be used as a guideline by telco and financial services regulators, security auditors, and DFS providers for internal and external security audits.
Section 4 describes the process the security auditors may adopt by outlining a series of questions from Table 1 grouped by category for easy reference.

3 DFS SECURITY ASSURANCE FRAMEWORK CONTROLS AND AUDIT GUIDELINE

The guideline includes a checklist with questions that the auditor can use to evaluate the security controls.

Impacted DFS Entity	Group	Risk and vulnerability	Control	Security audit question	Applicable policy or procedure
DFS Provider	Access Control	- 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	Are the following logical controls set for DFS user sessions: i) auto logouts and session time out ii) Maximum failed password login attempts iii) Password and PIN complexity. iv) Password/PIN reuse periods	Access control Policy - System and application access control
DFS Provider	Access Control	- Inadequate controls on dormant accounts (SD: authentication)	C2: Require user identity validation for dormant DFS accounts users before re-activating accounts.	Is there a sufficient way of validating user identity before activating previously dormant accounts for example biometric validation?	Access control Policy - User access management
DFS Provider	Access Control	- 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.	Does the DFS system have capability to detect out-of-pattern transactions based on customer profile? For example: Does the DFS provider check authenticity of transactions using location-based validation of transactions, for example through geo-velocity tracking or other means?	Access control Policy - System and application access control
DFS Provider	Access control	- 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.	Has the DFS provider limited concurrent user logins and provided the option for customers to opt into other login channels? For example, are customers who use USSD able to optionally choose to use a DFS app channel before the DFS provider activates access through this channel?	Access control Policy - System and application access control
DFS Provider	Authentication	- 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.	Does the DFS provider enforce server-based authentication for all access requests?	Access control Policy - System and application access control
DFS Provider	Privacy and Confidentiality	- Weak encryption algorithms for password storage (SD: data confidentiality)	C6: Store DFS user passwords using strong salted cryptographic hashing algorithms.	Is there a mechanism in place to ensure that data-at-rest is encrypted and stored securely?	Data Security and Data Leakage Prevention Standard
MNO	Access Control	- Session timeouts not specified for DFS services	C7: Add session timeouts for USSD, STK application, and web access to DFS services.	Has the DFS provider set USSD and STK DFS sessions to automatically disconnect after a set period of user inactivity?	Access control Policy - System and application access control
MNO	Access control	- User credentials for DFS application are sent in inherently insecure ways like SMS or through agents (SD: data confidentiality)	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.	Is the password transmitted securely? Is the user required to change password after first time login?	Access control Policy - User access management
	Access control	- Failure to perform login monitoring, leaving systems susceptible to brute force attacks (SD: access control)	C12: 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)	Is there a maximum number of failed login attempts set before account is locked?	Access control Policy - System and application access control
MNO	Authentication	- Insecure transfer of customer credentials (SD: access control)	C14: DFS providers should transmit the user authentication credentials securely over a different channel (out of band).	Are DFS user authentication credentials transmitted via a different channel/out-of-band? (e.g. if account setup is done via USSD channel are one-time passwords transmitted via e-mail or voice calls?)	Access control Policy - System and application access control

(continued)

Impacted DFS Entity	Group	Risk and vulnerability	Control	Security audit question	Applicable policy or procedure
MNO	Network Security	- Exposure of internal network to external adversaries (SD: access control)	C15: Use Network Address Translation to limit external exposure of DFS IP address and routing information.	Are there technical controls in place to limit exposure of internal DFS systems addresses (like database IP addresses?	Communications Security Policy - Network security management
DFS Provider	Network Security	- Insufficient protection of internal systems against external adversaries (SD: access control)	C16: Avoid direct access by external systems to the DFS backend systems by setting up a DMZ that logically separates the DFS system from all other internal and external systems.	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)	Communications Security Policy - Network security management
DFS Provider	Privacy and Confidentiality	- Reliance by DFS application on security libraries offered by operating systems (SD: communication security)	C17: Ensure that security libraries offered by the operating system are correctly designed and implemented and that the cipher suites they support are sufficiently strong.	Are the cryptographic libraries used by the operating system or by the application correctly designed and implemented and are they up to date? Do the cryptographic libraries support strong cryptographic ciphersuites and do they prevent or discourage use of weak ciphersuites? Are hashing algorithms used that have not been deprecated and are adequate digest lengths supported? (Anything less than SHA512 is considered weak today. MD5 and SHA1 have been broken.)	Cryptography policy - Cryptographic controls
				For symmetric encryption ciphers, are strong ciphers used and are adequate key lengths supported? (For example, AES is considered secure to use while 3-DES is no longer a preferred cipher because of the SWEET-32 attack, and it is encouraged to move away from it to AES as soon as possible.) - For public-key encryption, are key lengths chosen to be an appropriate size for the public key algorithm being used?	
				Are the criteria used for selecting cryptographic algorithms and key sizes based on public and well-examined standards? (For example, NIST 800-57 special publication has guidelines on minimum key sizes for each algorithm and how long this key size is good for)	
MNO	Privacy and Confidentiality	- Weak encryption practices or sending sensitive information in clear text over insecure traffic channels like SMS and USSD (SD: communication security)	C18: Ensure all sensitive consumer data such as PINs and passwords are encrypted, when traversing the network and while the data is at rest.	Has all sensitive consumer data been encrypted by the application or the operating system? Are unencrypted versions of the data accessible in the device, for example, in temporary buffers or in memory? Is all information sent over a network connection encrypted with a strong encryption cipher? (See C17 for more discussion of what comprises a strong encryption cipher.)	Cryptography policy - Cryptographic controls
DFS Provider and Third-party providers	Fraud Detection	- Inadequate data protection controls (SD: privacy)	C19: Remove customer sensitive data from trace logs. Examples of data that should be removed include cash retrieval voucher codes, bank account numbers, credentials. Instead, use place holders, where possible, to represent this data in logs.	Do trace logs and event data records capture/store sensitive user data? (e.g. are customer PINs stored in EDRs)	Operations security - Logging and monitoring
DFS Provider and Third-party providers	Privacy and Confidentiality	- Exposure of customer sensitive information during transactions or through APIs (SD: privacy)	C20: DFS providers should restrict sharing of DFS user information to the minimum amount required for transactions with third parties and service providers.	Is there limitation on customer sensitive information shared during transaction processing with third parties? (e.g. Only information needed for processing the transaction is shared with the third party)	Operations security policy - Operational procedures and responsibilities

(continued)

Impacted DFS Entity	Group	Risk and vulnerability	Control	Security audit question	Applicable policy or procedure
DFS Provider and Third-party providers	Fraud Detection	- Weak encryption on the API interfaces (SD: privacy)	C21: Monitor the use of APIs and encrypt all data shared with third parties. Additionally, put into place data management procedures and controls such as signed non-disclosure agreements with payment service providers to avoid information/ data leakage.	Are there sufficient mechanisms to monitor transactions processed through payment APIs? Does the DFS provider have nondisclosure agreements pertaining to customer sensitive data with third parties? Are there strong cryptographic algorithms used when transferring data with third parties?	Operations security policy - Logging and monitoring
MNO	Availability	- Network failure due to insufficient network capacity or to maintenance or design (SD: availability)	C22: The mobile network operator should take steps to ensure high network availability to allow access to DFS services through USSD, SMS, and the Internet.	Are there systems in place to ensure service availability? Example (service redundancy) Are there reports and utilities to measure system response time and down time?	Information security incident management - Redundancies
MNO	Availability	- Network failure due to insufficient network capacity or to maintenance or design (SD: availability)	C23: The MNO should perform technical capacity tests simulating different transactions based on customer numbers, expected growth, expected number of transactions, and expected peak periods to ensure continued system performance.	Are there systems to measure quality of service and quality of experience? Do the QoS and QoE conform to the standards for DFS?	System acquisition, development, and maintenance - Security in development and support processes
DFS Provider	Network Security	- Lack of monitoring of network traffic and individual network packets (SD: availability, communication security)	C24: The DFS provider should protect against network attacks by the 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.	Are there adequate protections against network attacks like firewalls and traffic filters with proper configurations?	Operations security - Protection from malware
DFS Provider	Network Security	- Enabling unnecessary services (SD: data confidentiality)	C25: Inbound internet traffic should be limited and continuously monitored.	Is there adequate monitoring of traffic for internet facing DFS applications?	Operations security - Protection from malware
DFS Provider	Network Security	- Enabling unnecessary services (SD: data confidentiality)	C26: Set restrictive firewall rules by default, use port whitelisting, use packet filters, and continuously monitor access to whitelisted/permitted ports and IP's.	Are the firewall rules adequately configured? e.g., port whitelisting, packet filtering	Operations security - Protection from malware
DFS Provider	Fraud detection	- Insufficient internal controls on critical operations (SD: access control)	C27: Where possible, limit critical changes using the four-eye principle (maker-checker/two-person rule) for critical actions including (but not limited to) an administrator creating, modifying, or deleting another administrator account, changing, attaching and detaching of DFS account from mobile number/user ID, and transaction reversal.	Are there sufficient controls to review and approve for critical changes on accounts? e.g., is there maker-checker and approval process before changes are made?	Access control Policy - System and application access control
DFS Provider	Fraud detection	- Lack of validation of data inputs (SD: data integrity)	C28: DFS providers should ensure sufficient separation of duties for maker-approver; for example, an administrator may not have access rights to both create and activate a DFS account.	Is there more than one person required to complete a critical DFS tasks?	Access control Policy - System and application access control
DFS Provider	Access Control	- Insufficient privilege management (SD: access control)	C29: Limit, control, and monitor physical access to sensitive physical DFS infrastructure. Physically isolate and put in place logical and physical deterrents/barriers to DFS infrastructure from other infrastructure. Employ least privilege techniques such that preventative access is allowed for authorized persons, supplanted by detection and enforcement (e.g., alarms if forced). Monitor system activity by logging all access (e.g., who accessed, what they accessed, where they accessed from, and when they accessed it).	Are there sufficient physical and logical barriers to limit access to DFS infrastructure?	Physical and environmental security - Secure areas

(continued)

Impacted DFS Entity	Group	Risk and vulnerability	Control	Security audit question	Applicable policy or procedure
DFS Provider	Network Security	- Addition of test data into production data (SD: data integrity)	C30: The DFS provider should employ robust input validation routines on external-facing services by checking out-of-range values and unpermitted characters in fields, and by constraining and sanitizing input. Input validation should happen at the earliest possible point and should be done both on the client, and server-side, however, the server should not rely solely on client-side validation. Additionally, block, log and review all requests that violate the Web Services Description Language (WSDL) and schemas.	Is the DFS provider performing input validation checks?	System acquisition, development, and maintenance - Security in development and support processes
DFS Provider	Fraud detection	- Addition of test data into production data (SD: data integrity)	C31: Use database fingerprinting to detect tampering and modification of data after it has been stored	Are there mechanisms in place to detect data modification and tampering on the database?	Operations security - Logging and monitoring
DFS Provider		- Addition of test data into production data (SD: data integrity)	C32: Ensure all test data is removed from code before it is migrated to the production environment.	Is test data and test user accounts deleted from the production environment?	System acquisition, development, and maintenance - Test data
DFS Provider	Fraud detection	- Absence of logging, ability to alter logs, and insufficient information in logs (SD: non-repudiation)	C33: DFS systems should use logging mechanisms, including capturing the provenance of user actions or logging of critical actions into tamper-proof storage, secure DFS system logs from tampering, editing, deleting, stopping.	Are DFS logs stored securely in a tamper proof module? e.g., SIEM	Operations security - Logging and monitoring
DFS Provider	Network Security	- Inaccurate and unsynchronised clocks (SD: data integrity)	C34: Ensure clock accuracy synchronization on all systems connected to the DFS system. NTP and SNTP are some of the protocols used to sync accurate time; however, these must be deployed securely.	Are the clocks within the DFS ecosystem synchronized?	Operations security - Operational procedures and responsibilities
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 call spoofing? E.g., CLI analysis?	Communications security: Information transfer
DFS Provider	Authentication	-Missing/Inadequate account configuration and authorisation controls (SD: authentication)	C40: Require user authentication and authorization for high-risk account changes and transaction and deny performing of transactions even when the device is logged in until knowledge of PIN or password has been demonstrated.	Is there additional authorisation and authentication for high value transactions and changes on DFS user accounts? For example, what additional checks are done when increasing transaction limits?	Access control Policy - User access management
Third-Party Providers	Privacy and confidentiality	- Weak encryption algorithms used on data stored in the device and data transmitted (SD: privacy)	C41: Sufficiently secure encryption should be employed for both data protection within the mobile application and communication with backend DFS systems and whenever possible, mask, truncate or redact customer confidential information.	Have strong encryption ciphers and integrity protection mechanisms such as message authentication codes been used for data stored on the device and when data is communicated to backend DFS systems? (See C17 for a discussion of strong encryption algorithms.) Are policies in place to assure the reaction of sensitive customer confidential information?	Cryptography policy - Cryptographic controls
Third-Party Providers	Privacy and confidentiality	- Lack of encryption of communications (SD - communication security)	C42: Use digital signatures to identify third parties connected to the DFS system when transactions are performed.	Are digital signatures used to identify third party providers that connect to the DFS systems?	Access control Policy - System and application access control

(continued)

Impacted DFS Entity	Group	Risk and vulnerability	Control	Security audit question	Applicable policy or procedure
Third-Party Providers	Privacy and confidentiality	- Insufficient management of certificate or key materials (SD: access control)	C43: Use trusted keys and certificates to allow data exchange between DFS providers and third parties, and they should be protected from disclosure.	Are procedures in place to assure the trustworthiness and protection of private and secret keys? Are certificates and other cryptographic information protected by operating system controls?	Access control Policy - System and application access control
Third-Party Providers	Availability	- DFS Provider or MNO System Failure leading to agents/third parties reverting to offline processes (SD: availability)	C44: Set procedural and technical controls for effective management during system downtime with related service providers. For example, set controls to manage offline transactions (e.g., SIM swaps) when access to the DFS system is intermittent. Have additional checks for remittances and third-party payments when DFS system or 3rd party system access is intermittent.	Are there policies in place to assure management during system downtime?	Operations security - Operational procedures and responsibilities
DFS Provider	Authentication	- Insecure and inadequate access controls on user accounts (SD: access control)	C45: Use multi-factor or multi-model authentication for access to DFS accounts.	Is multifactor authentication used when connecting to DFS accounts?	Access control Policy - User access management
	Access Control	- Untested restoration practices (SD: availability)	C46: Deactivate and remove default accounts and credentials from databases, applications, operating systems, and other access interfaces that interact with the production DFS system.	Are default system accounts removed from the DFS system and all systems that connect to DFS systems?	Access control Policy - User access management
DFS Provider	Access Control	- Untested restoration practices (SD: availability)	C47: Review installation, vendor, support accounts, and access points to DFS systems and infrastructure. All of those accounts should be deactivated or assigned appropriate user profiles.	Are DFS vendor and support system accounts deactivated after support duties are completed?	Access control Policy - User access management
DFS Provider	Availability	- Inadequate data controls like failure to implement atomicity of transactions, allowing them to exist in a partially completed state (SD: data integrity)	C48: Perform end-to-end tests after any changes to the DFS, MNO, SP, and third-party systems, include regression and capacity tests in the acceptance tests. Also, ensure there is a fall-back/blackout plan.	Are end to end tests been performed after changes or upgrades to the DFS systems? End to end tests may include capacity tests, security tests, Quality of Service tests, user acceptance tests etc.	System acquisition, development, and maintenance - Security in development and support processes
DFS Provider	Availability	- Inadequate data controls like failure to implement atomicity of transactions, allowing them to exist in a partially completed state (SD: data integrity)	C49: Have scheduled, regular backups for DFS systems. Regularly test and securely store backups offline and offsite in an encrypted form.	Does the DFS provider have regular scheduled backups? Are the backups encrypted and stored on an offsite location?	Operations security - Backup policy
DFS Provider		- Inadequate data controls like failure to implement atomicity of transactions, allowing them to exist in a partially completed state (SD: data integrity)	C50: Use standard ACID (Atomicity, Consistency, Isolation, Durability) functionality of the databases to ensure transaction integrity. DFS operations should either succeed completely or fail completely. DFS provider should also ensure there are checks to prevent duplicate transactions (unique transaction IDs, timestamps and use of cryptographic nonce)	Are there pending transactions, duplicate transactions in the DFS system? Has the transaction been fully executed?	Operations security - Operational procedures and responsibilities
Third-Party Provider	Privacy and confidentiality	- Inadequate mechanisms to assure data integrity and over-reliance on external trust anchors (SD: non-repudiation)	C51: DFS applications/3rd parties should support the use of digital signatures; a secure digital signature provides irrefutable evidence of the transaction's origin. Digital signatures are only valid as long as the PKI has not been compromised and must be tested with plans for assuring agility. By demonstrating that signing keys are adequately protected up to the root key, the DFS provider can withstand legal challenges about the authenticity of a specific user and disputed transactions.	Are digital signatures used by DFS applications or by third-party providers? Are the digital signatures based on sufficiently strong cryptographic algorithms and key sizes? Are the implementations of the cryptographic algorithms secure and up to date and do they provide sufficient randomness? (For example, strong digital signature algorithms include RSA, DSA, and ECDSA. Elliptic-curve cryptographic algorithms can use shorter keys to provide equivalent security to other ciphers.)	Access control Policy - System and application access control

(continued)

Impacted DFS Entity	Group	Risk and vulnerability	Control	Security audit question	Applicable policy or procedure
MNO	Authentication	- Inadequate controls for user identification and verification before SIM swap and SIM recycling (SD: Authentication)	C52: MNOs should ensure that an identity verification process is in place before SIM swaps is performed.	Are processes and policies in place to ensure that identity verification is in place prior to SIM swap operations? Are there technical mechanisms in place to prevent any leakage or transfer of information until the SIM swap has been confirmed?	Access control Policy - User access management
MNO	Authentication	- Inadequate controls for user identification and verification before SIM swap and SIM recycling (SD: Authentication)	C53: The user's identity should be verified using a combination of something they are, something they have, or something they know. For example, with the presentation of a valid ID, biometric verification, and knowledge about the DFS account details before a SIM swap/ SIM replacement is performed.	Does the mobile network operator perform biometric authentication before SIM swaps or SIM replacement?	Access control Policy - User access management
MNO	Authentication	- Inadequate controls for user identification and verification before SIM swap and SIM recycling (SD: Authentication)	C54: DFS and Payment Service Providers should be able to detect real-time whenever a SIM card with DFS services has swapped or replaced. And perform further verification before any high-value transaction or account changes are authorised with new SIM.	Is the DFS provider able to detect a SIM swap or SIM change for a DFS account?	Access control Policy - System and application access control
MNO	Authentication	- Inadequate controls for user identification and verification before SIM swap and SIM recycling (SD: Authentication)	C55: The mobile operator should safeguard and securely store SIM data like IMSI and SIM secret key values (KI values).	Does the mobile network operator securely store SIM data like IMSI, Kc and Ki?	Asset management - Media handling
MNO	Authentication	- Inadequate controls for user identification and verification before SIM swap and SIM recycling (SD: Authentication)	C56: A mobile number recycling process should be in place that involves communicating with DFS providers on Mobile Subscriber Identification Numbers (MSIDN) being churned or recycled. (in this context: number recycling is when the MNO reallocates a dormant/inactive Mobile Subscriber Identification Number (MSISDN) to a new customer). When a SIM is recycled, the mobile operator will report a new IMSI of the related account phone number. The DFS provider should block the account until the identity of the new person holding the SIM card is verified as the account holder.	Is the DFS provider involved in the SIM recycling process for DFS accounts?	Asset management - Media handling
	Privacy and Confidentiality	- Mobile device theft (SD: data confidentiality)	C57: DFS users should have the ability to perform remote wipes on a mobile device and encrypting their data in case the device is lost or stolen.	Does the application or underlying operating system provide support for remote wipes of DFS data or of the mobile device, and are there mechanisms in place to ensure that data is encrypted in the event of device loss or theft?	Operations security - Operational procedures and responsibilities
DFS Provider	Access control	- Inadequacies in SIM swap and recycling process[ii] (SD: data integrity)	C58: DFS providers should ensure they have procedures in place to detect and avert suspicious SIM swaps and SIM recycle by:	Are there procedures in place for the DFS provider to detect suspicious SIM swaps and SIM recycling?	Operations security - Operational procedures and responsibilities
			a) Check if the IMSI associated with the phone number has changed, this is an indication of SIM swap.		
			b) If there is an indication of a SIM swap, check the IMEI of the phone holding the SIM. If the IMEI has also changed, there is a high probability of a SIM swap. In that case, the DFS provider should block the account until performing account verification procedures, for example, via a voice call or an agent.		

(continued)

Impacted DFS Entity	Group	Risk and vulnerability	Control	Security audit question	Applicable policy or procedure
DFS provider	Fraud Detection	- Unauthorized changes to system configuration and log files and data (SD: Data Integrity)	C59: Protect against tampering and allow only online transactions	Does the app store transactions for later transmission?	Operations security: Operational procedures and responsibilities
			a) Protect and monitor DFS application files from tampering and changes using file integrity monitors, e.g., by calculating checksums or validating digital signatures.		
			b) By policy, the DFS provider or merchant should not use the mobile payment solution to authorize transactions offline or store transactions for later transmission.		
DFS provider	Authentication	- Inadequate user access validation or user input validation (SD: Authentication)	C60: Use strong multi-factor authentication for user and 3rd party provider access to DFS systems, e.g., token or biometrics, the use of multi-factor authentication to verify system users increases non-repudiation of origin.	Is multi factor used for authenticating users?	Access control Policy - System and application access control
DFS provider	Authentication	- Inadequate user access validation or user input validation (SD: Authentication)	C61: Check incoming data against expected values in API related data schema, for USSD, perform XML validation .	Is the DFS provider performing XML validation of data through APIs and USSD requests? E.g., input validation, amounts, special characters in amounts, currency checks etc.	Communications security - Information transfer
DFS provider	Authentication	- Inadequate user access validation or user input validation (SD: Authentication)	C62: Use analytics systems to check user velocity between transactions, transaction time of day access tracking for additional authorization validation checks.	Does the DFS system have capability to detect out-of-pattern transactions based on customer profile?	Access control Policy - System and application access control
				Are the DFS provider performing checks based on user transactions profile? E.g. agent shops performing late transactions, DFS users perfuming transactions in two different locations?	
DFS provider	Authentication	- Inadequate user access validation or user input validation (SD: Authentication)	C63: Regardless of the method used for producing receipts (e.g., e-mail, SMS, or attached printer), the method should mask the Primary Account Number (PAN) in support of applicable laws, regulations, and payment-card policies. By policy and practice, the DFS Provider/merchant should not permit the use of non-secure channels such as e-mail and SMS to send PAN or Sensitive authentication data (SAD).	Does the DFS app stores or transmits Personal Account Number/Sensitive Authentication Data in plain text over SMS/email?	Asset management - Media handling
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 based 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

(continued)

Impacted DFS Entity	Group	Risk and vulnerability	Control	Security audit question	Applicable policy or procedure
MNO	Network Security	- Unprotected sensitive traffic and weak encryption practices (SD: Communication Security)	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	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)	Access control Policy - User access management
MNO	Network Security	- Unprotected sensitive traffic and weak encryption practices (SD: Communication Security)	C76: Use 2-way Secure OTP to the original phone number to verify the legitimacy of the transaction[iv]	Is transaction validation performed using secure OTP?	Access control Policy - User access management
MNO	Privacy and Confidentiality	- Unprotected sensitive traffic and weak encryption practices (SD: Communication Security)	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.	Are the encryption algorithms and keys used are strong enough to protect customer PINs and data?	Cryptography - Cryptographic controls
MNO	Access Control	- Unprotected sensitive traffic and weak encryption practices (SD: Communication Security)	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.	Are there controls in place to prevent multiple simultaneous logons through multiple channels? Is the DFS provider only allowing a single session per user at a time to connect to the DFS network? (multiple sessions through different channels could be an indication of a breach)	Access control Policy - System and application access control
MNO	Network Security	- Unprotected sensitive traffic and weak encryption practices (SD: Communication Security)	C79: The mobile operator should deploy SS7 and diameter signaling security controls specified by the GSMA (FS.11, FS.07, IR.82, and IR.88) to limit threats due to SS7 attacks [3]	Has MNO implemented the SS7 and diameter signaling controls to protect against SS7 vulnerabilities?	Communications security - Network security management
DFS Provider	Privacy and confidentiality	- Inadequate protection of DFS customer registration data. (SD: Authentication)	C80: Protect and guard customer data used for DFS registration, where physical forms are used, store, and transmit the data securely.	Is the DFS data and forms used for customer registration securely stored, transmitted, and stored to prevent any data leakages using RBAC, data encryption etc.?	Asset management - Media handling
DFS Provider	Network Security	- Use of weak encryption. (SD: Communication Security)	C81: Use strong encryption standards like TLS encryption v1.2 and higher for API communication.	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?	Communications security - Information transfer
DFS Provider	Network security	- Inadequate DFS user access control and monitoring. (SD: Access Control)	C82: Extend threat detection to explicitly incorporate threats associated with APIs.	Are there operational controls to detect threats associated with APIs? Are there controls in place to detect rouge/malicious APIs?	Operations security - Technical vulnerability management
DFS Provider	Access control	- Inadequate DFS user access control and monitoring. (SD: Access Control)	C83: Limit remote login access and minimize privileges to remote login sessions to backend DFS systems.	Are there controls to limit access to DFS systems especially for remote login users?	Access control Policy - User access management
DFS Provider	Privacy and confidentiality	- Inadequate DFS user access control and monitoring. (SD: Access Control)	C84: Limit the lifetime of TLS certificates to 825 days.	Is the TLS lifetime certificate up to date? I.e. the certificate age should be less than 825 days	Communications security - Network security management
DFS Provider	Authentication	- Inadequate DFS user access control and monitoring. (SD: Access Control)	C85: Authenticate user IP, device, and login time for all privileged users, agents, and merchants connecting to the DFS system. For example, configure a merchant and agent access to the DFS system to be accessible only during open trading hours.	Are there controls to check validate privileged users? For example, through IP validation and checking login time?	Access control Policy - User access management
DFS Provider	Network Security	- Inadequate DFS user access control and monitoring. (SD: Access Control)	C86: Code and changes should be tested in the test environment before moving to the production platform; the test environment should be physically and logically separated from the production environment.	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.	System acquisition, development and maintenance - Security in development and support processes

(continued)

Impacted DFS Entity	Group	Risk and vulnerability	Control	Security audit question	Applicable policy or procedure
DFS Provider	Network Security	- Inadequate DFS user access control and monitoring. (SD: Access Control)	C87: To improve security, use a trusted tamper-resistant device like a Hardware Security Module (HSM) to Securely manage the process and store cryptographic keys to protect user PINs, transactions, tokens, money vouchers.	Does the DFS provider have a mechanism in place to securely store cryptographic keys?	Cryptography - Cryptographic controls
DFS Provider	Access control	- Inadequate DFS user access control and monitoring. (SD: Access Control)	C88: Set user roles to define access rights based on the principle of least privilege.	Does the DFS provider use Role Based Access Controls?	Access control Policy - User access management
DFS Provider	Access control	- Inadequate DFS user access control and monitoring. (SD: Access Control)	C89: After termination of a user, agent, merchant, payment service providers or third parties disable/deactivate respective accounts	Are login credentials of terminated DFS administrators, agents and users deactivated? Are dormant DFS accounts deactivated?	Access control Policy - User access management
DFS Provider	Access control	- Inadequate DFS user access control and monitoring. (SD: Access Control)	C90: Set account dormancy period and disable dormant accounts at dormancy maturity.	Has the DFS provider set a dormancy period after which inactive admin accounts are deactivated? Are all inactive dormant internal staff and API accounts deactivated?	Access control Policy - User access management
DFS Provider	Fraud detection	- Inadequate DFS user access control and monitoring. (SD: Access Control)	C91: Set schedules for logons and session limitations based on DFS roles. (session limitations can include the maximum number of reversals per day based on the role)	Does the DFS provider implement Role Based Access Controls?	Access control Policy - User access management
DFS Provider	Fraud detection	- Inadequate DFS user access control and monitoring. (SD: Access Control)	C92: Limit control, monitor, and periodically review privileged access to DFS systems, including user addition, modification, and deletion.	Is there a mechanism in place to review administrative privileges?	Access control Policy - User access management
DFS Provider	Privacy and confidentiality	- Inadequate DFS user access control and monitoring. (SD: Access Control)	C93: Monitor the use of APIs, and encrypt all data shared with third parties, put in place data management procedures and controls like signed non-disclosure agreements with payment service providers to avoid information/data leakage.	Is there a monitoring mechanism in place to track data sharing through APIs? Are there controls in place to prevent data leakage?	Communications security - Network security management
DFS Provider	Network Security	- Inadequate monitoring of the wireless network (SD: Data Confidentiality)	C94: Protect wireless transmissions per PCI DSS Requirements. Controls should include, but are not limited to, the following: - Ensure vendor default encryption keys, passwords, and SNMP community strings are changed. - Facilitate the use of industry best practices to implement strong encryption for authentication and transmission. - Ensure that clear-text account data is not stored on a server connected to the Internet.	Are encryption keys were changed from default at installation? Are default SNMP strings changed?	Communications security - Network security management
Third-party	Privacy and confidentiality	- Failure perform data destruction/erasing before disposing of devices (SD: Privacy)	C95: DFS Providers/Merchants should consistently dispose of old devices. When the solution provider provides guidance, the merchant should follow it. Some items to consider include: - Remove all tags and business identifiers. - Where possible, develop a contract with an authorized vendor who can help securely dispose of electronic materials and components. - Do not dispose of devices in trash containers or dumpsters associated with your business.	Are there security guidelines followed when disposing of DFS related data?	Operations security - Protection from malware

(continued)

Impacted DFS Entity	Group	Risk and vulnerability	Control	Security audit question	Applicable policy or procedure
Third-Party, DFS Provider	Network Security	- Inadequate collaboration with the solution provider on the security of mobile devices purchased (SD: Availability and Confidentiality)	C99: Merchants and DFS providers should require the following from their solution provider:	Are there procedures in place to monitor software updates and are the updates installed ~~in a~~ securely?	Operations security - Technical vulnerability management
			- The solution provider should regularly update their payment application and indicate to the merchant when updates are available and are safe to install.		
			- The solution provider should have restrictions on their payment application so that it only functions on a device running approved firmware.		
			- The solution provider should supply documentation that details any update procedures the merchant needs to follow.		
			- The DFS solution provider should communicate with the DFS provider and make them aware of newly discovered vulnerabilities in their payment-acceptance solution. Additionally, the solution provider should guide merchants when new vulnerabilities are discovered, as well as provide tested patches for any of these vulnerabilities.		
Third-Party, DFS Provider	Fraud detection	- Open undetected system application weaknesses (SD: Data Confidentiality)	C100: The merchant should work with its solution provider to ensure that any audit or logging capability is enabled. The solution provider should ensure that logging capabilities exist with enough granularity to detect abnormal events.	Do the audit logs provided sufficiently track all changes on the DFS system or MNO systems that affect DFS services?	Operations security - Technical vulnerability management
			The solution provider should guide the merchant on the merchant's responsibility to review the logs. Additionally, regularly inspect system logs and reports for abnormal activity. If abnormal activity is suspected or discovered, discontinue access to the mobile device and its payment application until the issue has been resolved. Abnormal activities include, but are not limited to, unauthorized access attempts, escalated privileges, and unauthorized updates to software or firmware.		
Third-Party, DFS Provider	Network Security	- Network exposure to outside attacks (SD: Availability)	C101: DFS Applications should be subjected to regular security penetration scans and penetration testing. In particular, applications should be designed to be robust against phishing software.	Is there regular penetration testing of the DFS systems?	Operations security - Technical vulnerability management
MNO	Availability	- Network exposure to outside attacks (SD: Availability)	C107: Perform regular vulnerability scans and penetration tests on MNO infrastructure to check exposure to attacks that could affect system availability.	Are there regular vulnerability scans that are performed on the DFS systems?	Operations security - Technical vulnerability management
MNO	Network Security	- Network exposure to outside attacks (SD: Availability)	C108: Install and regularly update the latest anti-malware software (if available) and make this available to end-users. Consider application wrapping, which can be employed with an MDM (Mobile Device Management) solution to prevent and remove malicious software and applications.	Are the DFS systems updated to the latest versions to protect against new threats?	Operations security - Protection from malware

(continued)

Impacted DFS Entity	Group	Risk and vulnerability	Control	Security audit question	Applicable policy or procedure
MNO, DFS providers, and Third parties	Network Security	- Discovery of new exploits against deployed systems and the inability to deploy solutions against these exploits (SD: Data Confidentiality, Access Control, Availability)	C109: 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	Are the DFS systems patched against known vulnerabilities?	Operations security - Technical vulnerability
MNO, DFS providers, and Third parties	Access control	- Discovery of new exploits against deployed systems and the inability to deploy solutions against these exploits (SD: Data Confidentiality, Access Control, Availability)	C110: Providers and MNOs should have contingency plans in place with vendors to quickly acquire patches and system remediation if a zero-day attack has been found in the wild. Part of this strategy involves the proper use of backups.	Are there policies and processes in place to manage a new threats and attacks to the DFS systems?	Operations security - Technical vulnerability management
MNO	Network Security	- Insecure devices connected to the DFS infrastructure (SD: Data Integrity)	C111: 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.	Are all devices used to connect to DFS systems scanned for threats and checked for the latest software patches?	Operations security - Technical vulnerability management
	Authentication	- Overly permissive access to the DFS infrastructure (SD: Authentication)	C115: Before authenticating DFS users, when possible, validate the IMSI, device, and location, and IP address of the user to establish their identity and to prevent unauthorized access to the network infrastructure.	Is the DFS provider checking the IMSI of mobile numbers used for DFS transactions to protect against SIM swaps?	Access control Policy - User access management
Third-Party Provider	Fraud detection	- Inadequate transaction verification (SD: Non-Repudiation)	C116: Payment service providers should ensure that companion general-purpose reloadable cards linked to DFS accounts require the use of EMV chips with cardholder verification methods, such as PINs or biometrics, when practical, and that all transactions result in an alert to customers.	Do the DFS customers get alerts when DFS transactions are performed on their accounts?	Access control Policy - User access management
DFS Provider	Privacy and Confidentiality	- Inadequate oversight and controls in test environments (SD: privacy)	C117: 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.	Is there proper segregation of data implemented for tests and production environments? Are there processes that limit the use of customer data for test purposes? Such as data anonymization.	Asset management - Media handling
Third-Party Provider	Privacy and Confidentiality	- Exposure of customer-sensitive information in transactions or through APIs (SD: privacy)	C118: Third-party providers should restrict the sharing of information with other parties such as payment service providers and DFS providers to the minimum required to assure the integrity of the transaction.	Are there processes that limit the data shared with third parties when transactions are being performed?	Asset management - Media handling
Third-Party Provider	Privacy and Confidentiality	- Insufficient data protection controls (SD: privacy)	C119: Providers should ensure that customer-sensitive data is removed from environments such as trace logs (for example, cash retrieval voucher codes, bank account numbers, and credentials). Use place holders whenever possible to represent this data in log files.	Do event logs contain customer-sensitive data such as PINs?	Operations security - Logging and monitoring

This audit checklist table [4] above is available to download in excel using this link: https://itu.int/en/ITU-T/extcoop/figisymposium/Documents/Digital%20Financial%20Services%20security%20audit%20checklist.xlsm

4 SECURITY AUDIT CHECKLIST

4.1 Access Control

4.1.1 Are login credentials of terminated DFS administrators, agents and users deactivated. Are dormant DFS accounts deactivated?

4.1.2 Are default system accounts removed from the DFS system and all systems that connect to DFS systems?

4.1.3 Are DFS vendor and support system accounts deactivated after support duties are completed?

4.1.4 Are the following logical controls set for DFS user sessions: i) auto logouts and session time out ii) Maximum failed password login attempts iii) Password and PIN complexity. iv) Password/PIN reuse periods

4.1.5 Are there procedures in place for the DFS provider to detect suspicious SIM swaps and SIM recycling?

4.1.6 Are there controls in place to prevent multiple simultaneous logons through multiple channels? Is the DFS provider only allowing a single session per user at a time to connect to the DFS network? (multiple sessions through different channels could be an indication of a breach)

4.1.7 Are there controls to limit access to DFS systems especially for remote login users?

4.1.8 Are there policies and processes in place to manage a new threats and attacks to the DFS systems?

4.1.9 Are there sufficient physical and logical barriers to limit access to DFS infrastructure?

4.1.10 Does the DFS provider use Role Based Access Controls?

4.1.11 Does the DFS system have capability to detect out-of-pattern transactions based on customer profile? For example: Does the DFS provider check authenticity of transactions using location-based validation of transactions, for example through geo-velocity tracking or other means?

4.1.12 Has the DFS provider limited concurrent user logins and provided the option for customers to opt into other login channels? For example, are customers who use USSD able to optionally choose to use a DFS app channel before the DFS provider activates access through this channel?

4.1.13 Has the DFS provider set a dormancy period after which inactive admin accounts are deactivated? Are all inactive dormant internal staff and API accounts deactivated?

4.1.14 Has the DFS provider set USSD and STK DFS sessions to automatically disconnect after a set period of user inactivity?

4.1.15 Is the DFS provider performing real time device validation before transaction processing?

4.1.16 Is the password transmitted securely? Is the user required to change password after first time login?

4.1.17 Is there a maximum number of failed login attempts set before account is locked?

4.1.18 Is there a sufficient way of validating user identity before activating previously dormant accounts for example biometric validation?

4.2 Authentication

4.2.1 Are processes and policies in place to ensure that identity verification is in place prior to SIM swap operations? Are there technical mechanisms in place to prevent any leakage or transfer of information until the SIM swap has been confirmed?

4.2.2 Are DFS user authentication credentials transmitted via a different channel/out-of-band? (e.g., if account setup is done via USSD channel are one-time passwords transmitted via e-mail or voice calls?)

4.2.3 Are there controls to check validate privileged users? For example, through IP validation and checking login time?

4.2.4 Does the DFS app stores or transmits Personal Account Number/Sensitive Authentication Data in plain text over SMS/email?

4.2.5 Does the DFS provider enforce server-based authentication for all access requests?

4.2.6 Does the mobile network operator perform biometric authentication before SIM swaps or SIM replacement?

4.2.7 Does the mobile network operator securely store SIM data like IMSI, Kc and Ki?

4.2.8 Is multi factor used for authenticating users?

4.2.9 Is multifactor authentication used when connecting to DFS accounts?

4.2.10 Is the DFS provider able to detect a SIM swap or SIM change for a DFS account?

4.2.11 Is the DFS provider checking the IMSI of mobile numbers used for DFS transactions to protect against SIM swaps?

4.2.12 Is the DFS provider involved in the SIM recycling process for DFS accounts?

4.2.13 Is the DFS provider performing XML validation of data through APIs and USSD requests?

E.g., input validation, amounts, special characters in amounts, currency checks etc.

4.2.14 Is there additional authorisation and authentication for high value transactions and changes on DFS user accounts? For example, what additional checks are done when increasing transaction limits?

4.2.15 Does the DFS system have capability to detect out-of-pattern transactions based on customer profile? Are the DFS provider performing checks based on user transactions profile? E.g., agent shops performing late transactions, DFS users perfuming transactions in two different locations?

4.3 Availability

4.3.1 Are there policies in place to assure management during system downtime?

4.3.2 Are there end to end tests been performed after changes or upgrades to the DFS systems? End to end tests may include capacity tests, security tests, QoS tests, user acceptance tests etc.

4.3.3 Are there regular vulnerability scans that are performed on the DFS systems?

4.3.4 Are there systems in place to ensure service availability? Example (service redundancy) Are there reports and utilities to measure system response time and down time?

4.3.5 Are there systems to measure quality of service and quality of experience? Do the QoS and QoE conform to the standards for DFS?

4.3.6 Does the DFS provider have regular scheduled backups? Are the backups encrypted and stored on an offsite location?

4.4 Fraud Detection

4.4.1 Are DFS logs stored securely in a tamper proof module? E.g., SIEM

4.4.2 Are there mechanisms in place to detect data modification and tampering on the database?

4.4.3 Are there mechanisms to detect SMS and call spoofing? E.g., CLI analysis?

4.4.4 Are there sufficient controls to review and approve for critical changes on accounts? e.g., is there maker-checker and approval process before changes are made?

4.4.5 Are there sufficient mechanisms to monitor transactions processed through payment APIs? Does the DFS provider have nondisclosure agreements pertaining to customer sensitive data with third parties? Are there strong cryptographic algorithms used when transferring data with third parties?

4.4.6 Do the audit logs provided sufficiently track all changes on the DFS system or MNO systems that affect DFS services?

4.4.7 Do the DFS customers get alerts when DFS transactions are performed on their accounts?

4.4.8 Do trace logs and event data records capture/store sensitive user data? (e.g., are customer PINs stored in EDRs)

4.4.9 Does the app store transactions for later transmission?

4.4.10 Does the DFS provider implement Role Based Access Controls?

4.4.11 Is there a mechanism in place to review administrative privileges?

4.4.12 Is there more than one person required to complete a critical DFS tasks?

4.5 Network 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?

4.5.12 Are there pending transactions, duplicate transactions in the DFS system? Has the transaction been fully executed?

4.5.13 Are there procedures in place to monitor software updates and are the updates installed securely?

4.5.14 Are there technical controls in place to limit exposure of internal DFS systems addresses (like database IP addresses?

4.5.15 Does the DFS provider have a mechanism in place to securely store cryptographic keys?

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?

4.6 Privacy & Confidentiality

4.6.1 Are digital signatures used by DFS applications or by third-party providers? Are the digital signatures based on sufficiently strong cryptographic algorithms and key sizes? Are the implementations of the cryptographic algorithms secure and up to date and do they provide sufficient randomness? (For example, strong digital signature algorithms include RSA, DSA, and ECDSA. Elliptic-curve cryptographic algorithms can use shorter keys to provide equivalent security to other ciphers.)

4.6.2 Are procedures in place to assure the trustworthiness and protection of private and secret keys? Are certificates and other cryptographic information protected by operating system controls?

4.6.3 Are digital signatures used to identify third party providers that connect to the DFS systems?

4.6.4 Are the cryptographic libraries used by the operating system or by the application correctly designed and implemented and are they up to date? Do the cryptographic libraries support strong cryptographic ciphersuites and do they prevent or discourage use of weak ciphersuites? Are hashing algorithms used that have not been deprecated and are adequate digest lengths supported? (Anything less than SHA512 is considered weak today. MD5 and SHA1 have been broken.) For symmetric encryption ciphers, are strong ciphers used and are adequate key lengths supported? (For example, AES is considered secure to use while 3-DES is no longer a preferred cipher because of the SWEET-32 attack, and it is encouraged to move away from it to AES as soon as possible.) - For public-key encryption, are key lengths chosen to be an appropriate size for the public key algorithm being used? Are the criteria used for selecting cryptographic algorithms and key sizes based on public and well-examined standards? (For example, NIST 800-57 special publication has guidelines on minimum key sizes for each algorithm and how long this key size is good for)

4.6.5 Are the encryption algorithms and keys used are strong enough to protect customer PINs and data?

4.6.6 Are there processes that limit the data shared with third parties when transactions are being performed?

4.6.7 Are there security guidelines followed when disposing of DFS related data?

4.6.8 Do event logs contain customer-sensitive data such as PINs?

4.6.9 Does the application or underlying operating system provide support for remote wipes of DFS data or of the mobile device, and are there mechanisms in place to ensure that data is encrypted in the event of device loss or theft?

4.6.10 Has all sensitive consumer data been encrypted by the application or the operating system? Are unencrypted versions of the data accessible in the device, for example, in temporary buffers or in memory? Is all information sent over a network connection encrypted with a strong encryption cipher? (See C17 for more discussion of what comprises a strong encryption cipher.)

4.6.11 Have strong encryption ciphers and integrity protection mechanisms such as message authentication codes been used for data stored on the device and when data is communicated to backend DFS systems? (See C17 for a discussion of strong encryption algorithms.) Are policies in place to assure the reaction of sensitive customer confidential information?

4.6.12 Is test data and test user accounts deleted from the production environment?

4.6.13 Is the DFS data and forms used for customer registration securely stored, transmitted, and stored to prevent any data leakages using RBAC, data encryption etc.?

4.6.14 Is the TLS lifetime certificate up to date? I.e., the certificate age should be less than 825 days

4.6.15 Is there a mechanism in place to ensure that data-at-rest is encrypted and stored securely?

4.6.16 Is there a monitoring mechanism in place to track data sharing through APIs? Are there controls in place to prevent data leakage?

4.6.17 Is there limitation on customer sensitive information shared during transaction processing with third parties? (e.g., Only information needed for processing the transaction is shared with the third party)

4.6.18 Is there proper segregation of data implemented for tests and production environments? Are there processes that limit the use of customer data for test purposes? Such as data anonymization.

5 BIBLIOGRAPHY

[1] K. Butler and V. Mauree, "Digital Financial Service Security Assurance Framework," https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/ITU_SIT_WG_Technical%20report%20on%20Digital%20Financial%20Services%20Security%20Assurance%20Framework_f.pdf.

[2] "Information Security Management" https://www.iso.org/isoiec-27001-information-security.html .

[3] A. Klinger, "SS7 vulnerabilities and mitigation measures for Digital Financial Services transaction," http://itu.int/en/ITU-T/extcoop/figisymposium/Documents/ITU_SIT_WG_Technical%20report%20on%20the%20SS7%20vulnerabilities%20and%20their%20impact%20on%20DFS%20transactions_f.pdf .

[4] "Digital Financial Services audit checklist,"https://itu.int/en/ITU-T/extcoop/figisymposium/Documents/Digital%20Financial%20Services%20security%20audit%20checklist.xlsm.

International Telecommunication Union
Place des Nations
CH-1211 Geneva 20
Switzerland