FIGI

FINANCIAL INCLUSION
GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services security assurance framework

REPORT OF SECURITY WORKSTREAM

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Digital Financial Services security assurance framework

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.

About this report

This report was written by Kevin Butler, University of Florida and Vijay Mauree, ITU. The authors would like to thank Arnold Kibuuka, ITU for his support and assistance in the review and edits to the report. The authors would also like to thank the following persons for their inputs and feedback: Assaf Klinger, Vaulto; Leon Perlman, Columbia University; Rehan Masood, State Bank of Pakistan and members of the FIGI Security Infrastructure and Trust working group.

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

Contents

Executive Summary

The provision of digital finance services (DFS) involves a complex ecosystem with the participation of different stakeholders such as banks, DFS provider, mobile network operators (MNOs), DFS platform providers, regulators, agents, merchants, payment service providers, device manufacturers, application developers, token service providers, OEMs, and clients. The interconnectedness of these system entities and reliance on several parties in the ecosystem extends the security boundaries beyond the digital financial service (DFS) provider to the customers, network providers, mobile phone manufacturer, and other third-party providers in the ecosystem (see sections 4.1 and 4.2 of the report).

In addition, DFS providers must also deal with an increasingly complex mobile ecosystem, developing applications for multiple versions of operating systems each with their specific vulnerabilities and support different types of mobile devices. In this fast-evolving dynamic environment, DFS providers face certain challenges concerning knowledge about the actual security threats and possible security controls to mitigate the risks.

The DFS Security Assurance Framework provides an overview of the security threats and vulnerabilities facing the DFS providers (banks, non-banks providing mobile money services), mobile network operators, customers, payment system providers, merchants, and technology services/third-party service providers. Regulators including telecom authorities, banking, and payment regulators could also make use of the DFS Security Assurance Framework for establishing security baselines for the DFS providers as well.

The framework, when implemented, would complement established risk and information security management practices of the stakeholders involved in DFS ecosystem. For example, the security control measures in the document can be included as part of the ICT Security programme of the DFS provider.

The DFS Security Assurance Framework recommends a structured methodology for managing security risks that the DFS providers offering digital financial services could implement to:

- Enhance customer trust and confidence in digital financial services.
- Clarify the role and responsibilities of each of the stakeholders in the ecosystem.
- Identify security vulnerabilities and related threats within the ecosystem.
- Establish security controls to provide end to end security.
- Strengthen management practices with respect to security risk management that is inclusive of all DFS stakeholders.

The DFS Security Assurance Framework provides a systematic security risk management process for assessing threats and vulnerabilities and identifies appropriate security control measures to be implemented by the DFS provider and mobile network operator for threats targeting the user, mobile device, mobile network operator and DFS provider. Threats related to merchants, payment service providers and other financial services organizations and the specific mitigations for addressing the threats that they face are out of scope for this document. The report complements the work undertaken under the Cybersecurity workstream in the Security, Infrastructure, and Trust Working Group, on the methodology for financial services organizations to manage and respond to cybersecurity incidents.

The DFS Security Assurance framework consists of the following components:

a) A security risk management methodology based on ISO/IEC 27005 –Security techniques -Information security risk management (Section 7 of the report).
b) Assessment of threats and vulnerabilities to the underlying infrastructure of the mobile network operator and DFS provider, DFS applications, services, network operations and third-party providers involved in the ecosystem for DFS delivery.
c) Mitigation strategies based on the outcome of (b) above. The mitigation measures identify 119 security controls for the security threats which are outlined in Section 8 of the report.

Section 9 of the report provides a template for security best practices for mobile money smartphone applications which could be included in an app security policy document by DFS providers. The template strictly considers the mobile application on the device unless stated otherwise, and subsections describing recommendations deal with various aspects of the operation or underlying policy relating

to the mobile application. The focus is primarily on Android applications given their large market share, though many recommendations are applicable across mobile operating systems. Section 10 of the report provides a framework for managing security incidents related to DFS.

The report is meant to be a living document and should be kept updated over time to take into account new platforms and application services as well as threats that would evolve over time and new vulnerabilities.

Acronyms

API	Application Programming Interface
DFS	Digital Financial Services
GW	Gateway
HCE	Hosted Card Emulation
HLR	Home Location Register
HSM	Hardware Security Module
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU FG DFS	ITU Focus Group on Digital Financial Services
IVR	Interactive Voice Response
MFA	Multi-Factor Authentication
MNO	Mobile Network Operator
MSC	Mobile Switching Centre
MSISDN	Mobile Station International Subscriber Directory Number
MST	Magnetic Secure Transmission
MVNO	Mobile Virtual Network Operator
NFC	Near Field Communication
OS	Operating System
OTP	One Time Password
OWASP	Open Web Application Security Project
PA-DSS	Payment Application Data Security Standard
PCI-DSS	Payment Card Industry Data Security Standard
POS	Pont of Sale
PSD2	Payment Services Directive 2
QR Code	Quick Response Code
RP	Relying Party
SCA	Strong Customer Authentication
SD	Security Dimension
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
TEE	Trusted Execution Environment
TPP	Third-Party (Payment Service) Providers
TSP	Token Service Provider
UICC	Universal Integrated Circuit Card
URL	Uniform Resource Locator
USSD	Unstructured Supplementary Service Data

Digital Financial Services security assurance framework

1 INTRODUCTION

Digital technology has spurred financial access to millions of people due to its ease of use through mobile phones, providing customer-centric financial services that are affordable, scalable and offer convenience.

According to the World Bank Global Findex database[1] *"the share of adults around the world making or receiving digital payments increased by 11 percentage points between 2014 and 2017. In high-income economies 51 percent of adults (55 percent of account owners) reported making at least one financial transaction in the past year using a mobile phone or the internet. In developing economies 19 percent of adults (30 percent of account owners) reported making at least one direct payment using a mobile money account, a mobile phone, or the Internet"*.

However, as providers harvest digital means to offer a wider range of financial services with greater reach, improved efficiency and minimal operating costs, the rapid growth and uptake of digital financial services makes its ecosystem uniquely vulnerable to various security threats. The interconnectedness of the system entities and reliance/involvement of a number of parties in the ecosystem extends the security boundaries beyond the digital financial service (DFS) provider to the customers, network providers, mobile phone manufacturers, and other third-party providers in the ecosystem.

In addition, DFS providers must also deal with an increasingly complex mobile ecosystem, developing applications for multiple versions of operating systems each with their specific vulnerabilities and support different types of mobile devices. In this fast-evolving dynamic environment, DFS providers face certain challenges concerning knowledge about the actual security threats and possible security controls to mitigate the risks.

The DFS Security Assurance Framework aims to bridge the above knowledge gap and recommends a structured methodology for managing security risks that the stakeholders of the digital financial services (DFS) ecosystem could implement to:

- Enhance customer trust and confidence in digital financial services.
- Clarify the role and responsibilities for each of the stakeholders in the ecosystem.
- Identify security vulnerabilities and related threats within the ecosystem.
- Establish security controls to provide end to end security.
- Strengthen management practices in respect to security risk management that is inclusive of all DFS stakeholders.

The DFS Security Assurance Framework provides an overview of the security threats and vulnerabil-

ities facing the DFS providers (banks, non-banks providing mobile money services), mobile network operators, customers, payment system providers, merchants, and technology services/third-party service providers. Regulators including telecom authorities, banking and payments regulators could also make use of the DFS Security Assurance Framework for establishing security baselines for the DFS providers as well.

The framework when implemented would complement established risk and information security management practices of the stakeholders involved in DFS ecosystem. For example, the security control measures in the document, can be included as part of the ICT Security programme of the DFS provider.

An underlying assumption is made that organisations have already implemented good security governance principles and standards, like information security policy documentation, data classification, allocation of information security responsibilities, data privacy policies, security awareness and training for their staff, secure development, testing and maintenance of infrastructures, devices, applications and processes, vulnerability management, backup procedures, incident management, business continuity and disaster recovery processes as these are outside the scope of this document

2 ITU-T RECOMMENDATION X.805 OVERVIEW

The Security Assurance Framework uses the ITU-T Recommendation X.805 as its foundation for applying security control measures to achieve end-to-end network security, it also largely suggests controls based on the recommendations in the technical report "Security Aspects of Digital Financial Services"[2] by the ITU-T Focus group Digital Financial Services.

The end-to-end communications environment of the DFS ecosystem is considered in terms of the ITU-T Recommendation X.805 and provides a useful reference framework for security management. The ITU-T Recommendation X.805 security architecture has eight '*security dimensions*', which are measures designed to address a particular aspect of network security.

The eight security dimensions that provide a systematic way of encountering network threats are as follows.

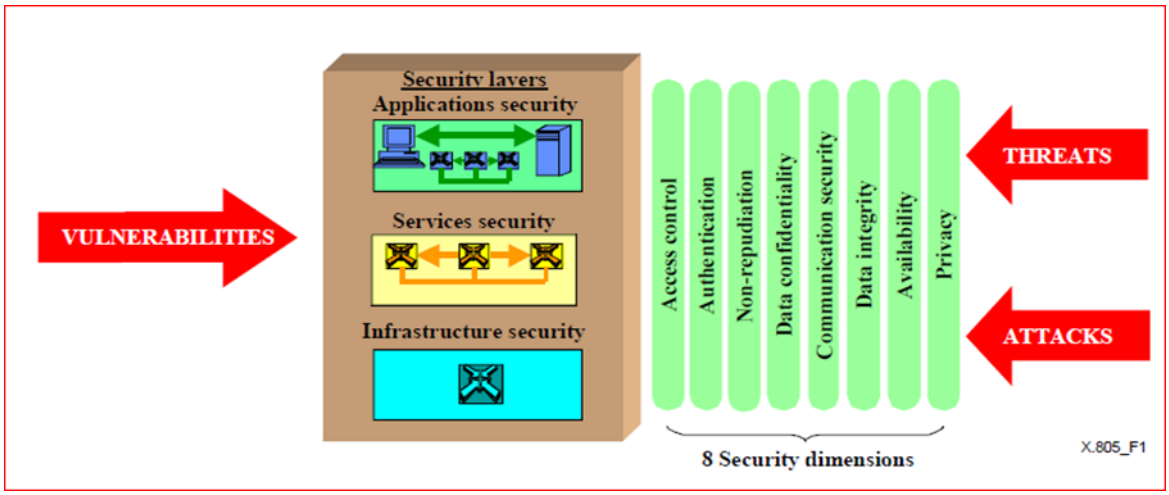
- **Access control:** Protection against unauthorized use of network resources.
- **Authentication:** Methods of confirming the identities of communicating entities.
- **Non-repudiation:** Methods to prevent an individual or entity from denying cause of an event or action.
- **Data confidentiality:** Protection of data from unauthorized disclosure.
- **Communication security:** Assurance that information only flows between authorized endpoints without being diverted or intercepted.
- **Data integrity:** Protection of the correctness and accuracy of data.
- **Availability:** Prevention of denial of authorized access to network elements and data.
- **Privacy:** Protection of data information that might be derived from observing network activity.

ITU-T Recommendation X.805 defines a hierarchy of network equipment and facility groupings into three security layers. These security layers provide comprehensive, end-to-end security solutions and identify where security must be addressed in products and solutions because each layer may be exposed to different types of threats and attacks.

The security layers are as follows:

i. **Infrastructure Security Layer:** consists of the basic building blocks used to build telecommunications networks, services and applications, and consists of individual transmission links and network elements including their underlying hardware and software platforms
ii. **Services Security Layer:** consists of services that customers/end-users receive from networks. These services range from basic connectivity and transport
iii. **Applications Security Layer:** focuses on network-based applications that are accessed by customers/end-users.

Figure 1 - ITU-T Recommendation X.805 Security Dimensions



3 DFS PROVIDER BUSINESS MODELS

Seven main stakeholders within the DFS ecosystem are considered: the DFS user, a merchant, government or non-government institution etc., Mobile Network Operator (MNO), the bank, a third party and a Mobile Virtual Network Operator (MVNO). We also consider the five main functions across the DFS value chain for these stakeholders: deposit holder, e-money issuer, payment service provider, agent network manager, and mobile communications provider.

Depending on the role/s played by each of the stakeholders, we consider the four most common DFS provider business models:

a) Bank led
b) MNO led
c) MVNO
d) Hybrid

3.1 Bank led business model

In this model, financial services offered by the bank are extended to mobile users, the signup process may be at the bank or through an agent network. In this model, the bank performs the key financial roles, i.e. is the deposit holder, e-money issuer and payment service provider. The communications network to deliver these financial services to the user is provided by the MNO, through their different channels, which could be Unstructured Supplementary Service Data (USSD), Short Messaging Service (SMS), Interactive Voice Response (IVR), or through the SIM Application Toolkit (STK). Examples are Ucash offered by the United Commercial bank in Bangladesh

Figure 2 below, shows an illustration of the bank-led model.

Figure 2 - Bank led business Model

3.2 MNO led business model

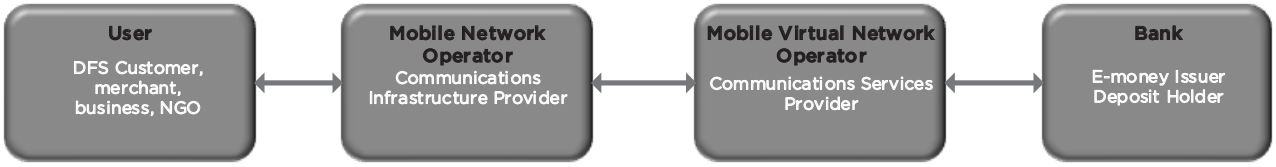
In an MNO led model, in parallel with the traditional role of providing the communications network, the MNO also undertakes the bulk of the financial roles and thus will issue the e-money, manage the agent network and the customer relationship and is the payment service provider. The MNO manages a wide DFS agent network that registers DFS users and receives physical cash from them in exchange for e-money on behalf of the MNO. Depending on financial regime, the MNO may be required to collaborate with a partner bank in which the DFS agents will deposit the physical funds collected from the customers on behalf of the MNO. The e-money issued by the MNO is backed by the funds in the trust or escrow account in the partner bank, examples are, M-PESA by Safaricom, Airtel Money, and MTN Mobile Money.

Figure 3 - MNO led business model

3.3 Model with Mobile Virtual Network Operator

In some implementations, there is Mobile Virtual Network Operator (MVNO) that provides the telecommunications services required for DFS. The MVNO may be either independent or owned by a bank. An example is Equity Bank in Kenya, which owns Equitel, an MVNO that extends the bank's financial services to its mobile network customers in the form of mobile money. MVNOs make use of the infrastructure provided by an MNO, but will offer their customers a different range of telecom services including digital financial services. Airtel, which is an MNO, provides the wireless network infrastructure for Equitel.

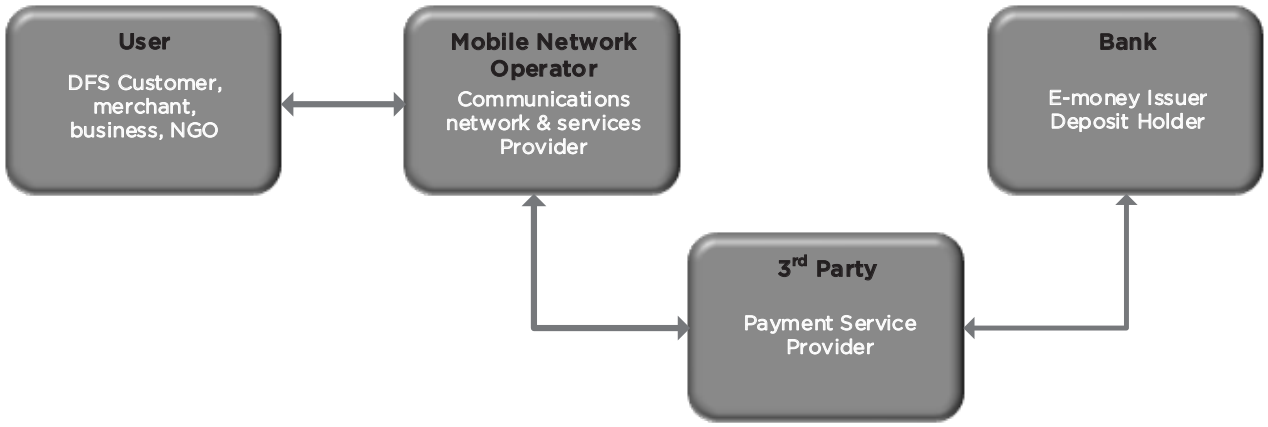
Figure 4 - MVNO Model



3.4 Hybrid Model

In a hybrid model, the critical roles are shared between the bank and MNO. They may involve a third party in the ecosystem who provides services that are not provided by either the MNO or the bank. For example, a third party could own the agent network and also plays the role of the payment service provider. Example is the Visa Qiwi wallet

Figure 5 - Hybrid model



4 ELEMENTS OF DFS ECOSYSTEM

In the scope of this report are five categories of mobile payments:

- Mobile money transfer using the MNO's channels (e.g. SMS, USSD, voice telephony) without a specific payment application downloaded onto the customer's mobile device which would be a featurephone (e.g. MPESA).
- Mobile payment application on mobile device of user linked to a bank account, debit card or credit card (e.g. Square, Venmo, Facebook messenger)
- Contactless payment technologies: Contactless payment technologies involve use of digital wallets, which can use different types of communications technologies for sending payment data from the user mobile device to the merchant POS. Some of the communications technologies used to transmit the information to the POS include Near Field Communication (NFC), QR code, magnetic secure transmission (MST), Bluetooth, SMS and Internet. The digital wallet could be stored either on the user mobile device or in the cloud.
- Near Sound Data Transfer (NSDT) Payments: NSDT uses the audio channel of the mobile phone to encrypt the data for payment transactions.
- Remote payments: This includes Internet payments (via credit card on an e-commerce website/Card-on-file transactions), direct carrier billing, SMS premium payments and mobile banking.

Digital currency wallets (e.g. Bitcoin) are outside the scope of this report.

In the next sections, the elements of the DFS ecosystem are considered for:

1) Mobile payments using USSD, SMS, IVR and STK
2) Mobile payment applications and digital wallets (e.g. Google Pay, Apple Pay, WeChat Pay).

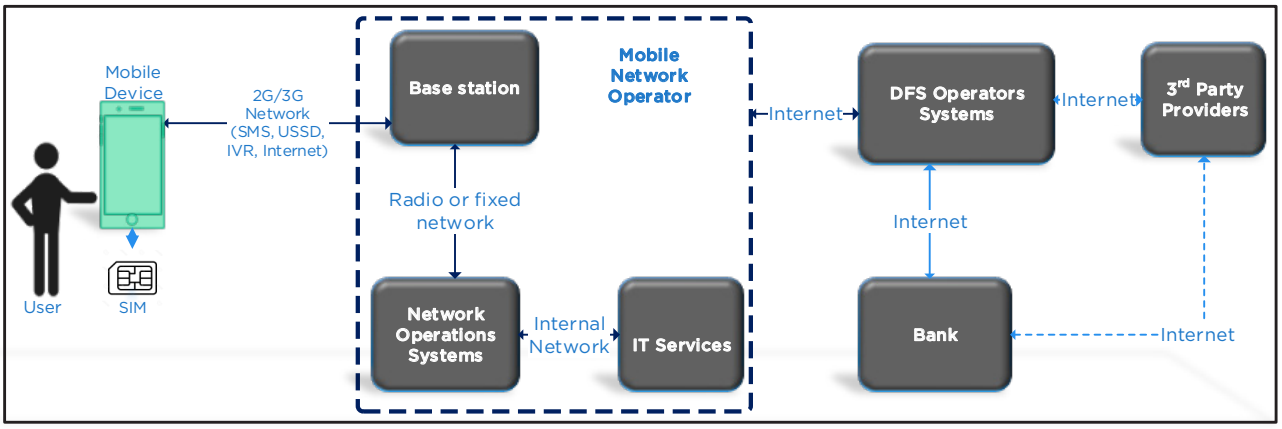
4.1 Elements of a DFS ecosystem using USSD, SMS, IVR, STK and NSDT

In figure 6, the major constituents within the ecosystem are shown. Not every element will be used in every deployment; for example, in cases where there is no Wi-Fi access or smartphone app available for a DFS service, communications from the user would be constrained to interactions through the mobile network, rather than through external Internet gateways or through reliance on a cloud service.

The stakeholders throughout the ecosystem are comprised of the following:

a) **User/Customer:** The customer is the target audience for a DFS service, who makes use of a mobile money application to interact with the service. Such interaction can happen either directly, through the mobile network or through the Internet (depending on features of the underlying mobile platform and the mobile money application); alternatively, a DFS agent who interacts with the DFS service on behalf of the customer can mediate such interaction. The agent can either

Figure 6 - Major Elements of the DFS Ecosystem



interface directly with the network or use a web gateway to provide such services.

b) **Mobile device:** The mobile device provides a platform for deploying a mobile money application. It is the main channel through which the customer (or agent interacting on the customer's behalf; for ease of exposition it is assumed that all further interactions with the service as being through the customer unless there are actions specifically required of the agent) interfaces with the DFS service. Mobile devices can be either feature phones or smartphones. Feature phones often containing limited resources and supporting limited interfaces for applications as well as limited connectivity options (e.g., 2G GSM services). Smartphones on the other hand, can support very powerful services with secure hardware elements and support for advanced networking and Wi-Fi connectivity. Both feature phones and smartphones contain SIM cards, some of which contain secure elements that can be leveraged by applications. The mobile device has an operating system, whose capabilities will be dependent on the resources available to it. Lightweight operating systems modelled after the Symbian OS are often found on feature phones, while smartphones commonly have the Android versions, IOS, Windows and other operating system installed.

c) **Base Station:** The communication link between the base station and the mobile handset is the primary channel for sending information between the user and the DFS provider. Notably, in systems where apps are not delivered to handsets but open networks are instead used (e.g., SMS, STK, IVR and USSD-based communication), this link is the only part of the overall architecture where encryption is in place on data transmitted to and from the consumer – once data is received at the base station, it is sent unencrypted through the provider networks. It is vital to the sustainability and feasibility of a DFS system that this link be robust, reliable, and virtually ubiquitous.

d) **Mobile Network:** The carrier network provides transit connectivity for information originating at the customer handset. It is comprised of different nodes that enable communication including the different gateways to external providers and to DFS providers, which may be associated with the particular carrier or may be external entities requiring Internet communication. Within this network resides gateways such as for USSD, IVR, STK and SMS, internal databases such as HLRs and VLRs, and Internet gateways that can act as connection points to the DFS provider. In cases where the mobile network operator also provides the DFS services, gateways to those services will be maintained within their internal network. The Mobile Switching Center (MSC) is at the core of the different nodes within the mobile network, to facilitate routing of communications using user data from the HLR or VLR. in Annex 1 shows detailed network nodes in the Mobile network, the SMSC gateway (GW), SAT(SIM Application Toolkit) GW, USSD gateway, IVR and internet GW enable use of the respective access modes for the user, we also show the MNO billing system for its purpose when used in some deployments by the MNO for charges on SMS, IVR or internet. A Mobile Virtual Network Operator (MVNO) may provide the services of the MNO to the DFS provider and the customer but the wireless network infrastructure is still provided by a network operator or enabler.

e) **DFS Provider:** The DFS provider interfaces the application contents originating in mobile opera-

tor networks with the back-end financial providers and for administering the customer's information in a secure fashion, and allowing for services, such as audits. In order for these operations to be secure, the DFS operator must be confident that the person accessing the data is who they claim to be. Audit logs must also be enabled to allow assessment of the contents of data within the network and of commands issued through the DFS application. Determining customer identity, credentialing, storing customer transaction data, providing enabling interfaces like API's for third parties, processing transactions from the different sources, is also a role performed by the DFS operator.

f) **Third-Party Providers:** External providers allow for the interfacing between carrier-based mobile money systems and provide the basis for connecting with back-end financial networks such as the banking infrastructure. Other roles that can be assumed by these external providers include operating the IT system or performing customer support, and, in some cases, they may interface directly between DFS systems or act as service and transaction aggregators.

g) **Digital Financial Services Application:** The application provides the interface by which the customer interacts with the DFS ecosystem. Applications can vary widely in the interfaces and richness of experience they provide to the customer, from menu-based systems on feature phones, designed to communicate via USSD, STK or SMS to voice designs that make use of IVR, or rich graphical interfaces on smartphones with end-to-end transport security provided by Internet-standard cryptographic algorithms. Interactions may occur using special application menus enabled by code, password, fingerprint, etc., enabling users to send money, make bill payments, top-up airtime, and check account balances.

4.2 Elements of a DFS ecosystem based on applications and digital wallets (e.g Google Pay, Apple pay, WeChat Pay, Samsung Pay).

There are different elements in ecosystems based on digital wallet models, among the key models are; device-centric mobile proximity wallet, device-centric mobile in-app wallet, Card-not-present card-on-file wallet, QR code and digital checkout wallets. All these have different technology platforms and employ different security models.

We describe each of the components of this ecosystem below:

a) Mobile Device

The mobile device provides a platform for the mobile wallets to be accessed, it hosts the digital wallet/application, the device OS and the secure element which is key for securing the DFS and application data.

The figure below illustrates some of the components of the user's mobile device.

i. **The NFC controller and the NFC antenna:** The NFC controller handles Near Field Communication protocols and routes communication between the application and the Secure Element, and between the Secure Element and the point-of-sale terminal. The NFC antenna relays the signals between the controller and the POS terminal.

ii. **The Secure Element:** The Secure Element (SE) is a tamper-resistant platform, typically a one-chip secure microcontroller designed for securely hosting applications and their confidential and cryptographic data. The use of the SE depends on the type of mobile wallet application and the type of mobile payment modes, for example, the SE in Apple devices emulates the card when used for Apple Pay. SEs exist in different forms to address the requirements of the various payment applications or digital wallets and their market needs. The SE can be an embedded and integrated in the mobile device hardware such as the SE in the iPhone. The SE can also be a SIM/UICC, networks using the GSM standard prefer this more commonly in the form of SIM Toolkit (STK) applications that leverage on the SIM as the secure element to offer a secure mobile money application. The SE can also be a secure memory card that is pluggable into the mobile device.

iii. **Host Card Emulation:** Mobile devices can emulate a contactless card using Host Card Emulation (HCE), which does not rely on a hardware secure element for storage of sensitive data such as payment card data. The HCE is a software infrastructure solution that enables a mobile wallet app to securely communicate through the NFC controller to pass payment card credentials or payment tokens to a contactless NFC-enabled POS terminal or reader, eliminating the need to use a secure element (SE). HCE is most commonly used on Android mobile devices to support Google Pay.

iv. **Mobile Wallets:** Mobile Wallets are applications/services accessed through the device that allows

Figure 7 below shows an ecosystem that is based on applications and digital wallets.

Figure 7 - DFS ecosystem based on applications and digital wallets

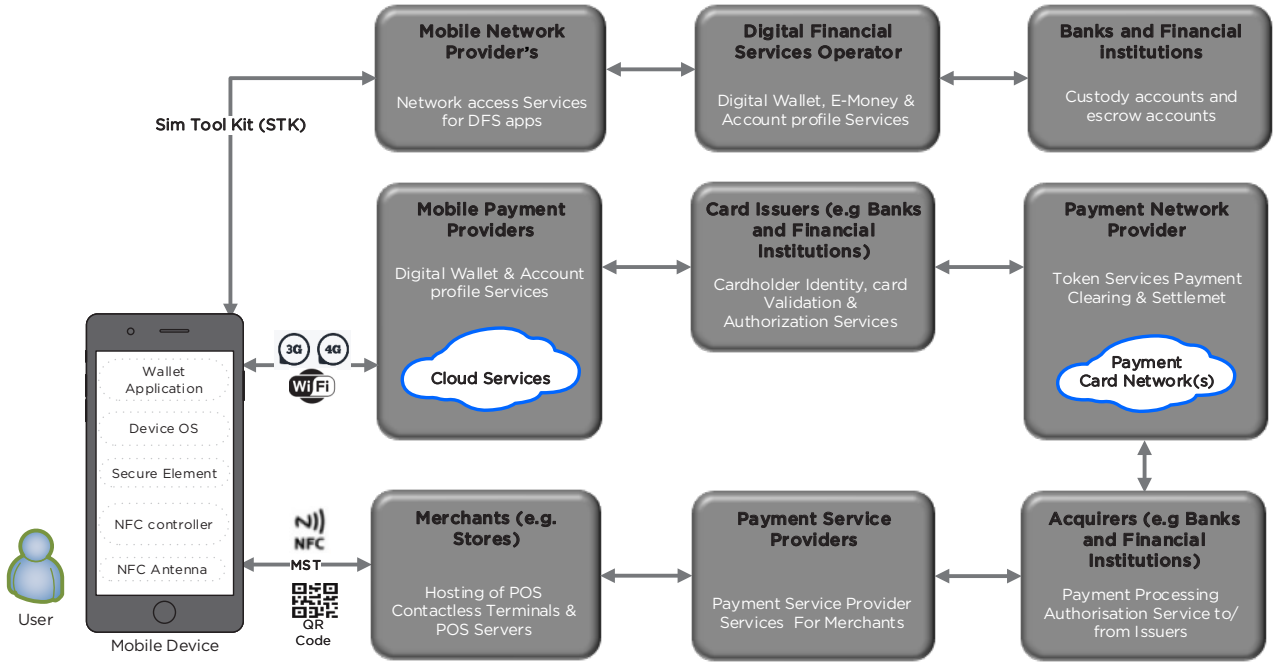
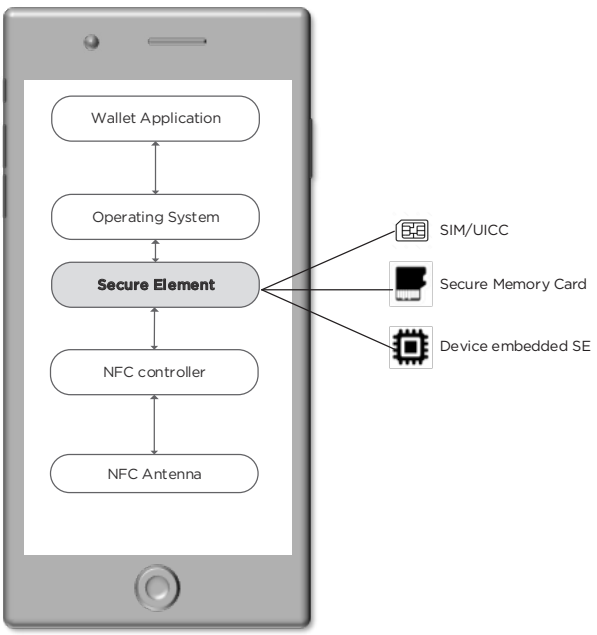


Figure 8 - Mobile device components



the wallet holder to securely access, manage and perform financial transactions like payments. Mobile Wallets like Samsung Pay and Apple Pay are specific to the device and the software and can be used as a replacement for credit and debit cards. On the other hand, other mobile/digital wallets are device agnostic and securely store the user's payment information and passwords for numerous payment methods and websites which enables completion of transactions easily and quickly and allows the use stronger authentication like biometrics, examples of other digital wallets are Google Pay, WeChat pay, Paypal, Alipay.

b) Merchant

Merchants accept payments from customers for goods or services, through a point of sale terminal or other means like a customer scanning a QR code or input of the merchant number into their payment application. Mobile devices are also used by merchants for payments, hence another inherent source of vulnerabilities.

c) Point of Sale Terminals

A Point of Sale (POS) terminal is an electronic device used to process mobile payments at the merchant location. The communication channels between the POS terminal and the Mobile device for proximity payments is through contactless Near Field Communication (NFC), Quick Response (QR) codes or

Magnetic Strip Technology (MST). 3G, 4G, and Wi-Fi are prevalently used for mobile wallets. Any risk that exists on a standard desktop or laptop computer may also exist on a mobile device.

Along with the standard communication methods of traditional desktop and laptop computers, mobile devices may also include multiple cellular technologies (e.g., LTE and GSM), GPS, Bluetooth, infrared (IR), and near-field communication (NFC) capabilities. Risk is further increased by removable media (e.g., SIM card and SD card), the internal electronics used for testing by the manufacturer, embedded sensors, and biometric readers.

i. **Near Field Communication (NFC):** NFC is a wireless communication protocol based on radio-frequency technology that allows data to be exchanged between devices that are a few centimetres apart. A wallet on an NFC-enabled mobile device is a software application stored on the mobile phone that manages and initiates payments. The mobile wallet accesses payment credentials such as tokenized payment cards, bank accounts, loyalty coupons, or financial information stored on the mobile phone in a trusted environment. The physical phone is used to initiate a payment transaction by tapping or holding the mobile device near a contactless-enabled POS terminal.
ii. **Magnetic Strip Technology (MST):** Magnetic Secure Transmission, or MST, generates a magnetic signal like that of a traditional payment card when swiped. The magnetic signal is then sent from the device to the POS terminal. MST is enabled on some Samsung mobile phones.
iii. **QR codes:** QR codes offer contactless payment alternatives in two ways:

    a. Payer scans the merchant's QR code, the merchant generates a transaction QR code or displays their assigned static QR code, the payer will then scan the code using their phone camera and the payment application will interpret the payment or merchant details to initiate the transaction that can be completed by entering a PIN
    b. Merchant scans payers QR code; the customer through their payment application will generate a unique transaction-specific QR code to the merchant; the merchant scans the code through their payment application using a QR scanner to initiate the transaction that can be completed by entering a PIN.

iv. **3G/4G and WiFi**

    In addition to 3G and 4G cellular networks, mobile devices can also connect to wireless (Wi-Fi) networks, these networks enable the mobile application on the device to interact with the payment service providers. 3G, 4G, and WiFi networks are usually provided by the Mobile Network Operator.

d) Token Service Provider (TSP)

The TSP manages the life cycle of tokens. Additional services typically include, creating and storing tokens, managing the token lifecycle, processing token transactions, performing token-to-PAN mapping, cardholder validation, including provisioning services, key management for device-based wallets using HCE, verification services for the transaction and device validity.

e) Acquirer

The acquirer is the financial institution or bank that passes the merchant's transactions along to the applicable issuing banks to receive payment.

f) Issuer

The issuer is the financial institution that issues credit cards to consumers on behalf of the card networks

g) Wallet Service Provider (WSP)

WSPs offer specific wallet solutions that use various communications technology for mobile payments.

h) Payment Service Provider (PSP)

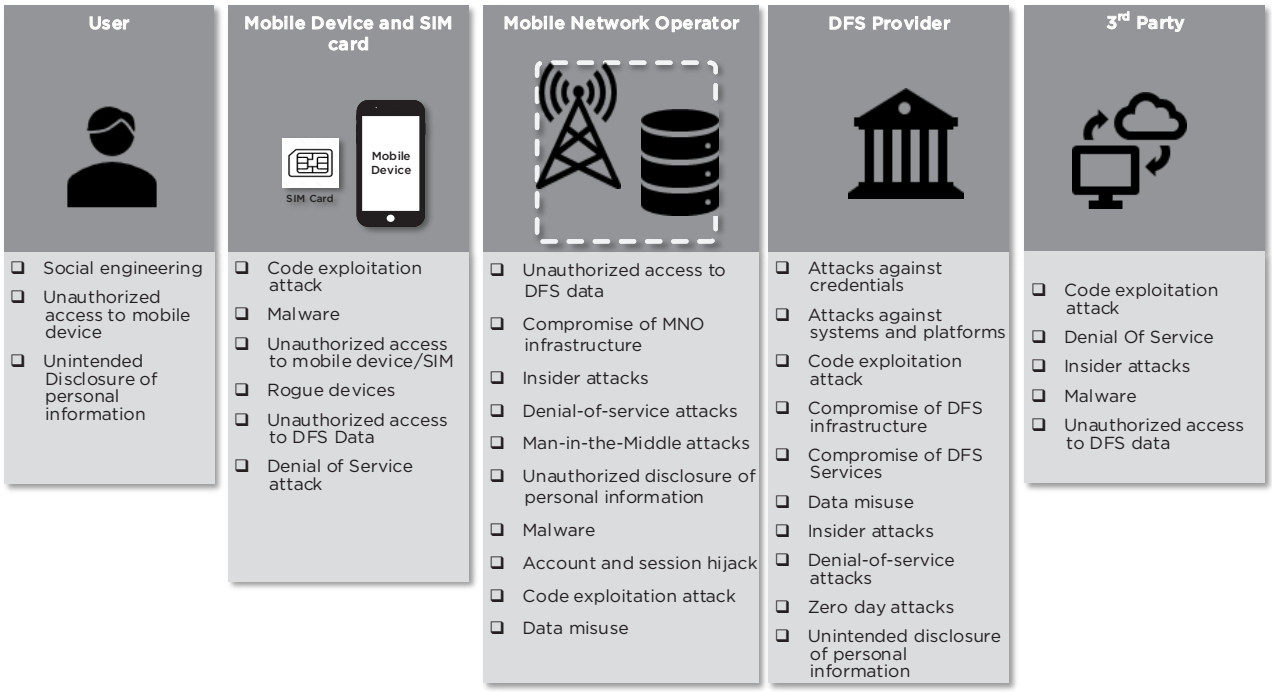
PSPs provide the various methods that allow a merchant to accept payments from mobile and digital wallets. The PSP can connect to multiple acquirers as well as payment and card networks. By enlisting the services of a PSP, the merchant becomes less dependent on financial institutions to manage transactions, since the PSP can manage bank accounts as well as relationships with the external network.

5 SECURITY THREATS

5.1 Threats to DFS using USSD, SMS, IVR, STK and NSDT

The diagram below summarises the threats of DFS applications based on USSD, SMS, IVR, STK and NSDT.

Figure 9 - Threats to DFS systems using USSD, SMS, IVR and NSDT



5.2 Threats to DFS ecosystem based on apps and digital wallets

Mobile payment applications/wallets enable digital financial services through applications installed on the mobile device, the nature of financial applications and channels used will depend on the device capabilities, for example Samsung pay and Apple pay only for Samsung devices and Apple devices, whereas Google Pay can be used on all android devices, mobile payment applications utilizing Quick Response codes like WeChat Pay and AliPay can be used by all smartphones with a camera.

Table 1 – Summary of threats to DFS ecosystem based on apps and digital wallets

Element	Threats
Mobile Payment application	• Reverse engineering the application source code • Tampering with the mobile payment application • Exploit of mobile payment application vulnerabilities • Installation of rootkits/malware • Mobile Operating System Access Permissions
Mobile Device	• Installation of rogue applications and malware • Unauthorized access to lost or stolen mobile device • Malware installation on the device
Merchant Threats	• OS malware: Attackers may upload POS malware on POS devices that could be used to remotely access and payment data. • QR code compromise: QR codes have inherent threats because they are not easily readable by the human eye, attackers could easily replace a merchants QR code with nefarious codes that could be embedded with malicious content. The malicious content may be phishing URLs, malicious mobile apps. • Man-in-the-Middle attacks against POS contactless terminal and POS server: attackers can exploit network security weaknesses such as lack of firewalls to protect the merchants' internal network. • Relay attacks against NFC enabled POS contactless terminals: Relay software installed on a mobile device can relay commands and responses between the Secure Element and a card emulator that is installed as a proxy on the mobile POS across a wireless network. • Use of default PINs to access POS terminals e.g. default 166816 and Z66816 (1)
Acquirers	• Payment processing systems compromise: When requesting tokens and cryptograms from the issuer payment network, an attacker can obtain a large amount of cardholder data by installing malware and remote access tools at any of the internal network payment processing servers. • Network and interface security compromise, attackers may exploit insecure point-to-point connections between the acquirer and issuer by compromising the network provider, attackers can then use this level of access to be able to monitor and manipulate API calls.
Payment Service Provider	• Compromise of payment gateways: payment gateways can be targeted by attackers with the intent of accessing and compromising the transaction data in transit from merchants to acquiring banks. • Compromise of software vulnerabilities in POS contactless terminals that are provided to merchants by PSPs that can process data from different channels including Card present, contactless payments, and card not present. • Compromise of insecure networks; attackers could perform Man in the middle attacks to spoof sensitive data in transit from the PSP to the acquirer is the provider is using weak or insecure connections like lower versions of TLS and SSL. • Design flaws and unpatched software vulnerabilities in POS terminal machines and POS systems and payment gateways to/from acquirers
Issuers	• Payment processing systems compromise: When requesting tokens and cryptograms from the issuer payment network, an attacker can obtain large amount of cardholder data by installing malware and remote access tools at any of the internal network payment processing servers. • Network and interface security compromise, attackers may exploit insecure point to point connections between the acquirer and issuer by compromising the network provider, attackers can then use this level of access to be able to monitor and manipulate API calls.

Digital payment applications communication between the device/application and the payment provider is mainly reliant on internet channel through Wi-Fi, 3G and 4G networks, and/or a payment can be effected to a merchant Point Of Sale device using Magnetic Secure Transmission, scanning a Quick Response code or Near Field Communication (NFC).

The use of these channels presents other threats and elements (POS, Acquirers, Payment Network Providers, Card issuers, Mobile Payment providers). Based on these components, we identify the following threats to DFS ecosystem based on mobile applications and wallets (i.e. Android, iOS).

Based on the stakeholders within the DFS ecosystem, we consider merchants, acquirers, payment service providers, and issuers to be third-party providers (we show these individual entities in the expanded figure of the DFS ecosystem in **Annex 1**). While we list the general threats that these entities face here, the specific mitigations for addressing the threats that they face are out of scope for this document. We recommend consulting the PCI-DSS

and the Cyber Resilience Oversight Expectations for Financial Market Infrastructures report[3] to read more about mitigations.

6 DFS SECURITY ASSURANCE FRAMEWORK

The DFS security assurance framework follows similar principles from the ISO/IEC 27000 family - Information Security Management Systems, Payment Card Industry Data Security Standard (PCI-DSS) v3.2, Payment Applications Data Security Standards (PA-DSS), National Institute of Standards and Technology Special Publication 800-53, Revision 4. Technical guidelines from the Centre for Internet Security (CIS controls Version 7), the Open Web Security Application Project (OWASP) commonly referred to as OWASP Top 10 and used these as benchmarks to identify controls that are particular to the digital financial services ecosystem.

This framework consists of the following components:

a) A security risk assessment based on ISO/IEC 27005 –Security techniques -Information security risk management (**Section 7**).
b) Assessment of threats and vulnerabilities to the underlying infrastructure, DFS applications, services, network operations and third-party providers involved in the ecosystem for DFS delivery (**Section 8**).
c) Mitigation strategies based on the outcome of (b) above (**Section 8**).

This framework identifies

i. The various security threats to DFS assets in each of the security dimensions
ii. The related vulnerabilities that can be exploited by these threats.
iii. Security control measures that can be implemented by DFS stakeholders against the threats and vulnerabilities are proposed. The security control measure can fall in one or more of the eight Security Dimensions in ITU-T Recommendation X.805

7 RISK ASSESSMENT METHODOLOGY

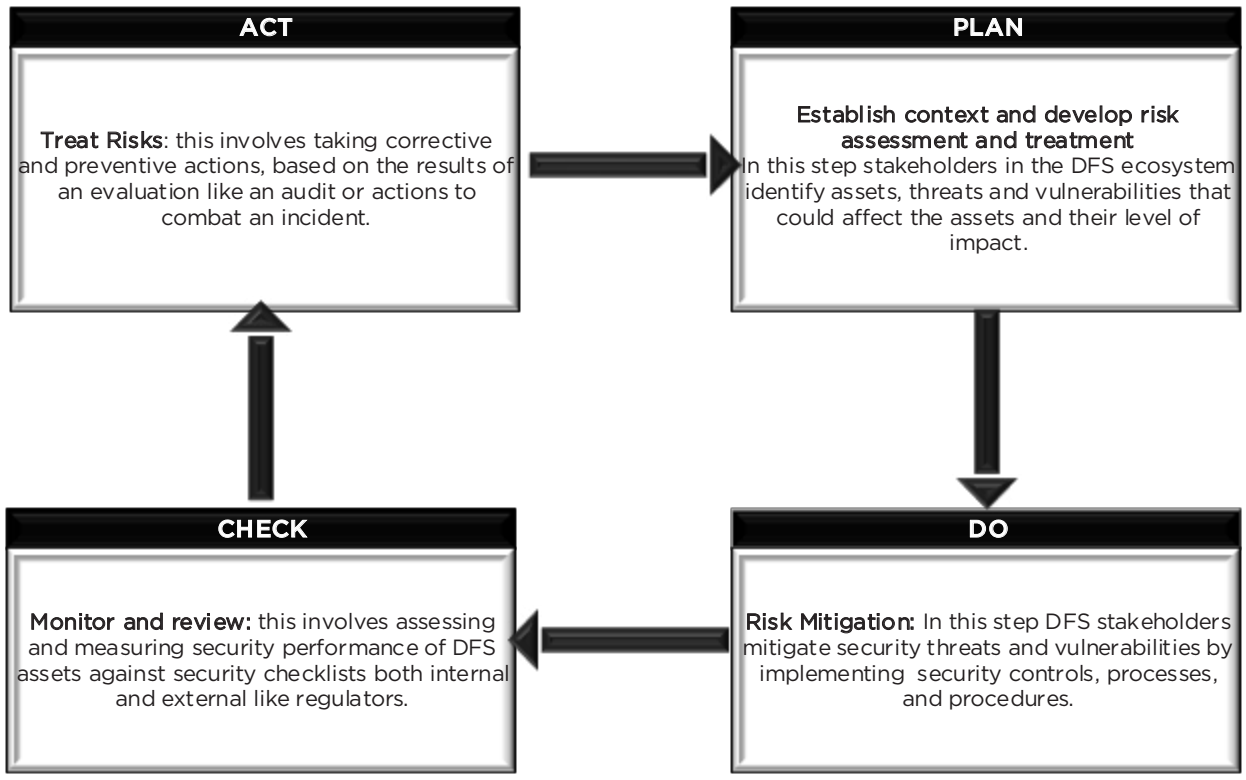
In order to ensure a security model that is sustainable and continuously improves DFS security, this framework uses the Deming cycle, a four-step quality model divided into four phases: Plan, Do, Check and Act (PDCA). In the PDCA based implementation methodology, activities and outcomes that have to be achieved in each of the four phases are identified.

In the DFS ecosystem, multiple stakeholders are involved and the PDCA is designed with activities that assure overall end to end security of the DFS ecosystem, the diagram below shows the DFS security framework model based on PDCA.

Monitoring and review in the DFS environment may take different forms depending on the stakeholder for example the regulator reviewing the security controls set by the DFS provider to assure security for the DFS users or internal and external reviews of the DFS environment by auditors. Thus, the monitoring phase also deals with escalating ad reporting of the risks to the relevant stakeholders.

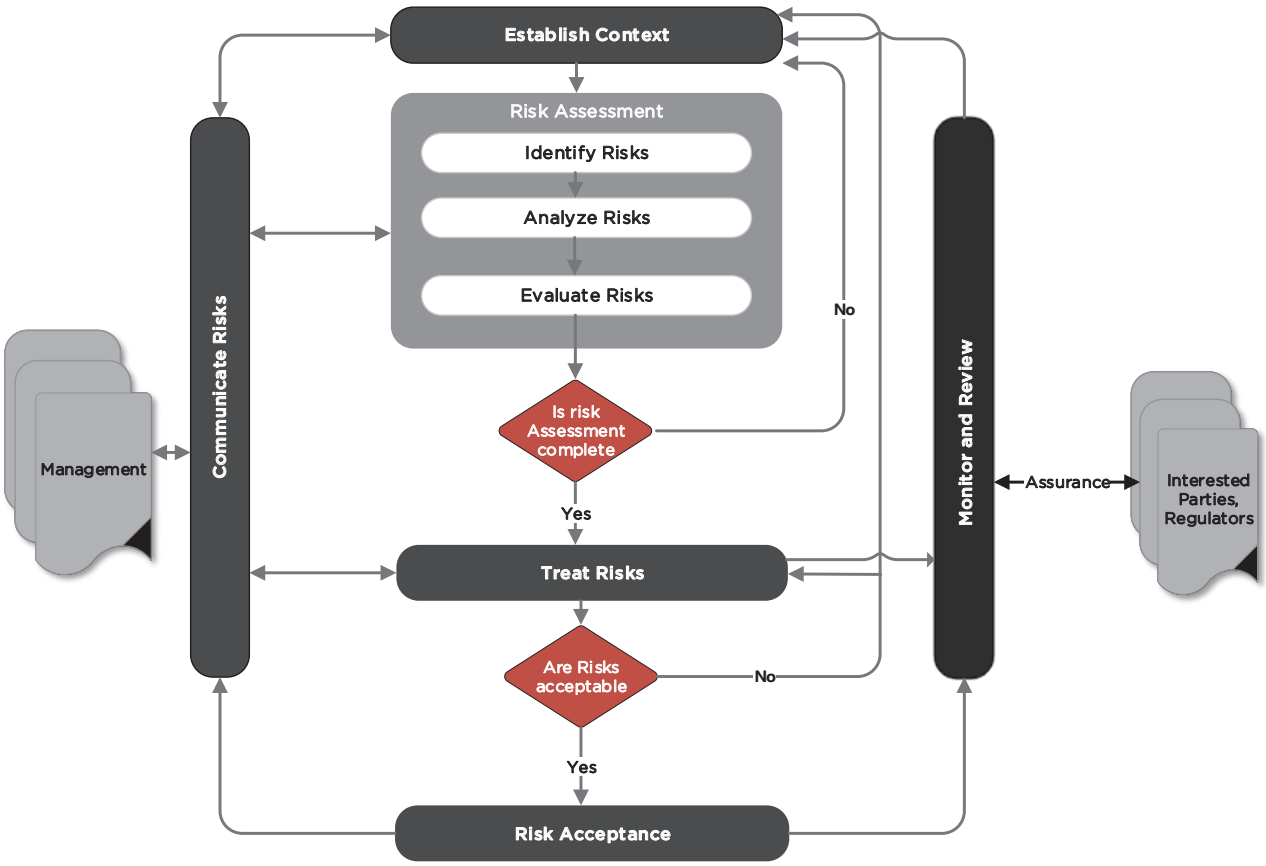
Communicating with management during all phases of the risk management process ensures understanding and ownership of the roles and responsibilities which is key for establishing the context appropriately, adequate identification of risks, multi-stakeholder risk analysis and evaluation. The communication with management gives a platform for a broader consultation and process review with all the DFS stakeholders which helps to secure endorsement and support for the risk treatment plans based on relevant and accurate view of the risks within the ecosystem.

Figure 10 - Plan, Do, Check, Act



A high-level risk management process plan is shown in figure 11 below, which encompasses the four phases of the PDCA.

Figure 11 - Risk Management process



7.1 Scope

The DFS security assurance framework is applicable to stakeholders in the DFS ecosystem. It defines security controls to be adopted by DFS users, mobile network operators, providers including banks and other licensed non-bank financial institutions, who supply financial products and services through digital means; these controls can be applied to the assets such as the infrastructure, applications and devices that make digital financial services possible.

For the user, the framework focuses on the security controls for the devices like mobile handsets used to access digital financial services. The means and technology are usually provided by a mobile network operator that allows for communication between the user and the DFS provider, the framework focuses on what the communications network provider has to do to secure the ecosystem.

This framework also includes the controls that have to be deployed by the DFS provider who may be a financial institution like a bank or non-bank provider, in some cases the communications network provider is also the digital financial services provider.

7.2 Establishing a context

This is the initial step in the risk management process and the objective is for the stakeholder to gain an understanding the DFS operating environment. This involves identifying internal and external events that affect the ability to achieve end to end security, it is therefore important for the stakeholder to understand and assess the internal and external context within which digital financial services operate, this also helps frame the scope of the risk assessment.

In order to establish the internal context, the following must be formulated.

a. The Information Security Management System based on the ISO/IEC 27001 the normative documents must be considered or implemented.
b. DFS stakeholder overall organization structure and how DFS fit into this structure of the organizations and its objectives.
c. The DFS assets this includes the supporting technology and information systems, physical infrastructure, software applications, hardware, agent networks, customer/agent/merchant devices that are used to access DFS.
d. Existing internal controls, previous security risk events, previous fraud incidents, previous audit reports and DFS project documents.
e. Regulatory requirements.
f. The risk tolerance and risk appetite.

Amongst other aspects, the external context considers the following.

a. Law and regulations related to digital financial services
b. Key DFS stakeholders.
c. Political and social environment, this includes demographics like level of education of the population, mobile device uptake and level of smartphone penetration to the target population.
d. Competing alternatives and complementing services to digital financial services.
e. Emerging risks and their influence, both to the financial service and stakeholders.

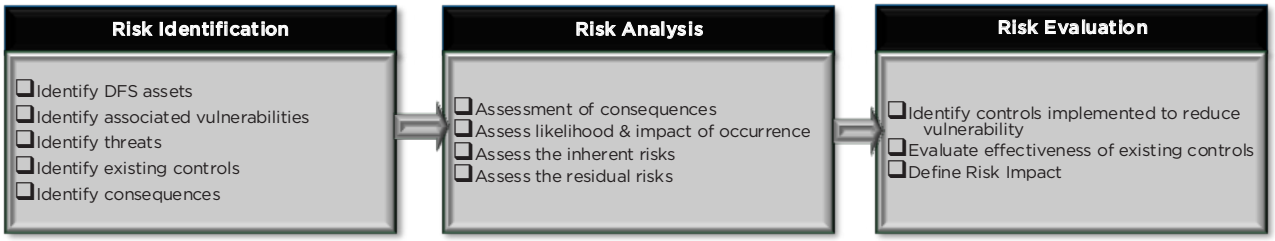
The outcome of this phase is a recorded summary of all information gathered. The information will form input into the risk assessment process.

7.3 Security Assessment

The risk assessment helps stakeholders to get indicative measures of the current security level in the DFS ecosystem, the security risk assessment process includes identification, analysis and evaluation of risks. The DFS risk assessment should be conducted periodically and the results feedback to management.

The overview of the process flow is shown below.

Figure 12 - Risk assessment process flow



7.4 Risk Identification

Risk identification is to determine what, how, where and why DFS vulnerabilities might be exploited, this involves identifying critical DFS assets, associated threats and vulnerabilities, probability of occurrence, weaknesses in existing controls, impact or consequences of threats and vulnerabilities once exploited. In the process of risk identification, the stakeholder should be cognizant of the internal and external considerations in section 7.2 above.

In risk identification DFS stakeholders should consider five critical actions:

i. **Asset Identification:** This entails listing all assets in the DFS ecosystem and who is responsible for them, assets in DFS include, but not limited to the physical infrastructure, software applications, hardware, agent equipment, customer/agent/merchant devices used to access DFS services and the communication network devices. Identification enables the stakeholder to classify the DFS assets based the impact an incident to the asset will have to the DFS ecosystem, classification aims at categorizing assets based on the value and criticality to the DFS ecosystem.
ii. **Vulnerability Identification:** a vulnerability is a weakness or flaw that enables a threat to attack an asset, these include, but are not limited to, weaknesses in the: physical layout, organization procedures, personnel, management, hardware, software, network etc. They may be exploited by a threat, which may cause harm or damage to the system. The vulnerabilities identified should be

highlighted in the risk assessment alongside the threats that affect an asset.

iii. **Threat identification:** A threat is a potential for a source to exploit (accidentally or intentionally) a specific vulnerability. Threats can to DFS assets can be natural e.g. earthquake and floods, human e.g. theft and fraud or technical e.g. malware or server failures. Once a threat is identified, all information assets should be analyzed to uncover any vulnerabilities present that can be exploited by the threat.

iv. **Existing control identification:** a list of all existing and planned controls, their implementation and usage status.

v. **Consequence identification:** The magnitude of damage that could be caused by an incidents or a threat successfully exploiting a vulnerability. This process identifies the assets that can be affected and severity of impact. The magnitude of damage to a DFS asset in most cases is higher than the simple replacement cost, they are various damage considerations which may be monetary, technical, human and regulatory.

7.5 Risk Analysis

Risk analysis helps to understand the overall likelihood and impact of the threat on asset, which are both important for decision making and prioritizing actions to address the most critical risks and significant risks (risks with the greatest impact). The output of the risk analysis is an updated risk register that includes the probability and impact ratings of each risk, Risk analysis may be done quantitatively or qualitatively, or a combination of both.

The following process should be outputs of the risk analysis phase

i. Assessment of consequences; the business impact upon the organization that might result from possible or actual information security incidents should be assessed, taking into account the consequences of a breach of information security such as loss of confidentiality, integrity or availability of the assets. Amongst others, the security consequences to DFS can also be in terms of financial loss, image reputation, loss goodwill, regulatory bans and fines.

ii. Assess the probability of occurrence of a potential threat that can exploit vulnerability and its impact if successful. The probability of occurrence should take into consideration the preventive, detective controls in place, their effectiveness, implementation and usage.

iii. Define Inherent risk rating as a product of Probability and Impact. The purpose of the inherent risk rating is to assist management in prioritizing management actions to address the most significant risks.

iv. Define residual risk by assessing the effectiveness of the controls that exist for treating the risk. The controls implemented should reduce the risks to an acceptable level based on the DFS stakeholders risk appetite.

7.6 Risk Evaluation

During the risk evaluation process, the DFS stakeholder will compare identified risks and evaluate them against predetermined risk criteria to help determine the risks net effect to the DFS ecosystem. It also involves determining the effectiveness of the existing controls; that is, analyzing the probability and impact of the risks after considering existing controls then estimating the residual risks, this process facilities prioritization and decision making relating to the risk treatment and implementation.

When performing a risk evaluation, the following should be considered:

i. Determine the effectiveness of existing controls in place for each threat vulnerability combination for an asset class i.e. effectiveness of controls in place that would mitigate the threat vulnerability pairing

ii. Determine the Risk Impact

iii. Determine the Residual Risk Rating as product of Probability of occurrence and Impact

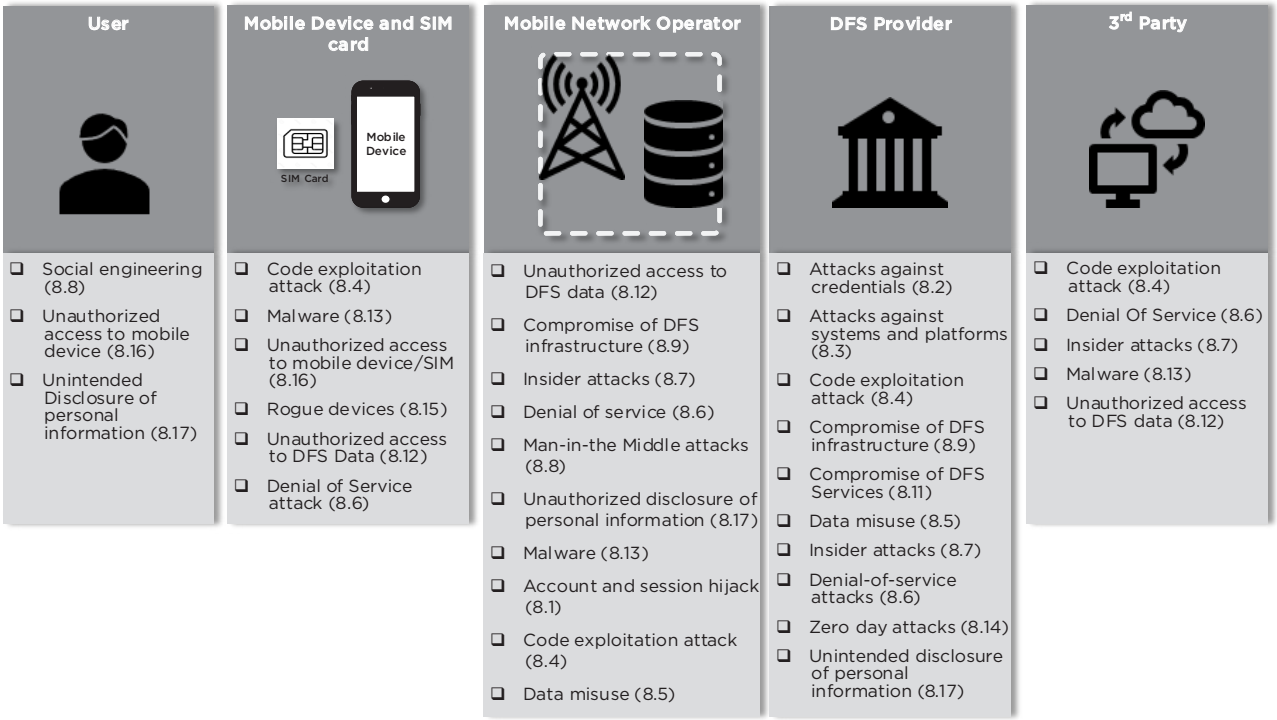
8 ASSESSMENT OF DFS SECURITY VULNERABILITIES, THREATS AND MITIGATION MEASURES

In order to systematically counter the threats and vulnerabilities to the DFS ecosystem described in the above sections, we suggest controls for each of the entities within the ecosystem based on the eight security dimensions aimed at achieving end-to-end security.

Because there are often commonalities in the threats faced by entities throughout the DFS ecosystem, for ease of discussion we first consider a standardized threat that we have identified, the entity affected by the general threat, and the vulnerabilities, risks, and suggested mitigations and controls that can be deployed by that particular entity. We place the vulnerabilities in the context of their impact on the ITU-T X.805 security dimensions (SD).

The diagram in Figure below shows how the security threats identified earlier in Figure 9, are mapped to the 119 security control measures outlined in the sections below (the section number of the report appears in parentheses indicating where the relevant control is discussed).

Figure 13 - Mapping of threats to security controls



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 confidentiality)	**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 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.

8.2 Threat: Attacks against credentials

We broadly characterize these threats as those designed to steal or tamper with the credentials for users of DFS systems and mobile devices

Affected entities	Risk and Vulnerability	Controls
Mobile Device	The risk of ***unauthorized access and takeover of a user's DFS account*** occurs due to the following vulnerabilities:	
	- Use of weak passwords/PINs at the application level, making these credentials susceptible to brute-force attacks (SD: authentication)	**C9:** Require the use of longer and not easily guessed PINs/passwords in mobile money applications. Caution should be exercised before mandating the use of complex PINs; ensure that any such adoption goes hand-in-hand with user education, as overly complex PINs are likely to be written down or entered by others, thus degrading their security.
	- Use of simple PINs for accessing the mobile device (SD: authentication)	**C10:** Use robust authentication mechanisms to demonstrate ownership of the device. Because the keyspace of PINs makes them susceptible to a brute-force attack, consider the use of longer PINs or alphanumeric PINs, such as easily remembered passphrases.
	The risk of ***credential-stealing through Man in the Middle attacks*** is due to the following vulnerability: - Server misconfiguration (SD: authentication)	**C11:** DFS applications should be designed to verify the server name they are connecting to.
DFS provider	The risk of ***DFS system compromise*** is due to the following vulnerability: - 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)

8.3 Threat: Attacks against systems and platforms

We characterize these attacks as those that a remote adversary can carry out to spy on or modify information without insider credentials or other privileged access.

Affected entities	Risk and vulnerability	Controls
Mobile user	The risk of ***spying on and remotely stealing credentials from user devices*** is due to the following vulnerabilities:	
	- Unverified malicious binary SMS SIM updates (SD: authentication)	**C13:** Provide the mobile user with the ability to trust or distrust individual binary-based SMS messages. Doing so could prevent malicious updates to the SIM card
MNO	- 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).
	The risks of ***account access and compromise*** and ***denial of service*** are due to the following vulnerability: - 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.
DFS Provider	The risks of ***account access, compromise,*** and ***denial of service*** are due to the following vulnerability: - Insufficient protection of internal systems against external adversaries (SD: access control)	**C16:** Avoid direct access by external systems to the DFS back-end systems by setting up a DMZ that logically separates the DFS system from all other internal and external systems.

8.4 Threat: Code Exploitation Attacks

We characterize these attacks as being those that are aimed at the code comprising DFS applications.

Affected entity	Risk and vulnerability	Control
DFS Provider	The risk of ***DFS application compromise*** is due to the following vulnerability: - 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.

8.5 Threat: Data Misuse

We characterize this threat as relating to the mishandling of sensitive customer data[4].

Affected entity	Risks and vulnerabilities	Controls
MNO	The risks of ***unauthorized access*** *to user data* and ***interception of data in transit*** are due to the following vulnerability: - 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.
DFS Provider and Third-party providers	The risk of ***sensitive data exposure*** is due to the following vulnerabilities:	
	- 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.
	- Exposure of customer sensitive information during transactions or through APIs (SD: privacy)	**C20:** DFS providers should restrict the sharing of information to be only the minimum amount required for transactions with third parties and service providers.
	- 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.

8.6 Threat: Denial of Service Attacks

We characterize these attacks as being designed to prevent services within the DFS ecosystem from being offered.

Affected entity	Risks and vulnerabilities	Controls
MNO	The risks of ***inability to perform a transaction due to a service outage*** and ***transaction failure due to high transaction delays*** are due to the following vulnerabilities:	
	- Network failure due to insufficient network capacity or to maintenance or design (SD: availability)	**C22:** The mobile network operator should take steps to ensure network high network availability to allow access to DFS services through USSD, SMS, and the Internet.
		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.
DFS Provider	- 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.
	The risks of ***unauthorised access*** *to user data are* also due to the following vulnerability: - Enabling unnecessary services (SD: data confidentiality)	**C25:** Inbound internet traffic should be limited and continuously monitored.
		C26: Set restrictive firewall rules by default, use ports whitelisting, use packet filters, and continuously monitor access to whitelisted/permitted ports and IP's.

8.7 Threat: Insider Attacks

We characterize these attacks as being performed by adversaries within the organization's perimeter, often who have elevated access and privileges to resources.

Affected entity	Risks and vulnerabilities	Controls
DFS Provider	The risk of ***data exposure and modification*** is due to the following vulnerabilities:	
	- 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.
	- 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.
	- 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 only 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).

(continued)

Affected entity	Risks and vulnerabilities	Controls
DFS Provider	The following vulnerabilities cause the risk of ***data inaccuracy and inconsistency***:	**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.
	- 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. Techniques such as digital signatures across database columns can be used to detect user data modification.
		C32: Ensure all test data is removed from code before it is migrated to the production environment.
	- 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. Use digital signatures attached to actions, particularly those that arrive over a network connection.
	- 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 have to be deployed securely.

8.8 Threat: Man-in-the-middle and social engineering attacks

We group these two types of attacks because they both involve an adversary actively interposing themselves into communication or interaction (e.g., between a user and device or MNO, or a communication interposition between parties).

Affected entity	Risks and vulnerabilities	Controls
Mobile User	The risk of ***data exposure and modification*** is due to the following vulnerabilities:	
	- Unverified and unsigned applications (SD: privacy, data integrity)	**C35:** Critical focus should be on guiding the customer to access and download DFS applications through official application release channels to mitigate the risk of running malware-infected apps.
	- Unverified inputs such as unsolicited SMS messages, in-app advertisements, or e-mails (SD: data integrity)	**C36:** MNOs and DFS providers should undertake active customer awareness campaigns to educate consumers and internal staff about malicious messages, phishing attacks, and spoofing.
	- Insufficiently protected credentials (SD: access control)	**C37:** Mask user passwords and PINs, actively educate customers on shoulder surfing and safe PIN/password usage to avoid shoulder surfing and writing down of passwords.

(continued)

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.
DFS Provider	The risk of ***user account takeover*** is due to the following vulnerability: - 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.
Third-Party Providers	The risk of ***exposure of sensitive information*** is due to the following vulnerabilities:	
	- 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.
	- Lack of encryption of communications (SD: communication security)	**C42:** Use digital signatures to identify third parties connected to the DFS system when transactions are being performed.
	- Insufficient management of certificate or key materials (SD: access control)	**C43:** Only trusted keys and certificates should be accepted to allow data exchange between DFS providers and third parties, and they should be protected from disclosure.
	The risk of ***identity theft and failed transactions*** is due to the following vulnerability: - 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.

8.9 Threat: Compromise of DFS Infrastructure

We characterize these attacks as targeting the underlying infrastructure of the DFS ecosystem.

Affected entity	Risks and vulnerabilities	Controls
DFS Provider	The risk of ***infrastructure and data compromise*** is due to the following vulnerability: - Insecure and inadequate access controls on user accounts (SD: access control)	**C45:** Use multi-factor or multi-model authentication for access to DFS accounts.

(continued)

Affected entity	Risks and vulnerabilities	Controls
DFS Provider	The risk of ***service outages and inability to transact*** is due to the following vulnerability: - 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.
		C47: Review installation, vendor, support accounts, and access points to DFS systems and infrastructure. All of these accounts should be deactivated or allocated to appropriate user profiles.
	The risks of ***data exfiltration and modification, compromise of transaction integrity,*** and ***interruption of service*** are due to the following vulnerability: - 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.
		C49: Have scheduled, regular backups for DFS systems. Regularly test and securely store backups offline and offsite in an encrypted form.
		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)
Third-Party Provider	The risk of ***inability for the user to transact*** is due to the following vulnerability: - 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.

8.10 Threat: SIM attacks

The general threat is the ability of an attacker to gain unauthorized access to a DFS user's SIM card. The vulnerabilities are manifested in different ways at the Mobile network operator, DFS provider, and Mobile user.

Affected entity	Risks and vulnerabilities	Controls
MNO	The risks of ***account takeover and unauthorized transactions*** occur because of the following vulnerabilities: - 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.
		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.
		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.

(continued)

Affected entity	Risks and vulnerabilities	Controls
MNO	The risks of ***account takeover and unauthorized transactions*** occur because of the following vulnerabilities: - 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).
		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.
Mobile User	The risk of ***unauthorized access to user mobile data*** occurs because of the following vulnerability: - 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.
DFS Provider	The risk of ***lost access to accounts or reputational damage*** occurs because of the following vulnerability: - Inadequacies in SIM swap and recycling process[5] (SD: data integrity)	**C58:** DFS providers should ensure they have procedures in place to detect and avert suspicious SIM swaps and SIM recycle by: 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.

8.11 Threat: Compromise of DFS Services

The general threat is the ability of an attacker to breach a financial service without being detected. The vulnerabilities are manifested in different ways at the DFS provider

Affected Entity	Risks and vulnerabilities	Controls
DFS provider	The risks of ***service failure and compromise of DFS services and data*** occurs because of the following vulnerabilities:	
	- Unauthorized changes to system configuration and log files and data (SD: Data Integrity)	**C59:** Protect against tampering and allow only online transactions 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.

(continued)

Affected Entity	Risks and vulnerabilities	Controls
DFS provider	- 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.
		C61: Check incoming data against expected values in API related data schema, for USSD, perform XML validation of XML over HTTP requests.
		C62: Use analytics systems to check user velocity between transactions, transaction time of day access tracking for additional authorization validation checks.
		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).

8.12 Threat: Unauthorized access to DFS data

The general threat is the ability of an attacker to gain unauthorized access to DFS users' DFS data. The vulnerabilities are manifested in different ways at the Mobile network operator, DFS provider and Mobile User.

Affected Entity	Risks and vulnerabilities	Controls
Mobile User	The risk of ***unauthorized access to DFS user mobile data*** occurs because of the following vulnerabilities:	
	- Inadequate user account access control mechanisms (SD: Access Control)	**C64:** DFS users should set their account PIN. Where the first-time PIN is set by the DFS provider system or its agents, the PIN is unique for each user and must require use change at first login.
	- Limited controls to access sensitive data on the device (SD: Access Control)	**C65**: DFS users should set strong passwords and avoid easily guessable pins for their devices like birthdays.
		C66: Ensure sensitive DFS information is stored in secure portions of the mobile device.
		C67: App developers should ensure that before application installation on the device, user authentication is required.
		C68: App developers should ensure that access to DFS infrastructure, application, and services should only be authorised after identity authentication. Use multi-factor authentication, Something the user knows (such as a PIN), Something they have (such as a SIMcard), Something they are (such as a fingerprint or other biometric method).
		C69: App developers should ensure that DFS applications securely manage access credentials.

(continued)

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]
DFS Provider	The risk of ***exposure of sensitive customer data occurs*** because of the following vulnerabilities.	
	- 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.
	- Use of weak encryption. (SD: Communication Security)	**C81:** Use strong encryption standards like TLS encryption v1.2 and higher for API communication.

(continued)

Affected Entity	Risks and vulnerabilities	Controls
DFS Provider	- Inadequate DFS user access control and monitoring. (SD: Access Control)	**C82:** Extend threat detection to explicitly incorporate threats associated with APIs.
		C83: Limit remote login access and minimize privileges to remote login sessions to backend DFS systems.
		C84: Limit the lifetime of TLS certificates to 825 days.
		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.
		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.
		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.
		C88: Set user roles to define access rights based on the principle of least privilege.
		C89: After termination of a user, agent, merchant, payment service providers or third parties disable/deactivate respective accounts
		C90: Set account dormancy period and disable dormant accounts at dormancy maturity.
		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)
		C92: Limit control, monitor, and periodically review privileged access to DFS systems, including user addition, modification, and deletion.
		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.
	- 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.
Third-party	- 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.

8.13 Threat: Malware

We characterize this general threat as that of elements within the DFS being susceptible to infected by malware.

Affected Entity	Risks and vulnerabilities	Controls
Third-Party, DFS Provider	The risks due to ***malware attacks and inability to transact, service outages, and unauthorised access to data*** occur at the Merchant / DFS provider because of the following vulnerabilities:	
	- Failure to use anti-malware or anti-virus software is used or updated regularly (SD: Availability)	**C96:** Deploy security software products on all mobile devices, including antivirus, antispyware, and software authentication products to protect systems from current and evolving malicious software threats. All software should be installed from a trusted source.
		C97: If anti-malware software is not available, employ MAM (Mobile Application Management) or MDM solutions that can monitor, evaluate, and remove malicious software and applications from the device. Furthermore, if possible, it is ideal to deploy both anti-malware and MDM solutions (mentioned above) to protect the device from malicious software and applications.
		C98: Disable unnecessary device functions and install only trusted software Merchants and DFS providers should disable any communication capabilities not necessary for the functioning of the payment solution. To avoid introducing new attack vectors onto a mobile device, install only allow communication with trusted software that is necessary to support business operations, and to facilitate payment.
	- 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: - 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.
	- 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. 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.

(continued)

Affected Entity	Risks and vulnerabilities	Controls
Third-Party, DFS Provider	- Network exposure to outside attacks (SD: Availability)	**C101:** DFS Applications should be subjected to regular security pentration scans and penetration testing. In particular, applications should be designed to be robust against phishing software.
Mobile User	The risks of ***installation of malware such as spyware and trojans*** occur because of the following vulnerability: - No anti-malware or anti-virus software is used or updated regularly (SD: Availability)	**C102:** Keep mobile device OS updated regularly; do not allow installation of programs without user validation.
	The risk of ***remote code execution*** is due to the following vulnerabilities:	
	- Obsolete device software (SD: Data Confidentiality)	**C103:** Mobile users should be encouraged to perform regular security updates on their mobile devices used for DFS transactions and ensure they are updated with the latest security patches from device manufacturers and application providers.
	- No anti-malware or anti-virus software is used or updated regularly (SD: Availability)	**C104:** Install security software from trusted sources on mobile devices including antivirus, anti-spyware, and software authentication products to protect devices from current and evolving malware threats
	- User device tampering and rooting (SD: Integrity)	**C105:** Because a tampered or "rooted" device can potentially compromise the confidentiality, integrity, and privacy of user data.
		C106: The mobile app developer should ensure that DFS applications are sandboxed, such that other untrusted applications on the mobile device should not be able to interact with the DFS application, and interaction with the operating system should be limited.
MNO	The risks of ***inability to transact and service compromise*** occur because of the following vulnerability: - 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.
		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) solutions to prevent and remove malicious software and applications.

8.14 Threat: Zero-Day Attacks

We consider this subset of malware threats specifically because traditional means of defending against malware are ineffective against a threat that has not previously been seen.

Affected Entity	Risks and vulnerabilities	Controls
MNO, DFS providers, and Third parties	The risks of ***unauthorised access to confidential user data and unauthorised modification of user data*** occur because of the following vulnerability: - 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
		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.

8.15 Threat: Rogue Devices

We consider the threat that unauthorized devices can present to DFS network infrastructure.

Affected Entity	Risks and vulnerabilities	Controls
MNO	The risks of **fraud and data modification** occur because of the following vulnerability - 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.

8.16 Threat: Unauthorised Access to Mobile Devices

This set of threats is characterized as specific attacks against mobile devices from adversaries.

Affected Entity	Risks and vulnerabilities	Controls
	The risk of ***impersonation and data loss/ fraudulent transactions*** occur because of the following vulnerabilities:	
Mobile User/ Device	- Inadequate user authentication on the device (SD: Data Confidentiality)	**C112:** Mobile devices should automatically lock after a period of inactivity, forcing device authentication to be performed to unlock the device before it is used for DFS transactions.
		C113: Use Strong PINs, remote data wipe, PIN lock, use biometric authentication (e.g., fingerprint, iris) when such device features are available.
	- Outdated application software versions making devices susceptible to malware (SD: Data Confidentiality	**C114:** Device manufacturers must ensure that critical updates are available for consumers to directly acquire or are made available to the network provides to be pushed to users.
DFS Provider	The risk of *DFS* ***user account takeover*** occurs because of the following vulnerability: - 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.
Third-Party Provider	The risk of ***denied transactions*** occurs because of the following vulnerability: - 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.

8.17 Threat: Unintended Disclosure of Personal Information

We characterize this set of threats as those resulting in user data being inadvertently exposed.

Affected Entity	Risks and vulnerabilities	Controls
DFS Provider	The risk of ***exposure of personally identifiable information*** occurs because of the following vulnerability: - 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.

(continued)

Affected Entity	Risks and vulnerabilities	Controls
Third-Party Provider	The risk of ***exposure of sensitive information*** occurs because of the following vulnerabilities:	
	- 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.
	- 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.

9 TEMPLATE FOR APPLICATION SECURITY BEST PRACTICES

In this section, we discuss a template for a mobile money smartphone application security framework. The focus here is on general best practices and not specific individual technologies except where explicitly discussed. For this template, we draw on recent works on examining digital financial services applications from the standpoint of the mobile money application space, including the GSMA study on mobile money app security best practices,[9] the ENISA smartphone secure development guidelines,[10] and a mobile payment applications security framework developed by the State Bank of Pakistan.[11] This template can also be used also as input to an app security policy by DFS Providers.

In this section, we summarize the recommendations as a starting point for regulators or application security examiners to perform security assessments. The template strictly considers the mobile application on the device unless stated otherwise, and subsections describing recommendations deal with various aspects of the operation or underlying policy relating the mobile application. The focus is primarily on Android applications given their large market share, though many recommendations are applicable across mobile operating systems. Privacy is also an important factor to consider, but these recommendations focus on security.

9.1 Device and Application Integrity

i. The safest devices for performing financial transactions on are ones that have not been "jailbroken" or "rooted", as it can be difficult or impossible to assess the security of the underlying operating system when it has been replaced or exploited. Applications should thus use the mobile platform services to determine that they and the underlying platform have not been modified.
ii. Remove any extraneous code that might have been added to the application during development, such as features that are not designed for the device platforms that the app is to be deployed upon or developer/debug features to reduce the attack surface of the deployed production code.
iii. On the server-side, determine whether the app is running in a high integrity state through signature validation or hashing over the app or certain program function blocks.

9.2 Communication Security and Certificate Handling

i. Apps should be making use of standardised cryptographic libraries and for communication with back-end services, should use end-to-end encryption with standardized protocols, specifically TLS. The minimum recommended version of TLS that should be used is version 1.2.
ii. TLS certificates should not be expired and should present strong cipher suites, specifically AES-128 encryption and SHA-256 for hashing. Authenticated encryption modes of operation such as GCM are encouraged.
iii. Limit the lifetime of issued certificates to 825 days in accordance with the CA/Browser Forum best practices.
iv. Assure the trustworthiness of the certificate authority and consider a contingency plan for if the CA is no longer trusted.
v. Ensure the configuration of TLS is performed in a secure fashion and avoid misconfiguration issues

that could result in failure to authenticate or poor algorithm selection.

vi. Certificate pinning is recommended to prevent replacement of certificates.

vii. Client devices must ensure that they correctly validate server certificates.

9.3 User Authentication

i. PINs and passwords should not be easily guessable and weak credentials should be disallowed; however, users should not be forced to change passwords on a regular basis.

ii. Multi-factor authentication before performing financial or other sensitive functions is strongly encouraged.

iii. Smartphone authenticator apps should be used for sending one-time passwords rather than SMS due to the possibility of SS7 hijacking and other insecurities.

iv. If biometric information is used for authentication, it must be stored with appropriate security measures such as encrypted in the Android Keystore or with the use of trusted hardware.

9.4 Secure Data Handling

i. Mobile devices should securely store confidential information, for example by using the Android KeyStore framework.

ii. Trusted hardware should be used for the storage of sensitive information if it is available on client smartphones.

iii. Avoid storing information in external storage and if it is done, ensure that strong input validation is performed prior to using this data.

iv. Delete confidential data from caches and memory after it is used and avoid general exposure of information (e.g., placing the secret key on the stack). Assure the clean-up of memory prior to the application exiting.

v. Restrict data shared with other applications through fine-grained permissions. Minimized the number of permissions requested by the app and ensure that the permissions correlate to functionality required for the app to work.

vi. Do not hard-code sensitive information such as passwords or keys into the application source code.

vii. Validate any input coming from the client that is to be stored in databases to avoid SQL injection attacks.

9.5 Secure Application Development

i. Develop applications according to industry-accepted secure coding practices and standards.

ii. Assure a means of securely updating applications and assure that all dependent libraries and modules are secure; provide updates for these when required.

iii. Have code independently assessed and tested by internal or external code review teams.

10 DFS SECURITY INCIDENT MANAGEMENT

Often even after relevant controls have been applied security incidents do occur, especially in financial services where attackers have a financial motive to evade systems, this causes system disruption, alteration or disclosure of data. Organizations and stakeholders offering and involved in digital financial services need to develop the right procedures, reporting, data collection, management responsibilities, legal protocols, and communications strategies that will allow organization to successfully understand, manage, and recover from security incidents. A DFS provider without an incident management plan may not discover an attack in the first place, or, if the attack is detected, the provider may not have procedures in place to quickly contain damage, eradicate and respond to the attacker's presence, and recover its assets with minimal impact.

A security incident management plan defines consistent procedures to be followed for orderly, quick and effective reporting, response analysis, investigation and recovery from security incidents that compromise any of the eight security dimensions.

The ISO/IEC 27035:2016, Information security incident management acknowledges that information security controls are imperfect and has detailed processes for managing incidents.

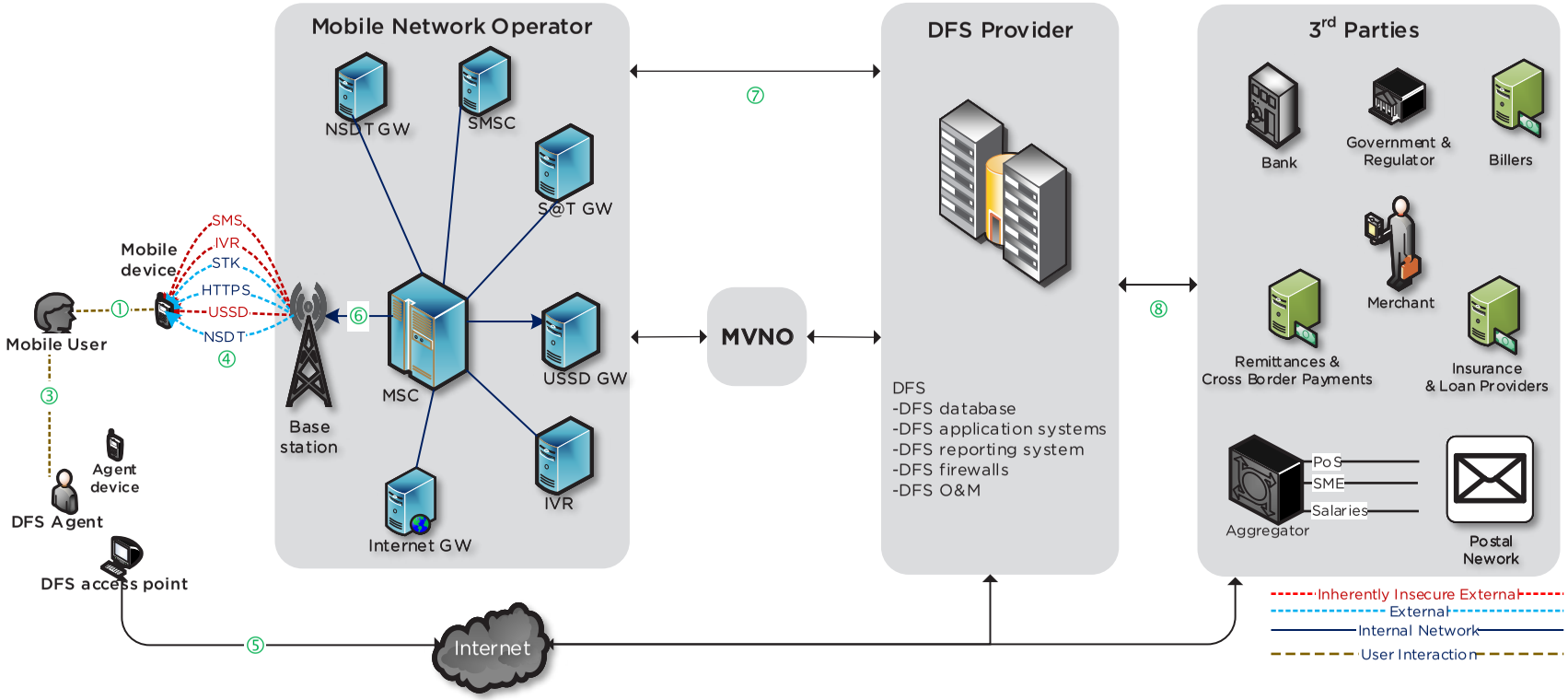
The Center for Internet Security [12] suggests the following guidelines for incident management, that DFS system network operators, DFS providers, and service providers could adopt.

1. Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management
2. Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution.
3. Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.
4. Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.
5. Assemble and maintain information on third party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors and device manufactures.
6. Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities.
7. Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real-world threats. Exercises should test communication channels, decision-making, and incident responder's technical capabilities using tools and data available to them.
8. Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.

Annex 1 Detailed DFS ecosystem infrastructure and threats

There are many interaction points between different parties within the DFS. Consequently, there are also a number of ways in which attackers can leverage these interfaces to attack the system, with successful exploits often having consequences that affect not merely the exploited stakeholders but others within the ecosystem. We consider the detailed diagram below showing the different vulnerable points in the DFS infrastructure in this section. The numbers will be used as a means of describing the vulnerability surface that occurs at that interaction point.

Figure 14 - Mapping of threats to security controls



1. Customer - mobile device

a. Exposure of sensitive customer information due to the customer sharing the device with others, or having it lost, stolen, or seized or by an adversary shoulder surfing user credentials.
b. Unauthorized access to the device by an attacker guessing the PIN or password on the device or otherwise defeating the authentication mechanisms - if they are set up - on the mobile device.
c. Tampering with the device in order to compromise the security of the underlying platform, for example, installing malware on the underlying storage or extracting secrets from the device's memory through its manipulation.
d. Altering the call settings by an unauthorized malicious attacker to set call and SMS forwarding, this enables attacker get access to DFS information sent through messages, like OTP.

2. Mobile device - mobile application

a. Code vulnerabilities within the mobile application can be leveraged by attackers who gain access to the mobile device, e.g., through over-applications. This can result in a compromise of customer data, loss of privacy, and loss of integrity.
b. Compromise of the underlying mobile platform can introduce viruses, trojans, worms, ransomware, and other malware/rootkits that can allow for the compromise of customer information, or make the user more susceptible to phishing attempts to gain credentials for the application, allowing the attacker to gain unauthorized access to the customer account.
c. Insufficient access controls within the application, e.g., an authentication mechanism required before sensitive operations occur (e.g., registration, payment transfer) based on assumptions about trust can lead to application compromise and consequent exfiltration of customer data or unauthorized money transfer.
d. A lack of logging/audit capabilities within the app, and the lack of storing such log data in a protected part of the device storage, can prevent guarantees of non-repudiation and leave the user vulnerable to not being able to prove that they were attacked.
e. A lack of or misuse of encryption within the application such that it is written in an insecure manner to application logs, or stored in databases with no or weak encryption can also lead to an adversary exposing this information.
f. If the application allows for the negotiation of weak cipher suites, the application can be subject to downgrade attacks to older versions that contain potentially weak ciphers. If session keys are not periodically renegotiated, the accumulation of enciphered material can make the key vulnerable to attack.
g. Unauthorized access to lost or stolen mobile device.
h. Mobile application tampering.

3. Customer - DFS agent

a. Customers can be vulnerable to SIM swap attacks, where the attacker represents themselves to the agent as the customer in order to gain a new SIM card that provides access to the DFS account.
b. Similar vulnerabilities can be exposed against companion cards linked to DFS accounts if insufficient authentication of the customer's credentials is performed by the agent or if the agent is colluding with the adversary.

4. Mobile device - Base station

a. Legacy GSM networks where DFS applications are primarily using SMS or USSD or IVR rely on security provided by the network is based on GSM networks encryption algorithms such as A5/1 and A5/2. These algorithms have been demonstrated to be vulnerable. Recent work has demonstrated that similar approaches can be used to compromise the A5/3 cipher. In some systems, the A5/0 algorithm is specified, which provides null encryption and hence no protection of data confidentiality, leading to the ability for an attacker to exfiltrate sensitive information over the air interface. Regardless of the underlying transport network security threats STK and https do provide end to end encryption.
b. Legacy networks relying on GSM encryption (STK, USSD and IVR) are also subject to "man-in-the-middle" attacks from rogue base stations that are placed by an attacker, maliciously claiming to be legitimate provider towers (i.e., a fake base station, often called an "IMSI-catcher") and decrypting communication before re-sending it into the mobile carrier's network. Such a scheme can allow the attacker to gain full access to all communicated information, including transaction and financial data.

5. Mobile Device - Internet

a. The security of the communication link is contingent on the negotiated cipher suite between the application and the back-end services in end-to-end systems over the Internet. Information in applications has been demonstrated to flow to a variety of sinks outside the authorized end-point, including into logs and databases. Consequently, only strong encryption mechanisms such as TLS ensure data security in public telecommunications networks.
b. It is also important to ensure that the cipher suites used are not subject to downgrade attacks to older versions that contain potentially weak ciphers. If session keys are not periodically renegotiated, the accumulation of enciphered material can make the key vulnerable to attack. Protocols such as SSL and transport layer security (TLS) can be set to renegotiate ciphers, but it is important for the protocols to be resistant to renegotiation attacks from attackers injecting traffic into legitimate client-server exchanges. Negotiation of weak cipher suites that downgrade security can allow an adversary to modify transactions and, hence, the integrity of financial data.
c. Without proper encryption on information passing through Internet connections, information can be eavesdropped over the Wi-Fi link between the mobile device and access point. Recent attacks against key TLS key negotiation demonstrate that even strong Wi-Fi protocols such as WPA2 can potentially be at risk of compromise.

6. Base station-Mobile Switching Station - Gateways

a. Insufficient internal controls can allow insider access to customer data. This is particularly important for SMS and USSD solutions that do not provide encryption within the provider network.
b. A malicious actor with access to the SS7 network could send Message Transfer Part (MTP) management messages to fake network congestion, reroute messages or deny service/link availability.
c. Mobile network are also susceptible Denial of Service (DoS) threats that can be executed through overloading the SS7 Links. An attacker sends a high number of SCCP (Signaling Connection Control Part) requests that require a lot of processing, for example translation of Global Titles.
d. Information can be spoofed by insiders, particularly in protocols that provide no notion of message integrity.
e. The increased ease of access to the SS7 network allows an attacker to use MAP(Mobile Application Part) operations to insert or modify subscriber data, intercept mobile communication or identify subscriber location.
f. The communication link between the mobile base station and the provider network is a wireline link in some scenarios, while in others, depending on the topography of the mobile network, the base stations may be connected to the provider network wirelessly, such as through a microwave link. If this communication is unencrypted then, particularly for SMS and USSD-based transactions where encryption is strictly provided through GSM algorithms between the handset and base station, that data could potentially be sent back to the network in the clear, facilitating a breach of confidentiality.
g. In the DFS context, a bad actor with SS7 network-level access can emulate ('spoof') the Caller Line Identity (CLI) of a trusted person or entity, and call the DFS customer to attempt to extract DFS and bank credentials from the customer, ultimately leading to financial loss.
h. MNO customers can fall victim to unauthorised SIM Swaps, and attackers can leverage on subscriber information obtained from SS7 attacks to obtain information that can be used for successful execution of SIM swap or in collaboration with internal personnel within the MNO.
i. Privileged users within the MNO can misuse their access to core nodes like the HLR, and MSC to perform activities like call and SMS transfers, call forwarding, unauthorised interception and collection of DFS subscriber call data records.

7. Mobile Network - DFS operator

a. There is often little in the way of data protection, particularly data encryption, once information is transmitted into the provider network. There are many reasons for this, including, primarily, the computational cost and overhead required to maintain encrypted high-bandwidth connections within the network. There is also often the assumption that threats to the network primarily arise from outside rather than within. The result is vulnerabilities exist from both insider adversaries and outside threats that are able to penetrate the network.

b. Data within the operator network is at risk due to the lack of integrity protections employed within these networks. Such information can be arbitrarily modified by an adversary capable of gaining access to the network (e.g., through compromise of perimeter defences) or by a malicious insider.
c. DFS providers who rely on the SIM as the secure element and SIM/mobile numbers are used as the financial account are likely to lose their accounts during SIM recycling. Mobile operators who perform periodic SIM recycling in which a mobile numbers are reallocated to new users if they have been dormant/inactive for a specified period on the GSM network, the process of SIM recycling may create avenues for loss of access to a financial account or its illicit transfers to another user.
d. Configurations and capacity limitations on the MNO equipment could limit the service and availability of digital financial services, limitations on USSD session length could interrupt DFS transactions.
e. The large expanse of the mobile operator's network and physical infrastructure makes it susceptible to access compromise through planting rogue devices that can enable unauthorised remote access, the interconnectedness of the DFS ecosystem may allow one with rogue access to access beyond the MNO to the different stakeholders.
f. Air interface and MSC interceptions: The MSC has capabilities that allow for lawful interception, privileged access to the MSC means one can intercept communication, this access could be misused for fraudulent financial gains by monitoring or denying DFS activity.
g. Denial of service attacks on Mobile networks, this risk is increased by the fact that the operators nodes like the MSC gateways connect to other network operators using IP, this increases risk for flooding and resource attacks which usually increase the amount of incoming traffic and can overload the IP stack and node processors, which will force the node to either stop or restart directly affecting availability.
h. Call re-routing and forwarding; An external attacker could gain access or one with access to the Network equipment could reroute DFS communication to another number, this could be done through changing the Home location profile of the Mobile Subscriber allowing the attacker to have access to confidential DFS information.

8. DFS operator - 3rd Party

a. Data is subject to exposure if encryption is not rigorously employed within and between provider networks. Threats arise from information that is retrieved from outside the provider's network perimeter (i.e., the external network), while the insider threat exists within the network perimeter (i.e., the internal network). Additionally, data can be exposed if systems within the provider network are infected with malware, which can be transmitted both over the network and through malicious peripheral devices attached to host systems (e.g., malicious USB flash drives, or keyloggers installed in a keyboard). Such devices can exfiltrate data from the provider environment back to the adversary.
b. An attacker who is able to gain access to external provider databases, e.g. through compromising software vulnerabilities, has the ability to tamper with financial data and sensitive provider information. In particular, the interfaces between networks provide a potential point of entry for an adversary and must be closely monitored. Additionally, data at rest is only as secure as the protections put in place on the hosts and servers storing this information.
c. A DFS server on which security updates are not rigorously updated can be victimized by malware and rootkits. All machines facing a public network interface are potentially subject to network-based exploit, including "zero-day" attacks that have never previously been seen. Systems can also be compromised through other I/O interfaces such as CD/DVD drives, USB ports, and other peripheral interfaces where devices can potentially inject malicious code and data.
d. Inadequacy in DFS operating system hardening like default access and password settings, active non-essential services, active insecure protocol like telnet and ftp, file access permissions, default network configurations, and user rights like who is allowed to perform a shutdown.
e. Uncontrolled access to external boot devices such as CD, DVD and USB, open access to BIOS without a password are attack surfaces to the DFS system.

Endnotes

1 https://globalfindex.worldbank.org/

2 ITU-T Focus Group Digital Financial Services, Security Aspects of Digital Financial Services, January 2017, https://www.itu.int/en/ITU-T/studygroups/2017-2020/09/Documents/ITU_FGDFS_SecurityReport.pdf

3 https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

4 Report on big data ML & consumer privacy highlights risks and how consumer financial and telecom data can be misused.

5 See Technical Report on SS7 vulnerabilities and mitigation measures for DFS – Section 12.5 Detecting, preventing and mitigating SIM card recycle

6 See Technical Report on SS7 vulnerabilities and mitigation measures for DFS – Refer to sections 8 and 9 in the report.

7 See Technical Report on SS7 vulnerabilities and mitigation measures for DFS – Section 12.1 Detecting and mitigating account takeover using intercepted OTP SMS

8 See Technical Report on SS7 vulnerabilities and mitigation measures for DFS – See Section 10 Mitigation strategies for mobile operators

9 GSM Association, Official Document MM.01 – MM App Security Best Practices, Version 1.0, 28 June 2018.

10 European Union Agency for Cybersecurity (ENISA), Smartphone Secure Development Guidelines, 10 February 2017.

11 State Bank of Pakistan, Mobile Payment Applications (App) Security Framework (DRAFT version 1.0), April 2019.

12 https://www.cisecurity.org/controls/incident-response-and-management/

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