SECURITY ASPECTS OF DFS

ITU-T FOCUS GROUP ON DIGITAL FINANCIAL SERVICES

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

FG-DFS

(01/2017)

ITU-T Focus Group Digital Financial Services

Security Aspects of Digital Financial Services (DFS)

Focus Group Technical Report

International Telecommunication Union

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7. TSAG set up the ITU-T Focus Group Digital Financial Services (FG DFS) at its meeting in June 2014. TSAG is the parent group of FG DFS.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

© ITU 2017

This work is licensed to the public through a Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International license (CC BY-NC-SA 4.0). For more information visit https://creativecommons.org/licenses/by-nc-sa/4.0/ .

Security Aspects of Digital Financial Services (DFS)

About this Report

This Technical report was written by the following authors, contributors and reviewers:

Kevin Butler, Leon Perlman, Paul Makin, Henry Gerwitz, Patrick Traynor, Yury Grin, Evgeniy Bondarenko, and Richard Miller.

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

Table of contents

List of Tables

List of Figures

Executive Summary

Digital financial services promise to enable financial inclusion and can improve the physical security of their users. However, emerging threats to the security of DFS can compromise stakeholders at every level within the ecosystem.

This report considers the stakeholders involved within the DFS ecosystem and examines the security vulnerabilities and recommendations to mitigate risks for each of them. Using criteria set out by the Recommendation ITU-T X.805 standard, security criteria are considered in light of existing and emerging attacks. Recommendations are given for each stakeholder environment. The specific security recommendations made in the report are listed below:

R1 – Consider the use of strong authentication mechanisms to demonstrate ownership of the device.

R2 – Make use of hardware and software mechanisms within mobile devices, such as secure elements and TEEs, which can ensure device integrity, and promote the use of devices equipped with security features for use in DFS.

R3 – Whether an application is designed for deployment on the handset or secure element, it should be designed and implemented in accordance with best practices, including encrypted and authenticated communication and secure coding practices to harden the app.

R4 – Apps should be subjected to external security review and penetration testing, and any recommendations acted upon.

R5 – Apps should securely manage username and password information so that adversaries cannot easily forge credentials, and should use strong authentication mechanisms to protect against unauthorized access.

R6 – Regular security updates are critical to ensure that mobile operating systems running on user devices operate using the latest security patches.

R7 – Ensure that security libraries offered by the operating system are correctly designed and implemented and that the cipher suites they support are sufficiently strong.

R8 – The handset operating system should be configured in a way to reduce the size of the trusted computing base.

R9 – Harden the security of SIM cards by using strong cryptographic ciphers, and protect updates through whitelisting techniques such as in-network filtering.

R10 – Discontinue the use of A5/0, A5/1, and A5/2 GSM encryption ciphers.

R11 – Consider transitioning away from mobile applications that leverage SMS and USSD in favour of solutions that use strong public key cryptography and end-to-end security.

R12 – MNOs should implement the security policies that maintain the integrity of their networks and prevent unauthorized access to customer accounts.

R13 – The integrity of backend DFS systems must also be maintained through continuous testing, intrusion filtering, and monitoring of networks and infrastructure.

R14 – MNOs and regulators should undertake active customer awareness campaigns to educate consumers about malicious messages, phishing, and spoofing attacks.

R15 – MNOs should monitor incoming calls from interconnect carriers and undertake fake CLI analysis, and implement a black or white list of CLIs, as well as other security mechanisms, associated with attempts to steal customer credentials.

R16 – The development of security benchmark assessments and regular testing of defences to protect against new attacks is vital to assuring the continued confidentiality and integrity of stored data in these environments.

R17 – MNOs should ensure that when DFS agents are involved in SIM swap operations, mechanisms are in place to ensure that the verified, legal owner is being provided with a new customer SIM.

R18 – PSPs 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 (where practical), and that all card transactions result in an alert to customers.

R19 – Employ strong cryptography practices to assure confidentiality and integrity of data as it enters the provider network and as it is processed and stored within this environment.

R20 – Keep systems up to date and monitored against malicious threats from outside code and employ robust input validation routines on external-facing services.

R21 – Maintain a trustworthy supply chain to assure the integrity of systems supporting DFS used within these networks.

More information about the recommendations is given within the report. Additionally, a larger set of recommendations based on securing the information technology systems used within and across stakeholders, such as DFS providers and external entities, is also provided. The conclusions summarize and encapsulate the most important of our findings, particularly the need for the safe and secure transmission of data between users and data providers, the use of hardware-enabled security on mobile devices to assure the security of information on those platforms, and best practices for handling data within DFS provider systems and networks, as well as the development of security benchmark assessments and regular testing of defences.

1 Introduction

Digital financial services (DFS) offer tremendous promise to enable financial inclusion, the delivery of financial services at low cost to low-income and otherwise disadvantaged segments of society. Mobile money and payment systems, also known as branchless banking systems, have had particular impact on consumers. Generally deployed by companies outside of the traditional financial services sector (e.g., telecommunications providers), branchless banking systems rely on the common deployment of cellular networks and mobile devices around the world. Over the past decade, these systems have revolutionized the way in which money is used in developing economies.

Because citizens no longer need to carry large amounts of currency or travel long distances to make payments, DFS systems have been largely viewed as an improvement to physical security. However, there are many other emerging security threats within the DFS ecosystem from cyber-enabled attackers to the expansion of the stakeholders into numerous and sometimes competing parties. This document provides an overview of security challenges and threats that face the DFS environment. Multiple stakeholders need to be involved in order to secure the DFS environment. This requires that security be managed at multiple layers, from operational policy to securing associated hardware and software.

2 Recommendation ITU-T X.805 Security Management Standard

We consider the end-to-end communications environment of the DFS ecosystem in terms of the Recommendation ITU-T X.805 defined by ITU-T [7], which provides a useful reference framework for security management, and will be referred to throughout the remainder of this document (see Figure 1).

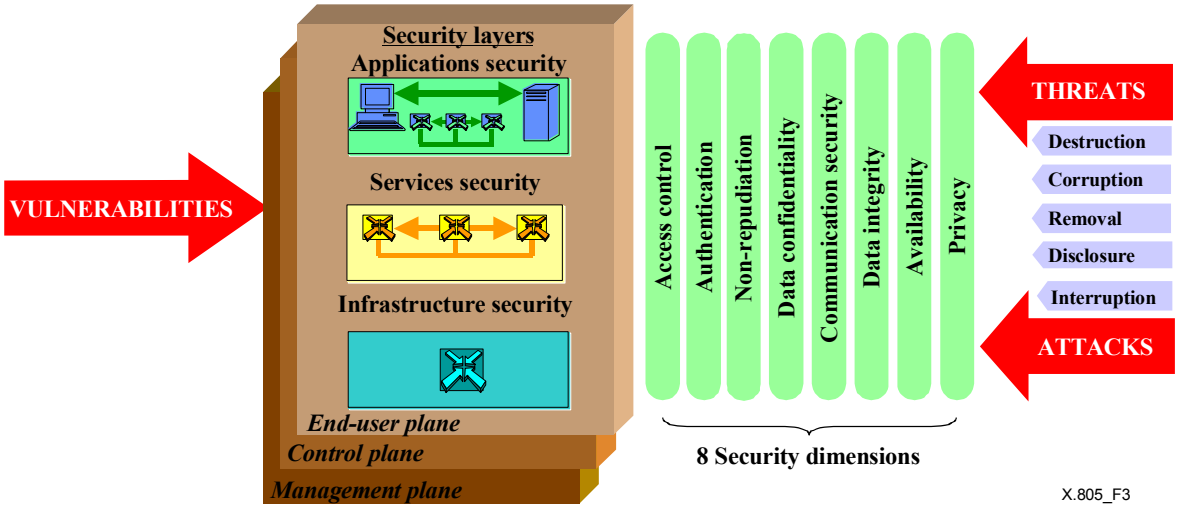

Figure 1 – Security architecture for end-to-end network security

The service management approach taken by [ITU-T X.805] is founded upon eight 'security dimensions', which are measures designed to address a particular aspect of network security, taken originally from [ITU-T X.800] [6]. The eight dimensions are as follows:

- **Access control:** Protection against unauthorised use of network resources.
- **Authentication:** Methods of confirming the identities of communicating entities.

- **Non-repudiation:** Methods to prevent an individual or entity from denying having performed a particular action.
- **Data confidentiality:** Protection of data from unauthorised disclosure.
- **Communication security:** Assurance that information only flows between authorized endpoints.
- **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.

As we consider each of the elements comprising the DFS ecosystem, we will discuss the security challenges they face in terms of the security dimensions listed above, as well as distinguishing the security layer at which solutions are to be deployed. [ITU-T X.805] defines three layers: an infrastructure security layer, a security services layer, and an applications security layer. Protections are additive, with vulnerabilities first addressed at the infrastructure security layer, then at the services security layer, and finally, at the applications layer.

Finally, there are three planes of security defined by [ITU-T X.805] comprising management, control, and end-user planes. These address the security needs associated with activities that occur at each of these levels and solutions and should ensure that events on one plane are isolated from others. In this report, we will discuss security challenges and solutions.

2.1 Security stakeholders in the DFS ecosystem

In the DFS environment, security and service integrity needs to be addressed at multiple levels simultaneously, an approach that must be applied from design to live operation. Our discussion of the DFS ecosystem is concentrated on the security perspective within a wireless communications environment – note that other access models are possible within the DFS ecosystem, such as the use of computing devices such as laptops or smartphones, communication over Wi-Fi that connect to DFS providers over the Internet, or business customers who leverage mobile money services through APIs. The full role of stakeholders is discussed in the ITU-T FG-DFS Technical Report, "The Digital Financial Services Ecosystem" [15]. We expand on the role of certain stakeholders where necessary to fully describe security requirements; these stakeholders are also informed by [ITU-T Y.2741], "Architecture of secure mobile financial transactions in next generation networks" [9].

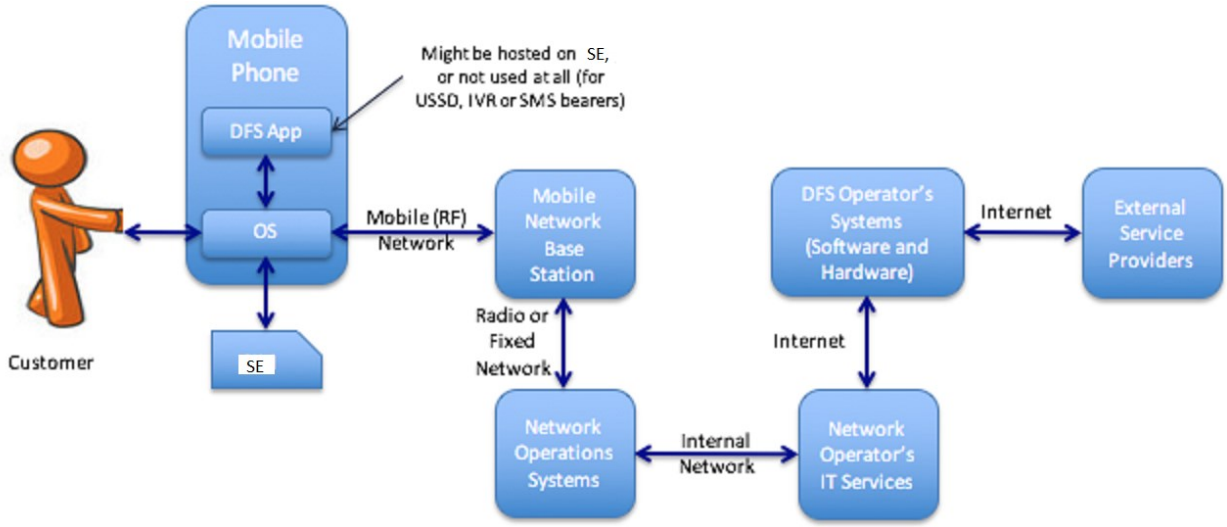

Figure 2 – Security stakeholders in DFS

The stakeholders throughout the ecosystem are comprised of: the end-user making use of a mobile money application; the application developer of the mobile money app; the mobile handset manufacturer; the mobile carrier, who is responsible for provisioning the SIM card and the infrastructure through which to allow transactions to occur; the digital financial services provider, who operates the back-end systems to process the financial transactions; and the external service providers who continue the monetization of the transaction and finalize the operations.

A key feature of this ecosystem is communication between the customer and the back-end services through a variety of communication media. In advanced systems, these interactions may occur directly over IP networks, but in many cases, and in the vast legacy systems in use, other methods of connectivity are employed, including short message service (SMS), unstructured supplementary service data (USSD), or cellular voice (via interactive voice response (IVR)).

Security vulnerabilities can be present and capitalized on by adversaries at any of the many interfaces between these parties. Security must therefore be a primary design and implementation consideration within every connected component of the system in order to ensure end-to-end security. In the optimal functioning of the ecosystem, each principal would be independently secure, i.e., they would not rely on trusting any other party in the system. For end-to-end security, it is necessary that critical information be encrypted to ensure confidentiality of DFS transactions. Transactions themselves must be authenticated following best practice from the global payments industry.

2.2 Security planes and layers

With reference to the security architecture set out in [ITU-T X.805] and referenced earlier in this document, we consider the security layers for DFS:

- The infrastructure security layer is comprised of various pieces of hardware, including the equipment of MNO and DFS operators, networking connections, and mobile devices.
- The applications security layer includes all software elements of the system and mobile devices.
- The services security layer includes all subcontractors' services, such as the Internet, leased transport lines, content providers, etc.

Similarly, the three security planes as defined in [ITU-T X.805] are interpreted for DFS as follows:

- The end user security plane defines the rules for the customer: How to choose the mobile device; how to treat it; how to repair it; and how to be careful when downloading applications to the mobile device. Agent training to provide this information to the customer would also fall within the end user plane.
- The management security plane defines the rules for the O&M of the system by the DFS operator's staff (instructions, regulations, access, etc.).
- The control security plane relates to the operation of controlling systems and signals, such as: Measurement procedures; synchronization; transaction monitoring; etc.

When considering these security layers and planes, the end-to-end system may be represented as a matrix forming the intersection of the three security layers with the three security planes. However, since both the management and control security planes represent service elements under the control of a single entity – the service provider/operator – we may consider these security planes as merged.

The result is a simplified cross reference, as illustrated in Figure 3, which represents the responsibilities across each layer of:

- Personnel of service providers and subcontractors,
- Subscribers (end users).

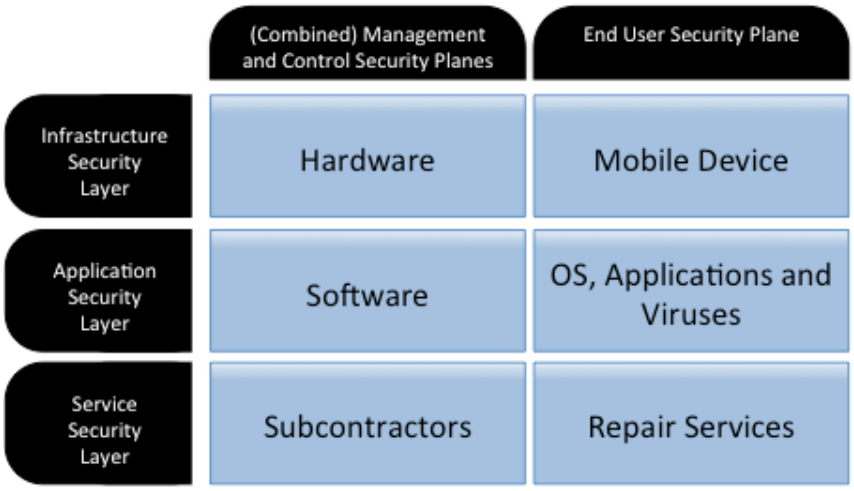

Figure 3 – DFS security architecture

2.3 X.805 Security dimensions and Y.2740 security levels

Recommendation [ITU-T Y.2740] "Security requirements for mobile remote financial transactions in next generation networks" [8], describes 4 security levels for mobile financial systems defined by the set of security dimension implementations, as defined in [ITU-T X.805]. While security level 1 (the lowest) is ensured by the standard features of mobile communication networks, security level 4 (the highest) must have the strongest implementations of the security dimensions, such as multi-factor authentication, encryption, and a hardware secure element of some form. Nevertheless, the requirements for some security dimensions are unified for all security levels, as illustrated in Table 1. To maintain assurances at these security levels, the DFS ecosystem will need to ensure that information managed in accordance with a given level maintains that level throughout its lifetime. For example, all authentication operations involving system services must be multi-factor in order to adhere with security level 3.

Table 1 – Correlation of security levels and security dimensions implementation

<table>
<tr><th rowspan="2">Security dimension</th><th colspan="4">Security level</th></tr>
<tr><th>Level 1</th><th>Level 2</th><th>Level 3</th><th>Level 4</th></tr>
<tr><td>Access control</td><td colspan="4">The access to every system component shall be granted to authorised system personnel only. The activation of special applications uploaded to mobile terminals should be permitted to authorised clients only.</td></tr>
<tr><td>Authentication</td><td>System authentication is ensured by the next-generation network (NGN) data transfer environment.</td><td>Single-factor authentication at system services usage.</td><td>Multifactor authentication at system services usage.</td><td>In-person subscription to services where personal data with obligatory identification is used.
Multifactor authentication at system services usage.
Obligatory usage of a hardware cryptographic module.</td></tr>
<tr><td>Non-repudiation</td><td colspan="4">The impossibility of a transaction initiator or participant denying his or her actions upon their completion is ensured by explicit and implicit legal contracts legally stated or reserved in mutual contracts means and accepted authentication mechanisms. All system personnel and end-user actions shall be logged. Event logs shall be change-proof and hold all actions of all users.</td></tr>
<tr><td>Data confidentiality</td><td colspan="2" rowspan="2">During data transfer, data confidentiality is ensured by the data transfer environment (communications security), and by the mechanism of data storage, together with the means of system access control – at data storage and processing.</td><td rowspan="3">During data transfer, data confidentiality is ensured by additional message encryption together with data transfer protocols that ensure the security of the data being transferred by the interoperation participants (including data integrity verification). During data storage and processing, their confidentiality, integrity, and privacy are ensured by additional mechanisms of encryption and masking together with well-defined distribution of access in concordance with privileges and permissions.</td><td rowspan="3">The implementation of the level 3 requirements with the obligatory usage of hardware cryptographic and data security facilities on the client's side (hardware cryptographic module).</td></tr>
<tr><td>Data integrity</td></tr>
<tr><td>Privacy</td><td colspan="2">Privacy is ensured by the absence of sensitive data in the messages being transferred, as well as by the implementation of the required mechanisms of data storage and system access control facilities.
System components must not have latent possibilities of unauthorized data acquisition and transfer.</td></tr>
<tr><td>Communication security</td><td colspan="4">The delivery of a message to the addressee is ensured as well as the security against unauthorized disclosure at time of transfer over the communications channels. The message delivery is ensured by the next-generation network (NGN) providers.</td></tr>
<tr><td>Availability</td><td colspan="4">Ensures that there is no denial of authorized access to the system data and services. Availability is assured by the NGN providers, as well as by the mobile payment system (MPS) service providers.</td></tr>
</table>

3 Components of DFS ecosystem

3.1 Mobile device hardware

3.1.1 Role within the ecosystem

The mobile device comprises the physical platform on which a DFS user or an agent interacts with a mobile money application. Hence, it is critically important that the security of the device itself be assured. One of the main security features of mobile devices is hardware security. The first generation of DFS did not use any secure elements in mobile devices. Second-generation systems used SIM cards for storage and execution of sensitive data. Third-generation mobile devices have embedded secure elements (SE) or additional slots for special secure SD cards, which make them more flexible and not dependent on SIM cards owned by mobile network operators (MNOs). The latest devices contain trusted execution environments (TEEs), protecting not only storage and execution of sensitive data, but also signals to and from the keyboard and display, strengthening the security of these mobile devices. A TEE is a secure area that resides in the application processor of an electronic device. Separated by hardware from the main operating system, a TEE ensures the secure storage and processing of sensitive data and trusted applications. It protects the integrity and confidentiality of key resources, such as the user interface and service provider assets. A TEE manages and executes trusted applications built in by device makers, as well as trusted applications installed as people demand them. Trusted applications running in a TEE have access to the full power of a device's main processor and memory, while hardware isolation protects these applications from user-installed apps running in a main operating system. The software and cryptographic isolation inside the TEE protect the trusted applications contained within from each other.

3.1.2 Security threats and vulnerabilities

As discussed above, there are a variety of threats to the mobile hardware platform from a number of vectors. The hardware itself, depending on its configuration, can provide strong security guarantees against these threats. Device and chip makers use TEEs to build platforms that have trust built in from the start, while service and content providers rely on integral trust to start launching innovative services and new business opportunities.

3.1.2.1 Access control

The owner of the mobile device should not to trust it to outsiders, as this presents a risk of exposing information to others. Such a vulnerability also exists if the mobile device is stolen, lost, or seized. It is strongly recommended that strong authentication be used in order to mitigate these concerns.

3.1.2.2 Authentication

Insufficient authentication measures on the device can allow a malicious attacker to gain access to information on it. Such insufficient mechanisms include not setting a password on the device or having one that is weak and easily guessable. If a personal identification number (PIN) code is used for authentication, then not setting a PIN or having one that is easily guessable can also compromise authentication. Handsets and operators may not be deploying mechanisms that can allow for second-factor authentication, which is a means of providing better authentication guarantees.

3.1.2.3 Data confidentiality

Without strong controls on data confidentiality, a malicious adversary can gain access to confidential information. The device should be resistant to allowing access to sensitive information. It is therefore recommended to choose mobile devices with SEs and TEEs to protect data confidentiality.

3.1.2.4 Data integrity

Any unauthorised modification of the mobile device can compromise platform security. Tampering with the device can lead to the storage being replaced with the installation of malware. Such an attack is called the "Evil Maid" attack, and it works even on devices with encrypted storage [10]. A similar type of attack, the "Cold Boot" attack, involves freezing the device after it is powered down and extracting details from the memory [11]. Both attacks can compromise data integrity and are possible if the user loses possession of the mobile device.

3.1.2.5 Availability

The device's availability is contingent on its being in a serviceable condition. Tampering with the device or damaging it can hinder availability.

3.1.2.6 Privacy

A user's privacy can be compromised if the device has been made vulnerable. A device that has been tampered with can be exfiltrating information in a manner contrary to a user's privacy settings. Improper configuration can also leak information that the user had not intended to share with others.

3.1.3 Recommendations for mitigation

R1 – Consider the use of strong authentication mechanisms to demonstrate ownership of the device. Because the key space of PINs makes them susceptible to a brute-force attack, consider the use of longer PINs or alphanumeric PINs, such as easily remembered passphrases, as arbitrarily long random sequences can lead to password information being written down. Caution should be exercised before mandating complex PINs and it should be ensured 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. Also, it should be considered how biometrics may aid with authentication and provide a second factor if they are stored securely within the device. To prevent uncontrolled access to the mobile device, the owner must use available means of authentication, such as a PIN code, password, control figure, fingerprint, etc. Additionally, back-end analytics systems providing services such as IP velocity, geolocation, and time of day access expectations, can act as authentication factors for the mobile device user.

R2 – Make use of hardware and software mechanisms within mobile devices, such as secure elements and TEEs, which can ensure device integrity, and promote the use of devices equipped with security features for use in DFS. Because a tampered or "rooted" device can potentially compromise the confidentiality, integrity, and privacy of user data, it is important to ensure that only properly functioning devices are able to participate in DFS transactions. The use of mechanisms such as TEEs can provide a means for attesting the integrity of devices as well as providing private storage for sensitive data. Such mechanisms can also provide the ability to perform remote wipes of a mobile device and locking data in case a mobile device is lost or stolen.

3.2 DFS application (software)

3.2.1 Role within the ecosystem

The DFS app is the primary means by which the customer interfaces with the DFS ecosystem. Users either directly use the application or have transactions performed by an agent on their behalf. Both agents and users interact with the DFS application, which can reside on the mobile device, or on the device's SE. Interactions may occur over USSD, SMS, or a special application menu enabled by code, password, fingerprint, etc., enabling users to send money, make bill payments, top up airtime, and

check account balances. From the DFS security point of view, it is important that mobile applications adhere to Security Level, 4 as described in [ITU-T Y.2740].

3.2.2 Security threats and vulnerabilities

These applications are subject to a variety of security risks that differ based on how the application is deployed. In many cases, the applications have minimal security and no encryption built in, while even if the application is deployed on a smartphone, deficiencies in the application code can render these applications vulnerable to attack and outright compromise.

3.2.2.1 Access control

As a result of implementation or design decisions, applications are at risk of attackers leveraging code vulnerabilities. Past analysis has shown that smartphone applications can be running on devices where other applications have permissions to read incoming SMS messages and thus gain access to sensitive customer information [1]. Applications can also be vulnerable if their credential storage mechanisms are weak, since an adversary can then extract these credentials and gain unauthorized access to customer data. In addition, applications whose access control is compromised face risks from viruses and Trojans controlled by remote adversaries, malicious and fraudulent activity that can compromise customer accounts; privacy threats from advertising; and plug-in services which can be cracked. They can potentially lower resistance to phishing attempts designed to exfiltrate or tamper with customer sensitive information.

Access control is a risk in applications that run over SMS and USSD because of the lack of protections on those channels, allowing an adversary to read and tamper with data to gain unauthorized access.

3.2.2.2 Authentication

If the application does not sufficiently protect password and PIN credentials, application users are at risk, in which case an adversary who acquires this information can maliciously authenticate as the customer. A study of smartphone-based systems found that some applications are vulnerable due to the lack of PIN authentication prior to performing sensitive operations such as acquiring financial balance information or paying bills. Additionally, once mobile terminal applications are successfully accessed on the mobile platform, they may be considered trusted. Malicious applications accessing the mobile platform can then put the entire platform at risk.

One-time passwords (OTP) may provide improved security compared to constant passwords. Biometric authentication may provide additional and more usable security beyond passwords but suffer from revocation issues.

3.2.2.3 Non-repudiation

Applications that do not support the use of digital signatures cannot provide non-repudiation guarantees when transactions are performed. If transactions occur over a communication channel that does not support integrity measures, transaction details can be tampered with, calling into question who performed the transaction. Furthermore, insecure applications are subject to having PINs stolen. A malicious adversary can use these stolen credentials to perform transactions not approved by the authorized PIN holder, which could be cause for complaint to the DFS provider in the case of fraudulent transactions. Digital signatures and the issuance of certificates during application registration can mitigate these risks; however, there is strong reliance on the security of the PKI roots in public-key infrastructures, many of which have been subject to compromise in the past.

3.2.2.4 Data confidentiality

Any application using a clear text channel such as USSD or unauthenticated SMS provides over-the air encryption between the mobile device and base station, but the encryption is weak and beyond the base station the message is unencrypted as it traverses the carrier network. Hence, there is no confidentiality at this point. The incorrect use of key cipher suites by the application as it communicates with other elements of the ecosystem can also provide an attacker with the means to break weak cryptography and expose information, breaching confidentiality. The GSM ciphers are known to be vulnerable to attack. In smartphone applications using IP transactions, the incorrect use of secure sockets layer (SSL) or the negotiation of known weak cipher suites can also lead to breaks in the encryption and the exposure of user data, again breaching confidentiality. Data left unencrypted within the application, 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. Caches can also be exploited to harvest sensitive information. Minimizing the amount of sensitive data stored within the application can mitigate confidentiality risks, such as the use of DFS with host card emulation (HCE).

3.2.2.5 Communication security

The security of the communication link is contingent on the negotiated cipher suite between the application and the back-end services. 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 SSL ensure data security in public telecommunications networks. 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.

3.2.2.6 Data integrity

The integrity of information is at risk from the lack of a secure communication channel in applications that use USSD or unauthenticated SMS. There are no integrity guarantees provided in these environments. Similarly, with smartphone applications, negotiation of weak cipher suites that downgrade security can allow an adversary to modify transactions and, hence, the integrity of financial data. Within applications, a lack of access control amongst some applications provides an avenue for adversaries to modify financial data. Applications that do not require credentials prior to performing sensitive operations such as bill pay are subject to adversaries modifying this information. If the application does not provide stateful tracking mechanisms, the adversary can easily perform remote exploits leading to data compromise.

3.2.2.7 Availability

Application availability is a measure of code quality and security. If applications do not perform robust input validation an adversary can potentially perform buffer overflow attacks that may end up crashing the application. Denial of service can also occur if resources are not sufficiently allocated from the application or if logging mechanisms are subverted by the adversary. Partially-completed actions can have negative effects on availability and lead to lack of system consistency; as such, it is important that interactions with applications are atomic.

3.2.2.8 Privacy

The use of weak cryptographic algorithms by the application can lead to privacy violations as data and metadata can be inferred through network activity. In the worst case, weak ciphers can be completely compromised, leading to full breaches of privacy.

3.2.3 Recommendations for mitigation

R3 – Whether an application is designed for deployment on the handset or secure element, it should be designed and implemented in accordance with best practices, including encrypted and authenticated communication and secure coding practices to harden the app. Such practices should additionally extend to software embedded in third party systems and web pages for communication with mobile money systems. Sufficiently strong encryption should be employed for both data protection within the app and for communication with backend DFS systems. These applications should also be designed to be resilient against denial-of-service attacks.

R4 – Apps should be subjected to external security review and penetration testing, and any recommendations acted upon. In particular, applications should be designed to be robust against phishing software. Other methods of increasing application security may include increasing the complexity of Java reflections and anti-compilation countermeasure, although software obfuscation remains an arms race between code writers and reverse engineers. An important focus should be on guiding the customer to access and download the application through official channels to mitigate the risk of running malware-infected code.

R5 – Apps should securely manage username and password information so that adversaries cannot easily forge credentials, and should use strong authentication mechanisms to protect against unauthorized access. Default usernames and passwords should be removed or reset so that an adversary cannot easily guess credentials. It is strongly recommended to use PIN codes, passwords, or biometric authentication to protect mobile device and DFS application from unauthorized access. Multi-factor authentication may provide additional security guarantees and is required for Y.2740 Security Levels 3 and 4. Credential information must be securely stored and managed so that they are not accessible to adversaries. Encryption of at-rest data along with strong access control mechanisms can aid in ensuring tamper-resistance.

Within the application, ensure support for password complexity (enforced by the server), unsuccessful login attempts, password history and reuse periods, account lock-out periods to a reasonable minimal value in order to minimize the potential for offline attack. Sensitive information should also be transferred using methods to assure its integrity and authenticity, through the use of protection mechanisms such as message authentication codes (MACs) and digital signatures, employing primitives, such as nonces, to prevent replay attacks.

To ensure application consistency, complete fault recovery and synchronization mechanisms should be required to ensure the reliability of information storage.

3.3 Mobile phone operating system

3.3.1 Role within the ecosystem

The operating system represents the software base that applications (whether app-based or USSD/SMS/IVR-based) rely upon. It is also used to monitor and contain other applications and users in a mobile device. The security of the operating system is critical to the security of applications that run on it, including DFS applications.

3.3.2 Security threats and vulnerabilities

3.3.2.1 Access control

Mobile operating systems offer only very coarse-grained controls over dialling. In Android, this means that any application with dialling privileges can also dial USSD codes, allowing an unauthorized or malicious application to perform actions on behalf of a user. Additionally, if an adversary has access to the physical phone, it may be possible to recover billing information or passwords if this information remains in text messages. Such conditions can become possible when the operating system is overly permissive; in other words, it provides a surfeit of interfaces that are not essential for applications to possess and thus become potential vectors for vulnerability. More generally, the operating system itself has numerous ways by which access to privileged instructions can be made, and numerous processes that can possess highly privileged access, such that if they are compromised, the security of the entire system is at risk. This set of processes and interfaces is known as the *trusted computing base* of the operating system, and an important goal from the standpoint of the operating system vendor, or the handset manufacturer if they make modifications to the operating system, is to minimize the set of processes and interfaces that have highly-privileged access to reduce the size of the trusted computing base.

3.3.2.2 Authentication

Poor or non-existent user authentication is a major risk in mobile devices. Users should be encouraged to enable device authentication, including device PINs, gesture locks, and/or biometric authentication, and carriers should provide devices that include these features (this is especially important for feature phones).

3.3.2.3 Non-repudiation

Without adequate logging mechanisms, including capturing the provenance of user actions or logging of critical actions into tamper-proof storage, it can be difficult to audit systems after the fact to establish culpability of actions. Without the use of digital signatures attached to actions, particularly those that arrive over a network connection, non-repudiation is not possible.

3.3.2.4 Data confidentiality

Applications are often reliant on security libraries offered by the operating system – this is the preferred practice to applications designing their own cryptography. Hence, it becomes particularly important to ensure that these libraries are correctly designed and implemented and that the cipher suites they support are sufficiently strong. The Heartbleed bug [5] was an example of a large-scale reliance on a security library that had been found to contain a long-lived security vulnerability, potentially compromising confidentiality of tens of millions of devices including smartphones.

3.3.2.5 Communication security

Support for encryption across network connections may be provided through libraries within the operating system. It is critical to ensure that such libraries remain updated to prevent attacks against encryption ciphers that can compromise confidentiality. Such attacks such as Heartbleed and POODLE have already been seen in commodity operating systems.

3.3.2.6 Data integrity

Similar to issues with communication security, it is vital that cryptographic libraries be updated in response to attacks against underlying cryptosystems and that applications are linked to these updated libraries, in order to support data integrity.

3.3.2.7 Availability

A major concern for mobile operating systems is the threat of malware or other offensive code that can be wielded by an attacker, as well as insufficient protection against malformed input. Such malicious input can potentially lead to buffer overflows or other exploits in the operating system, which can cause applications and other services to crash, denying access for the DFS app to contact the external network.

3.3.2.8 Privacy

User privacy can be compromised by attacks such as phishing, which is often the first activity in advance of an advanced persistent threat (APT) that can lead to larger scale compromise. Attacks against operating systems have been numerous and virulent, from malware and privacy-compromising advertising to ransomware and targeted zero-day attacks.

3.3.3 Recommendations for mitigation

R6 – Regular security updates are critical to ensure that mobile operating systems running on user devices operate using the latest security patches. This is a means of protecting users against recently developed attacks that can be widely packaged and deployed. Device manufacturers must be involved to ensure that critical updates are part of the device life cycle.

R7 – Ensure that security libraries offered by the operating system are correctly designed and implemented and that the cipher suites they support are sufficiently strong. This will help to address risks to confidentiality as detailed above.

R8 – The handset operating system should be configured in a way to reduce the size of the trusted computing base. This is an essential part of secure operating system design and is crucial to reducing the attack surface. Usability indicators for end users interacting with the operating system can also help make clear when users are potentially operating on compromised documents containing malware. Integration of operating system services with secure hardware facilities on the mobile platform (e.g., trusted execution environments and secure enclaves on the chip, can further protect operating systems against compromise.

3.4 Mobile phone SIM card

3.4.1 Role within the ecosystem

The SIM card is an integrated circuit chip that is intended to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices. In some cases, the SIM card is used as a secure element for storage of sensitive data and execution of applications, particularly in early-generation feature phones where tools such as the SIM Application Toolkit can provide functionality directly through the SIM card's capabilities, which many mobile banking applications take advantage of. In smartphones, the SIM card can still be leveraged to retrieve information about customer identity, but per Recommendation [ITU-T Y.2740], high security level DFS should use their own authentication credentials.

3.4.2 Security threats and vulnerabilities

3.4.2.1 Access control

Past work has demonstrated that SIM cards are vulnerable to privilege escalation attacks based on a variety of threat vectors. Over-the-air updates to SIM cards that arrive via SMS messaging have been shown to use the insecure DES cipher [3], which is very easy to compromise. The result of a cracked

update to a SIM card includes the ability to compromise Java applications on board the card, some of which have been demonstrated to be vulnerable. This could potentially allow for cloning of IMSIs and SIM authentication keys, allowing for vast unauthorized access to mobile services.

3.4.2.2 Authentication

Based on the attack against SIM card updates detailed above, coupled with the potential issues with Java virtual machine implementations on Java SIM cards, an adversary can perform cloning attacks against a user's mobile identity, putting many copies of these credentials out into the open. Such an attack would compromise authentication.

3.4.2.3 Non-repudiation

There are no facilities for non-repudiation at the SIM level, given the lack of digital signature usage.

3.4.2.4 Data confidentiality

Data confidentiality is at risk based on the insecure SIM updates that are performed with known-weak ciphers such as DES and A5/1.

3.4.2.5 Communication security

Communications are also at risk based on the insecure SIM updates that are performed with known-weak ciphers such as DES and A5/1.

3.4.2.6 Data integrity

There are no integrity mechanisms built into the SIM card communication.

3.4.2.7 Availability

DFS solutions relying on the presence and use of a specific SIM card run the risk of unavailability if the SIM card is damaged, lost, or stolen.

3.4.2.8 Privacy

The loss of a SIM card can mean that an attacker who stole this information could then learn the identity of the victim by examining the IMSI number that is securely stored by the SIM card itself.

3.4.3 Mitigation strategies

R9 – Harden the security of SIM cards by using strong cryptographic ciphers, and protect updates through whitelisting techniques such as in-network filtering. As documented by [4], the following solutions could aid in improving the security of the SIM card infrastructure:

- SIM cards should use strong cryptographic ciphers with sufficiently long keys, should not disclose signed plaintexts, and must implement Java software that is resistant to attack.
- At the handset level, providing the user with the ability to trust or distrust certain binary-based SMS messages could prevent malicious updates to the SIM card.
- In-network SMS filtering could allow whitelisting of SMS updates, but would need to be a feature implemented by the provider.

3.5 Mobile network: Base station and link to handset

3.5.1 Role within the ecosystem

The link between the base station and the mobile handset is the primary communication mechanism for DFS, and unless the mobile device has other functionality, e.g., the ability to make Wi-Fi connections, it is the exclusive conduit for information destined for or retrieved from the network. Notably, in systems where apps are not delivered to handsets but open networks are instead used (e.g., SMS 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.

3.5.2 Security threats and vulnerabilities

3.5.2.1 Access control

Any compromise of access control mechanisms, such as malicious insiders obtaining access to the base station, can capture information as it is decrypted by the base station.

3.5.2.2 Authentication

Described below in more detail, the ability to compromise a communication through an active adversary interposing on a transaction (e.g., through a "man-in-the-middle" attack) also compromises the ability to ensure authentication of both parties, as there are no guarantees that the client is communicating with an authenticated base station.

3.5.2.3 Non-repudiation

The lack of use of digital signatures across the wireless link, or any use of message authentication codes, has the consequence that non-repudiation cannot be provided as a property within this portion of the communication. Such guarantees would have to be provided from protocols employed by the encapsulated data (e.g., SSL over IP).

3.5.2.4 Data confidentiality

In legacy networks where mobile banking primarily occurs through SMS, any security provided by the network is based on GSM network encryption algorithms such as A5/1 and A5/2. These algorithms have been demonstrated to be vulnerable, with attacks against A5/1 in 6 hours if 64 bits of keystream information are known [2]. Recent work has demonstrated that similar approaches can be used to compromise the A5/3 cipher [3]. In some systems, the A5/0 algorithm is specified, which provides null encryption and hence no protection of data confidentiality.

3.5.2.5 Communication security

Legacy networks relying on GSM encryption are also subject to "man-in-the-middle" attacks from base stations that are placed by an attacker, maliciously claiming to be legitimate provider towers 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.

3.5.2.6 Data integrity

Attacks such as the "man in the middle" rogue base station attack described above can compromise the integrity of financial and transactional data that originates from a DFS application. A malicious

adversary actively interposing on a communication between the mobile handset and the back-end services has the ability to arbitrarily add, delete or modify data, thus removing all guarantees of integrity.

Furthermore, and as discussed in more detail in section 3.6.2.5, vulnerabilities in the Signalling System 7 (SS7) protocol can impair the integrity of SMS messages. Using SS7 requests, a bad actor can pose as a short message service centre (SMSC) to obtain *inter alia* the IMSI[1] of the target customer, and even the location.[2] This may be used to gain access via SS7 to all SS7 traffic relating to that IMSI, wherein the attacker is able to intercept a customer's SMS messages and request the customer's account balance. They can even initiate a transfer of funds from the target DFS customer's account to the attacker's DFS account.

While these attacks may appear to be mitigated through two-factor authentication via an OTP in parallel with a USSD-based DFS or banking session, a SS7 attack to gain access to the customer's account to change messages and alter call routing – coupled with intercepting a customer's SMSs – means that the OTP may never reach the target customer,[3] or may be intercepted *en route*.[4]

3.5.2.7 Availability

An adversary capable of mounting a rogue base station attack can choose not to relay information to the financial provider, thus denying the ability of a transaction to go through. This threat exists to both SMS-based mobile money systems and newer smartphone-based systems where SSL over IP is used. While in this latter case the fidelity of the data is not at risk, the availability of the back-end service can be in question.

3.5.2.8 Privacy

An adversary who has compromised communication at the base station has significant capabilities to breach the privacy of the client, by gaining access to sensitive financial and potentially personal information, and with the ability to profile all network activity performed by the client.

3.5.3 Recommendations for mitigation

R10 – 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.

---

[1] An IMSI is the serial number of the subscriber SIM card. The IMSI is sent as rarely as possible to avoid it being identified and tracked. Instead, the temporary mobile subscriber identity (TMSI) is the identity that is most commonly sent between the mobile phone and the MNO, and is randomly assigned.

[2] An attacker for example would send a specific "update-location" (UL) request message directly to the customer's MNO via SS7. See Cellusys (2016) SS7 Vulnerabilities Ebook, available from http://www.cellusys.com/thank-you/ss7-vulnerabilities/?source=Ibn

[3] Using the 'processUnstructuredSS' SS7 message, the attacker is able to send USSD codes on behalf of the customer, possibly authorizing a credit or money transfer transaction from the target. Engel, T. (2014) CAMEL. In "SS7: Locate, Track & Manipulate", available at http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf. While this interception is technically possible and has been described, it should be noted that interception of the SUTLP may be difficult to achieve, since the USSD session that elicits that response is from a live and active handset, and secured by the MNO's PIN. To re-route the SMS destination from the known location of the handset to the hacker would have to take place almost instantaneously, and is likely to throw exception warnings at the MNO.

[4] See, for example, the massive breach of the supposedly secure instant messaging application, Telegram, by hackers. Vulnerability in Telegram and other apps using OTP via SMS lies in their use of OTPs via cleartext SMS text messages to activate new devices. When users want to log on to Telegram from a new phone, the company sends them authorization codes via SMS, which can be intercepted. With these codes, hackers can add new devices to a person's account, enabling them to read chat histories as well as new messages. See Reuters (2016) Exclusive: Hackers accessed Telegram messaging accounts in Iran, available at http://www.reuters.com/article/us-iran-cyber-telegram-exclusive-idUSKCN10D1AM

R11 – Consider transitioning away from mobile applications that leverage SMS and USSD in favour of solutions that use strong public key cryptography and end-to-end security. Such solutions could include the use of specifically smartphone-based solutions that use OpenSSL and up-to-date versions of TLS. The use of SIM App Toolkit can also provide the means for supporting cryptography. While existing architectures may be in place for the near-term future and it will likely take years for smartphones to become widespread enough to supplant feature phones, hence decommissioning SMS and USSD-based DFS services and transitioning high-value and high-volume accounts (e.g., business and merchants) to smartphones that support end-to-end security can protect those accounts while ensuring that risk mitigation strategies are in place for feature phones.

Because of the SS7 vulnerabilities described above, the US standards body, National Institutes of Standards & Technology (NIST), has recommended that SMS no longer be used for any authentication purposes for financial transactions.[5]

3.6 Mobile network: Network operations

3.6.1 Role within the ecosystem

The carrier network provides transit connectivity for information originating at the customer handset. It provides the gateway to external providers and to DFS providers, which may be associated with the particular carrier or may be external entities requiring Internet communication.

3.6.2 Security threats and vulnerabilities

3.6.2.1 Access control

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.

3.6.2.2 Authentication

Information can be spoofed by insiders, particularly in protocols that provide no notion of message integrity.

3.6.2.3 Non-repudiation

Without digital signatures, there is no notion of non-repudiation in these networks.

3.6.2.4 Data confidentiality

The communication link between the mobile base station and the provider network must be secured. In some cases, this is a wireline link, while in other scenarios, 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. In many cases, this communication is unencrypted. Particularly for SMS and USSD-based transactions where encryption is strictly provided through GSM algorithms between the handset and base station, this means that data could potentially be sent back to the network in the clear, facilitating a breach of confidentiality.

[5] SMS as an authentication mechanism has been deemed 'usable, but regarded as obsolete and best avoided' by the US National Institutes of Standards & Technology in its recent Digital Authentication Guideline on SMS verification mechanisms. See NIST (2016) *DRAFT NIST Special Publication 800-63B Digital Authentication Guideline*, available at https://pages.nist.gov/800-63-3/sp800-63b.html.

3.6.2.5 Communication security

Recent attacks against the SS7 protocol have demonstrated that communication is very vulnerable in unencrypted networks. Tracking users through SS7 hijacking is possible and may have been performed already in real networks. The Ukrainian Telecom regulator [12] described the intrusion of external SS7 packets into the network and the potential for location tracking and surveillance as a result.

In the DFS context, a bad actor at the SS7 network level is able to emulate ('spoof') the Caller Line ID (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.

The need to facilitate roaming using SS7 introduces vulnerabilities in these networks and affects the core network and base stations at the extremieties of the networks. These SS7 vulnerabilities can be exploited via the SS7 component 'MAP' – which in turn powers USSD, one of the primary customer UIs for accessing DFS around the world.

This SS7-derrived vulnerability is a systemic problem with all USSD-based mobile access systems, ostensibly allowing a bad actor with relatively basic telecommunications skills to perform dangerous attacks that may lead to direct customer financial loss, confidential data leakage, or disruption of communication services.

For user security and privacy, it is vital for providers to mitigate the impact of SS7 attacks.

3.6.2.6 Data integrity

As described above, communication between the base station and the provider network may occur without any cryptographic protections. In this situation, there are no integrity guarantees for data that is transmitted in SMS and USSD-based systems. Additionally, MNO customers can fall victim to trusted phone number spoofing, otherwise known as fake caller line ID (CLI) attacks that can be the starting point of SIM swap attacks or other activities to compromise user accounts.

3.6.2.7 Privacy

As described above in the communication security section, there are substantial issues with SS7 network security that can compromise user privacy.

3.6.3 Recommendations for mitigation

R12 – MNOs should implement the security policies that maintain the integrity of their networks and prevent unauthorized access to customer accounts. This includes logical and physical access controls, including ensuring there is no unauthorized access to and any use of SS7 core components of the MNO's infrastructure, as well as the use of SS7 components of the MNO's infrastructure by any parties that may be undertaking unauthorized or fraudulent activities. Controls against SIM swaps should also be implemented.

R13 – The integrity of backend DFS systems must also be maintained through continuous testing, intrusion filtering, and monitoring of networks and infrastructure.

Tests and monitoring shall include, but not be limited to, those for:

- Unauthorized access to and use of any SS7 core components of the MNO's infrastructure;
- Use of any SS7 components of the MNO's infrastructure by any parties where that use may be designed to undertake unauthorized or fraudulent activities.
- Detection, as far as may be technically possible, of unauthorized radio frequency devices operated by unauthorized parties that may be designed to disrupt the MNO's licensed activities

and/or to gain unauthorized access to customer handsets, customer access rights to MNO and MFS facilities, and customer data.

- Expeditiously provide to the telecommunications regulator reports on penetration tests that relate to the security of their systems. These reports must include any remedial action taken, if applicable.
- Expeditiously provide to the telecommunications regulator reports on incidents that relate to authorized access to their systems and data. These reports must include any actual and potential data losses and breaches of consumer data protection measures, and any remedial action taken.

R14 – MNOs and regulators should undertake active customer awareness campaigns to educate consumers about malicious messages, phishing, and spoofing attacks. MNOs and regulators should undertake active customer awareness campaigns to educate consumers about malicious messages, phishing, and spoofing attacks.

R15 – MNOs should monitor incoming calls from interconnect carriers and undertake fake CLI analysis, and implement a black or white list of CLIs, as well as other security mechanisms, associated with attempts to steal customer credentials.

3.7 DFS operator services

3.7.1 Role within the ecosystem

The DFS operator is in charge of interfacing the application contents originating in provider networks with the back-end financial providers and for administering the customer's information in a secure fashion, and also 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 and credentialing is also a role performed by the DFS operator.

3.7.2 Security threats and vulnerabilities

3.7.2.1 Non-repudiation

There is no notion of non-repudiation in operator networks where information is not transmitted with digital signatures.

3.7.2.2 Data confidentiality

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.

3.7.2.3 Data integrity

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. Additionally, so-called "SIM swap" frauds are possible when customers fall prey to attacks which obtain their financial information through attacks such as phishing emails, and then call the mobile provider posing as a customer needing a new SIM on account of their phone being lost or damaged.

When PSPs are issuing companion general purpose reloadable cards that are linked to DFS accounts, these cards become vectors for attack if they possess insufficient authentication mechanisms. Customers can also lose money if these cards are used without their authorization.

3.7.3 Recommendations for mitigation

R16 – The development of security benchmark assessments and regular testing of defences to protect against new attacks is vital to assuring the continued confidentiality and integrity of stored data in these environments: Best practices for data handling within DFS provider systems and networks, such as the maintenance of audit logs, the use of least privilege, and assuring data confidentiality, are essential to ensuring the security of data and increasing its resistance to data breach attacks.

R17 – MNOs should ensure that when DFS agents are involved in SIM swap operations, mechanisms are in place to ensure that the verified, legal owner is being provided with a new customer SIM. Additionally, systems should be made available by MNOs to ensure that PSPs can determine in real time whether a SIM has recently been swapped before high value transaction and payments to new beneficiaries are allowed.

R18 – PSPs 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 (where practical), and that all card transactions result in an alert to customers.

3.8 External service providers

3.8.1 Role within the ecosystem

External providers allow for the interfacing between carrier-based mobile money systems and provide the basis for connecting with back-end financial systems. 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. If providers are performing these latter roles, then in addition to the vulnerabilities and recommended mitigations listed below, they may also be acting in roles more associated with IT service providers and network operations, in which case the vulnerabilities discussed under those roles must also be considered.

3.8.2 Security threats and vulnerabilities

3.8.2.1 Non-repudiation

Without the use of digital signatures on data processed and stored in the external service provider network, non-repudiation is not a property that can be provided.

3.8.2.2 Data confidentiality

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.

3.8.2.3 Data integrity

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. A 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.

3.8.3 Recommendations for mitigation strategies

R19 – Employ strong cryptography practices to assure confidentiality and integrity of data as it enters the provider network and as it is processed and stored within this environment. Ensuring that data is encrypted as it enters the network mitigates external threats to confidentiality, while ensuring that all sensitive consumer data such as PINs and passwords are encrypted within the internal network and while at rest mitigates internal threats against this data.

R20 – Keep systems up to date and monitored against malicious threats from outside code and employ robust input validation routines on external-facing services. Such measures may include the use of virus and malware detection software on systems, robust filtering within provider networks, and blacklisting known-malicious apps prior to their download by customers.

R21 – Maintain a trustworthy supply chain to assure the integrity of systems supporting DFS used within these networks.

4 Guidelines for protecting data confidentiality, integrity and availability

The following are guidelines that all system and network operators, including network providers, DFS providers, and service providers, should follow. Proper IT security policies are crucial to the protection of DFS data. These guidelines are informed by NIST Special Publication 800-171 [13] and PCI DSS Requirements version 3.1 [14].

4.1 Policies and access control

4.1.1 Recommendation summary

- Ensure organizational support for IT security policies.
- Enforce physical access controls to critical information systems and networks, and maintain audit logs of physical access.
- Enforce and maintain robust access control through least privilege assigning of permissions to roles, and ensure confidentiality of information through mechanisms such as encryption.
- Ensure that identity is vetted before access is allowed to information systems and move to multifactor authentication systems.

4.1.2 Develop and document security policies and procedures

- Obtain executive management support for IT security policies and procedures.

4.1.3 Physical security

- Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- Protect and monitor the physical facility and/or areas that contain support infrastructure.
- Escort and monitor visitor activity.
- Maintain audit logs of physical access.
- Control and manage physical access to critical infrastructure and devices.

4.1.4 Access control

- Remove or reset default usernames and passwords on system and/or infrastructure devices.
- Limit access to information systems, ability to conduct transactions or functions, and ability to execute processes on devices without authorization. Apply the principle of least privilege.
- Ensure personnel's duties are separated to reduce the risk of fraudulent activities.
- Ensure usernames/user IDs are unique to allow system activities to be traceable to individuals.
- Configure password complexity, unsuccessful login attempts, password history and reuse periods, and account lock-out periods to a reasonable minimal value.
- Enable session timeout after pre-defined inactivity.
- Monitor and control remote access sessions.
- Store and transmit only encrypted passwords.
- Promptly disable or remove access for terminated or transferred employees.

4.1.5 Identification and authentication

- Verify the identities of users, processes, or devices before allowing access to the organization's information systems.
- Use multifactor authentication for local and network access to privileged accounts.

4.2 Systems development

4.2.1 Recommendation summary

Maintain systems to reflect patches to firmware and software and use integrity monitoring tools for information. Develop policy to prevent the use of unauthorized software. Use defensive software such as firewalls and intrusion detection systems to protect network perimeters. Implement cryptographic mechanisms and ensure they are using updated libraries to protect data in transit, and ensure appropriately strong cipher suites are in use. Migrate away from communication paradigms that do not support end-to-end security such as SMS and USSD in favour of SIM toolkit and smartphone apps.

4.2.2 System development, configuration and change management

- Establish and maintain baseline configurations and inventories of organization's information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
- Establish and enforce security configuration settings for information technology products employed in organization's information systems.
- Track, review, approve, or disapprove as consistent with organizational policy, and audit changes to information systems.
- Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

- Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
- Identify, report, and correct information system flaws in a timely manner.
- Apply firmware, software, and operating system patches when new releases are available.
- Ensure anti-virus software is installed, configured, and running on all DFS information systems. In addition, ensure antivirus definitions are regularly updated, periodic system scans are performed, and real-time files scans are performed on external sources as files are downloaded, opened, or executed.
- Deploy a change detection mechanism, such as file integrity monitoring tools, to detect and alert personnel to unauthorized changes, additions, or deletion of critical files, such as those associated with consumer accounts or financial data.
- Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within the organization's information systems.

4.2.3 Communication channel protection

- Protect the trusted network perimeter from untrusted sources through the use of network and application firewalls, intrusion detection, and protection devices.
- Authorize and protect wireless access allowing limited connections and using authentication and encryption methods. Limit or, preferably, eliminate the use of wireless connections to data centres and segregate data centres from office LANs.
- Monitor, control, and protect the organization's communications (i.e., information transmitted or received by the organization's information systems) at the external boundaries and key internal boundaries.
- Segment publicly accessible system components from internal networks.
- Prevent devices from being simultaneously connected to the organization's trusted internal network and untrusted external network (i.e. establishing connectivity via Ethernet adapter and wireless adapter on the same device).
- Implement cryptographic mechanisms to prevent unauthorized disclosure of information as it traverses public or untrusted networks.
- Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. If communications are designed to be long-lived (e.g., API connections that periodically exchange data), monitor these connections to ensure the detection of unauthorized activity.
- Establish and manage cryptographic keys for cryptography employed in the information system.

4.2.4 Media protection

- Protect (i.e., physically control and securely store) both paper and digital information system media.
- Protect data at rest using cryptographic methodologies.
- Limit access to information system media to authorized users only.
- Sanitize or destroy data on information system media before disposal or reuse of the media.
- Control access to media and maintain accountability for media during transport outside of controlled areas.
- Implement cryptographic mechanisms to protect the data confidentiality stored on digital media during transport unless otherwise protected by alternative physical safeguards.
- Control the use of removable media on information system components.
- Prohibit the use of portable storage devices when such devices have no identifiable owner.

- Protect the confidentiality of backups at storage locations.

4.3 Audit and response

4.3.1 Recommendation summary

Develop risk management frameworks and robust audit controls within organizations and regulatory environments. Regulators and DFS providers should both develop incident report handling mechanisms and test capabilities, as well as performing penetration tests to ensure robustness of provider architectures and client-side mobile money applications against attack.

4.3.2 Establish audit logs and monitoring

- Create, protect, and retain information system audit logs to enable the monitoring, analysis, investigation, and reactions for inappropriate information system activity.
- Use automated mechanism to analyse, correlate and report inappropriate, suspicious or unusual activities across systems, particularly for application level behaviour and transaction monitoring. Periodically test to ensure control is operating effectively.
- Ensure a process is in place to respond to inappropriate, suspicious, or unusual activities.
- Use Network Time Protocol to synchronize events across systems.
- Monitor the information systems and the network perimeter (e.g., firewalls) including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
- Monitor information system security alerts and advisories and take appropriate actions in response.

4.3.3 Provide security awareness, training, and screening

- Ensure all personnel are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of the information systems.
- Ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
- Screen individuals in high risk positions (e.g., DFS managers, finance teams, etc.) prior to authorizing sensitive access to information systems in accordance with the appropriate Y.2740 security levels.

4.3.4 Risk and security assessment

- Periodically assess the risk to the organization's operations, assets, individuals, and the associated processing, storage, or transmission of critical data.
- Periodically assess the security controls applied to the information systems to determine if the controls are operating effectively.
- Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities.
- Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

4.3.5 Incident response

- Establish an operational incident-handling capability for the organization's information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.

- Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.
- Periodically test the organization's incident response capability.

4.3.6 Network scanning and penetration testing

- Periodically perform network scanning to detect system and application vulnerabilities.
- Periodically conduct penetration testing in order to identify vulnerabilities.
- Remediate vulnerabilities in accordance with assessment of risk.

4.3.7 External/third party service providers

- Maintain and implement policies and procedures to manage service providers with whom data is shared, or that could affect the security of the organization's data.
- Maintain a list of service providers and which services they are managing.
- Maintain a written agreement that includes an acknowledgement that the service provider(s) is responsible for the security of the organization's data that the service provider(s) possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's data environment.
- Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.
- Maintain a program to monitor service providers' performance at least annually.

5 Conclusion

It is clear that the security of payment transactions rests on the safe and secure transmission of data between users and payment providers. We thus strongly recommend the development and implementation of end-to-end security techniques to ensure data stays confidential and has integrity protection from the time it leaves the user's handset until it is delivered to its destination.

Mobile devices increasingly contain additional hardware to improve data security; we recommend that DFS providers make use of these technologies to assure the security of information on the mobile device platform.

Best practices for data handling within DFS provider systems and network, such as the maintenance of audit logs, the use of least privilege, and assuring data confidentiality, are essential to ensuring the security of data and increasing its resistance to data breach attacks. The development of security benchmark assessments and regular testing of defences to protect against new attacks is vital to assuring the continued security of stored data in these environments.

References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[1] B. Reaves, N. Scaife, A. Bates, P. Traynor, K.R.B. Butler, Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World, in: 24th USENIX Security Symposium (Security'15), Washington, DC, USA, 2015. https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-reaves-mobile_0.pdf .

[2] T. Gendrullis, M. Novotný, A. Rupp, A Real-World Attack Breaking A5/1 within Hours, in: Cryptographic Hardware and Embedded Systems – CHES 2008, Springer Berlin Heidelberg, 2008: pp. 266–282.

[3] P. Papantonakis, D. Pnevmatikatos, I. Papaefstathiou, C. Manifavas, Fast, FPGA-based Rainbow Table creation for attacking encrypted mobile communications, in: 23rd Internaional Conference on Field Programmable Logic and Applications (FPL), 2013. http://ieeexplore.ieee.org/document/6645525/

[4] K. Nohl. Rooting SIM Cards. BlackHat, July 2013. https://srlabs.de/rooting-sim-cards/

[5] US CERT. OpenSSL 'Heartbleed' vulnerability (CVE-2014-0160). https://www.us-cert.gov/ncas/alerts/TA14-098A

[6] [ITU-T X.800] Recommendation ITU-T X.800 (March 1991), *Security Architecture for Open Systems Interconnection for CCITT Applications*.

[7] [ITU-T X.805] Recommendation ITU-T X.805 (January 2004), *Security architecture for systems providing end-to-end communications.*

[8] [ITU-T Y.2740] Recommendation ITU-T Y.2740 (January 2011), *Security requirements for mobile remote financial transactions in next generation networks.*

[9] [ITU-T Y.2741] Recommendation ITU-T Y.2741 (January 2011), *Architecture of secure mobile financial transactions in next generation networks.*

[10] J.Rutkowska."Evil Maid goes after TrueCrypt!" October 2009. http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html

[11] Halderman, J. A., Schoen, S. D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J. A, & Felten, E. W. (2009). Lest we remember: cold-boot attacks on encryption keys. Communications of the ACM, 52(5), 91-98.

[12] Ukrainian National Commission for the State Regulation of Communications and Information, Verification of Telecommunications Compliance, May 2014.

[13] National Institute of Standards and Technology, Publication 800-171 "Protecting Uncontrolled Unclassified Information in Nonfederal Information Systems and Organizations"

[14] PCI Data Security Standards Council, PCI Data Security Standards Requirements v3.1.

[15] Carol Coye Benson, Charles Niehaus, Mina Mashayekhi, Nils Clotteau, Trevor Zimmer, Bruno Antunes, Yury Grin, Peter Potgieser, Quang Nguyen, Graham Wright, Nathalie Feingold, Ashwini Sathnur, Johan Bosini, Jeremy Leach, Oksana Smirnova, Evgeniy Bondarenko, May 2016: ITU-T Focus Group Digital Financial Services Technical Report: The Digital Financial Services Ecosystem.