Union internationale des télécommunications

INITIATIVE MONDIALE EN FAVEUR DE L'INCLUSION FINANCIÈRE (FIGI)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

11/2019

Groupe de travail sur la sécurité, l'infrastructure et la confiance

Cadre de garantie de la sécurité des services financiers numériques

Rapport sur l'axe de travail "Sécurité"

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée de l'Organisation de Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

Un nouveau programme mondial visant à faire progresser la recherche sur la finance numérique et à accélérer l'inclusion financière numérique dans les pays en développement, l'Initiative mondiale en faveur de l'inclusion financière (FIGI), a été lancé par le Groupe de la Banque mondiale, l'UIT et le Comité sur les paiements et les infrastructures de marché (CPMI), avec l'appui de la Bill and Melinda Gates Foundation.

Le Groupe de travail sur la sécurité, l'infrastructure et la confiance est l'un des trois groupes de travail qui ont été créés dans le cadre de la FIGI et qui sont dirigés par l'UIT. Les deux autres sont le Groupe de travail sur l'identité numérique et le Groupe de travail sur l'acceptation des paiements électroniques. Ils sont dirigés par le Groupe de la Banque mondiale.

À propos du présent rapport

Ce rapport a été rédigé par Kevin Butler, de l'Université de Floride, et Vijay Mauree, de l'UIT. Les auteurs tiennent à remercier Arnold Kibuuka, de l'UIT, pour l'aide et le soutien qu'il a apportés à la relecture et à la révision de ce document. Les auteurs souhaitent également remercier les personnes suivantes pour leurs contributions et leurs commentaires: Assaf Klinger, de Vaulto; Leon Perlman, de l'Université Columbia; Rehan Masood, de la Banque d'État du Pakistan, ainsi que les membres du Groupe de travail sur la sécurité, l'infrastructure et la confiance de la FIGI.

Si vous souhaitez nous communiquer des informations complémentaires, veuillez contacter Vijay Mauree à l'adresse tsbfigisit@itu.int.

Table des matières

Acronymes **4**
Sommaire de direction **6**
1 Introduction **8**
2 Aperçu de la Recommandation UIT-T X.805 ..... **9**
3 Modèles économiques des fournisseurs de DFS **10**
3.1 MODELE ECONOMIQUE PILOTE PAR LES BANQUES 11
3.2 MODELE ECONOMIQUE PILOTE PAR LES MNO 11
3.3 MODELE AVEC OPERATEUR DE RESEAU VIRTUEL MOBILE 11
3.4 MODELE HYBRIDE 12
4 Éléments de l'écosystème de DFS **12**
4.1 ÉLEMENTS D'UN ECOSYSTEME DE DFS UTILISANT LES TECHNOLOGIES USSD, SMS, IVR, STK ET NSDT 13
4.2 ÉLEMENTS D'UN ECOSYSTEME DE DFS BASE SUR DES APPLICATIONS ET DES PORTEFEUILLES NUMERIQUES (PAR EXEMPLE, GOOGLE PAY, APPLE PAY, WECHAT PAY, SAMSUNG PAY) 15
5 Menaces de sécurité **19**
5.1 MENACES POUR LES DFS UTILISANT LES TECHNOLOGIES USSD, SMS, IVR, STK ET NSDT 19
5.2 MENACES POUR L'ECOSYSTEME DE DFS BASE SUR DES APPLICATIONS ET DES PORTEFEUILLES NUMERIQUES 19
6 Cadre de garantie de la sécurité des DFS **21**
7 Méthodologie d'évaluation des risques **22**
7.1 DOMAINE D'APPLICATION 23
7.2 ÉTABLISSEMENT D'UN CONTEXTE 24
7.3 ÉVALUATION DE LA SECURITE 24
7.4 IDENTIFICATION DES RISQUES 25
7.5 ANALYSE DES RISQUES 26
7.6 ÉVALUATION DES RISQUES 26
8 Évaluation des vulnérabilités en matière de sécurité des DFS, des menaces et des mesures d'atténuation **27**
8.1 MENACE: PIRATAGE DE COMPTE ET DE SESSION 28
8.2 MENACE: ATTAQUES CIBLANT LES IDENTIFIANTS 29
8.3 MENACE: ATTAQUES CIBLANT LES SYSTEMES ET LES PLATES-FORMES 30
8.4 MENACE: ATTAQUES PAR EXPLOITATION DE CODE 31
8.5 MENACE: UTILISATION ABUSIVE DES DONNEES 31
8.6 MENACE: ATTAQUES PAR DENI DE SERVICE 32
8.7 MENACE: ATTAQUES D'INITIES 32
8.8 MENACE: ATTAQUES PAR INTERCEPTION ET D'INGENIERIE SOCIALE 34
8.9 MENACE: COMPROMISSION DE L'INFRASTRUCTURE DE DFS 35
8.10 MENACE: ATTAQUES SIM 37
8.11 MENACE: COMPROMISSION DES DFS 38
8.12 MENACE: ACCES NON AUTORISE AUX DONNEES DE DFS 39
8.13 MENACE: LOGICIELS MALVEILLANTS 42
8.14 MENACE: ATTAQUES ZERO-DAY 45
8.15 MENACE: APPAREILS NON AUTORISES 45
8.16 MENACE: ACCES NON AUTORISE AUX APPAREILS MOBILES 46
8.17 MENACE: DIVULGATION INVOLONTAIRE D'INFORMATIONS PERSONNELLES 47
9 Modèle pour l'application de bonnes pratiques en matière de sécurité **47**
9.1 INTEGRITE DES APPAREILS ET DES APPLICATIONS 48
9.2 SECURITE DES COMMUNICATIONS ET GESTION DES CERTIFICATS 48
9.3 AUTHENTIFICATION DES UTILISATEURS 48
9.4 TRAITEMENT SECURISE DES DONNEES 48
9.5 DEVELOPPEMENT D'APPLICATIONS SECURISE 49
10 Gestion des incidents de sécurité dans le cadre des DFS **50**
Annexe 1: Infrastructure détaillée de l'écosystème de DFS et menaces **51**

Acronymes

API	Interface de programmation d'applications
CCM	Centre de commutation du service des mobiles
Code QR	Code de réponse rapide
DFS	Services financiers numériques
DS	Dimension de sécurité
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information
GSMA	Global System Mobile Association
HCE	Émulation de carte hôte
HLR	Enregistreur de localisation nominale
IMEI	Identité internationale de l'équipement mobile
IMSI	Identité internationale d'abonnement mobile
ISO	Organisation internationale de normalisation
IVR	Réponse vocale interactive
MNO	Opérateur de réseau mobile
MSIN	Numéro d'identification d'abonné mobile
MVNO	Opérateur de réseau virtuel mobile
NFC	Communication en champ proche
PAN	Numéro de compte principal
PCI-DSS	Norme de sécurité de l'industrie des cartes de paiement
PDCA	Planifier, déployer, contrôler, agir
PDV	Point de vente
SIM	Module d'identité de l'abonné
SMS	Service de messages courts
SSL	Couche de sockets sécurisés
STK	Boîte à outils SIM
TLS	Sécurité dans la couche transport
UIT	Union internationale des télécommunications
UIT FG-DFS	Groupe spécialisé de l'UIT sur les services financiers numériques
URL	Localisateur uniforme de ressource
USSD	Données de service complémentaire non structurées

Sommaire de direction

La prestation de services financiers numériques (de l'anglais *Digital Financial Services*, ou DFS) repose sur un écosystème complexe impliquant différents acteurs comme les banques, le fournisseur de DFS, les opérateurs de réseaux mobiles (MNO), les fournisseurs de plate-forme de DFS, les organismes de réglementation, les agents, les commerçants, les fournisseurs de services de paiement, les fabricants d'appareils, les développeurs d'applications, les fournisseurs de services de jetons, les fabricants d'équipement d'origine et les clients. L'interconnexion de ces entités et la dépendance à l'égard de plusieurs parties au sein de l'écosystème étendent le périmètre de sécurité au-delà du fournisseur de DFS jusqu'aux clients, fournisseurs de réseaux, fabricants de téléphones mobiles et autres fournisseurs tiers de l'écosystème (voir les sections 4.1 et 4.2 du présent rapport).

En outre, les fournisseurs de DFS doivent également gérer un écosystème mobile de plus en plus complexe, en développant des applications pour plusieurs versions de systèmes d'exploitation présentant des vulnérabilités spécifiques et prenant en charge différents types d'appareils mobiles. Dans cet environnement dynamique en évolution rapide, les fournisseurs de DFS sont confrontés à certains enjeux en matière de connaissance des menaces de sécurité réelles et des mesures de sécurité à mettre en œuvre pour atténuer les risques.

Le *Cadre de garantie de la sécurité des DFS* offre une vue d'ensemble des menaces et des vulnérabilités en matière de sécurité auxquelles sont confrontés les fournisseurs de DFS (banques, non-banques fournissant des services financiers mobiles), les MNO, les clients, les fournisseurs de systèmes de paiement, les commerçants et les fournisseurs de services technologiques/services tiers. Les organismes de réglementation, y compris les autorités du secteur des télécommunications, les organismes bancaires et les organismes de réglementation des paiements, pourraient également utiliser le présent Cadre pour établir des principes de sécurité de référence pour les fournisseurs de DFS.

Le Cadre, une fois mis en œuvre, compléterait les pratiques établies de gestion des risques et de la sécurité des informations des acteurs impliqués dans l'écosystème de DFS. Par exemple, les mesures de contrôle de la sécurité présentées dans ce document peuvent être intégrées au programme de sécurité des technologies de l'information et de la communication (TIC) du fournisseur de DFS.

Le *Cadre de garantie de la sécurité des DFS* recommande une méthodologie structurée de gestion des risques de sécurité que les fournisseurs de DFS pourraient mettre en œuvre pour:

- Renforcer la confiance des clients dans les DFS;
- Définir plus clairement les rôles et les responsabilités de chaque partie prenante de l'écosystème;
- Identifier les vulnérabilités en matière de sécurité et les menaces associées au sein de l'écosystème;
- Établir des mesures de sécurité pour garantir la sécurité de bout en bout;
- Renforcer les pratiques de gestion en ce qui concerne la gestion des risques de sécurité impliquant l'ensemble des acteurs de l'écosystème de DFS.

Le *Cadre de garantie de la sécurité des DFS* fournit un processus systématique de gestion des risques de sécurité pour évaluer les menaces et les vulnérabilités. Il recense également les mesures de contrôle de la sécurité adéquates à mettre en œuvre par le fournisseur de DFS et le MNO pour les menaces ciblant l'utilisateur, l'appareil mobile, le MNO et le fournisseur de DFS. Les menaces liées aux commerçants, aux fournisseurs de services de paiement et aux autres organisations de services financiers, ainsi que les mesures d'atténuation spécifiques pour faire face à ces menaces sont en dehors

du champ d'application du présent document. Le rapport complète les travaux entrepris par le Groupe de travail sur la sécurité, l'infrastructure et la confiance dans le domaine de la cybersécurité sur la méthodologie que les organisations de services financiers peuvent appliquer pour gérer les incidents de cybersécurité et lutter contre les cybermenaces.

Le *Cadre de garantie de la sécurité des DFS* comprend les éléments suivants:

a) Une méthodologie de gestion des risques de sécurité basée sur la norme ISO/IEC 27005 – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information (section 7 du rapport).
b) Une évaluation des menaces et des vulnérabilités pour l'infrastructure sous-jacente du MNO et du fournisseur de DFS, les applications de DFS, les services, les opérations réseau et les fournisseurs tiers impliqués dans l'écosystème pour la prestation de DFS.
c) Des stratégies d'atténuation fondées sur le résultat de l'étape b) ci-dessus. Les mesures d'atténuation définissent 117 mesures de sécurité pour les menaces de sécurité décrites à la section 8 du présent rapport.

La section 9 du rapport fournit un modèle de bonnes pratiques de sécurité pour les applications d'argent mobile pour smartphones qui pourraient être incluses dans une politique relative à la sécurité applicative par les fournisseurs de DFS. Le modèle porte strictement sur l'application mobile installée sur l'appareil, sauf indication contraire, et les sous-sections décrivant les recommandations traitent de divers aspects de l'exploitation ou de la politique sous-jacente relative à l'application mobile. L'accent est principalement mis sur les applications Android étant donné leur part de marché importante, bien que de nombreuses recommandations s'appliquent à l'ensemble des systèmes d'exploitation mobiles. La section 10 du rapport fournit un cadre de gestion des incidents de sécurité liés aux DFS.

Ce rapport se veut comme un document évolutif et doit être mis à jour périodiquement afin de prendre en compte les nouvelles plates-formes et les nouveaux services d'application, ainsi que l'évolution des menaces et l'émergence de nouvelles vulnérabilités au fil du temps.

1 Introduction

La technologie numérique a élargi l'accès aux services financiers pour des millions de personnes en raison de sa facilité d'utilisation grâce aux téléphones mobiles, offrant des services financiers orientés client, abordables, évolutifs et pratiques.

Selon la base de données Global Findex de la Banque mondiale[1]: "*la part des adultes effectuant ou recevant des paiements numériques dans le monde a augmenté de 11 points de pourcentage entre 2014 et 2017. Dans les pays à revenu élevé, 51% des adultes (55% des titulaires de comptes) ont déclaré avoir effectué au moins une transaction financière au cours de l'année écoulée en utilisant un téléphone portable ou Internet. Dans les économies en développement, 19% des adultes (30% des titulaires de compte) ont déclaré avoir effectué au moins un paiement direct à l'aide d'un compte d'argent mobile, d'un téléphone portable ou d'Internet.*"

Cependant, à mesure que les fournisseurs s'équipent de ressources numériques pour offrir une plus large gamme de services financiers avec une plus grande portée, une efficacité accrue et des charges opérationnelles minimales, la croissance et l'adoption rapides des DFS rendent leur écosystème particulièrement vulnérable à diverses menaces de sécurité. L'interconnexion de ces entités et la dépendance/l'implication de plusieurs parties au sein de l'écosystème étendent le périmètre de sécurité au-delà du fournisseur de DFS jusqu'aux clients, fournisseurs de réseaux, fabricants de téléphones mobiles et autres fournisseurs tiers de l'écosystème.

En outre, les fournisseurs de DFS doivent également gérer un écosystème mobile de plus en plus complexe, en développant des applications pour plusieurs versions de systèmes d'exploitation présentant des vulnérabilités spécifiques et prenant en charge différents types d'appareils mobiles. Dans cet environnement dynamique en évolution rapide, les fournisseurs de DFS sont confrontés à certains enjeux en matière de connaissance des menaces de sécurité réelles et des mesures de sécurité à mettre en œuvre pour atténuer les risques.

Le *Cadre de garantie de la sécurité des DFS* a pour objectif de combler les lacunes de connaissances susmentionnées et recommande une méthodologie structurée de gestion des risques de sécurité que l'écosystème d'argent mobile au sein de l'écosystème des DFS pourrait mettre en œuvre pour:

- Renforcer la confiance des clients dans les DFS.
- Définir plus clairement les rôles et les responsabilités de chaque partie prenante de l'écosystème.
- Identifier les vulnérabilités en matière de sécurité et les menaces associées au sein de l'écosystème.
- Établir des mesures de sécurité pour garantir la sécurité de bout en bout.
- Renforcer les pratiques de gestion en ce qui concerne la gestion des risques de sécurité impliquant l'ensemble des acteurs de l'écosystème de DFS.

Le *Cadre de garantie de la sécurité des DFS* offre une vue d'ensemble des menaces et des vulnérabilités en matière de sécurité auxquelles sont confrontés les fournisseurs de DFS (banques, non-banques fournissant des services financiers mobiles), les MNO, les clients, les fournisseurs de systèmes de paiement, les commerçants et les fournisseurs de services technologiques/services tiers. Les organismes de réglementation, y compris les autorités du secteur des télécommunications, les organismes bancaires et les organismes de réglementation des paiements, pourraient également

[1] https://openknowledge.worldbank.org/bitstream/handle/10986/29510/211259ovFR.pdf.

utiliser le présent Cadre pour établir des principes de sécurité de référence pour les fournisseurs de DFS.

Le Cadre, une fois mis en œuvre, compléterait les pratiques établies de gestion des risques et de la sécurité des informations des acteurs impliqués dans l'écosystème de DFS. Par exemple, les mesures de contrôle de la sécurité présentées dans ce document peuvent être intégrées au programme de sécurité des TIC du fournisseur de DFS.

Le rapport repose sur l'hypothèse que les entreprises ont déjà mis en œuvre des principes et des normes de gouvernance de la sécurité efficaces, tels que des politiques relatives à la sécurité de l'information, la classification des données, l'attribution des responsabilités en matière de sécurité de l'information, les politiques de confidentialité des données, les programmes de sensibilisation et de formation à la sécurité à l'intention du personnel, le développement sécurisé, le contrôle et la maintenance des infrastructures, périphériques, applications et processus, la gestion des vulnérabilités, les procédures de sauvegarde, ainsi que les processus de gestion des incidents, de continuité des activités et de reprise après une catastrophe, car ces éléments ne sont pas couverts par ce document.

2 Aperçu de la Recommandation UIT-T X.805

Le *Cadre de garantie de la sécurité des DFS* utilise la Recommandation UIT-T X.805 comme fondement pour l'application de mesures de contrôle de la sécurité, afin de garantir la sécurité du réseau de bout en bout. Il propose également des mesures de contrôle fondées sur les recommandations du rapport technique *Security Aspects of Digital Financial Services*[2] du Groupe spécialisé de l'UIT sur les DFS.

L'environnement de la communication de bout en bout de l'écosystème de DFS est considéré au regard de la Recommandation UIT-T X.805 et constitue un cadre de référence utile pour la gestion de la sécurité. L'architecture de sécurité de la Recommandation UIT-T X.805 comprend huit "*dimensions de sécurité*", qui sont des mesures conçues pour traiter un aspect particulier de la sécurité réseau.

Les huit dimensions de sécurité qui fournissent un moyen systématique de lutter contre les menaces réseau sont les suivantes:

- **Contrôle des accès:** protection contre l'utilisation non autorisée des ressources réseau.
- **Authentification:** méthodes de confirmation des identités des entités communicatrices.
- **Non-répudiation:** méthodes pour empêcher une personne ou une entité de nier la cause d'un événement ou d'une action.
- **Confidentialité des données:** protection contre la divulgation non autorisée des données.
- **Sécurité des communications:** garantie que les informations circulent uniquement entre des terminaux autorisés, sans être détournées ou interceptées.
- **Intégrité des données:** protection de l'exactitude des données.
- **Disponibilité:** prévention du refus d'accès autorisé aux éléments et données du réseau.
- **Confidentialité:** protection des informations pouvant être déduites de l'observation de l'activité réseau.

[2] Groupe spécialisé de l'UIT sur les DFS, *Security Aspects of Digital Financial Services*, janvier 2017. Disponible en ligne à l'adresse suivante: https://www.itu.int/en/ITU-T/studygroups/2017-2020/09/Documents/ITU_FGDFS_SecurityReport.pdf.

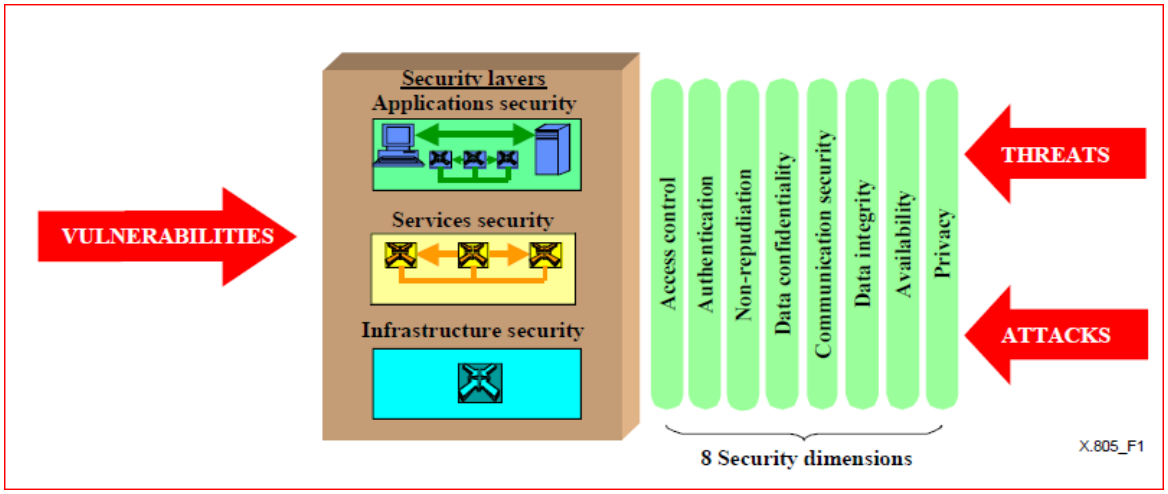

Figure 1: Dimensions de sécurité de la Recommandation UIT-T X.805

La Recommandation UIT-T X.805 définit une hiérarchie de groupes d'équipements et d'installations réseau en trois couches de sécurité. Ces couches de sécurité fournissent des solutions de sécurité complètes de bout en bout et permettent de déterminer où il convient de mettre en œuvre des mesures de sécurité dans les produits et les solutions, car chaque couche peut être exposée à différents types de menaces et d'attaques.

Les couches de sécurité sont les suivantes:

i. **Couche de sécurité de l'infrastructure:** comprend les éléments de base utilisés pour créer des réseaux de télécommunication, des services et des applications, et se compose de liaisons de transmission individuelles et d'éléments de réseau, y compris les plates-formes matérielles et logicielles sous-jacentes.

ii. **Couche de sécurité des services:** comprend les services que les clients/utilisateurs finaux reçoivent des réseaux. Ces services vont de la connectivité et du transport de base aux facilitateurs de services comme ceux étant nécessaires pour fournir un accès Internet pour des services d'appel gratuit, de qualité de service, de VPN, de localisation, et de messagerie instantanée, etc.

iii. **Couche de sécurité applicative:** cible les applications réseau utilisées par les clients/utilisateurs finaux.

3 Modèles économiques des fournisseurs de DFS

Sept principaux acteurs de l'écosystème de DFS sont pris en compte: l'utilisateur des DFS, un commerçant, une institution gouvernementale ou non gouvernementale, etc., le MNO, la banque, un tiers et un opérateur de réseau virtuel mobile (MVNO). Nous examinons également les cinq principales fonctions dans la chaîne de valeur des DFS pour ces acteurs: le détenteur du dépôt, l'émetteur de fonds électroniques, le fournisseur de services de paiement, le gestionnaire du réseau d'agents et le fournisseur de communications mobiles.

Selon le(s) rôle(s) joué(s) par chaque partie prenante, les quatre modèles économiques les plus courants des fournisseurs de DFS sont examinés:

a) Piloté par les banques;

b) Piloté par les MNO;
c) MVNO;
d) Hybride.

3.1 Modèle économique piloté par les banques

Dans le cadre de ce modèle, les services financiers offerts par la banque sont proposés aux utilisateurs mobiles; le processus d'inscription peut se faire à la banque ou par l'intermédiaire d'un réseau d'agents. Dans ce modèle, la banque remplit les rôles financiers clés, c'est-à-dire ceux du détenteur du dépôt, de l'émetteur de fonds électroniques et du fournisseur de services de paiement. Le réseau de communication utilisé pour fournir ces services financiers à l'utilisateur est mis à disposition par le MNO, par le biais de ses différents canaux, qui peuvent être des données de service complémentaire non structurées (USSD), un service de messages courts (SMS), un système de réponse vocale interactive (IVR) ou par le biais de la boîte à outils SIM (STK). Par exemple, les services Ucash proposés par la United Commercial Bank au Bangladesh.

La figure 2 ci-dessous illustre le modèle piloté par les banques.

Figure 2: Modèle économique piloté par les banques

3.2 Modèle économique piloté par les MNO

Dans le cadre d'un modèle piloté par un MNO, parallèlement à son rôle traditionnel de fournisseur de réseau de communication, le MNO assume également la majeure partie des rôles financiers et, par conséquent, émet les fonds électroniques, gère le réseau d'agents et les relations client et constitue le fournisseur de services de paiement. Le MNO gère un vaste réseau d'agents de DFS qui inscrit les utilisateurs des DFS et reçoit de l'argent physique de leur part en échange de fonds électroniques pour le compte du MNO. Selon le régime financier, le MNO peut être tenu de collaborer avec une banque partenaire dans laquelle les agents de DFS déposent les fonds physiques collectés auprès des clients pour le compte du MNO. Les fonds électroniques émis par le MNO sont garantis par les fonds en fiducie ou du compte séquestre de la banque partenaire, comme dans le cas de M-PESA (Safaricom), Airtel Money et MTN Mobile Money.

Figure 3: Modèle économique piloté par les MNO

3.3 Modèle avec opérateur de réseau virtuel mobile

Dans le cadre de certains processus de mise en œuvre, le MVNO fournit les services de télécommunication nécessaires aux DFS. Le MVNO peut être indépendant ou rattaché à une banque. C'est le cas d'Equity Bank au Kenya, qui détient Equitel, un MVNO qui étend les services financiers de la banque à ses clients sous forme d'argent mobile. Les MVNO utilisent l'infrastructure fournie par un MNO, mais proposent à leurs clients une gamme différente de services de télécommunication, notamment des DFS. Airtel, un MNO, met à disposition l'infrastructure de réseau hertzien utilisée par Equitel.

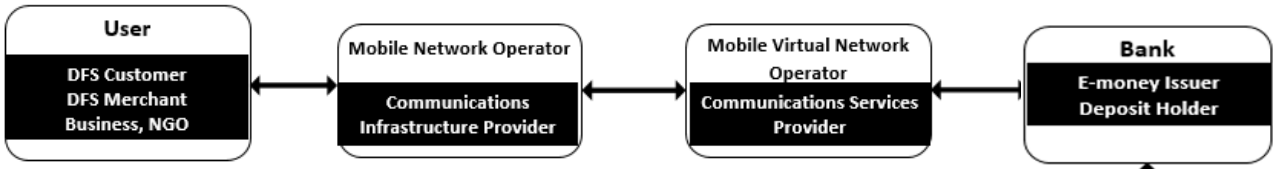

Figure 4: Modèle MVNO

3.4 Modèle hybride

Dans un modèle hybride, les rôles critiques sont partagés entre la banque et le MNO. Ces deux acteurs peuvent impliquer une partie tierce dans l'écosystème, en vue de fournir des services qu'ils ne proposent pas. Par exemple, cette partie peut être propriétaire du réseau d'agents et jouer également le rôle du fournisseur de services de paiement. C'est le cas du portefeuille Qiwi de Visa.

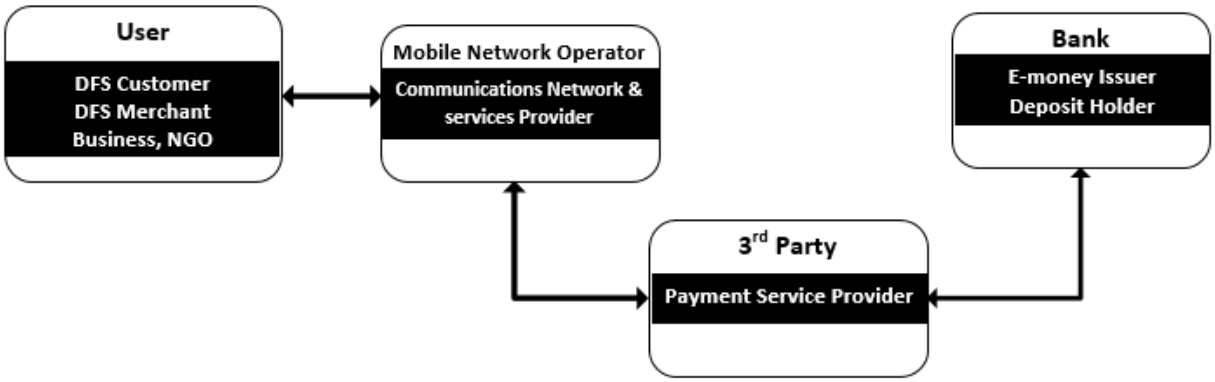

Figure 5: Modèle hybride

4 Éléments de l'écosystème de DFS

Le champ d'application de ce rapport couvre cinq catégories de paiements mobiles:

- Transfert d'argent mobile via les canaux du MNO (par exemple, SMS, USSD, téléphonie vocale) sans application de paiement spécifique téléchargée sur l'appareil mobile du client qui serait un téléphone portable basique (par exemple, M-PESA).
- Application de paiement mobile sur l'appareil mobile d'un utilisateur, associée à un compte bancaire, à une carte de débit ou à une carte de crédit (par exemple, Square, Venmo, Facebook Messenger).

- Technologies de paiement sans contact: les technologies de paiement sans contact impliquent l'utilisation de portefeuilles numériques, qui peuvent exploiter différents types de technologies de communication pour envoyer des données de paiement depuis l'appareil mobile de l'utilisateur au point de vente du commerçant. Les technologies de communication utilisées pour transmettre les informations au point de vente incluent la communication en champ proche (NFC), les codes QR, la transmission magnétique sécurisée, le Bluetooth, les SMS et Internet. Le portefeuille numérique peut être stocké sur l'appareil mobile de l'utilisateur ou dans le nuage.
- Paiements Near Sound Data Transfer (NSDT): la technologie NSDT utilise le canal audio du téléphone mobile pour chiffrer les données des transactions de paiement.
- Paiements à distance: les paiements à distance incluent les paiements effectués sur Internet (par carte de crédit sur un site de commerce électronique ou des transactions avec une carte enregistrée), la facturation directe par l'opérateur, les paiements par SMS et les services bancaires mobiles.

Les portefeuilles de cryptomonnaies comme Bitcoin ne sont pas couverts dans le cadre de ce rapport.

Dans les sections suivantes, les éléments de l'écosystème de DFS examinés sont les suivants:

1) Les paiements mobiles utilisant les technologies USSD, SMS, IVR et STK;
2) Les applications de paiement mobiles et les portefeuilles numériques (par exemple, Google Pay, Apple Pay, WeChat Pay).

4.1 Éléments d'un écosystème de DFS utilisant les technologies USSD, SMS, IVR, STK et NSDT

La figure 6 ci-dessous illustre les principaux éléments de l'écosystème. Tous les éléments ne seront pas utilisés lors de chaque déploiement. Par exemple, dans les cas où aucun accès Wi-Fi ou aucune application pour smartphone n'est disponible pour un DFS, les communications de l'utilisateur sont limitées aux interactions via le réseau mobile, plutôt qu'au moyen de passerelles Internet externes ou d'un service d'informatique en nuage.

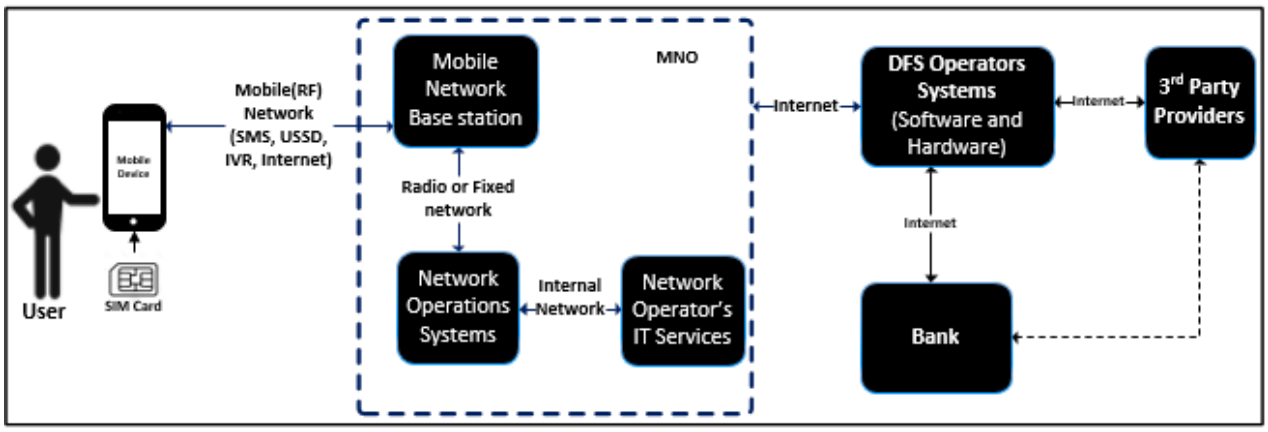

Figure 6: Principaux éléments de l'écosystème de DFS

Les parties prenantes de l'écosystème sont les suivantes:

a) **Utilisateurs/clients:** Les utilisateurs sont le public cible d'un DFS. Ils utilisent une application d'argent mobile pour interagir avec le service. Cette interaction peut se faire directement, via le réseau mobile ou via Internet (selon les fonctionnalités de la plate-forme mobile sous-jacente et de l'application d'argent mobile). Un agent de DFS qui interagit avec le DFS pour le compte du client peut également servir de médiateur pour cette interaction. L'agent peut communiquer directement avec le réseau ou utiliser une passerelle Web pour fournir ces services.

b) **Appareil mobile:** L'appareil mobile fournit une plate-forme pour le déploiement d'une application d'argent mobile. Il s'agit du canal principal par lequel le client (ou l'agent interagissant pour le compte du client; pour faciliter l'explication, il est supposé que toutes les autres interactions avec le service sont effectuées par le client, sauf si des actions spécifiques sont requises de la part de l'agent) interagit avec le DFS. Les appareils mobiles peuvent être des téléphones portables basiques ou des smartphones. Les premiers contiennent souvent un nombre limité de ressources et prennent en charge des interfaces applicatives limitées. Leur connectivité est également limitée (par exemple, services GSM 2G). Par opposition, les smartphones peuvent prendre en charge des services très performants avec leurs éléments matériels sécurisés et leur connectivité réseau et Wi-Fi avancée. Ces deux types de téléphones contiennent des cartes SIM, qui sont parfois équipées d'éléments sécurisés pouvant être utilisés par les applications. L'appareil mobile dispose d'un système d'exploitation dont les capacités dépendent des ressources disponibles. Les systèmes d'exploitation légers qui s'inspirent du système d'exploitation Symbian sont souvent utilisés dans les téléphones mobiles basiques, tandis que les smartphones utilisent généralement les systèmes Android, iOS, Windows ou autres.

c) **Station de base:** La liaison de communication entre la station de base et le téléphone mobile constitue le canal principal pour l'envoi d'informations entre l'utilisateur et le fournisseur de DFS. Notamment, dans les systèmes où les applications ne sont pas livrées aux appareils, mais où des réseaux ouverts sont utilisés (par exemple, communications reposant sur les technologies SMS, STK, IVR et USSD), cette liaison est la seule partie de l'architecture globale dans laquelle les données envoyées par l'usager ou transmises à l'usager sont chiffrées. Une fois les données reçues au niveau de la station de base, elles sont envoyées sans chiffrement par le biais des réseaux du fournisseur. Pour garantir la viabilité et la faisabilité d'un système de DFS, il est essentiel que cette liaison soit solide, fiable et pratiquement universelle.

d) **Réseau mobile:** Le réseau de l'opérateur fournit une connectivité de transit pour les informations provenant de l'appareil du client. Il est composé de différents nœuds qui permettent la communication, y compris les différentes passerelles vers des fournisseurs externes et vers des fournisseurs de DFS, qui peuvent être associés à un opérateur particulier ou être des entités externes nécessitant une communication Internet. Au sein de ce réseau se trouvent des passerelles pour les technologies USSD, IVR, STK et SMS, par exemple, des bases de données internes, telles que l'enregistreur de localisation nominale (HLR) ou l'enregistreur de localisation des visiteurs (VLR), ainsi que des passerelles Internet qui peuvent servir de points de connexion au fournisseur de DFS. Dans les cas où le MNO est également le fournisseur des DFS, les passerelles vers ces services restent dans son réseau interne. Le centre de commutation du service des mobiles (CCM) est au cœur des différents nœuds du réseau mobile, en vue de faciliter le routage des communications à l'aide de données utilisateur provenant du HLR ou du VLR. L'annexe 1 présente des nœuds du réseau détaillés dans le réseau mobile; les passerelles SMSC (centre de services de messages courts), SAT (kit d'application SIM), USSD, IVR et Internet permettent l'utilisation de ces modes d'accès respectifs pour l'utilisateur. Nous montrons également le système de facturation du MNO lorsqu'il est utilisé dans certains déploiements par le MNO pour les paiements par SMS, IVR

ou Internet. Un MVNO peut fournir les services du MNO au fournisseur de DFS ainsi qu'au client, mais l'architecture de réseau hertzien est toujours fournie par un opérateur de réseau ou un facilitateur.

e) **Fournisseur de DFS:** Le fournisseur de DFS connecte le contenu de l'application provenant des réseaux d'opérateurs mobiles aux fournisseurs financiers internes, pour gérer les informations du client de manière sécurisée et permettre des services tels que des audits. Pour que ces opérations soient sécurisées, l'opérateur de DFS doit être sûr que la personne accédant aux données est bien celle qu'elle prétend être. Des journaux d'audit doivent également être activés pour permettre l'évaluation du contenu des données au sein du réseau et des commandes émises par le biais de l'application de DFS. L'opérateur de DFS se charge également de la vérification de l'identité du client, de la gestion des identifiants, du stockage des données de transaction du client, de la fourniture d'interfaces telles que des interfaces de programmation d'applications (API) pour les parties tierces, ainsi que du traitement des transactions provenant de différentes sources.

f) **Fournisseurs tiers:** Les fournisseurs tiers permettent les interactions entre les systèmes d'argent mobile fondés sur les opérateurs, ainsi que la connexion avec les réseaux financiers internes tels que l'infrastructure bancaire. Ces fournisseurs externes peuvent également jouer d'autres rôles comme l'exploitation du système informatique ou le service client et, dans certains cas, peuvent interagir directement avec les systèmes de DFS ou agir comme des agrégateurs de services et de transactions.

g) **Application de DFS:** L'application fournit l'interface par laquelle le client interagit avec l'écosystème de DFS. Les applications peuvent varier considérablement en termes d'interfaces et de richesse de l'expérience utilisateur, des systèmes de menus sur les téléphones portables basiques conçus pour communiquer grâce aux technologies USSD, STK ou SMS aux conceptions vocales qui emploient la technologie IVR, en passant par les interfaces graphiques enrichies sur les smartphones avec une transmission sécurisée de bout en bout assurée par des algorithmes de chiffrement utilisés sur Internet. Les utilisateurs peuvent interagir grâce à des menus d'application spéciaux accessibles par code, mot de passe, empreinte digitale ou autre pour envoyer de l'argent, payer leurs factures, recharger leur carte SIM sans abonnement et consulter le solde de leur compte bancaire.

4.2 Éléments d'un écosystème de DFS basé sur des applications et des portefeuilles numériques (par exemple, Google Pay, Apple Pay, WeChat Pay, Samsung Pay)

Il existe différents éléments fondés sur des modèles de portefeuilles numériques au sein des écosystèmes. Les principaux modèles sont les suivants: portefeuille mobile de proximité basé sur l'appareil, portefeuille mobile intégré à une application et basé sur l'appareil, portefeuille sans carte/avec carte enregistrée, portefeuilles de paiement numérique ou par code QR. Tous ces modèles reposent sur des plates-formes technologiques différentes et emploient différents modèles de sécurité.

La figure 7 ci-dessous illustre un écosystème fondé sur des applications et des portefeuilles numériques.

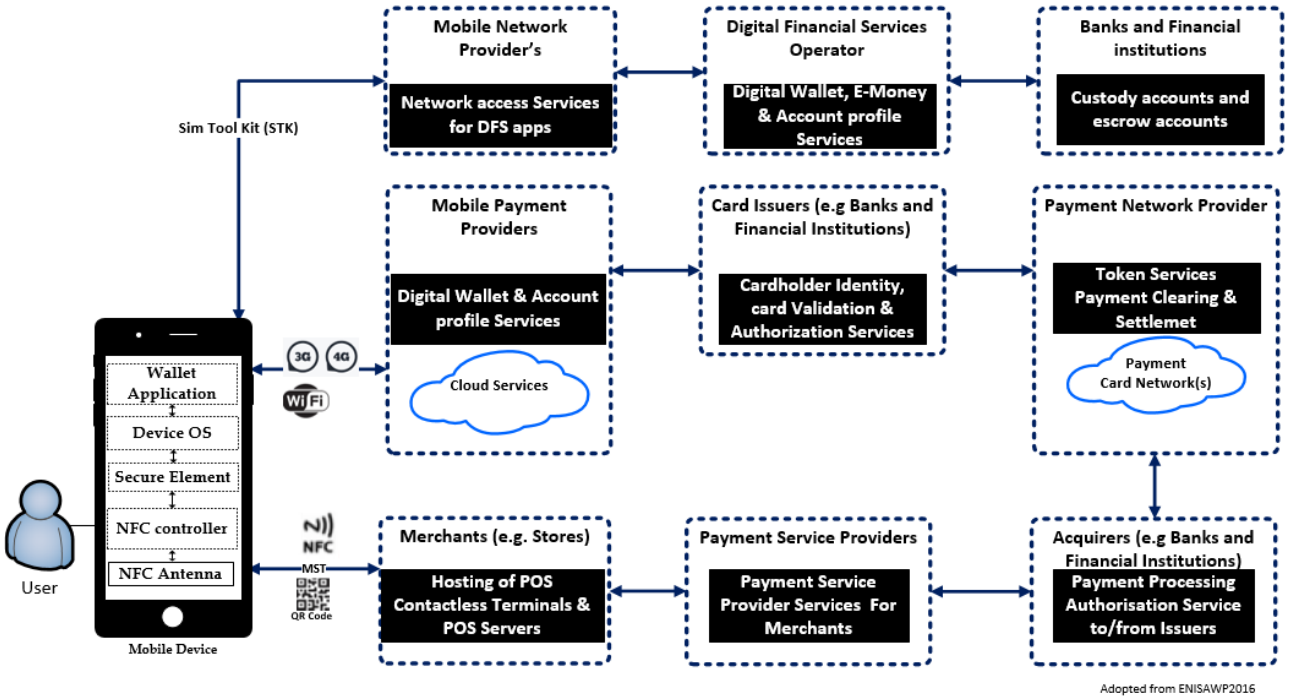

Figure 7: Écosystème de DFS fondé sur des applications et des portefeuilles numériques

Les composants de cet écosystème sont décrits ci-dessous:

a) Appareil mobile

L'appareil mobile fournit une plate-forme permettant d'accéder aux portefeuilles mobiles. Il inclut le portefeuille/l'application numérique, le système d'exploitation de l'appareil et l'élément sécurisé qui est essentiel pour sécuriser les DFS et les données applicatives.

La figure ci-dessous illustre certains des composants de l'appareil mobile de l'utilisateur.

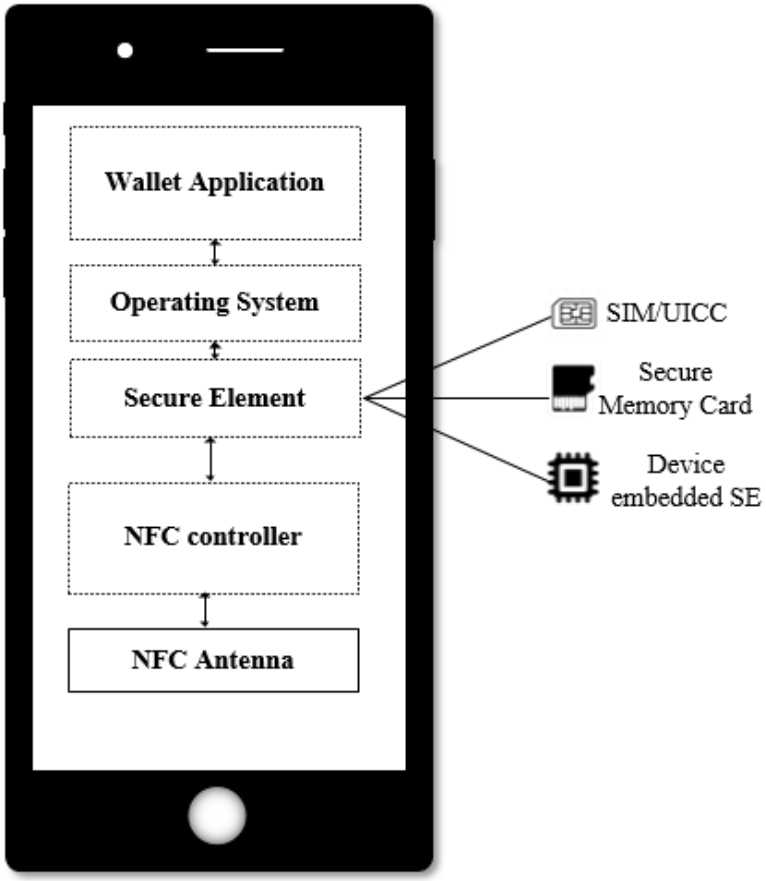

Figure 8: Composants d'un appareil mobile

i. **Le contrôleur NFC et l'antenne NFC:** Le contrôleur NFC gère les protocoles de communication NFC et assure le routage des communications entre l'application et l'élément sécurisé, ainsi qu'entre l'élément sécurisé et le terminal de paiement du point de vente (PDV). L'antenne NFC relaie les signaux entre le contrôleur et le terminal du PDV.

ii. **L'élément sécurisé:** L'élément sécurisé est une plate-forme inviolable, généralement un microcontrôleur sécurisé à puce conçu pour héberger en toute sécurité des applications ainsi que leurs données confidentielles et de chiffrement. Son utilisation dépend du type d'application de portefeuille mobile et des modes de paiement mobile. Par exemple, l'élément sécurisé des appareils Apple émule la carte lorsqu'elle est utilisée pour Apple Pay. Les éléments sécurisés existent sous différentes formes pour répondre aux exigences des applications de paiement ou des portefeuilles numériques et à leurs besoins sur le marché. L'élément sécurisé peut être intégré aux composants matériels de l'appareil, comme c'est le cas pour celui de l'iPhone. Il peut également être une carte SIM ou une carte de circuit intégré universelle (UICC). Les réseaux utilisant la norme GSM préfèrent cette option plus généralement sous la forme d'applications STK qui utilisent la carte SIM comme élément sécurisé pour protéger l'application d'argent mobile. L'élément sécurisé peut également être une carte mémoire sécurisée qui peut être insérée dans l'appareil mobile.

iii. **Émulation de carte hôte:** Les appareils mobiles peuvent émuler une carte sans contact grâce à la technologie d'émulation de carte hôte (HCE). Cette technologie n'a pas besoin d'élément sécurisé matériel pour stocker des données sensibles comme les numéros de

cartes bancaires. La HCE est une solution d'infrastructure logicielle permettant à une application de portefeuille mobile de communiquer en toute sécurité par le biais du contrôleur NFC pour transmettre le numéro de carte de paiement ou des jetons de paiement à un terminal ou lecteur de carte sans contact compatible avec la technologie NFC au PDV. Ainsi, l'utilisation d'un élément sécurisé n'est pas nécessaire. La HCE est le plus souvent utilisée sur les appareils mobiles Android pour les paiements effectués par Google Pay.

iv. **Portefeuilles mobiles:** Les portefeuilles mobiles sont des applications ou des services accessibles par le biais de l'appareil qui permettent au titulaire du portefeuille de consulter, de gérer et d'effectuer des transactions financières en toute sécurité, telles que des paiements. Les portefeuilles mobiles tels que Samsung Pay et Apple Pay sont spécifiques à l'appareil et au logiciel, et peuvent être utilisés à la place des cartes de crédit et de débit. Cependant, d'autres portefeuilles mobiles/numériques sont indépendants des appareils et stockent en toute sécurité les informations de paiement et les mots de passe de l'utilisateur pour de nombreux modes de paiement et sites Web. Ainsi, les transactions peuvent être finalisées rapidement et facilement, et l'utilisateur peut bénéficier de méthodes d'authentification plus fortes, telles que celles ayant recours à la biométrie. Parmi ces portefeuilles figurent Google Pay, WeChat Pay, PayPal et Alipay.

b) Commerçant

Les commerçants acceptent les paiements des clients pour leurs biens ou services grâce à un terminal de paiement ou un autre moyen (par exemple: lecture d'un code QR ou saisie de la référence du commerçant dans l'application de paiement de l'utilisateur). Les appareils mobiles sont également utilisés par les commerçants pour les paiements, ce qui représente une source inhérente de vulnérabilité.

c) Terminaux de point de vente

Un terminal de PDV est un appareil électronique utilisé pour traiter les paiements mobiles sur le site du commerçant. Les canaux de communication entre le terminal de PDV et l'appareil mobile pour les paiements de proximité sans contact sont la technologie NFC, les codes QR ou la transmission magnétique sécurisée. La 3G, la 4G et le Wi-Fi sont couramment utilisés pour les portefeuilles mobiles. Tout risque existant sur un ordinateur de bureau ou portable peut également exister sur un appareil mobile.

Outre les méthodes de communication standard des ordinateurs de bureau et portables traditionnels, les appareils mobiles peuvent également inclure diverses technologies cellulaires (par exemple, la 4G et la norme GSM), le système mondial de positionnement (GPS), le Bluetooth, l'infrarouge et la technologie NFC. Les supports amovibles (par exemple, cartes SIM et SD), les composants électroniques internes utilisés pour les tests par le fabricant, les capteurs intégrés et les lecteurs biométriques augmentent également les risques.

i. **Communication en champ proche:** Ce protocole de communication sans fil basé sur la technologie de radiofréquence permet l'échange de données entre des appareils situés à quelques centimètres l'un de l'autre. Un portefeuille sur un appareil mobile compatible avec la technologie NFC est une application logicielle stockée sur le téléphone qui gère et exécute les paiements. Le portefeuille mobile accède aux identifiants de paiement, tels que des cartes de paiement tokénisées, des comptes bancaires, des cartes de fidélité ou des données financières stockées sur le téléphone mobile dans un environnement de confiance. Le

téléphone physique est utilisé pour effectuer une transaction de paiement en l'approchant d'un terminal de PDV sans contact.

ii. **Transmission magnétique sécurisée:** La transmission magnétique sécurisée génère un signal magnétique similaire à celui des cartes bancaires à bande magnétique. Le signal magnétique est alors envoyé de l'appareil au terminal du PDV. Certains modèles de smartphones de la marque Samsung sont compatibles avec cette technologie.

iii. **Codes QR:** Les codes QR offrent deux options de paiement sans contact:
   a. L'acheteur scanne le code QR du commerçant: le commerçant génère un code QR associé à la transaction ou affiche un code QR statique. L'acheteur scanne alors le code avec la caméra de son téléphone, l'application de paiement interprète les données de paiement ou du commerçant pour lancer la transaction, puis l'acheteur finalise cette dernière en saisissant un code PIN.
   b. Le commerçant scanne le code QR de l'acheteur: l'acheteur génère un code QR unique et spécifique à la transaction depuis son application de paiement pour le commerçant. Ce dernier scanne le code dans son application de paiement grâce à un lecteur de codes QR pour lancer la transaction, qui peut ensuite être validée en saisissant un code PIN.

iv. **3G/4G et Wi-Fi**

En plus des réseaux cellulaires 3G et 4G, les appareils mobiles peuvent également se connecter à des réseaux sans fil (Wi-Fi). Ces réseaux permettent à l'application mobile de l'appareil d'interagir avec les fournisseurs de services de paiement. Les réseaux 3G, 4G et Wi-Fi sont généralement fournis par le MNO.

d) Fournisseur de services de jetons

Le fournisseur de services de jetons gère le cycle de vie des jetons. Les services supplémentaires incluent généralement la création et le stockage de jetons, la gestion du cycle de vie des jetons, le traitement des transactions de jetons, la mise en correspondance des jetons avec le numéro de compte principal (de l'anglais *Primary Account Number*, ou PAN), la validation des titulaires de carte, y compris les services de provisionnement, la gestion des clés pour les portefeuilles basés sur les appareils et utilisant la technologie HCE, ainsi que les services de vérification de la validité des transactions et des appareils.

e) Acquéreur

L'acquéreur est l'institution financière ou la banque qui transmet les transactions du commerçant aux banques émettrices applicables pour recevoir le paiement.

f) Émetteur

L'émetteur est l'institution financière qui émet des cartes de crédit aux consommateurs pour le compte des réseaux de cartes.

g) Fournisseur de services de portefeuille

Les fournisseurs de services de portefeuille proposent des solutions de portefeuille spécifiques qui utilisent diverses technologies de communication pour les paiements mobiles.

h) Fournisseur de services de paiement

Les fournisseurs de services de paiement mettent à disposition les différentes méthodes permettant à un commerçant d'accepter des paiements à partir de portefeuilles mobiles et numériques. Le fournisseur de services de paiement peut se connecter à plusieurs acquéreurs ainsi qu'à des réseaux de paiement et de cartes. En utilisant les services d'un fournisseur de services de paiement, le commerçant devient moins dépendant des institutions financières pour gérer les transactions, puisque le fournisseur de services de paiement peut gérer les comptes bancaires ainsi que les relations avec le réseau externe.

5 Menaces de sécurité

5.1 Menaces pour les DFS utilisant les technologies USSD, SMS, IVR, STK et NSDT

Le schéma ci-dessous synthétise les menaces pesant sur les applications de DFS utilisant les technologies USSD, SMS, IVR, STK et NSDT.

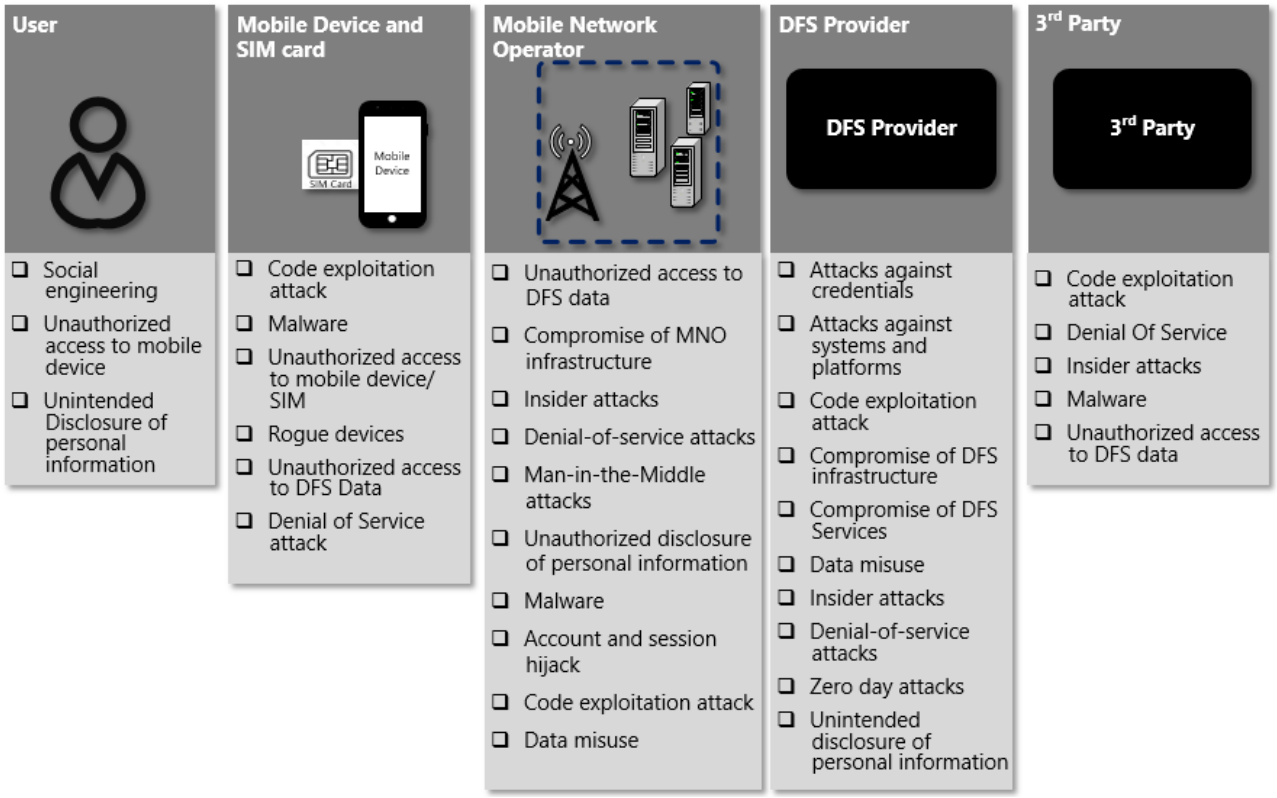

Figure 9: Menaces pour les systèmes de DFS utilisant les technologies USSD, SMS, IVR, STK et NSDT

5.2 Menaces pour l'écosystème de DFS basé sur des applications et des portefeuilles numériques

Les applications/portefeuilles de paiement mobiles permettent l'utilisation de DFS par le biais d'applications installées sur l'appareil mobile. La nature des applications et canaux financiers utilisés dépendra des capacités de l'appareil. Par exemple, Samsung Pay et Apple Pay sont uniquement utilisables sur les appareils des marques Samsung et Apple respectivement, alors que Google Pay peut être utilisé sur tous les appareils Android. Enfin, les applications mobiles de paiement utilisant des codes QR telles que WeChat Pay et Alipay peuvent être utilisées sur l'ensemble des smartphones équipés d'une caméra.

La communication des applications de paiement entre l'appareil/l'application et le fournisseur du paiement se fait principalement par le biais des réseaux Wi-Fi, 3G et 4G. Un paiement peut également être effectué à destination d'un appareil de PDV commerçant à l'aide de la transmission magnétique sécurisée, de la lecture d'un code QR ou de la technologie NFC.

L'utilisation de ces canaux présente d'autres menaces et éléments (PDV, acquéreurs, fournisseurs de réseaux de paiement, émetteurs de cartes, fournisseurs de paiements mobiles). Ces composants permettent d'identifier les menaces suivantes pour les écosystèmes de DFS utilisant des applications et portefeuilles mobiles (à savoir Android, iOS).

Tableau 1: Synthèse des menaces pour les écosystèmes de DFS utilisant des applications et portefeuilles numériques

Élément	Menaces
Application de paiement mobile	• Rétro-ingénierie du code source de l'application. • Altération de l'application de paiement mobile. • Exploitation des vulnérabilités de l'application de paiement mobile. • Installation de rootkits ou de logiciels malveillants. • Autorisations d'accès au système d'exploitation mobile.
Appareil mobile	• Installation d'applications indésirables et de logiciels malveillants. • Accès non autorisé à un appareil mobile perdu ou volé. • Installation de logiciels malveillants sur l'appareil.
Menaces pour les commerçants	• Logiciel malveillant ciblant le système d'exploitation: Les attaquants peuvent installer des logiciels malveillants sur les terminaux de PDV pour accéder à distance aux données de paiement. • Compromission de code QR: Les codes QR comportent des menaces inhérentes, car ils ne sont pas facilement lisibles par l'œil humain. Les attaquants pourraient facilement remplacer le code QR d'un commerçant par un autre code contenant des éléments malveillants, tels que des URL d'hameçonnage ou des applications mobiles malveillantes. • Attaques par interception contre les terminaux sans contact et les serveurs du PDV: les attaquants peuvent exploiter des lacunes de sécurité comme l'absence de pare-feu au sein du réseau interne des commerçants. • Attaques par relais contre des terminaux de PDV sans contact compatibles avec la technologie NFC: un logiciel de relais installé sur un appareil mobile peut transmettre des commandes et des réponses entre l'élément sécurisé et un émulateur de carte installé en tant que proxy sur le PDV mobile au sein d'un réseau hertzien. • Utilisation de codes PIN par défaut pour accéder aux terminaux de PDV, par exemple 166816 et Z66816 (1).
Acquéreurs	• Compromission des systèmes de traitement des paiements: lors de la requête de jetons et cryptogrammes auprès du réseau de paiement de l'émetteur, un attaquant peut obtenir une grande quantité de données sur les titulaires de cartes en installant des logiciels malveillants et des outils d'accès à distance sur n'importe lequel des serveurs de traitement des paiements du réseau interne. • Compromission de la sécurité du réseau et des interfaces: les attaquants peuvent exploiter des connexions point à point non sécurisées entre l'acquéreur et l'émetteur en compromettant le fournisseur de réseau. Ils peuvent alors utiliser ce niveau d'accès pour surveiller et manipuler les appels d'API.

Élément	Menaces
Fournisseur de services de paiement	• Compromission des passerelles de paiement: les attaquants peuvent cibler les passerelles de paiement pour consulter et compromettre les données de transaction en transit entre les commerçants et les banques recevant les paiements. • Compromission de vulnérabilités logicielles au niveau des terminaux de PDV sans contact mis à la disposition des commerçants par les fournisseurs de services de paiement, qui peuvent traiter les données de différents canaux, y compris les paiements par carte, les paiements sans contact et les paiements sans carte. • Compromission de réseaux non sécurisés: les attaquants peuvent exécuter des attaques par interception pour usurper des données sensibles en transit depuis le fournisseur de services de paiement vers l'acquéreur lorsque le fournisseur utilise des connexions peu ou pas sécurisées comme les versions antérieures des protocoles de sécurité dans la couche transport (de l'anglais *Transport Layer Security*, ou TLS) et de la couche de sockets sécurisés (de l'anglais *Secure Sockets Layer*, ou SSL). • Défauts de conception et vulnérabilités logicielles non corrigées dans les terminaux et les systèmes de PDV ainsi que les passerelles de paiement vers/depuis les acquéreurs.
Émetteurs	• Compromission des systèmes de traitement des paiements: lors de la requête de jetons et cryptogrammes auprès du réseau de paiement de l'émetteur, un attaquant peut obtenir une grande quantité de données sur les titulaires de cartes en installant des logiciels malveillants et des outils d'accès à distance sur n'importe lequel des serveurs de traitement des paiements du réseau interne. • Compromission de la sécurité du réseau et des interfaces: les attaquants peuvent exploiter des connexions point à point non sécurisées entre l'acquéreur et l'émetteur en compromettant le fournisseur de réseau. Ils peuvent alors utiliser ce niveau d'accès pour surveiller et manipuler les appels d'API.

Les acteurs de l'écosystème de DFS considérés sont les commerçants, les acquéreurs, les fournisseurs de services de paiement et les émetteurs comme des fournisseurs tiers (ces entités individuelles figurent dans la présentation détaillée de l'écosystème de DFS à l'annexe 1). Bien que nous recensions ici les menaces générales auxquelles ces entités sont confrontées, les mesures d'atténuation spécifiques pour faire face à ces menaces ne sont pas détaillées dans le présent document. Nous vous recommandons de consulter la norme de sécurité de l'industrie des cartes de paiement (PCI-DSS) et le rapport intitulé *Cyber Resilience Oversight Expectations for Financial Market Infrastructures*[3] de la BCE pour en savoir plus sur les mesures d'atténuation.

6 Cadre de garantie de la sécurité des DFS

Le *Cadre de garantie de la sécurité des DFS* applique des principes similaires à la famille de normes ISO/IEC 27000 (Systèmes de management de la sécurité de l'information), à la norme PCI-DSS v3.2, à la norme de sécurité des données d'application de paiement, à la publication spéciale 800-53, révision 4, du National Institute of Standards and Technology, aux lignes directrices techniques

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

du Centre for Internet Security (contrôles CIS, version 7), ainsi qu'à l'Open Web Security Application Project, communément appelé OWASP Top 10. Nous avons utilisé ces ressources comme repères pour identifier les mesures de contrôle spécifiques à l'écosystème de DFS.

Ce cadre comprend les éléments suivants:

a) Une évaluation des risques de sécurité basée sur la norme ISO/IEC 27005 – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information (section 7);
b) Une évaluation des menaces et des vulnérabilités pour l'infrastructure sous-jacente, les applications de DFS, les services, les opérations réseau et les fournisseurs tiers impliqués dans l'écosystème pour la prestation de DFS (section 8);
c) Des stratégies d'atténuation fondées sur le résultat de l'étape b) ci-dessus (section 8).

Ce cadre identifie:

i. Les différentes menaces de sécurité pour les ressources des DFS dans le cadre de chaque dimension de sécurité;
ii. Les vulnérabilités connexes qui peuvent être exploitées par ces menaces;
iii. Des suggestions de mesures de sécurité qui peuvent être mises en œuvre par les parties prenantes de l'écosystème des DFS pour lutter contre ces menaces et vulnérabilités. La mesure de sécurité peut appartenir à une ou plusieurs des huit dimensions de sécurité de la Recommandation UIT-T X.805.

7 Méthodologie d'évaluation des risques

Afin de garantir un modèle de sécurité viable et d'améliorer en permanence la sécurité des DFS, le présent cadre utilise le cycle de Deming, un modèle de qualité divisé en quatre phases: planifier, déployer, contrôler, agir (de l'anglais *Plan, Do, Check and Act*, ou PDCA). La méthodologie de mise en œuvre fondée sur le cycle PDCA permet d'identifier les activités à mener et les résultats à atteindre lors de chacune des quatre phases.

Dans l'écosystème de DFS, plusieurs parties prenantes sont impliquées et le cycle PDCA est conçu avec des activités qui garantissent une sécurité globale de bout en bout dans l'écosystème de DFS. Le schéma ci-dessous présente un modèle de cadre de sécurité des DFS utilisant le cycle PDCA.

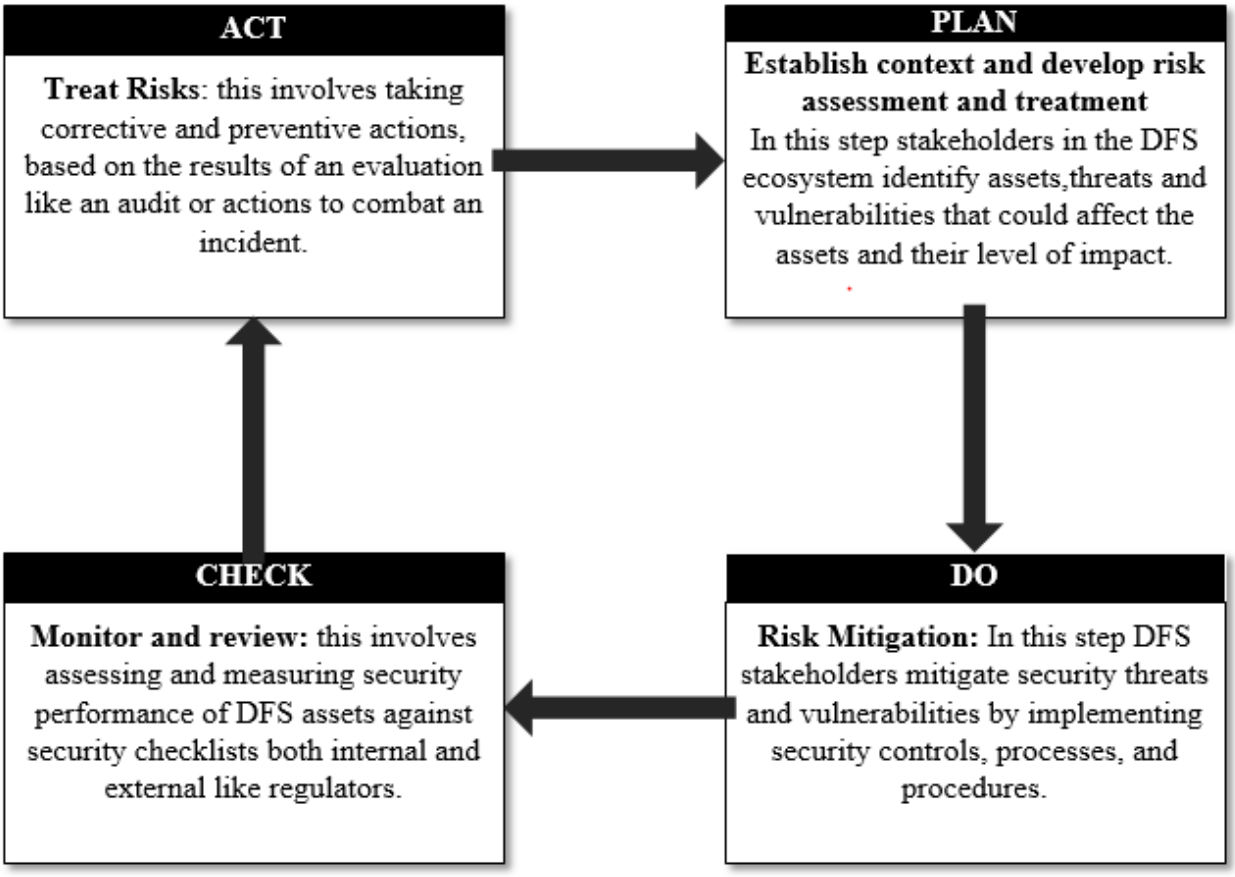

Figure 10: Planifier, déployer, contrôler, agir

Un plan de processus de gestion des risques de haut niveau est présenté dans la figure 11 ci-dessous. Il couvre les quatre phases du cycle PDCA.

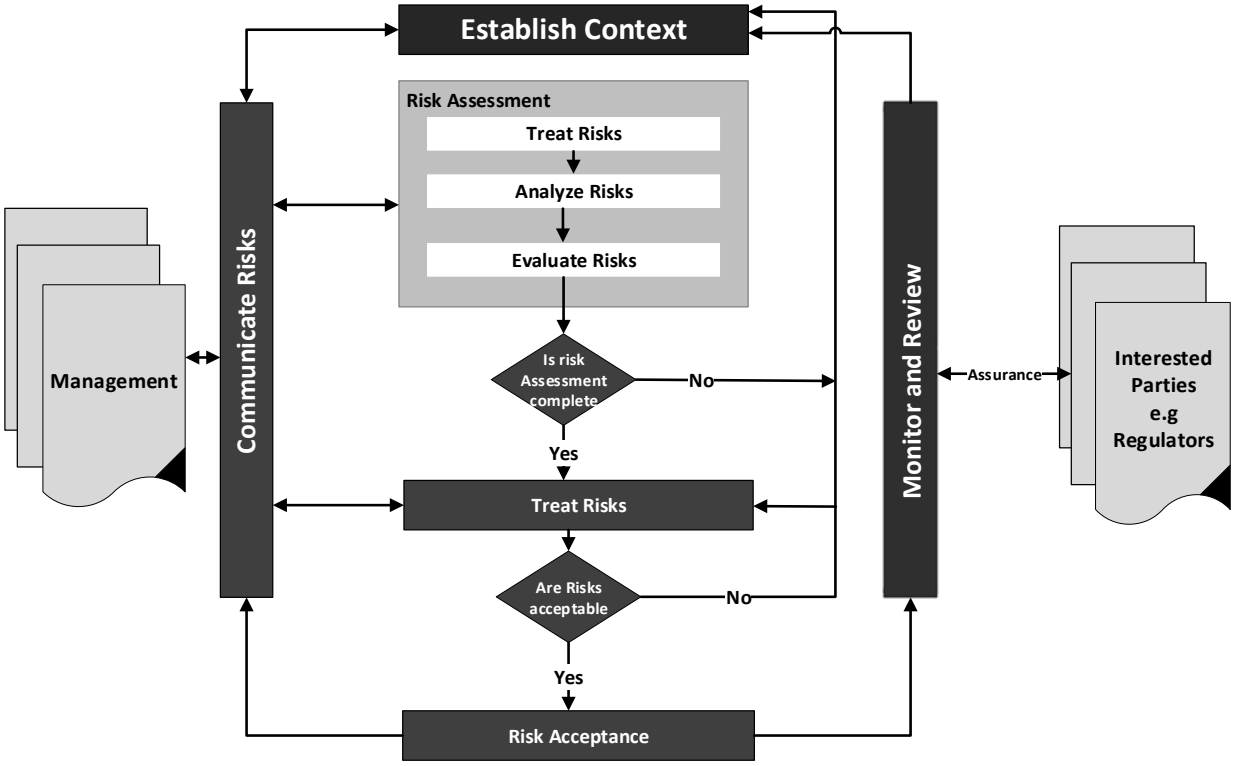

Figure 11: Processus de gestion des risques

Les activités de surveillance et d'évaluation dans l'environnement de DFS peuvent prendre différentes formes selon les parties prenantes. Par exemple, l'organisme de réglementation peut évaluer les mesures de sécurité appliquées par le fournisseur de DFS pour garantir la sécurité des utilisateurs de DFS, ou des examens internes et externes de l'environnement des DFS peuvent être réalisés par des auditeurs. Ainsi, la phase de surveillance concerne également la remontée et la communication des risques aux parties prenantes concernées.

Une communication constante avec la direction tout au long du processus de gestion des risques garantit la compréhension et l'appropriation des rôles et des responsabilités, ce qui est essentiel pour établir le contexte et identifier les risques de façon adéquate, ainsi que pour analyser et évaluer les risques conjointement avec d'autres parties prenantes. La communication avec la direction permet d'étendre la consultation et l'examen du processus à toutes les parties prenantes de l'écosystème de DFS, ce qui permet d'obtenir l'approbation et le soutien des plans de gestion des risques grâce à une vue pertinente et précise des risques au sein de l'écosystème.

7.1 Domaine d'application

Le *Cadre de garantie de la sécurité des DFS* est applicable aux acteurs de l'écosystème de DFS. Il définit les mesures de sécurité à adopter par les utilisateurs des DFS, les MNO et les fournisseurs (y compris les banques et autres institutions financières non bancaires autorisées) qui fournissent des produits et des services financiers par des moyens numériques. Ces mesures peuvent être appliquées aux ressources, telles que l'infrastructure, les applications et les appareils qui rendent possibles les DFS.

Pour l'utilisateur, le cadre se concentre sur les mesures de sécurité destinées aux appareils utilisés pour accéder aux DFS, tels que les téléphones portables. Les moyens et la technologie sont généralement fournis par un MNO qui permet la communication entre l'utilisateur et le fournisseur

de DFS; le cadre porte sur les mesures que le fournisseur de réseau de communication doit mettre en place pour sécuriser l'écosystème.

Ce cadre inclut également les mesures de contrôle qui doivent être déployées par le fournisseur de DFS, qui peut être une institution financière comme une banque ou un fournisseur non bancaire. Dans certains cas, le fournisseur de réseau de communication est également le fournisseur de services financiers.

7.2 Établissement d'un contexte

Il s'agit de la première étape du processus de gestion des risques dont l'objectif est que les acteurs comprennent l'environnement d'exploitation des DFS. Cela implique d'identifier les événements internes et externes qui affectent la capacité de garantir la sécurité de bout en bout. Il est donc important pour les parties prenantes de comprendre et d'évaluer le contexte interne et externe dans lequel opèrent les DFS, ce qui permet également de définir la portée de l'évaluation des risques.

Pour établir le contexte interne, il convient de formuler ce qui suit:

a. Le système de gestion de la sécurité de l'information basé sur la norme ISO/IEC 27001; les documents normatifs doivent être pris en compte ou appliqués.

b. La structure organisationnelle globale des acteurs des DFS et la place des DFS dans ladite structure, ainsi que dans les objectifs de celle-ci.

c. Les ressources des DFS: cela comprend la technologie sous-jacente et les systèmes d'information, l'infrastructure physique, les applications logicielles, le matériel, les réseaux d'agents ainsi que les appareils des clients/agents/commerçants utilisés pour accéder aux DFS.

d. Les mesures de contrôle internes existantes, les incidents de sécurité et de fraude antérieurs, les rapports d'audit précédents et les documents de projet de DFS.

e. Les exigences réglementaires.

f. La tolérance au risque et l'appétence au risque.

Entre autres aspects, le contexte externe tient compte des éléments suivants:

a. Les lois et règlements relatifs aux DFS.

b. Parties prenantes clés de l'écosystème de DFS.

c. L'environnement politique et social: cela inclut des données démographiques telles que le niveau d'études de la population, le taux d'adoption des appareils mobiles et le niveau de pénétration des smartphones dans la population cible.

d. Les alternatives concurrentes et services complémentaires aux DFS.

e. Les risques émergents et leur influence, à la fois sur les services financiers et les parties prenantes.

Le résultat de cette phase est un résumé enregistré de toutes les informations recueillies. Ces informations constitueront les données de base du processus d'évaluation des risques.

7.3 Évaluation de la sécurité

L'évaluation des risques aide les acteurs à mesurer le niveau de sécurité actuel de l'écosystème de DFS à titre indicatif. Le processus d'évaluation inclut l'identification, l'analyse et l'évaluation des risques. L'évaluation des risques au sein de l'écosystème des DFS doit être effectuée régulièrement et les résultats doivent être présentés à la direction.

Une vue d'ensemble du déroulement du processus est présentée ci-dessous.

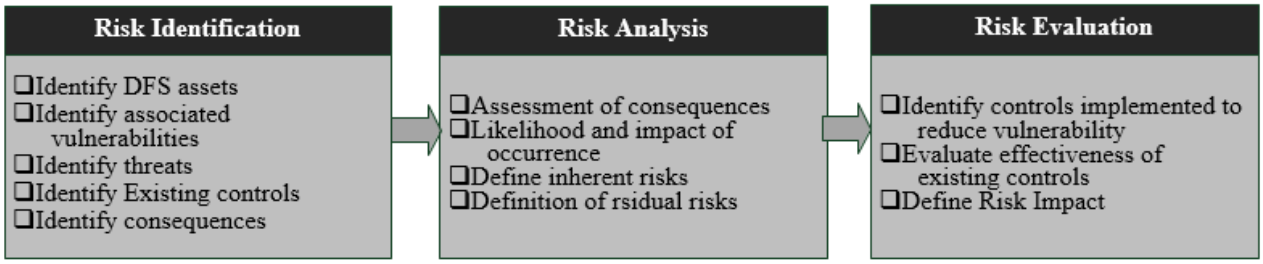

Figure 12: Déroulement du processus de gestion des risques

7.4 Identification des risques

L'identification des risques consiste à déterminer les vulnérabilités des DFS qui pourraient être exploitées, par quels moyens, à quel endroit et pour quelle raison. Pour cela, il est nécessaire d'identifier les ressources critiques des DFS, les menaces et vulnérabilités associées, la probabilité d'occurrence, les lacunes dans les mesures de contrôle existantes, ainsi que l'impact ou les conséquences des menaces et vulnérabilités si elles venaient à être exploitées. Au cours du processus d'identification des risques, l'acteur doit être conscient des facteurs internes et externes détaillés dans la section 5.2 ci-dessus.

À cette étape, les parties prenantes de l'écosystème des DFS doivent envisager cinq mesures critiques:

i. **Identification des ressources:** Cela implique de répertorier l'ensemble des ressources de l'écosystème des DFS ainsi que les responsables de ces ressources. Les ressources des DFS incluent, entre autres, l'infrastructure physique, les applications logicielles, le matériel, l'équipement des agents, les appareils des clients/agents/commerçants utilisés pour accéder aux DFS et les dispositifs du réseau de communication. L'identification permet à l'acteur de classer les ressources des DFS en fonction de l'impact qu'un incident aura sur l'écosystème des DFS. La classification vise à catégoriser les ressources en fonction de leur valeur et de leur importance pour l'écosystème des DFS.
ii. **Identification des vulnérabilités:** Une vulnérabilité est une faiblesse ou un défaut qui permet à une menace d'attaquer une ressource. Les vulnérabilités incluent, entre autres, les faiblesses dans l'agencement physique, les procédures opérationnelles, le personnel, la direction, le matériel, les logiciels, le réseau, etc. Elles peuvent être exploitées par une menace susceptible de nuire au système ou de l'endommager. Les vulnérabilités identifiées doivent être mises en évidence dans l'évaluation des risques, de même que les menaces qui affectent une ressource.
iii. **Identification des menaces:** Une menace désigne la possibilité pour une source d'exploiter (accidentellement ou intentionnellement) une vulnérabilité spécifique. Les menaces pour les ressources des DFS peuvent être naturelles (par exemple, séismes et inondations), humaines

(par exemple, vol et fraude), ou techniques (par exemple, logiciels malveillants ou pannes de serveurs). Une fois qu'une menace est identifiée, l'ensemble du patrimoine informationnel doit être analysé afin de mettre au jour toutes les vulnérabilités susceptibles d'être exploitées par la menace.

iv. **Identification des mesures de contrôle existantes:** Il s'agit d'une liste répertoriant toutes les mesures existantes et planifiées, leur mise en œuvre et leur état d'utilisation.

v. **Identification des conséquences:** Il s'agit de l'ampleur des dommages qui pourraient être causés en cas d'exploitation réussie d'une vulnérabilité par une menace. Ce processus permet de déterminer les ressources qui peuvent être affectées, ainsi que la sévérité de l'impact. L'ampleur des dommages causés à une ressource des DFS est généralement plus élevée que le coût de remplacement; il existe divers facteurs en termes de dommages à prendre en compte, notamment de nature monétaire, technique, humaine et réglementaire.

7.5 Analyse des risques

L'analyse des risques aide à comprendre la probabilité globale de la menace ainsi que son impact sur la ressource, deux facteurs importants pour la prise de décisions et la hiérarchisation des actions en vue de lutter contre les risques les plus critiques et les risques importants (risques ayant le plus grand impact). Le résultat de l'analyse des risques est un registre de risques mis à jour qui comprend les cotes de probabilité et d'impact de chaque risque. L'analyse des risques peut être effectuée de manière quantitative et/ou qualitative.

Les processus suivants doivent résulter de la phase d'analyse des risques:

i. Évaluation des conséquences: l'impact commercial qui pourrait résulter d'incidents de sécurité de l'information potentiels ou avérés doit être évalué, en tenant compte des conséquences d'une violation de la sécurité des informations, comme une perte de confidentialité, d'intégrité ou de disponibilité des ressources. Entre autres, les conséquences pour la sécurité des DFS peuvent également se traduire par des pertes financières, nuire à l'image ou à la réputation de l'organisation, et entraîner une perte de clientèle, des interdictions réglementaires et des amendes.

ii. Évaluation de la probabilité d'occurrence d'une menace susceptible d'exploiter une vulnérabilité et de son impact en cas de réussite. La probabilité d'occurrence doit tenir compte des mesures de prévention et de détection en place, de leur efficacité, de leur mise en œuvre et de leur utilisation.

iii. Définition de la cote de risque inhérent comme un produit de la probabilité et de l'impact. L'objectif de la cotation des risques inhérents est d'aider la direction à hiérarchiser les mesures de gestion afin de lutter contre les risques les plus importants.

iv. Définition du risque résiduel en évaluant l'efficacité des mesures de contrôle mises en place pour faire face au risque. Les mesures de contrôle mises en œuvre doivent réduire les risques à un niveau acceptable en fonction de l'appétence au risque des parties prenantes de l'écosystème des DFS.

7.6 Évaluation des risques

Au cours du processus d'évaluation des risques, l'acteur concerné compare les risques identifiés à des critères de risque prédéfinis afin de déterminer l'effet net des risques pour l'écosystème des DFS. Il convient également de déterminer l'efficacité des mesures existantes, en analysant la probabilité et l'impact des risques après avoir passé en revue les mesures de contrôle en place, puis en estimant les risques résiduels. Ce processus facilite la hiérarchisation et la prise de décisions en matière de gestion des risques et de mise en œuvre.

Au cours d'une évaluation des risques, il convient de procéder aux démarches suivantes:

i. Déterminer l'efficacité des mesures existantes pour chaque combinaison vulnérabilité-menace d'une classe de ressources donnée (c'est-à-dire le niveau d'efficacité des mesures en place qui permettrait d'atténuer la combinaison vulnérabilité-menace);
ii. Déterminer l'impact du risque;
iii. Déterminer la cote du risque résiduel en tant que produit de la probabilité d'occurrence et de l'impact.

8 Évaluation des vulnérabilités en matière de sécurité des DFS, des menaces et des mesures d'atténuation

Afin de contrer systématiquement les menaces pour l'écosystème des DFS et les vulnérabilités de celui-ci (décrites dans les sections ci-dessus), des mesures de contrôle sont proposées pour chacune des entités de l'écosystème, fondées sur les huit dimensions de sécurité visant à garantir une sécurité de bout en bout.

Étant donné qu'il existe souvent des points communs entre les menaces auxquelles sont confrontées les entités au sein de l'écosystème des DFS, pour faciliter la discussion, nous examinons d'abord une menace standardisée que nous avons identifiée, l'entité touchée par la menace générale, les vulnérabilités et les risques, ainsi que les mesures d'atténuation et de contrôle recommandées pouvant être déployées par l'entité en question. Les vulnérabilités sont étudiées dans le contexte dans lequel elles produisent un impact sur les dimensions de sécurité (DS) figurant dans la Recommandation UIT-T X.805.

Le schéma présenté dans la figure ci-dessous montre comment les menaces en matière de sécurité identifiées précédemment à la figure 9 sont associées aux 117 mesures de sécurité décrites dans les sections ci-dessous (le numéro de section du rapport apparaît entre parenthèses pour indiquer à quel endroit la mesure en question est abordée).

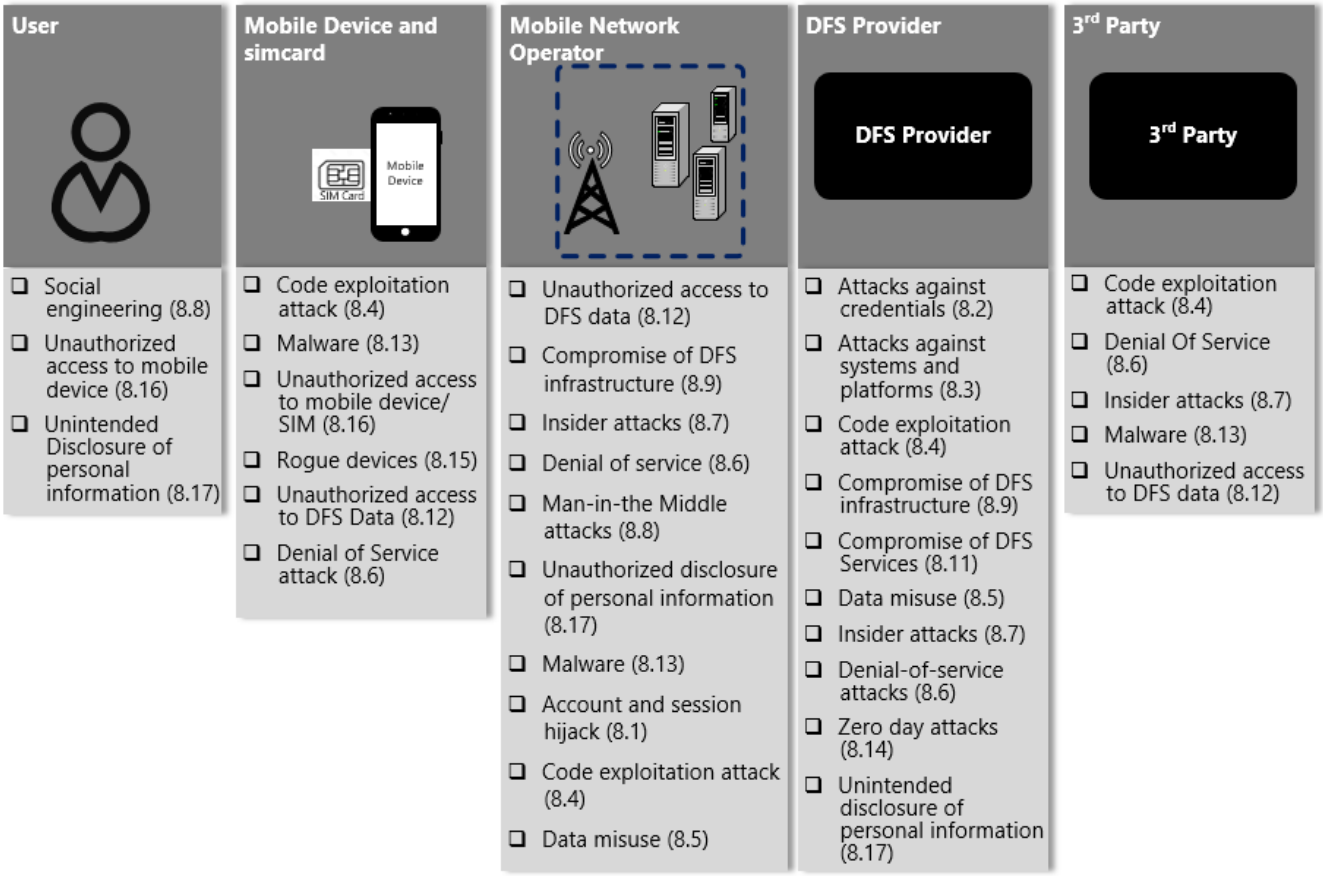

Figure 13: Risques et mesures de sécurité correspondantes

8.1 Menace: piratage de compte et de session

La menace générale étudiée ici est la capacité d'un attaquant à prendre le contrôle d'un compte ou d'une session de communication. Les vulnérabilités se manifestent de différentes manières au niveau du fournisseur de DFS et du MNO.

Entité affectée	Risque et vulnérabilité	Mesures de contrôle
Fournisseur de DFS	Le risque ***d'exposition et de modification des données*** est dû à la vulnérabilité suivante: - Mesures de contrôle insuffisantes au niveau des sessions utilisateur (DS: contrôle des accès)	**M1:** Prévoir des délais de connexion et des déconnexions automatiques pour les sessions utilisateur des applications de DFS (sessions logiques). Au sein de l'application, s'assurer que la complexité des mots de passe est encouragée (par le serveur), définir un nombre maximum de tentatives de connexion infructueuses, prévoir un historique et un délai de réutilisation des mots de passe, et mettre en place des délais de verrouillage des comptes suffisamment restreints pour minimiser les risques d'attaque hors ligne.
	Le risque ***de piratage d'un compte*** est dû à la vulnérabilité suivante: - Mesures de contrôle insuffisantes pour les comptes inactifs (DS: authentification)	**M2:** Exiger la vérification de l'identité pour les comptes d'utilisateurs de DFS inactifs, avant de procéder à leur réactivation.
	Le risque ***d'usurpation de l'identité d'un utilisateur autorisé par un attaquant*** est dû aux vulnérabilités suivantes:	
	- Échec de la vérification de la localisation (DS: sécurité des communications)	**M3:** Limiter l'accès aux services du système de DFS en fonction de la localisation de l'utilisateur (par exemple, désactiver l'accès aux codes USSD du système de DFS en cas d'itinérance, STK et SMS pour les commerçants et les agents) et, dans la mesure du possible, limiter l'accès par région pour les agents DFS et vérifier que l'agent et le numéro à l'origine du dépôt ou du retrait correspondent à la même zone de desserte.
	- Vérification incorrecte par l'utilisateur des canaux de communication sélectionnés pour l'accès aux DFS (DS: sécurité des communications)	**M4:** Limiter l'accès aux DFS à certains canaux de communication (lors de son inscription, l'utilisateur doit pouvoir choisir son canal d'accès aux services: protocole USSD uniquement, STK uniquement, application uniquement ou une combinaison de plusieurs canaux); bloquer et signaler les tentatives d'accès empruntant d'autres canaux que ceux sélectionnés par l'utilisateur.
	Le risque ***d'accès non autorisé aux données et aux identifiants de l'utilisateur*** est dû aux vulnérabilités suivantes:	

	- Rejeu d'une session par l'interception de jetons (DS: sécurité des communications)	**M5:** Le système de DFS ne doit pas se fier aux tentatives d'authentification ni aux jetons d'autorisation côté client; la vérification des jetons d'accès doit s'opérer côté serveur.
	- Faiblesse des algorithmes de chiffrement destinés au stockage des mots de passe (DS: confidentialité des données)	**M6:** Utiliser des algorithmes de hachage cryptographique salé puissants pour le stockage des mots de passe des utilisateurs des DFS.
MNO	Le risque ***d'usurpation de l'identité des utilisateurs autorisés*** est dû à la vulnérabilité suivante: - Absence de délai d'expiration des sessions pour les DFS	**M7:** Ajouter un délai d'expiration de session pour le protocole USSD, les SMS, l'application et l'accès Internet aux DFS.
	Le risque ***d'accès non autorisé aux données et aux identifiants de l'utilisateur*** est dû à la vulnérabilité suivante: - Les identifiants de l'utilisateur pour l'accès à l'application de DFS sont envoyés selon des modalités intrinsèquement exposées à des risques, telles que les SMS ou les agents (DS: confidentialité des données).	**M8:** Dans la mesure du possible, les utilisateurs des DFS doivent choisir leur propre mot de passe au moment de leur inscription, et ce mot de passe doit être chiffré tout au long du processus de transmission au système de DFS. Lorsque les informations d'identification à usage unique sont envoyées aux utilisateurs, assurez-vous que les informations d'identification pour l'application de DFS sont envoyées directement aux utilisateurs sans parties tierces/agents. Il doit ensuite être demandé aux utilisateurs de changer leur mot de passe après la première connexion.

8.2 Menace: attaques ciblant les identifiants

Cette catégorie globale regroupe les menaces conçues pour dérober ou altérer les identifiants des utilisateurs de systèmes de DFS et d'appareils mobiles.

Entités affectées	Risque et vulnérabilité	Mesures de contrôle
Appareil mobile	Le risque ***d'accès non autorisé et de piratage du compte de DFS d'un utilisateur*** est dû aux vulnérabilités suivantes:	
	- Utilisation de mots de passe/codes PIN faibles au niveau applicatif, ce qui rend ces identifiants vulnérables aux attaques par	**M9:** Exiger des codes PIN/mots de passe plus longs et difficiles à deviner dans les applications d'argent mobile. Il convient de faire preuve de prudence avant d'imposer l'utilisation de codes PIN complexes; veillez à ce qu'une telle mesure s'accompagne de campagnes de sensibilisation à l'intention des utilisateurs, car des codes PIN trop complexes

	force brute (DS: authentification)	risquent d'être écrits ou saisis par d'autres personnes, ce qui compromet la sécurité.
	- Utilisation de codes PIN simples pour accéder à l'appareil mobile (DS: authentification)	**M10:** Utiliser des mécanismes d'authentification solides pour démontrer la propriété du périphérique. Étant donné que l'espace des clés des codes PIN les rend vulnérables à une attaque par force brute, envisagez d'utiliser des codes PIN plus longs ou des codes PIN alphanumériques, tels que des phrases de passe faciles à mémoriser.
	Le risque de ***vol d'identifiants via des attaques par interception*** est dû à la vulnérabilité suivante: - Mauvaise configuration du serveur (DS: authentification)	**M11:** Les applications de DFS doivent être conçues pour vérifier le nom du serveur auquel elles se connectent.
Fournisseur de DFS	Le risque ***de compromission des systèmes de DFS*** est dû à la vulnérabilité suivante: - En l'absence d'un suivi des tentatives de connexion, les systèmes sont exposés aux attaques par force brute (DS: contrôle des accès).	**M12:** Imposer aux utilisateurs internes, aux commerçants, aux agents et aux utilisateurs externes un nombre limite de tentatives de connexion pour l'accès aux systèmes de DFS (base de données, système d'exploitation, application).

8.3 Menace: attaques ciblant les systèmes et les plates-formes

Il s'agit d'attaques qu'un adversaire peut mener à distance pour espionner ou modifier des informations sans identifiants internes ni accès privilégié.

EntitÉs affectÉes	Risque et vulnÉRABILITÉ	Mesures de contrÔle
Utilisateur mobile	Le risque ***d'espionnage et de vol à distance des identifiants sur les appareils utilisateur*** est dû aux vulnérabilités suivantes:	
	- Mises à jour par SMS binaires non vérifiées de la carte SIM (DS: authentification)	**M13:** Apprendre aux utilisateurs mobile de distinguer les messages SMS binaires isolés auxquels ils peuvent faire confiance ou pas. Cela pourrait empêcher les mises à jour malveillantes de la carte SIM.
MNO	- Transmission non sécurisée des identifiants de l'utilisateur (DS: contrôle des accès)	**M14:** Les fournisseurs de DFS doivent transmettre à l'utilisateur ses identifiants de connexion de manière sécurisée, par l'intermédiaire d'un canal distinct (hors bande).

	Les risques liés à ***l'accès aux comptes, à la compromission des comptes*** et au ***déni de service*** sont dus à la vulnérabilité suivante: - Exposition du réseau interne à des adversaires externes (DS: contrôle des accès)	**M15:** Utiliser la translation d'adresse réseau pour limiter l'exposition de l'adresse IP et des informations de routage du système de DFS à des adversaires externes.
Fournisseur de DFS	Les risques liés à ***l'accès aux comptes, à la compromission des comptes*** et au ***déni de service*** sont dus à la vulnérabilité suivante: - Protection insuffisante des systèmes internes contre des adversaires externes (DS: contrôle des accès)	**M16:** Mettre en place une zone démilitarisée pour créer une séparation logique entre le système de DFS et l'ensemble des autres systèmes internes et externes, et empêcher les systèmes externes d'accéder directement aux systèmes de DFS internes.

8.4 Menace: attaques par exploitation de code

Il s'agit d'attaques ciblant le code des applications de DFS.

Entité affectée	Risque et vulnérabilité	Mesures de contrôle
Fournisseur de DFS	Le risque ***de compromission des applications de DFS*** est dû à la vulnérabilité suivante: - Dépendance de l'application de DFS à l'égard des bibliothèques de sécurité mises à disposition par les systèmes d'exploitation (DS: sécurité des communications)	**M17:** Vérifier la qualité de la conception et de la mise en œuvre des bibliothèques de sécurité proposées par les systèmes d'exploitation, et s'assurer que les suites cryptographiques prises en charge sont suffisamment solides.

8.5 Menace: utilisation abusive des données

Il s'agit d'une menace relative à l'utilisation abusive de données client sensibles[i].

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
MNO	Le risque ***d'accès non autorisé aux données des utilisateurs*** et ***d'interception des données en transit*** est dû à la vulnérabilité suivante: - Pratiques insuffisantes en matière de chiffrement ou envoi d'informations sensibles en texte clair par	**M18:** S'assurer que l'ensemble des données sensibles des utilisateurs (telles que les codes PIN et les mots de passe) sont chiffrées lorsqu'elles traversent le réseau ou qu'elles sont au repos.

	l'intermédiaire de canaux non sécurisés tels que les SMS ou le canal USSD (DS: sécurité des communications)	
Fournisseur de DFS et fournisseurs tiers	Le risque ***d'exposition de données sensibles*** est dû aux vulnérabilités suivantes:	
	- Mesures de contrôle insuffisantes en matière de protection des données (DS: confidentialité)	**M19:** Effacer les données sensibles des utilisateurs des journaux d'événements. Parmi les données à effacer, on peut notamment citer les codes des bons de retrait en espèces, les numéros de comptes bancaires et les identifiants. Dans la mesure du possible, il convient de remplacer ces données par des caractères de remplissage dans les journaux d'événements.
	- Exposition d'informations sensibles concernant les utilisateurs pendant les transactions ou l'utilisation d'API (DS: confidentialité)	**M20:** Les fournisseurs de DFS doivent restreindre le partage des données en se limitant aux informations strictement nécessaires aux transactions avec des parties tierces et d'autres fournisseurs de services.
	- Faiblesse du chiffrement des API (DS: confidentialité)	**M21:** Surveiller l'utilisation des API et chiffrer l'ensemble des données partagées avec des parties tierces. Prévoir également des procédures et des mesures de contrôle en matière de gestion des données, par exemple en signant des accords de non-divulgation avec les fournisseurs de services de paiement, afin d'éviter les fuites d'informations ou de données.

8.6 Menace: attaques par déni de service

Il s'agit d'attaques conçues pour empêcher la prestation de services au sein de l'écosystème des DFS.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
MNO	Les risques ***d'impossibilité pour l'utilisateur d'effectuer une transaction en raison d'une interruption de service*** et ***d'échec de transaction en raison de retards de transaction importants*** sont dus aux vulnérabilités suivantes:	

	- Défaillance du réseau en raison de capacités insuffisantes, d'opérations de maintenance ou d'un défaut de conception (DS: disponibilité)	**M22:** Le MNO doit prendre des mesures pour garantir un niveau de disponibilité du réseau élevé et permettre l'accès aux DFS grâce au canal USSD, par SMS et par Internet.
		M23: Le MNO doit vérifier ses capacités techniques en procédant à des tests permettant de simuler différentes transactions en fonction du nombre d'utilisateurs, de la croissance prévue, du nombre de transactions attendues et des périodes de forte activité anticipées, afin d'assurer la continuité des performances du système.
Fournisseur de DFS	- Suivi insuffisant du trafic du réseau et des paquets réseau individuels (DS: disponibilité, sécurité des communications)	**M24:** Le fournisseur de DFS doit mettre en place des pare-feu et des filtres de trafic pour protéger le réseau des attaques. Il doit également protéger l'infrastructure du système de DFS en luttant contre le trafic suspect grâce à des techniques et des mécanismes de contrôle des accès au réseau tels que le CAPTCHA.
	Les risques ***d'accès non autorisé*** *aux données des utilisateurs* sont également dus à la vulnérabilité suivante: - Environnement favorable aux services inutiles (DS: confidentialité des données)	**M25:** Le trafic Internet entrant doit être limité et faire l'objet d'un suivi constant.
		M26: Définir des règles de pare-feu restrictives par défaut, configurer une liste blanche des ports, filtrer les paquets et assurer un suivi constant des accès pour les ports et les adresses IP autorisés ou figurant sur la liste blanche.

8.7 Menace: attaques d'initiés

Il s'agit d'attaques menées par des adversaires qui se trouvent dans le périmètre de l'organisation. Ces attaquants disposent souvent d'un accès aux ressources et de privilèges importants.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
Fournisseur de DFS	Le risque ***d'exposition et de modification des données*** est dû aux vulnérabilités suivantes:	
	- Les opérations critiques ne font pas l'objet de mesures de contrôle interne suffisantes (DS: contrôle des accès)	**M27:** Dans la mesure du possible, limiter les modifications importantes en utilisant le principe des *quatre yeux* (double approbation) pour l'ensemble des actions critiques, y compris la création, la modification ou la suppression d'un compte d'administrateur par un autre administrateur, la modification d'un compte d'utilisateur, le couplage ou le découplage du compte avec un numéro mobile ou un identifiant, ou encore l'annulation de transactions.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
	- Les données d'entrée ne font pas l'objet d'un processus de vérification suffisant (DS: intégrité des données)	**M28:** Dans le cadre de la double approbation, les fournisseurs de DFS doivent garantir une répartition claire des prérogatives. On peut par exemple envisager qu'un seul et même administrateur ne bénéficie pas de droits d'accès lui permettant d'assurer à la fois la création et l'activation des comptes de DFS.
	- Gestion insuffisante des privilèges d'accès (DS: contrôle des accès)	**M29:** Limiter, contrôler et surveiller l'accès physique aux infrastructures physiques sensibles du système de DFS. Isoler physiquement l'infrastructure du système de DFS et mettre en place des obstacles ou des mesures de dissuasion pour la séparer des autres infrastructures. Appliquer le principe du moindre privilège, de telle sorte que l'accès préventif dont bénéficient les personnes autorisées soit supplanté par des mesures de détection et de correction (par exemple, grâce à des alarmes permettant de détecter les tentatives de forçage). Surveiller l'activité des systèmes en enregistrant l'ensemble des informations d'accès (par exemple, qui est à l'origine de la tentative d'accès, à quels éléments cet individu a accédé, quelle est sa localisation et à quel moment la tentative a eu lieu).
Fournisseur de DFS	Le risque ***d'inexactitude et d'incohérence des données*** est dû aux vulnérabilités suivantes:	**M30:** Le fournisseur de DFS doit protéger les services exposés aux réseaux externes par des mesures solides de vérification des entrées en s'appuyant sur la détection des valeurs hors limites et des caractères interdits dans les champs de saisie, mais aussi sur la limitation et l'assainissement des données d'entrée. La vérification des données d'entrée doit avoir lieu le plus tôt possible, à la fois côté client et côté serveur. Toutefois, le serveur ne doit pas s'appuyer exclusivement sur les vérifications effectuées côté client. Il convient également de bloquer, d'enregistrer et d'examiner l'ensemble des requêtes constituant une violation des schémas et du langage de description des services Web (WSDL).
	- Ajout des données de test aux données de production (DS: intégrité des données)	**M31:** Utiliser la prise d'empreinte pour détecter toute modification ou falsification des données postérieure à leur stockage. Des techniques telles que l'utilisation de signatures numériques dans les colonnes de la base de données peuvent être utilisées pour détecter la modification des données utilisateur.
		M32: S'assurer que l'ensemble des données de test ont été supprimées du code avant sa migration vers l'environnement de production.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
	- Absence de suivi, journaux d'événements exposés aux modifications et informations de suivi insuffisantes (DS: non-répudiation)	**M33:** Les systèmes de DFS doivent s'appuyer sur des mécanismes de suivi tels que la détection de la provenance des actions des utilisateurs ou l'enregistrement des actions sur des espaces de stockage inviolables; ils doivent protéger les journaux d'événements contre toute tentative de falsification, de modification, de suppression ou d'interruption. Utiliser des signatures numériques associées aux actions, en particulier celles qui arrivent par le biais d'une connexion réseau.
	- Horloges imprécises et non synchronisées (DS: intégrité des données)	**M34:** S'assurer que les horloges de tous les systèmes connectés au système de DFS sont précises et synchronisées. Les protocoles NTP et SNTP sont utilisés pour garantir la précision et la synchronisation des horloges; toutefois, il convient de s'assurer que leur déploiement s'opère de manière sécurisée.

8.8 Menace: attaques par interception et d'ingénierie sociale

Ces deux types d'attaques sont regroupées, parce qu'elles impliquent toutes deux un adversaire qui s'interpose activement dans la communication ou l'interaction (par exemple, entre un utilisateur et un appareil ou un MNO, ou une interposition dans le cadre de la communication entre les parties).

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
Utilisateur mobile	Le risque ***d'exposition et de modification des données*** est dû aux vulnérabilités suivantes:	
	- Applications non vérifiées et non signées (DS: confidentialité, intégrité des données)	**M35:** Il est important de sensibiliser les clients pour qu'ils puissent télécharger leurs applications de DFS et y accéder par le biais de canaux officiels de publication des applications, afin de réduire le risque d'exécution d'applications infectées par des logiciels malveillants.
	- Éléments entrants non vérifiés tels que des messages SMS non sollicités, des publicités dans les applications ou des courriers électroniques (DS: intégrité des données)	**M36:** Les MNO et les fournisseurs de DFS doivent activement mener des campagnes de sensibilisation afin d'informer les usagers et le personnel interne sur les messages malveillants, les attaques par hameçonnage et les tentatives d'usurpation.
	- Protection des identifiants insuffisante (DS: contrôle des accès)	**M37:** Masquer les mots de passe et les codes PIN des utilisateurs, sensibiliser activement les clients concernant le risque d'espionnage par-dessus l'épaule et l'utilisation sécurisée des codes PIN/mots de passe

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
		pour éviter l'espionnage par-dessus l'épaule et l'écriture des mots de passe sur papier.
MNO	Le risque ***d'accès non autorisé aux données utilisateur*** est dû à la vulnérabilité suivante: - Faiblesse du chiffrement « over-the-air » (DS: sécurité des communications)	**M38:** Cesser d'utiliser les algorithmes de chiffrement GSM A5/0, A5/1 et A5/2. Surveiller de près les résultats de la communauté de la sécurité et de la cryptographie concernant la faisabilité et la facilité de compromettre A5/3 et A5/4, et commencer à envisager des chiffrements plus forts. Prévoir une stratégie de déploiement pour ces nouveaux algorithmes de chiffrement.
	Le risque ***d'usurpation d'identité des utilisateurs*** est dû à la vulnérabilité suivante: - Faiblesse du filtrage par identification des lignes téléphoniques (DS: sécurité des communications)	**M39:** Les MNO doivent procéder à l'identification des lignes téléphoniques afin de détecter les communications usurpées et destinées à apparaître comme des appels ou des SMS provenant du fournisseur de DFS.
Fournisseur de DFS	Le risque ***de piratage d'un compte utilisateur*** est dû à la vulnérabilité suivante: - Mesures de contrôle manquantes ou inadéquates pour la configuration et les autorisations des comptes (DS: authentification)	**M40:** Exiger l'authentification et l'autorisation de l'utilisateur pour les modifications de compte présentant un risque élevé ainsi que pour les transactions; exiger la saisie du code PIN ou du mot de passe avant toute transaction, y compris lorsque l'appareil de l'utilisateur est connecté.
Fournisseurs tiers	Le risque ***d'exposition d'informations sensibles*** est dû aux vulnérabilités suivantes:	
	- Faiblesse des algorithmes de chiffrement utilisés pour la transmission des données et pour les données stockées sur l'appareil (DS: confidentialité)	**M41:** Protéger les données de l'application mobile et les communications avec les systèmes internes du DFS en faisant appel à une méthode de chiffrement suffisamment sécurisée et, dans la mesure du possible, masquer, tronquer ou effacer les informations confidentielles concernant les utilisateurs.
	- Absence de chiffrement des communications (DS: sécurité des communications)	**M42:** Utiliser la signature numérique pour identifier les parties tierces connectées au système de DFS lorsque des transactions sont en cours.
	- Gestion insuffisante des certificats et des clés (DS: contrôle des accès)	**M43:** Utiliser des clés et des certificats fiables et secrets pour permettre l'échange de données entre les fournisseurs de DFS et les parties tierces.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
	Le risque ***d'usurpation d'identité et d'échec de transactions*** est dû à la vulnérabilité suivante: - Défaillance du système du fournisseur de DFS ou du MNO obligeant les agents et les parties tierces à se tourner vers des processus hors ligne (DS: disponibilité)	**M44:** Mettre en place des mesures de contrôle procédurales et techniques, en commun avec les fournisseurs de services, afin d'assurer une gestion efficace du système en cas d'indisponibilité. Par exemple, prévoir des mesures pour la gestion hors ligne des transactions (telles que des échanges de carte SIM) en cas d'accès intermittent au système de DFS. Mettre en place des vérifications supplémentaires pour les transferts de fonds et les paiements des parties tierces en cas d'accès intermittent au système de DFS ou du fournisseur tiers.

8.9 Menace: compromission de l'infrastructure de DFS

Il s'agit d'attaques ciblant l'infrastructure sous-jacente de l'écosystème des DFS.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
Fournisseur de DFS	Le risque ***de compromission de l'infrastructure et des données*** est dû à la vulnérabilité suivante: - Contrôle insuffisant et non sécurisé des accès aux comptes d'utilisateurs (DS: contrôle des accès)	**M45:** Utiliser l'authentification à facteurs multiples ou une combinaison de plusieurs modes d'authentification pour l'accès aux comptes du système de DFS.
Fournisseur de DFS	Le risque ***d'interruptions des services et des transactions*** est dû à la vulnérabilité suivante: - Pratiques de restauration non testées (DS: disponibilité)	**M46:** Désactiver les comptes et les identifiants de connexion par défaut et les supprimer des bases de données, des applications, des systèmes d'exploitation et de toute autre interface d'accès en contact avec le système de production de DFS.
		M47: Examiner les comptes liés à l'installation, à l'éditeur et à l'assistance technique, ainsi que les points d'accès aux systèmes et aux infrastructures de DFS. L'ensemble de ces comptes doivent être désactivés ou associés à des profils d'utilisateurs complets.
	Les risques ***d'exfiltration et de modification des données, de compromission de l'intégrité des transactions*** et ***d'interruption de service*** sont dus à la vulnérabilité suivante: - Mesures de protection des données insuffisantes; par exemple, incapacité à mettre en œuvre l'atomicité des	**M48:** Après chaque modification des systèmes de DFS, du MNO, des fournisseurs de services et des parties tierces, procéder à des tests de bout en bout et inclure notamment des tests de régression et de capacité dans les tests de validation. Prévoir également un plan de basculement ou une procédure en cas de coupure du réseau.
		M49: Programmer des sauvegardes régulières des systèmes de DFS. Procéder à la vérification régulière des sauvegardes et prévoir un stockage sécurisé, hors

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
	transactions, ouvrant ainsi la voie à des transactions en état d'achèvement partiel (DS: intégrité des données)	ligne et sur un site externe, en adoptant un format chiffré.
		M50: Appliquer les propriétés ACID (atomicité, cohérence, isolation et durabilité) aux bases de données afin de garantir l'intégrité des transactions. Les opérations des DFS doivent se faire complètement ou pas du tout. Le fournisseur de DFS doit également s'assurer que des vérifications sont mises en place pour éviter les transactions en double (identifiant de transaction unique, horodatage et nonce cryptographique).
Fournisseur tiers	Le risque ***d'impossibilité pour l'utilisateur d'effectuer des transactions*** est dû à la vulnérabilité suivante: - Insuffisance des mécanismes destinés à garantir l'intégrité des données et dépendance excessive à l'égard d'ancres de confiance externes (DS: non-répudiation)	**M51:** Les applications de DFS ou les parties tierces doivent prendre en charge l'usage de la signature numérique; une signature numérique sécurisée constitue une preuve irréfutable de l'origine de la transaction. Pour que les signatures numériques soient valides, l'infrastructure à clés publiques ne doit pas être compromise et doit faire l'objet de tests et de plans destinés à garantir sa souplesse. S'assurer que les clés de signature sont bien protégées jusqu'à la clé racine permet au fournisseur de DFS de se prémunir contre les transactions litigieuses et d'éventuelles procédures juridiques destinées à contester l'authenticité d'un utilisateur donné.

8.10 Menace: attaques SIM

La menace générale est la capacité d'un attaquant à accéder sans autorisation à la carte SIM d'un utilisateur de DFS. Les vulnérabilités se manifestent de différentes manières au niveau du MNO, du fournisseur de DFS et de l'utilisateur mobile.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
MNO	Les risques ***de piratage de compte et de transactions non autorisées*** sont dus aux vulnérabilités suivantes: - Mesures de contrôle insuffisantes pour l'identification et la vérification de l'utilisateur avant tout échange ou recyclage de carte SIM (DS: authentification)	**M52:** Les MNO doivent s'assurer qu'un processus de vérification de l'identité est mis en place avant de procéder à des échanges de carte SIM.
		M53: Le processus de vérification de l'identité doit s'appuyer à la fois sur quelque chose que l'utilisateur *est*, sur quelque chose qu'il *a* et sur quelque chose qu'il *sait*. L'utilisateur devra par exemple présenter une pièce d'identité valide, se soumettre à une vérification biométrique et fournir des informations

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
		sur son compte avant de pouvoir procéder à un échange ou un remplacement de carte SIM.
		M54: Les fournisseurs de DFS et de services de paiement doivent être en mesure de détecter en temps réel l'échange ou le remplacement d'une carte SIM associée à des DFS. Ils doivent également procéder à des vérifications supplémentaires avant d'autoriser la nouvelle carte SIM à effectuer des transactions de valeur élevée ou à apporter des modifications au compte de DFS.
MNO	Les risques ***de piratage de compte et de transactions non autorisées*** sont dus aux vulnérabilités suivantes: - Mesures de contrôle insuffisantes pour l'identification et la vérification de l'utilisateur avant tout échange ou recyclage de carte SIM (DS: authentification)	**M55:** Le MNO doit sauvegarder et stocker de manière sécurisée les données de carte SIM telles que le numéro d'identité internationale d'abonnement mobile (IMSI) et les valeurs de clé secrète (valeurs Ki).
		M56: Il convient de mettre en place un processus de recyclage des numéros mobiles impliquant de communiquer avec les fournisseurs de DFS sur le recyclage ou la résiliation des numéros d'identification d'abonné mobile (MSIN) (dans ce contexte, le recyclage désigne la réaffectation par le MNO d'un MSIN à un nouvel utilisateur). Lorsqu'une carte SIM est recyclée, le MNO signale un changement de numéro IMSI pour le numéro de téléphone du compte correspondant. Le fournisseur de DFS doit alors bloquer l'accès au compte en attendant de vérifier que le nouveau propriétaire de la carte SIM est bien le titulaire du compte.
Utilisateur mobile	Le risque ***d'accès non autorisé aux données mobiles de l'utilisateur*** est dû à la vulnérabilité suivante: - Vol d'appareil mobile (DS: confidentialité des données)	**M57:** En cas de perte ou de vol de leur appareil, les utilisateurs des DFS doivent avoir la possibilité de chiffrer leurs données et de les effacer à distance.
Fournisseur de DFS	Le risque ***de perte d'accès aux comptes et d'atteinte à la réputation*** est dû à la vulnérabilité suivante: - Processus d'échange et de recyclage de carte SIM incorrects[ii] (DS: intégrité des données)	**M58:** Les fournisseurs de DFS doivent s'assurer que des procédures sont mises en place pour détecter et éviter les cas suspects d'échange et de recyclage de carte SIM. Pour cela, ils doivent suivre les étapes suivantes: a) Vérifier que le numéro IMSI associé au numéro de téléphone est resté le même. S'il a changé, cela pourrait indiquer un échange de carte SIM.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
		b) Dans ce cas, vérifier le numéro d'identité internationale d'équipement mobile (IMEI) du téléphone associé à la carte SIM. S'il a changé également, cela indique une probabilité élevée d'échange de carte SIM. Dans ce cas, le fournisseur de DFS doit bloquer le compte en attendant de pouvoir procéder aux vérifications d'usage par l'intermédiaire d'un appel vocal ou d'un agent.

8.11 Menace: compromission des DFS

La menace générale est la capacité d'un attaquant à pirater un service financier sans être détecté. Les vulnérabilités se manifestent de différentes manières au niveau du fournisseur de DFS.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
Fournisseur de DFS	Les risques ***de panne de service et de compromission des DFS et des données de DFS*** sont dus aux vulnérabilités suivantes:	
	- Modifications non autorisées de la configuration du système ainsi que des données et des journaux d'événements (DS: intégrité des données)	**M59:** Protéger le système contre les tentatives de falsification et n'autoriser que les transactions en ligne. a) Assurer le suivi des fichiers de l'application de DFS et les protéger contre les tentatives de falsification et de modification en s'appuyant sur des outils de suivi destinés à préserver leur intégrité, par exemple à travers le calcul des sommes de contrôle ou la vérification des signatures numériques. b) La politique du fournisseur de DFS ou du commerçant ne doit pas permettre d'utiliser la solution de paiement mobile pour autoriser les transactions hors ligne ou pour stocker une transaction en vue d'une transmission ultérieure sur le serveur.
Fournisseur de DFS	- Vérification insuffisante des accès ou des données d'entrée des utilisateurs (DS: authentification)	**M60:** Utiliser une authentification forte à facteurs multiples pour l'accès des utilisateurs et des fournisseurs tiers aux systèmes de DFS, par exemple grâce à des jetons d'accès ou une vérification biométrique. L'usage de ces méthodes d'authentification favorise la non-répudiation de l'origine.
		M61: Comparer les données entrantes aux valeurs attendues dans le schéma de données associé à l'API; pour les requêtes issues du canal USSD, procéder à

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
		une vérification de la signature XML des requêtes HTTP.
		M62: Utiliser des systèmes d'analyse permettant de vérifier la vélocité des utilisateurs entre les transactions et surveiller les horaires des transactions afin de mettre en place des procédures d'autorisation complémentaires.
		M63: Quelle que soit la méthode utilisée pour produire les reçus (courriers électroniques, SMS, imprimante reliée au réseau, etc.), le PAN ne doit pas apparaître, conformément aux lois, aux réglementations et aux politiques en vigueur en matière de cartes de paiement. La politique et les pratiques du fournisseur de DFS et du commerçant ne doivent pas permettre l'usage de canaux non sécurisés tels que les courriers électroniques et les SMS pour l'envoi des PAN ou des données d'identification sensibles.

8.12 Menace: accès non autorisé aux données de DFS

La menace générale est la capacité d'un attaquant à accéder sans autorisation aux données de DFS d'un utilisateur de DFS. Les vulnérabilités se manifestent de différentes manières au niveau du MNO, du fournisseur de DFS et de l'utilisateur mobile.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
Utilisateur mobile	Le risque ***d'accès non autorisé aux données mobiles de DFS de l'utilisateur*** est dû aux vulnérabilités suivantes:	
	- Mécanismes insuffisants de contrôle des accès aux comptes des utilisateurs (DS: contrôle des accès)	**M64:** Les utilisateurs de DFS doivent définir le code PIN de leur compte. Lorsque le code PIN initial est défini par le système du fournisseur de DFS ou ses agents, le code PIN est unique à chaque utilisateur et doit être modifié lors de la première connexion.
	- Mesures de contrôle limitées pour l'accès aux données sensibles sur l'appareil (DS: contrôle des accès)	**M65**: Les utilisateurs de DFS doivent définir des mots de passe forts et éviter les codes PIN faciles à deviner (par exemple, date d'anniversaire) pour leurs appareils.
		M66: Il convient de s'assurer que les informations de DFS sensibles sont stockées dans des parties sécurisées de l'appareil mobile.
		M67: Les développeurs d'applications doivent s'assurer que l'authentification de l'utilisateur est

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
		demandée avant l'installation de l'application sur l'appareil.
		M68: Les développeurs d'applications doivent s'assurer que l'accès à l'infrastructure des DFS, aux applications de DFS ainsi qu'aux DFS eux-mêmes n'est possible qu'après la vérification de l'identité. Il convient d'utiliser l'authentification à facteurs multiples: une chose que l'utilisateur connaît (par exemple, un code PIN), une chose qu'il possède (par exemple, la carte SIM) et un élément de son identité (par exemple, empreinte digitale ou autre méthode biométrique).
		M69: Les développeurs d'applications doivent s'assurer que les applications de DFS gèrent les identifiants d'accès de manière sécurisée.
MNO	Le risque ***d'interception de données de DFS*** *en transit* est dû aux vulnérabilités suivantes:	**M70**: S'assurer que l'ensemble des données sensibles des utilisateurs, telles que les codes PIN et les mots de passe, sont stockées de manière sécurisée et protégées par des algorithmes de chiffrement solides, tant sur le réseau interne qu'au repos, afin de limiter les menaces internes auxquelles elles peuvent être exposées.
	- Vulnérabilités SS7 inhérentes [iii] (DS: sécurité des communications)	**M71:** Utiliser des pare-feu pour détecter et limiter les attaques exploitant des vulnérabilités SS7.
	- Interception des transactions USSD réalisées depuis un terminal mobile (DS: sécurité des communications)	**M72:** Vérifier que le numéro IMEI de l'appareil à l'origine de la transaction correspond bien au numéro IMEI enregistré pour le téléphone de la personne titulaire du compte (par un système d'attaque par interception, il est possible de cloner la carte SIM en utilisant un numéro IMEI différent).
	- Absence de protection du trafic sensible et faiblesse des pratiques de chiffrement (DS: sécurité des communications)	**M73:** Surveiller la vélocité de l'utilisateur en comparant la localisation du téléphone à l'origine des transactions à la dernière localisation connue du téléphone (dernier SMS ou appel entrant ou sortant).
		M74: Les MNO doivent imposer l'usage d'une clé personnelle de déverrouillage (code PUK) sur les cartes SIM afin d'offrir une sécurité supplémentaire en cas de perte ou de vol de l'appareil mobile.
		M75: Surveiller et contrôler l'usage du suivi MSC-MAP et des analyseurs de protocole pour l'infrastructure USSD et SMS afin de limiter l'accès interne aux transmissions SMS et USSD en texte clair.
		M76: Vérifier la légitimité de la transaction grâce à une procédure d'approbation bidirectionnelle avec

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
		envoi d'un mot de passe à usage unique au numéro de téléphone original[iv].
		M77: Avoir recours à des pratiques de chiffrement solides afin de garantir la confidentialité et l'intégrité des données au moment de leur entrée, de leur traitement et de leur stockage sur le réseau du fournisseur de DFS.
		M78: Limiter le nombre de sessions de DFS par utilisateur. Autoriser une seule session à la fois par utilisateur, quel que soit le canal d'accès (STK, USSD ou HTTPS); un compte d'utilisateur de DFS ne doit pas être accessible sur plusieurs canaux à la fois.
		M79: Le MNO doit déployer les protocoles de signalisation SS7 et Diameter recommandés par la GSM Association (FS.11, FS.07, IR.82 et IR.88) afin de limiter les menaces liées à des attaques SS7[v].
Fournisseur de DFS	Le risque ***d'exposition de données client sensibles*** est dû aux vulnérabilités suivantes:	
	- Protection insuffisante des données d'inscription des utilisateurs des DFS (DS: authentification)	**M80:** Protéger et sauvegarder les données d'inscription des utilisateurs des DFS; lorsque des formulaires physiques sont utilisés, les stocker et les transmettre de manière sécurisée.
	- Faiblesse du chiffrement (DS: sécurité des communications)	**M81:** Appliquer des normes de chiffrement solides aux communications avec les API, telles que le protocole TLS v1.2 et les versions supérieures.
Fournisseur de DFS	- Contrôle et suivi insuffisants de l'accès des utilisateurs au système de DFS (DS: contrôle des accès)	**M82:** Élargir les processus de détection des menaces afin d'inclure de manière explicite les menaces liées aux API.
		M83: Limiter l'accès à la connexion à distance et limiter les privilèges des sessions à distance pour l'accès aux systèmes internes de DFS.
		M84: Limiter la durée de vie des certificats TLS à 825 jours.
		M85: Authentifier l'adresse IP, l'appareil et l'horaire de connexion de tous les utilisateurs, agents et commerçants dotés de privilèges d'accès qui se connectent au système de DFS. Par exemple, paramétrer un accès spécifique pour les commerçants et les agents afin d'interdire l'accès au système de DFS en dehors de leurs horaires de travail.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
		M86: Les modifications du code doivent être testées dans l'environnement de test avec d'entrer dans l'environnement de production; l'environnement de test doit être séparé de l'environnement de production physiquement et logiquement.
		M87: Afin d'améliorer la sécurité, utiliser un appareil fiable et inviolable tel qu'une boîte noire transactionnelle pour la gestion sécurisée du processus et le stockage des clés cryptographiques destinées à protéger les codes PIN, les transactions, les jetons et les bons de retrait en espèces des utilisateurs.
		M88: Définir des rôles d'utilisateur afin de fixer des droits d'accès en s'appuyant sur le principe du moindre privilège.
		M89: Après le départ ou la résiliation d'un utilisateur, d'un agent ou d'un commerçant, les fournisseurs de services de paiement et les parties tierces doivent désactiver le compte correspondant.
		M90: Fixer un délai d'inactivité au-delà duquel les comptes seront désactivés.
		M91: Imposer des limitations et des horaires de connexion en fonction des rôles au sein des DFS (on peut par exemple envisager un nombre maximum d'annulations par session et par jour selon le rôle de titulaire de compte).
		M92: Limiter, contrôler, surveiller et examiner de manière régulière les privilèges d'accès aux systèmes de DFS, notamment l'ajout, la modification et la suppression d'utilisateurs.
		M93: Surveiller l'utilisation des API et chiffrer l'ensemble des données partagées avec des tiers; prévoir des procédures et des mesures de contrôle en matière de gestion des données, par exemple en signant des accords de non-divulgation avec les fournisseurs de services de paiement, afin d'éviter les fuites d'informations ou de données.
	- Surveillance insuffisante du réseau hertzien (DS: confidentialité des données)	**M94:** Protéger les transmissions sans fil en appliquant les exigences de la norme de sécurité de l'industrie des cartes de paiement. Les mesures de contrôle doivent inclure, sans s'y limiter, les éléments suivants: - S'assurer que les clés de chiffrement, les mots de passe et les chaînes de communauté SNMP installés par défaut par l'éditeur sont modifiés avant leur application.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
		- Favoriser la mise en œuvre des bonnes pratiques du secteur afin de garantir un chiffrement solide des données d'authentification et de transmission. - S'assurer que les données de compte en texte clair ne sont pas stockées sur un serveur connecté à Internet.
Fournisseurs tiers	- Les données ne sont pas détruites ou effacées lorsqu'un appareil est mis au rebut (DS: confidentialité)	**M95:** Les fournisseurs de DFS/commerçants doivent systématiquement se débarrasser des anciens appareils. Le cas échéant, ils doivent suivre les instructions données par le fournisseur de l'appareil. On peut notamment s'appuyer sur les étapes suivantes: - Retirer l'ensemble des étiquettes et des éléments permettant d'identifier l'entreprise. - Dans la mesure du possible, passer un contrat avec un fournisseur agréé qui pourra contribuer à l'élimination en toute sécurité des matériaux et des composants électroniques. - Ne pas jeter les appareils dans des poubelles ou des bennes associées à l'entreprise.

8.13 Menace: logiciels malveillants

Cette menace générale concerne les éléments des DFS susceptibles d'être infectés par des logiciels malveillants.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
Fournisseur tiers, fournisseur de DFS	Les risques liés aux ***attaques de logiciels malveillants, à l'incapacité d'effectuer des transactions, aux pannes de service et à l'accès non autorisé aux données*** surviennent au niveau du commerçant/fournisseur de DFS et découlent des vulnérabilités suivantes:	
	- Aucun logiciel de protection contre les programmes malveillants ou antivirus utilisé ou absence de mises à jour régulières (DS: disponibilité)	**M96:** Déployer des logiciels de sécurité sur tous les appareils mobiles, notamment des antivirus, des logiciels de protection contre les programmes-espions et des produits d'authentification logicielle, afin de protéger les systèmes contre les menaces logicielles actuelles et émergentes. Tous les logiciels doivent être installés à partir d'une source fiable.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
		M97: Si aucun logiciel de protection contre les programmes malveillants ou antivirus n'est disponible, utiliser des solutions de gestion d'applications mobiles ou de gestion des appareils mobiles capables de surveiller, d'évaluer et de supprimer les logiciels et applications malveillants de l'appareil. En outre, il convient dans l'idéal de déployer à la fois des solutions de protection contre les programmes malveillants et de gestion des appareils mobiles (voir ci-dessus) pour protéger l'appareil contre les logiciels et applications malveillants.
		M98: Désactiver les fonctions inutiles des appareils et installer uniquement des logiciels de confiance. Les commerçants et les fournisseurs de DFS doivent désactiver toutes les capacités de communication qui ne sont pas nécessaires au fonctionnement du dispositif de paiement. Pour éviter d'introduire de nouveaux vecteurs d'attaque sur un appareil mobile, il faut uniquement autoriser la communication avec un logiciel de confiance nécessaire à la prise en charge des opérations commerciales et au traitement des paiements.
	- Collaboration insuffisante avec le fournisseur concernant la sécurité des appareils mobiles achetés (DS: disponibilité et confidentialité)	**M99:** Les commerçants et les fournisseurs de DFS doivent poser les questions suivantes à leur fournisseur: - Le fournisseur doit assurer la mise à jour régulière de son application de paiement et informer le commerçant lorsque des mises à jour sont disponibles et peuvent être installées en toute sécurité. - Le fournisseur doit imposer des restrictions à son application de paiement afin qu'elle ne puisse fonctionner que sur un appareil équipé d'un micrologiciel approuvé. - Le fournisseur doit proposer au commerçant une documentation comprenant les procédures à respecter pour les mises à jour. - Le fournisseur doit communiquer avec le fournisseur de DFS et l'informer des dernières vulnérabilités découvertes dans sa solution de paiement. Lorsque de nouvelles vulnérabilités sont découvertes, le fournisseur doit également accompagner le commerçant et lui fournir des correctifs testés pour chacune de ces vulnérabilités.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
	- Vulnérabilités non détectées dans les applications du système (DS: confidentialité des données)	**M100:** Le commerçant doit travailler avec son fournisseur pour s'assurer que toutes les capacités d'audit et de suivi sont activées. Le fournisseur doit s'assurer que les capacités de suivi offrent une granularité suffisante pour détecter les activités suspectes. Le fournisseur doit expliquer au commerçant quelles sont ses responsabilités en matière d'examen des journaux. Il convient également d'inspecter de manière régulière les journaux et les rapports du système pour détecter d'éventuelles activités suspectes. En cas d'activité anormale suspectée ou découverte, l'accès à l'appareil mobile et à son application de paiement doit être bloqué jusqu'à la résolution du problème. Les activités suspectes comprennent notamment les tentatives non autorisées d'accès, de mise à niveau des privilèges et de mise à jour du logiciel ou du micrologiciel.
Fournisseur tiers, fournisseur de DFS	- Exposition du réseau aux attaques extérieures (DS: disponibilité)	**M101:** Les applications de DFS doivent être soumises à des analyses et à des tests d'intrusion réguliers. Elles doivent notamment être conçues pour résister aux logiciels d'hameçonnage.
Utilisateur mobile	Les risques liés à ***l'installation de logiciels malveillants tels que les logiciels espions et les chevaux de Troie*** sont dus à la vulnérabilité suivante: - Aucun logiciel de protection contre les programmes malveillants ou antivirus utilisé ou absence de mises à jour régulières (DS: disponibilité)	**M102:** Mettre à jour le système d'exploitation de l'appareil mobile régulièrement; interdire l'installation de programmes sans validation de l'utilisateur.
	Le risque ***d'exécution de code à distance*** est dû aux vulnérabilités suivantes:	
	- Logiciel de l'appareil obsolète (DS: confidentialité des données)	**M103:** Les utilisateurs doivent être encouragés à installer régulièrement des mises à jour de sécurité sur les appareils mobiles utilisés pour les transactions effectuées dans le cadre de DFS, et à s'assurer qu'ils sont mis à jour avec les derniers correctifs de sécurité des fabricants d'appareils et des fournisseurs d'applications.
	- Aucun logiciel de protection contre les programmes malveillants ou antivirus utilisé ou absence de mises à	**M104:** Installer des logiciels de sécurité provenant de sources de confiance sur les appareils mobiles, notamment des antivirus, des logiciels de protection contre les programmes-espions et des produits d'authentification logicielle, afin de protéger les

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
	jour régulières (DS: disponibilité)	appareils contre les menaces logicielles actuelles et émergentes.
	- Modification et rooting de l'appareil utilisateur (DS: intégrité des données)	**M105:** L'utilisateur DFS doit éviter d'utiliser Un appareil altéré ou rooté car il peut potentiellement compromettre la confidentialité et l'intégrité de ses propres données.
		M106: Le développeur d'applications mobiles doit s'assurer que ses applications de DFS sont isolées dans un environnement de "bac à sable", pour empêcher d'autres applications non fiables installées sur l'appareil mobile d'interagir avec elles, tout en limitant l'interaction avec le système d'exploitation.
MNO	Le risque ***d'impossibilité d'effectuer des transactions et de compromission des services*** est dû à la vulnérabilité suivante: - Exposition du réseau aux attaques extérieures (DS: disponibilité)	**M107:** Soumettre l'infrastructure du MNO à des analyses de vulnérabilité et à des tests d'intrusion réguliers afin de vérifier l'exposition à des attaques susceptibles d'affecter la disponibilité du système.
		M108: Installer et mettre à jour de manière régulière le logiciel de protection contre les programmes malveillants le plus récent (en fonction de sa disponibilité) et le proposer aux utilisateurs finaux. Envisager l'encapsulation des applications, qui peut être employée avec une solution de gestion des terminaux mobiles pour combattre et supprimer les applications et les logiciels malveillants.

8.14 Menace: attaques zero-day

Ce sous-ensemble de menaces liées aux logiciels malveillants est considéré avec une attention particulière, car les moyens traditionnels de protection contre les logiciels malveillants sont inefficaces contre une menace inédite.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
MNO, fournisseurs de DFS et fournisseurs tiers	Le risque ***d'accès non autorisé aux données confidentielles des utilisateurs et de modification non autorisée de données utilisateur*** est dû à la vulnérabilité suivante: - Découverte de nouveaux exploits contre les systèmes existants et incapacité à déployer des solutions pour combattre ces exploits (DS: confidentialité des données,	**M109:** Les MNO et les fournisseurs de DFS et de services de paiement doivent appliquer des correctifs à leurs systèmes pour se mettre au niveau des dernières versions proposées par l'éditeur et se défendre contre les attaques qui ont été créées à partir de vulnérabilités plus anciennes.
		M110: Les fournisseurs et les MNO doivent mettre au point des plans d'urgence en collaboration avec les éditeurs, afin de bénéficier rapidement de correctifs et de mesures de correction en cas d'attaque de type zero-day. Cette stratégie repose

	contrôle des accès, disponibilité)	notamment sur un usage avisé des procédures de sauvegarde.

8.15 Menace: appareils non autorisés

Les périphériques non autorisés peuvent représenter une menace pour l'infrastructure de réseau des DFS.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
MNO	Les risques ***de fraude et de modification des données*** sont dus à la vulnérabilité suivante: - Connexion d'appareils non sécurisés à l'infrastructure des DFS (DS: intégrité des données)	**M111:** Les MNO doivent assurer le suivi des appareils utilisés pour se connecter ou accéder au système de DFS afin de s'assurer que ces appareils bénéficient des derniers correctifs et d'un logiciel antivirus à jour, qu'ils sont analysés pour détecter la présence d'outils de dissimulation d'activité (rootkits) et d'enregistreurs de frappe et qu'ils ne prennent pas en charge la fonction d'extension de réseau.

8.16 Menace: accès non autorisé aux appareils mobiles

Il s'agit d'attaques spécifiques menées par des adversaires contre des appareils mobiles.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
	Le risque ***d'usurpation d'identité et de perte de données/transactions frauduleuses*** est dû aux vulnérabilités suivantes:	
Utilisateur/appareil mobile	- Authentification de l'utilisateur sur l'appareil inadéquate (DS: confidentialité des données)	**M112:** Les appareils mobiles doivent se verrouiller automatiquement après une période d'inactivité afin d'obliger les utilisateurs à s'authentifier pour les déverrouiller et effectuer des transactions de DFS.
		M113: Utiliser des codes PIN forts, la suppression de données à distance, le verrouillage PIN, l'authentification biométrique (par exemple, par empreinte digitale, scan de l'iris) lorsque ces fonctionnalités sont disponibles sur l'appareil.
	- Versions logicielles obsolètes, rendant les appareils vulnérables aux programmes malveillants	**M114:** Les fabricants d'appareils doivent s'assurer que les mises à jour critiques sont directement téléchargeables par les usagers ou mises à la disposition des fournisseurs de

	(DS: confidentialité des données)	réseau pour leur permettre de les envoyer à leurs utilisateurs.
Fournisseur de DFS	Le risque de ***piratage d'un compte utilisateur de*** *DFS* est dû à la vulnérabilité suivante: - Accès trop permissif à l'infrastructure des DFS (DS: authentification)	**M115:** Avant d'authentifier un utilisateur des DFS et dans la mesure du possible, vérifier son numéro IMSI, son appareil, sa localisation et son adresse IP pour établir son identité et empêcher les accès non autorisés à l'infrastructure du réseau.
Fournisseur tiers	Le risque ***de transactions refusées*** est dû à la vulnérabilité suivante: - Processus de vérification des transactions insuffisant (DS: non-répudiation)	**M116:** Les fournisseurs de services de paiement doivent s'assurer que les cartes compagnons polyvalentes rechargeables associées à des comptes de DFS sont équipées de puces EMV, qu'elles sont protégées, dans la mesure du possible, par des méthodes de vérification telles que le code PIN ou la validation biométrique et que toutes les transactions donnent lieu à l'envoi d'une alerte à l'utilisateur.

8.17 Menace: divulgation involontaire d'informations personnelles

Il s'agit de menaces entraînant l'exposition accidentelle des données utilisateur.

Entité affectée	Risques et vulnérabilités	Mesures de contrôle
Fournisseur de DFS	Le risque ***d'exposition d'informations personnelles identifiables*** est dû à la vulnérabilité suivante: - Les environnements de test ne font pas l'objet d'une supervision et de mesures de contrôle adéquates (DS: confidentialité)	**M117:** Les fournisseurs de DFS doivent s'assurer que les données des utilisateurs associées à l'environnement de production ne sont pas exploitées dans des environnements de test, à moins de respecter les bonnes pratiques en matière d'anonymisation. De même, les données de test ne doivent pas migrer vers l'environnement de production.
Fournisseur tiers	Le risque ***d'exposition d'informations sensibles*** est dû aux vulnérabilités suivantes:	
	- Exposition d'informations sensibles concernant les utilisateurs pendant les transactions ou l'utilisation des API (DS: confidentialité)	**M118:** Les fournisseurs tiers doivent limiter le partage d'informations avec d'autres parties telles que les prestataires de services de paiement et de DFS, et s'en tenir au minimum requis pour garantir l'intégrité des transactions.
	- Mesures de contrôle insuffisantes en matière de protection des données (DS: confidentialité)	**M119:** Les fournisseurs doivent s'assurer que les données sensibles des utilisateurs (par exemple, les codes des bons de retrait en espèces, les numéros de compte bancaire et les identifiants de connexion) sont effacées des environnements tels que les journaux de suivi. Dans la mesure du possible, il

		convient de remplacer ces données par des caractères de remplissage dans les journaux.

9 Lignes directrices relatives aux bonnes pratiques en matière de sécurité des applications d'argent mobile

Dans cette section, nous présentons un modèle de cadre de sécurité pour les applications d'argent mobile, en nous concentrant sur de bonnes pratiques générales et non sur des technologies spécifiques, sauf lorsqu'elles sont explicitement mentionnées. Pour ce modèle, nous nous inspirons de travaux d'analyse récents sur les applications de DFS du point de vue des applications d'argent mobile. Ces travaux incluent l'étude de la Global System Mobile Association (GSMA) sur les bonnes pratiques en matière de sécurité des applications d'argent mobile[4], les lignes directrices de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour le développement sécurisé de smartphones[5], ainsi qu'un cadre de sécurité pour les applications de paiement mobiles élaboré par la Banque d'État du Pakistan[6]. Ce modèle peut également être utilisé par les fournisseurs de DFS pour étayer leur politique en matière de sécurité des applications.

Cette section vise à synthétiser les recommandations afin de fournir aux organismes de réglementation ou aux examinateurs de la sécurité applicative un point de départ pour leurs évaluations de la sécurité. Le modèle porte strictement sur l'application mobile installée sur l'appareil, sauf indication contraire, et les sous-sections décrivant les recommandations traitent de divers aspects de l'exploitation ou de la politique sous-jacente relative à l'application mobile. L'accent est principalement mis sur les applications Android étant donné leur part de marché importante, bien que de nombreuses recommandations s'appliquent à l'ensemble des systèmes d'exploitation mobiles. Bien que la confidentialité constitue également un facteur important, ces recommandations concernent avant tout la sécurité.

9.1 Intégrité des appareils et des applications

i. Les appareils les plus sûrs pour effectuer des transactions financières n'ont jamais subi de débridage ou de rooting, car il peut être difficile, voire impossible, d'évaluer la sécurité du système d'exploitation sous-jacent s'il a été remplacé ou exploité. Les applications doivent donc utiliser les services de la plate-forme mobile pour déterminer que la plate-forme sous-jacente et elles-mêmes n'ont pas été modifiées.
ii. Il convient de supprimer tout code superflu éventuellement ajouté à l'application pendant le développement, comme les fonctionnalités qui ne sont pas conçues pour les plates-formes d'appareils sur lesquelles l'application sera déployée ou les fonctionnalités de développement/débogage, afin de réduire la surface d'attaque du code de production déployé.
iii. Côté serveur, il convient de déterminer si l'application s'exécute dans un état d'intégrité élevée grâce à la validation de signature, au hachage sur l'application ou à certains blocs de fonction du programme.

[4] GSMA, "Official Document MM.01 – MM App Security Best Practices, Version 1.0", 29 juin 2018.
[5] ENISA, "Smartphone Secure Development Guidelines", 10 février 2017.
[6] Banque d'État du Pakistan, *Mobile Payment Applications (App) Security Framework* (PROJET DE DOCUMENT, version 1.0), avril 2019.

9.2 Sécurité des communications et gestion des certificats

i. Les applications doivent utiliser des bibliothèques cryptographiques normalisées. Pour la communication avec les services internes, elles doivent également appliquer un chiffrement de bout en bout en bout en utilisant des protocoles normalisés, en particulier TLS. La version minimale recommandée du protocole TLS est la version 1.2.
ii. Les certificats TLS ne doivent pas être expirés et doivent présenter des suites de chiffrement fortes, notamment le chiffrement AES-128 et SHA-256 pour le hachage. Nous recommandons l'utilisation de modes d'opération de chiffrement authentifiés tels que le Galois/Counter Mode (GCM).
iii. Il faut limiter la durée de vie des certificats émis à 825 jours, conformément aux bonnes pratiques préconisées par le Certification Authority Browser Forum.
iv. Il convient de vérifier la fiabilité de l'autorité de certification et de prévoir un plan d'urgence si celle-ci n'est plus fiable.
v. La configuration de TLS doit être effectuée de manière sécurisée et des mesures doivent être prises pour éviter les problèmes de configuration qui pourraient entraîner l'échec de l'authentification ou une mauvaise sélection de l'algorithme.
vi. L'épinglage des certificats est recommandé pour empêcher leur remplacement.
vii. Il convient de s'assurer que les certificats de serveur sont validés correctement au niveau des appareils côté client.

9.3 Authentification des utilisateurs

i. Les codes PIN et les mots de passe doivent être difficiles à deviner; il convient également d'interdire les identifiants faibles. Cependant, il ne faut pas forcer les utilisateurs à changer régulièrement de mot de passe.
ii. Nous recommandons fortement l'utilisation de l'authentification à facteurs multiples avant toute action financière ou sensible.
iii. Pour envoyer des mots de passe à usage unique, il faut privilégier les applications d'authentification pour smartphone, car le canal SMS est vulnérable au piratage du protocole SS7 et à d'autres menaces en matière de sécurité.
iv. Si des informations biométriques sont utilisées pour l'authentification, des mesures de sécurité adéquates doivent être prévues pour leur stockage, par exemple en les chiffrant dans le magasin de clés Android ou en utilisant du matériel de confiance.

9.4 Traitement sécurisé des données

i. Les appareils mobiles doivent stocker les informations confidentielles en toute sécurité, par exemple à l'aide du cadre Android KeyStore.
ii. Il convient, si possible, d'utiliser du matériel de confiance pour stocker les informations sensibles sur les smartphones des clients.
iii. Il faut éviter de stocker des informations dans un dispositif de stockage externe. Le cas échéant, il faut s'assurer d'effectuer une validation forte des données entrantes avant de les utiliser.
iv. Il convient de supprimer les données confidentielles des caches et de la mémoire après leur utilisation et évitez d'exposer les informations de manière générale (par exemple, en plaçant la clé secrète sur la pile). La mémoire doit être nettoyée avant de quitter l'application.
v. Il convient de limiter la quantité de données partagée avec d'autres applications en utilisant des autorisations granulaires. Il faut également limiter autant que possible le nombre d'autorisations demandées par l'application et s'assurer que lesdites autorisations correspondent aux fonctionnalités nécessaires au bon fonctionnement de l'application.

vi. Les informations sensibles (mots de passe ou clés, par exemple) ne doivent pas être codées en dur dans le code source de l'application.
vii. Toute entrée provenant du client qui doit être stockée dans les bases de données doit être validée pour éviter les attaques par injection SQL.

9.5 Développement d'applications sécurisé

i. Les applications doivent être développées selon les pratiques et les normes de programmation sécurisée reconnues par le secteur.
ii. Il convient de s'assurer d'être en mesure de mettre à jour les applications en toute sécurité et de veiller à ce que toutes les bibliothèques et tous les modules dépendants soient sécurisés. Les mises à jour pour ces éléments doivent être mises à disposition dès que nécessaire.
iii. Le code doit être testé et évalué de manière indépendante par des équipes de réviseurs internes ou externes.

10 Gestion des incidents de sécurité dans le cadre des DFS

Souvent, même après la mise en œuvre de mesures de contrôle adéquates, des incidents de sécurité se produisent, en particulier dans le cadre de services financiers où les attaquants ont un motif financier d'échapper aux systèmes. Ces attaques provoquent une interruption des services, une altération du système ou la divulgation des données. Les organisations et les parties prenantes qui fournissent des DFS ou font partie de l'écosystème doivent mettre en place des procédures, établir des mécanismes de signalement, mener des activités de collecte de données, attribuer des responsabilités en matière de gestion, établir des protocoles juridiques et élaborer des stratégies de communication efficaces qui leur permettront de comprendre les incidents de sécurité, de les gérer de manière adéquate et de s'en relever. En l'absence d'un plan de gestion des incidents, il est possible qu'un fournisseur de DFS ne détecte pas l'attaque ou, en cas de détection, il n'aura pas nécessairement les procédures nécessaires en place pour endiguer rapidement les dommages, éliminer la menace et réagir à la présence de l'attaquant, puis récupérer ses ressources avec un impact minimal.

Un plan de gestion des incidents de sécurité définit des procédures cohérentes à suivre pour garantir un signalement des incidents, des activités d'analyse des interventions, un déroulement de l'enquête et un relèvement fluides, rapides et efficaces en cas d'incident de sécurité compromettant l'une des huit dimensions de sécurité.

La norme ISO/IEC 27035:2016 "Gestion des incidents de sécurité de l'information" reconnaît que les mesures de sécurité de l'information sont imparfaites et propose des processus détaillés pour la gestion des incidents.

Le Center for Internet Security[7] recommande aux opérateurs de réseau de systèmes de DFS, aux fournisseurs de DFS et aux prestataires de services de suivre les lignes directrices suivantes pour la gestion des incidents:

1. Il convient de s'assurer qu'il existe des plans d'intervention écrits en cas d'incident qui définissent les rôles du personnel ainsi que les phases du processus de gestion des incidents.
2. Il faut attribuer des intitulés de poste et des responsabilités à des personnes spécifiques pour la gestion des incidents informatiques et de réseau, et assurer le suivi et la documentation tout au long du processus de gestion de l'incident, jusqu'à sa résolution.
3. Il convient également de désigner des responsables au sein de l'équipe de gestion, ainsi que des remplaçants, qui appuieront le processus de gestion des incidents en assumant des rôles de décideurs essentiels.
4. Il est nécessaire d'établir des normes à l'échelle de l'organisation concernant le temps requis pour que les administrateurs du système et les autres membres du personnel signalent les événements anormaux à l'équipe de gestion des incidents, les dispositifs de signalement de tels incidents et le type d'informations à inclure dans le rapport d'incident.
5. Il faut collecter et tenir à jour des informations sur les coordonnées de tierces parties à utiliser pour signaler un incident de sécurité, notamment les forces de l'ordre, les services publics concernés, les fournisseurs et les fabricants d'appareils.
6. L'ensemble du personnel doit pouvoir accéder aux informations concernant le signalement d'anomalies et d'incidents informatiques à l'équipe de gestion des incidents. Ces informations doivent être incluses dans des activités de sensibilisation régulières destinées au personnel.
7. Il convient d'organiser régulièrement des exercices et des scénarios d'intervention face aux incidents avec le personnel impliqué, en vue d'améliorer ses connaissances et de renforcer

[7] https://www.cisecurity.org/controls/incident-response-and-management/.

ses capacités à faire face à des menaces réelles. Ces exercices doivent tester les canaux de communication, le processus de prise de décisions et les capacités techniques des intervenants à l’aide des outils et données à leur disposition.

8. Il est recommandé de créer un système de notation et de hiérarchisation des incidents basé sur l'impact connu ou potentiel sur l'organisation. Ce système doit être utilisé pour définir la fréquence des mises à jour de statut et des procédures de transfert en escalade.

Annexe 1: Infrastructure détaillée de l'écosystème de DFS et menaces

Il existe une multitude de points d'interaction entre les différentes parties de l'écosystème des DFS. Les attaquants peuvent donc attaquer le système de nombreuses façons différentes. Les attaques réussies ont souvent des conséquences sur les parties prenantes exploitées, mais également sur d'autres acteurs de l'écosystème. Dans cette section, nous nous intéressons aux différents points vulnérables de l'infrastructure de DFS, détaillés dans le schéma ci-dessous. Les numéros en vert seront utilisés pour décrire la surface de vulnérabilité au point d'interaction considéré.

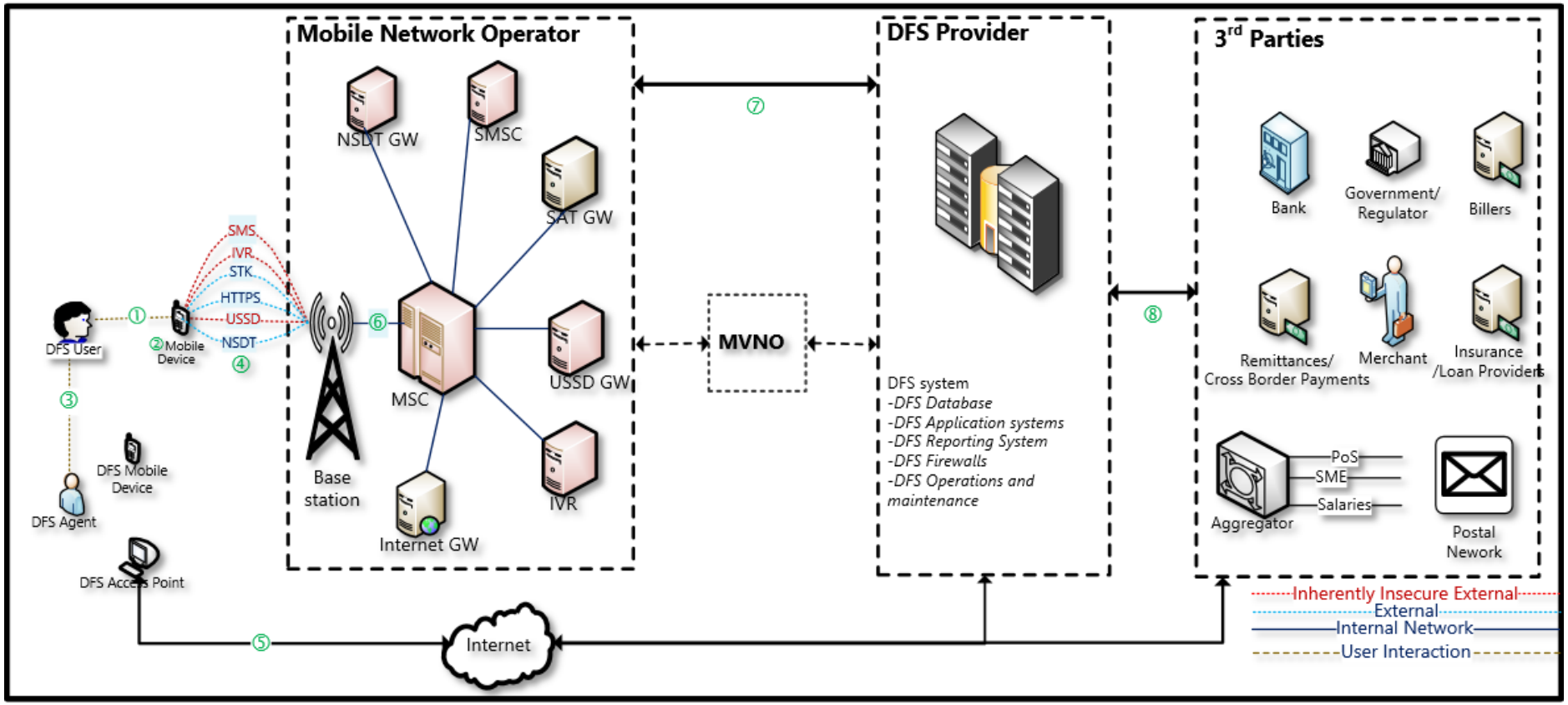

Figure 14: Risques et mesures de sécurité correspondantes

1. Client – appareil mobile

a. Exposition d'informations sensibles du client due au partage volontaire de son appareil mobile avec d'autres personnes, à la perte, à l'arrachage ou au vol de l'appareil, ou à l'espionnage par-dessus l'épaule des identifiants par un adversaire.

b. Accès non autorisé à l'appareil par un attaquant devinant le code PIN ou le mot de passe ou réussissant à contrecarrer les mécanismes d'authentification (s'ils sont configurés) de l'appareil.

c. Modification non autorisée de l'appareil en vue de compromettre la sécurité de la plate-forme sous-jacente, par exemple à travers l'installation d'un logiciel malveillant sur le dispositif stockage sous-jacent ou en manipulant la mémoire de l'appareil pour en extraire des secrets.

d. Modification des paramètres d'appel par un acteur malveillant non autorisé pour transférer les appels et les SMS. Cela permet à l'attaquant d'accéder aux informations de DFS envoyées par le biais de messages, telles que les mots de passe à usage unique.

2. Appareil mobile – application mobile

a. Des vulnérabilités de code au sein de l'application mobile peuvent être exploitées par des attaquants qui accèdent à l'appareil mobile, par exemple par le biais de surapplications. Cela peut compromettre les données du client et entraîner une perte de confidentialité et d'intégrité.

b. La compromission de la plate-forme mobile sous-jacente peut introduire des virus, des chevaux de Troie, des vers, des logiciels rançonneurs et d'autres programmes malveillants/rootkits qui peuvent compromettre les informations du client ou rendre l'utilisateur plus vulnérable aux tentatives d'hameçonnage visant à obtenir les identifiants pour l'application, ce qui permettrait à l'attaquant d'accéder au compte du client sans autorisation.

c. Des mesures de contrôle des accès insuffisantes au sein de l'application, par exemple un mécanisme d'authentification requis avant l'exécution d'opérations sensibles (par exemple, inscription, transfert de paiement) basé sur des hypothèses de confiance, peuvent entraîner la compromission de l'application et l'extraction de données du client ou des transferts d'argent non autorisés.

d. L'absence de capacités de journalisation/d'audit au sein de l'application, ainsi que l'absence de stockage de ces données dans une partie protégée de la mémoire de l'appareil, peuvent compromettre les garanties de non-répudiation et empêcher l'utilisateur de prouver qu'il a subi une attaque.

e. L'absence ou la mauvaise utilisation du chiffrement dans l'application, entraînant une consignation non sécurisée dans les journaux de l'application ou un stockage dans des bases de données sans chiffrement ou avec un chiffrement faible, peut également permettre à un acteur malveillant d'exposer ces informations.

f. Si l'application permet la négociation de suites de chiffrement faibles, elle peut faire l'objet d'attaques par rétrogradation vers des versions antérieures utilisant des algorithmes de chiffrement potentiellement faibles. Si les clés de session ne sont pas renégociées de manière régulière, l'accumulation de contenus chiffrés peut rendre la clé vulnérable aux attaques.

g. Accès non autorisé à un appareil mobile perdu ou volé.

h. Altération d'applications mobiles.

3. Client – agent de DFS

a. Les clients peuvent être vulnérables aux attaques d'échange de carte SIM, où l'attaquant se fait passer pour le client auprès de l'agent afin d'obtenir une nouvelle carte SIM qui donne accès au compte de DFS.

b. Des cartes complémentaires liées à des comptes de DFS peuvent s'exposer à des vulnérabilités similaires si l'agent effectue une vérification insuffisante des identifiants du client ou s'il coopère avec l'adversaire.

4. Appareil mobile – station de base

a. Les réseaux GSM existants au sein desquels les applications de DFS utilisent principalement les technologies SMS, USSD ou IVR reposent sur la sécurité offerte par le réseau. Cette sécurité est assurée par les algorithmes de chiffrement des réseaux GSM tels que A5/1 et A5/2. Il a été démontré que ces algorithmes sont vulnérables. Des travaux récents ont également démontré que des approches similaires peuvent être utilisées pour compromettre le chiffrement A5/3. Dans certains systèmes, l'algorithme A5/0 est spécifié, ce qui fournit un chiffrement nul et donc aucune protection de la confidentialité des données. Les attaquants peuvent ainsi exfiltrer des informations sensibles par le biais d'une interface "over-the-air". Indépendamment des menaces de sécurité pour le réseau de transport sous-jacent, les protocoles STK et HTTPS fournissent un chiffrement de bout en bout.

b. Les réseaux existants utilisant le chiffrement GSM (STK, USSD et IVR) sont également vulnérables aux attaques par interception depuis des stations de base malveillantes installées par un attaquant, qui les fait passer pour des installations légitimes du fournisseur (il s'agit donc de fausses stations de base, ou "intercepteurs d'IMSI"). Ces stations déchiffrent les communications, puis les renvoient dans le réseau de l'opérateur mobile. Il est ainsi possible d'accéder à l'intégralité des informations communiquées, y compris les données de transaction et les données financières.

5. Appareil mobile – Internet

a. La sécurité de la liaison de communication dépend de la suite de chiffrement négociée entre l'application et les services internes dans les systèmes de bout en bout sur Internet. Il a été démontré que les informations contenues dans les applications circulent vers diverses destinations en dehors du terminal autorisé, y compris dans des journaux d'événements et des bases de données. Par conséquent, seuls les mécanismes de chiffrement forts comme les protocoles TLS garantissent la sécurité des données dans les réseaux de télécommunication publics.

b. Il est également important de veiller à ce que les suites de chiffrement ne fassent pas l'objet d'attaques par rétrogradation qui pourraient les faire revenir à des versions antérieures pouvant utiliser des chiffrements faibles. Si les clés de session ne sont pas renégociées de manière régulière, l'accumulation de contenus chiffrés peut rendre la clé vulnérable aux

attaques. Des protocoles tels que SSL et TLS peuvent être configurés pour renégocier les algorithmes de chiffrement, mais il est important que les protocoles soient résilients face aux attaques par renégociation des acteurs malveillants qui injectent du trafic dans des échanges client-serveur légitimes. La négociation de suites de chiffrement faibles qui affaiblissent la sécurité peut permettre à un adversaire de modifier les transactions et, par conséquent, de compromettre l'intégrité des données financières.

c. Sans un chiffrement adéquat des informations transmises par le biais de connexions Internet, les adversaires peuvent espionner les données transférées par Wi-Fi entre l'appareil mobile et le point d'accès. Des attaques récentes contre des négociations de clés TLS démontrent que même les protocoles Wi-Fi sécurisés comme WPA2 peuvent être compromis.

6. Station de base – station de commutation mobile – passerelles

a. En l'absence de contrôles internes réguliers, il est possible d'accéder aux données des clients en interne. Il s'agit d'un facteur particulièrement important pour les solutions SMS et USSD qui ne fournissent pas de chiffrement au sein du réseau du fournisseur.

b. Un acteur malveillant ayant accès au réseau SS7 pourrait envoyer des messages de gestion du sous-système de transport de messages pour simuler une congestion du réseau, rediriger des messages ou interrompre un service/bloquer des liaisons.

c. Les réseaux mobiles peuvent également subir des attaques par déni de service, qui peuvent être exécutées en surchargeant les liaisons SS7. Un attaquant envoie un grand nombre de requêtes SCCP (protocole Signaling Connection and Control Part) qui nécessitent beaucoup de traitement, par exemple la traduction d'appellations globales.

d. Ces informations peuvent être falsifiées par des utilisateurs internes, en particulier dans les protocoles qui n'assurent pas l'intégrité des messages.

e. L'accès simplifié au réseau SS7 permet aux attaquants d'utiliser les opérations du sous-système application mobile pour insérer ou modifier les données de l'abonné, de situer son emplacement ou d'intercepter ses communications mobiles.

f. La liaison de communication entre la station de base mobile et le réseau du fournisseur est une liaison filaire dans certains cas, tandis que dans d'autres, selon la topographie du réseau mobile, les stations de base peuvent être connectées sans fil au réseau du fournisseur, par exemple par le biais d'une liaison micro-ondes. Si cette communication n'est pas chiffrée, en particulier pour les transactions par SMS et USSD où le chiffrement est strictement assuré par des algorithmes GSM entre l'appareil et la station de base, ces données pourraient être renvoyées au réseau sans être chiffrées, entraînant un risque de violation de la confidentialité.

g. Dans le contexte des DFS, un acteur malveillant avec un accès au niveau du réseau SS7 peut émuler (usurper) l'identité de la ligne appelante d'une personne ou d'une entité de confiance, et appeler l'utilisateur de DFS pour tenter d'obtenir ses identifiants bancaires et de DFS, ce qui peut entraîner des pertes financières.

h. Les clients du MNO peuvent être victimes d'un échange de carte SIM non autorisé, et les attaquants peuvent exploiter les informations des abonnés collectées lors d'attaques SS7 pour obtenir des données qui peuvent être utilisées pour l'exécution réussie d'un échange de carte SIM ou en collaboration avec le personnel interne du MNO.

i. Les utilisateurs privilégiés au sein du MNO peuvent utiliser de manière abusive leur accès aux nœuds centraux comme le HLR et le CCM pour mener des activités telles que les transferts d'appels et de SMS, le renvoi d'appels, ou l'interception et la collecte non autorisées de données d'appels des abonnés aux DFS.

7. Réseau mobile – opérateur de DFS

a. La protection des données est souvent insuffisante, en particulier en termes de chiffrement, une fois que les informations sont transmises au réseau du fournisseur, notamment en raison des coûts informatiques et des frais généraux nécessaires pour maintenir des connexions chiffrées à large bande au sein du réseau. Il est également souvent supposé que les menaces pesant sur le réseau proviennent principalement de l'extérieur plutôt que de l'intérieur. Il en résulte des vulnérabilités provenant à la fois d'adversaires internes et de menaces extérieures capables de pénétrer dans le réseau.

b. Les données au sein du réseau de l'opérateur sont menacées par le manque de mesures de protection de l'intégrité mises en place dans ces réseaux. Ces informations peuvent être modifiées arbitrairement par un adversaire parvenant à accéder au réseau (par exemple, en compromettant les défenses du périmètre) ou par un acteur interne malveillant.

c. Si les fournisseurs de DFS utilisent la carte SIM comme élément sécurisé et les numéros de SIM/numéros mobiles comme compte financier, ils risquent de perdre leurs comptes lors du recyclage des cartes SIM. Si les opérateurs mobiles effectuent un recyclage périodique des cartes SIM (en réaffectant des numéros mobiles inactifs/inutilisés pendant une période donnée sur le réseau GSM à de nouveaux utilisateurs), cela peut mener à la perte d'accès au compte financier ou à son transfert illicite à un autre utilisateur.

d. Les configurations et les limitations des capacités de l'équipement du MNO pourraient limiter le service et la disponibilité des DFS; les limitations de la durée de session USSD pourraient interrompre les transactions de DFS.

e. L'ampleur du réseau et de l'infrastructure physique de l'opérateur mobile le rend vulnérable à la compromission des accès grâce à l'installation d'appareils indésirables qui peuvent permettre un accès à distance non autorisé. L'interconnexion au sein de l'écosystème des DFS peut permettre à un appareil disposant d'un accès non autorisé d'accéder aux différentes parties prenantes, au-delà du MNO.

f. Interceptions par faisceau hertzien et CCM: Le CCM dispose de capacités permettant une interception légale. Grâce à un accès privilégié au CCM, il est donc possible d'intercepter les communications. Cet accès pourrait être utilisé de façon abusive pour des gains financiers frauduleux en surveillant ou en refusant l'activité des DFS.

g. Attaques par déni de service sur les réseaux mobiles: ce risque est accru par le fait que les nœuds opérateurs comme les passerelles du CCM se connectent à d'autres opérateurs de réseau en utilisant des adresses IP. Cela exacerbe le risque d'inondation et d'attaques de ressources, ce qui augmente généralement la quantité de trafic entrant et peut surcharger la pile IP et les processeurs du nœud, ce qui forcerait le nœud à s'arrêter ou à redémarrer et affecte donc directement la disponibilité.

h. Réacheminement et renvoi d'appel: un attaquant externe obtenant un accès ou un acteur interne disposant déjà d'un accès à l'équipement du réseau pourrait rediriger les communications des DFS vers un autre numéro, par exemple en modifiant le profil de localisation de l'abonné mobile, ce qui permettrait à l'attaquant d'avoir accès à des informations de DFS confidentielles.

8. Opérateur de DFS – partie tierce

a. Les données peuvent être exposées si le chiffrement n'est pas rigoureusement employé au sein des réseaux de fournisseurs et entre ceux-ci. Les menaces externes proviennent d'informations collectées depuis l'extérieur du périmètre réseau du fournisseur (c'est-à-dire le réseau externe), tandis que les menaces internes existent à l'intérieur du périmètre réseau (c'est-à-dire le réseau interne). De plus, les données peuvent être exposées si les systèmes du réseau du fournisseur sont infectés par des logiciels malveillants, qui peuvent être transmis à la fois par le biais du réseau et par celui de périphériques malveillants connectés à des systèmes hôtes (par exemple, des clés USB malveillantes ou des enregistreurs de frappe installés sur un clavier). Ces périphériques peuvent permettre aux adversaires d'exfiltrer les données de l'environnement du fournisseur.

b. Un attaquant capable d'accéder à des bases de données externes du fournisseur (par exemple, en compromettant des vulnérabilités logicielles) peut altérer les données financières et les informations sensibles du fournisseur. Les interfaces entre les réseaux constituent notamment un point d'entrée potentiel pour un adversaire et doivent être étroitement surveillées. De plus, la sécurité des données au repos dépend des mesures de protection mises en place sur les dispositifs hôtes et les serveurs utilisés pour stocker ces données.

c. Un serveur de DFS qui ne fait pas l'objet de mises à jour de sécurité régulières peut être victime de logiciels malveillants et de rootkits. Toutes les machines connectées à une interface au réseau public sont vulnérables aux codes d'exploitation de réseau, y compris à des attaques zero-day inédites. Les systèmes peuvent également être compromis par le biais d'autres interfaces d'entrée/sortie telles que les lecteurs CD/DVD, les ports USB et d'autres interfaces périphériques à partir desquelles des appareils pourraient injecter du code et des données malveillants.

d. Insuffisance du durcissement des systèmes d'exploitation des DFS comme les paramètres d'accès et les mots de passe par défaut, les services non essentiels actifs, les protocoles actifs non sécurisés (Telnet et FTP, par exemple), les autorisations d'accès aux fichiers, les configurations de réseau par défaut et les droits des utilisateurs (utilisateurs autorisés à effectuer un arrêt, par exemple).

e. L'accès non contrôlé aux périphériques de démarrage externes tels que les CD, les DVD et les périphériques USB et l'accès ouvert au système élémentaire d'entrée/sortie (BIOS) sans mot de passe créent des surfaces d'attaques au sein du système des DFS.

[i] Le rapport *Mégadonnées, apprentissage automatique, protection des usagers et confidentialité* souligne les risques et la manière dont les données financières et de télécommunication des usagers peuvent être utilisées de manière abusive.
[ii] Voir *Rapport technique sur les failles du SS7 et les mesures d'atténuation applicables aux transactions des services financiers numériques*, section 12.5, intitulée "Détecter, limiter et empêcher le recyclage de cartes SIM".
[iii] Voir *Rapport technique sur les failles du SS7 et les mesures d'atténuation applicables aux transactions des services financiers numériques*, sections 8 et 9.
[iv] Voir *Rapport technique sur les failles du SS7 et les mesures d'atténuation applicables aux transactions des services financiers numériques*, section 12.1, intitulée "Détecter et limiter les usurpations de compte fondées sur l'interception de mots de passe à usage unique envoyés par SMS".
[v] Voir *Rapport technique sur les failles du SS7 et les mesures d'atténuation applicables aux transactions des services financiers numériques*, section 10, intitulée "Stratégies d'atténuation des risques à destination des opérateurs de réseau mobile".