FIGI

INITIATIVE MONDIALE EN FAVEUR
DE L'INCLUSION FINANCIÈRE

GROUPE DE TRAVAIL SUR LA SÉCURITÉ, L'INFRASTRUCTURE ET LA CONFIANCE

Lignes directrices pour l'audit de sécurité des services financiers numériques

RAPPORT DE TRUST WORKSTREAM

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

Lignes directrices pour l'audit de sécurité des services financiers numériques

03/2021

L'Initiative mondiale en faveur de l'inclusion financière (FIGI) est un programme triennal mis en œuvre dans le cadre d'un partenariat entre le Groupe de la Banque mondiale, le Comité sur les paiements et les infrastructures de marché (CPMI) et l'Union internationale des télécommunications (UIT), et financé par la Fondation Bill & Melinda Gates. Il vise à faciliter et à accélérer l'application de réformes nationales en vue d'atteindre les objectifs nationaux en matière d'inclusion financière et, à terme, l'objectif mondial consistant à garantir un accès universel aux services financiers à l'horizon 2020. La FIGI finance des initiatives dans trois pays – la Chine, l'Égypte et le Mexique – et lutte contre les grands obstacles à l'accès universel aux services financiers à travers le soutien qu'elle apporte aux trois groupes de travail suivants: 1) le Groupe de travail sur l'acceptation des paiements électroniques (dirigé par le Groupe de la Banque mondiale); 2) le Groupe de travail sur l'identité numérique pour les services financiers (dirigé par le Groupe de la Banque mondiale); et 3) le Groupe de travail sur la sécurité, l'infrastructure et la confiance (dirigé par l'UIT). La FIGI organise également trois colloques annuels rassemblant les autorités nationales, le secteur privé et les parties prenantes du secteur public autour de thèmes transversaux, afin de partager les dernières conclusions des groupes de travail et des programmes nationaux.

Le présent rapport a été élaboré par le Groupe de travail de la FIGI sur la sécurité, l'infrastructure et la confiance, dirigé par l'UIT.

Les résultats, interprétations et conclusions exprimés dans ce rapport ne reflètent pas nécessairement les opinions des partenaires de la FIGI, notamment le CPMI, la Fondation Bill & Melinda Gates, l'UIT ou la Banque mondiale (y compris son Conseil d'administration ou les gouvernements qu'elle représente). Les références éventuelles à certaines sociétés ou aux produits de certains fabricants ne signifient pas que l'UIT approuve ou recommande ces sociétés ou ces produits de préférence à d'autres de nature similaire, mais dont il n'est pas fait mention. Sauf erreur ou omission, les noms des produits propriétaires comprennent une lettre majuscule initiale. Les partenaires de la FIGI ne garantissent pas l'exactitude des données figurant dans le présent rapport. Les frontières, couleurs, dénominations et autres informations figurant sur les cartes de ce document n'impliquent aucune prise de position de la part des partenaires de la FIGI concernant le statut juridique d'un pays, d'un territoire, d'une ville ou d'une région ou de ses autorités, ni aucune reconnaissance ou acceptation de ces frontières.

À propos du présent rapport

Ce rapport a été rédigé par Kevin Butler, de l'Université de Floride, ainsi que Vijay Mauree et Arnold Kibuuka, de l'UIT. Les auteurs souhaitent remercier Rehan Masood, de la Banque d'État du Pakistan, pour l'aide et le soutien qu'il a apporté à la relecture et à la révision de ce document. Les auteurs remercient également les membres du Groupe de travail sur la sécurité, l'infrastructure et la confiance pour leurs contributions et leurs remarques.

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

Table des matières

À propos du présent rapport **3**

Acronymes **6**

1 Introduction **7**

2 Lignes directrices pour l'audit de sécurité des services financiers numériques **7**

3 Mesures de contrôle du Cadre de garantie de la sécurité des DFS et lignes directrices pour les audits **10**

4 Liste de vérification pour les audits de sécurité **25**
4.1 Contrôle des accès 25
4.2 Authentification 25
4.3 Disponibilité 26
4.4 Détection des fraudes 26
4.5 Sécurité des réseaux 27
4.6 Confidentialité 28

5 Bibliographie **30**

Acronymes

API	Interface de programmation d'application
DFS	Services financiers numériques
DMZ	Zone démilitarisée
DS	Domaine de sécurité
ICP	Infrastructure à clés publiques
IMEI	Identité internationale d'équipement mobile
IMSI	Identité internationale d'abonnement mobile
MD	Synthèse de message
MFA	Authentification à facteurs multiples
MNO	Opérateur de réseau mobile
MSISDN	Numéro d'annuaire d'abonné international de station mobile
NTP	Protocole de temps réseau
OTP	Mot de passe à usage unique
PDV	Point de vente
RBAC	Contrôle des accès fondé sur les rôles
SE	Élément sécurisé – un circuit intégré officiellement certifié, inviolable et autonome que l'on désigne souvent comme une "puce", selon la définition qu'en donne le Conseil européen des paiements ou d'autres autorités de réglementation reconnues.
SHA	Algorithmes de hachage sécurisé
SIM	Module d'identité de l'abonné
SMS	Service de messages courts
STK	Boîte à outils SIM
USSD	Données de service complémentaire non structurées
XML	Langage de balisage extensible

Lignes directrices pour l'audit de sécurité des services financiers numériques

1 INTRODUCTION

Les lignes directrices pour l'audit de sécurité des services financiers numériques (DFS) ont vocation à compléter le *Cadre de garantie de la sécurité des DFS* [1] pour aider les parties prenantes à identifier d'éventuelles lacunes en matière de contrôle de la sécurité au sein de l'infrastructure du système de DFS. Ces lignes directrices s'appuient sur le *Cadre de garantie de la sécurité des DFS*, qui permet de repérer les menaces et les vulnérabilités grâce à un processus systématique de gestion des risques de sécurité. Le *Cadre de garantie de la sécurité des DFS* propose également des mesures de contrôle de la sécurité à destination des fournisseurs de DFS, des opérateurs de réseau mobile ainsi que d'autres acteurs de l'écosystème.

Lorsqu'elles ne respectent pas l'ensemble de ces mesures de contrôle, les applications de DFS s'exposent à des risques en matière d'atteinte à la vie privée, d'accès aux données DFS, de violation de la confidentialité, d'authentification et d'autorisation des utilisateurs, de disponibilité des DFS, de fraude (interne et externe) et de sécurité du réseau. Les organismes de régulation, les opérateurs et les fournisseurs de DFS peuvent prendre appui sur la liste de vérification pour les audits de sécurité afin de s'assurer de la présence et du bon fonctionnement des mesures de contrôle préconisées dans le *Cadre de garantie de la sécurité des DFS*.

2 LIGNES DIRECTRICES POUR L'AUDIT DE SÉCURITÉ DES SERVICES FINANCIERS NUMÉRIQUES

Les lignes directrices pour l'audit de sécurité des DFS sont réparties en six catégories et permettront aux organismes de régulation, aux auditeurs internes ou externes, aux opérateurs de réseau mobile et aux fournisseurs d'évaluer les mesures de contrôle mises en œuvre pour garantir la sécurité des DFS. Chacune de ces catégories comprend un ensemble de questions qui pourront servir de liste de vérification lors de la réalisation de l'audit de sécurité de l'infrastructure du système de DFS.

Les lignes directrices pour l'audit de sécurité des DFS sont classées selon les catégories suivantes:

i) Contrôle des accès

Les lignes directrices de cette catégorie visent à évaluer les restrictions sélectives mises en œuvre pour vérifier l'accès aux systèmes, aux services, aux ressources et aux mesures de contrôle liées aux DFS, afin de garantir leur protection contre l'exploitation non autorisée des ressources du réseau.

ii) Authentification

Les lignes directrices de cette catégorie visent à évaluer la capacité des applications de DFS à authentifier leurs utilisateurs.

iii) Disponibilité

Les lignes directrices de cette catégorie visent à évaluer la fiabilité des infrastructures et des applications de DFS ainsi que leur capacité à garantir un accès rapide aux utilisateurs autorisés des DFS. Il s'agit notamment de vérifier leur résistance aux attaques par déni de service.

iv) Détection des fraudes

Les lignes directrices de cette catégorie visent à évaluer les mesures de contrôle mises en place au sein des systèmes de DFS pour détecter les tentatives intentionnelles et illégales d'interception provenant d'entités internes ou externes et destinées à obtenir les données personnelles des utilisateurs et à voler leur argent.

v) Sécurité des réseaux

Les lignes directrices de cette catégorie visent à évaluer les mesures de contrôle mises en place pour protéger l'infrastructure des réseaux sous-jacents contre les tentatives d'accès non autorisé, les utilisations abusives, les dysfonctionnements et les phénomènes de modification, de destruction ou de divulgation indue des informations. Elles peuvent également permettre de vérifier que les informations ne circulent qu'entre des terminaux autorisés, sans tentative de détournement ou d'interception.

vi) Confidentialité

Les lignes directrices de cette catégorie visent à évaluer les mesures de contrôle mises en place pour protéger les participants ou les utilisateurs des DFS contre la divulgation non autorisée de leurs données, notamment à travers des processus de protection des données fondés sur l'observation de l'activité du réseau.

Les lignes directrices pour l'audit de sécurité des DFS sont présentées comme suit:

Entité DFS concernée	Catégorie	Risques et vulnérabilités	Mesures de contrôle	Question de vérification de la sécurité	Politique ou procédure applicable

Le tableau ci-dessus indique les risques et les vulnérabilités en matière de sécurité auxquels sont exposés les DFS, ainsi que les entités concernées par ces risques, les mesures de contrôle permettant de les atténuer, les questions que poserait un auditeur chargé de vérifier la sécurité des systèmes ainsi que les politiques et procédures applicables.

- La colonne "*Entité DFS concernée*" présente l'entité confrontée aux risques et aux vulnérabilités au sein de l'écosystème des DFS.
- La colonne "*Risques et vulnérabilités*" présente les menaces auxquelles sont exposées les entités de l'écosystème des DFS dans chacun des huit domaines de sécurité (DS).
- La colonne "Mesures de contrôle" présente les mesures à appliquer pour chacune des entités au sein de l'écosystème des DFS.
- La colonne "*Question de vérification de la sécurité*" présente les questions que peut poser l'auditeur pour vérifier la conformité des mesures de contrôle en question.
- La colonne "*Politique ou procédure applicable*" renvoie aux politiques ou aux procédures à consulter pour orienter au quotidien les actions et les stratégies d'une entité donnée en se fondant sur la norme ISO/IEC 27001 – Management de la sécurité de l'information [2].

Le tableau ci-dessus sera développé dans la section 3 et pourra servir de liste de vérification détaillée pour l'ensemble des mesures de contrôle comprises dans le *Cadre de garantie de la sécurité des DFS*. Il présente les diverses opérations à mener pour vérifier la conformité au niveau du fournisseur de DFS et de l'opérateur de réseau mobile. Ce tableau peut être utilisé par les organismes de régulation des services de télécommunications et des services financiers, par les auditeurs de la sécurité, ainsi que par les fournisseurs de DFS pour orienter leurs activités d'audit de sécurité internes et externes.
La section 4 reprend une partie des questions du tableau 1 et les classe en différentes catégories afin que les auditeurs de la sécurité puissent s'y référer plus facilement et s'en inspirer lors du processus de vérification.

3 MESURES DE CONTRÔLE DU CADRE DE GARANTIE DE LA SÉCURITÉ DES DFS ET LIGNES DIRECTRICES POUR LES AUDITS

Les lignes directrices comprennent une liste de questions de vérification que les auditeurs peuvent poser pour évaluer les mesures de contrôle mises en place en matière de sécurité.

Entité DFS concernée	Catégorie	Risques et vulnérabilités	Mesures de contrôle	Question de vérification de la sécurité	Politique ou procédure applicable
Fournisseur de DFS	Contrôle des accès	– Mesures de contrôle insuffisantes au niveau des sessions utilisateur (DS: contrôle des accès)	C1: 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.	Les sessions utilisateur des applications de DFS sont-elles soumises aux contrôles logiques suivants: i) Déconnexion automatique et délai d'expiration de la session; ii) Nombre maximum de tentatives de connexion infructueuses; iii) Complexité du mot de passe ou du code PIN; iv) Délai d'expiration du mot de passe ou du code PIN?	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications
Fournisseur de DFS	Contrôle des accès	– Mesures de contrôle insuffisantes pour les comptes inactifs (DS: authentification)	C2: Exiger la vérification de l'identité pour les comptes d'utilisateurs de DFS inactifs, avant de procéder à leur réactivation.	La réactivation des comptes inactifs est-elle soumise à des processus de vérification de l'identité suffisants, tels que la vérification biométrique?	Politique de contrôle des accès – Gestion des accès des utilisateurs
Fournisseur de DFS	Contrôle des accès	– Échec de la vérification de la localisation (DS: sécurité des communications)	C3: 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.	Le système de DFS est-il en mesure de détecter des transactions inhabituelles en s'appuyant sur le profil de l'utilisateur? Par exemple: Le fournisseur de DFS a-t-il mis en place une procédure d'authentification des transactions fondée sur la localisation, par exemple grâce à la détection intelligente de la géovélocité?	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications
Fournisseur de DFS	Contrôle des accès	– Vérification incorrecte par l'utilisateur des canaux de communication sélectionnés pour l'accès aux DFS (DS: sécurité des communications)	C4: 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 fournisseur de DFS a-t-il restreint le nombre de connexions concurrentes autorisées et offert aux utilisateurs la possibilité d'opter pour d'autres canaux de connexion? Les utilisateurs qui ont sélectionné les codes d'accès USSD ont-ils la possibilité d'opter pour le recours à une application pendant que le fournisseur de DFS active ce canal, par exemple?	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications
Fournisseur de DFS	Authentification	– Rejeu d'une session par l'interception de jetons (DS: sécurité des communications)	C5: 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.	Le fournisseur de DFS applique-t-il des procédures d'authentification côté serveur pour l'ensemble des tentatives d'accès?	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications
Fournisseur de DFS	Confidentialité	– Faiblesse des algorithmes de chiffrement destinés au stockage des mots de passe (DS: confidentialité des données)	C6: Utiliser des algorithmes de hachage cryptographique salé puissants pour le stockage des mots de passe des utilisateurs des DFS.	Existe-t-il un mécanisme permettant de garantir le chiffrement et la protection des données au repos stockées?	Norme relative à la sécurité et à la prévention des fuites de données
MNO	Contrôle des accès	– Absence de délai d'expiration des sessions pour les DFS	C7: Ajouter un délai d'expiration de session pour le protocole USSD, l'application STK et l'accès Internet aux DFS.	Le fournisseur de DFS a-t-il configuré la déconnexion automatique des sessions USSD et STK après une période d'inactivité déterminée?	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications

(continue)

Entité DFS concernée	Catégorie	Risques et vulnérabilités	Mesures de contrôle	Question de vérification de la sécurité	Politique ou procédure applicable
MNO	Contrôle des accès	– 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).	C8: 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 des identifiants de première connexion à l'application de DFS sont envoyés aux utilisateurs, s'assurer que ces derniers les reçoivent directement, sans l'intervention d'une tierce partie ou d'un agent. Il doit ensuite être demandé aux utilisateurs de changer leur mot de passe après la première connexion.	Le mot de passe est-il indiqué de manière sécurisée? L'utilisateur doit-il modifier son mot de passe après la première connexion?	Politique de contrôle des accès – Gestion des accès des utilisateurs
	Contrôle des accès	– En l'absence d'un suivi des tentatives de connexion, les systèmes sont exposés aux attaques par force brute (DS: contrôle des accès).	C12: 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).	Existe-t-il un nombre maximum de tentatives de connexion au-delà duquel le compte est verrouillé?	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications
MNO	Authentification	– Transmission non sécurisée des identifiants de l'utilisateur (DS: contrôle des accès)	C14: 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 identifiants de connexion aux DFS sont-ils transmis à l'utilisateur par l'intermédiaire d'un canal distinct/hors bande? (Lorsque le compte est configuré par l'intermédiaire d'un canal USSD, par exemple, l'envoi du mot de passe à usage unique se fait-il par courrier électronique ou appel vocal?)	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications
MNO	Sécurité des réseaux	– Exposition du réseau interne à des adversaires externes (DS: contrôle des accès)	C15: 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.	Des mesures de contrôle techniques sont-elles mises en place pour limiter l'exposition des adresses internes des systèmes de DFS (telles que les adresses IP de la base de données)?	Politique de sécurité des communications – Gestion de la sécurité des réseaux
Fournisseur de DFS	Sécurité des réseaux	– Protection insuffisante des systèmes internes contre des adversaires externes (DS: contrôle des accès)	C16: Mettre en place une zone démilitarisée (DMZ) 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.	Des obstacles logiques sont-ils mis en place afin de limiter l'accès aux systèmes de DFS pour tous les autres systèmes? (Sur le réseau, par exemple, les systèmes de traitement des DFS sont-ils protégés par des obstacles logiques et physiques permettant d'interdire l'accès aux utilisateurs internes non autorisés?)	Politique de sécurité des communications – Gestion de la sécurité des réseaux

(continue)

Entité DFS concernée	Catégorie	Risques et vulnérabilités	Mesures de contrôle	Question de vérification de la sécurité	Politique ou procédure applicable
Fournisseur de DFS	Confidentialité	– 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)	C17: 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.	Les bibliothèques cryptographiques utilisées par le système d'exploitation ou par l'application sont-elles à jour et correctement conçues et mises en œuvre? Ces bibliothèques prennent-elles en charge des suites cryptographiques solides et permettent-elles d'empêcher ou de décourager l'utilisation de suites cryptographiques faibles? Les algorithmes de hachage utilisés sont-ils toujours adaptés et prennent-ils en charge des condensés d'une longueur suffisante? (À l'heure actuelle, toute fonction de hachage antérieure à SHA512 est considérée comme obsolète. Les fonctions MD5 et SHA1 ont été compromises.)	Politique de cryptographie – Mesures de contrôle cryptographiques
				Les algorithmes de chiffrement symétrique sont-ils solides et dotés de longueurs de clé suffisantes? (L'attaque SWEET-32, par exemple, a rendu l'algorithme 3-DES obsolète et il est désormais recommandé d'adopter au plus vite la norme AES, considérée comme sûre.) – Dans le cas du chiffrement à clé publique, les longueurs de clé choisies sont-elles adaptées à l'algorithme de chiffrement à clé publique utilisé?	
				Les critères de sélection des algorithmes de chiffrement et des longueurs de clé sont-ils fondés sur des normes publiques et éprouvées? (La publication spéciale du NIST 800-57, par exemple, propose des orientations concernant les longueurs de clé minimales pour chaque algorithme et leur durée de validité.)	
MNO	Confidentialité	– Pratiques insuffisantes en matière de chiffrement ou envoi d'informations sensibles en texte clair par l'intermédiaire de canaux non sécurisés tels que les SMS ou le canal USSD (DS: sécurité des communications)	C18: 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'ensemble des données sensibles des utilisateurs ont-elles été chiffrées par l'application ou le système d'exploitation? La version chiffrée des données est-elle accessible depuis l'appareil, par exemple dans la mémoire ou dans une mémoire tampon temporaire? Toutes les informations sont-elles envoyées par l'intermédiaire d'une connexion réseau dotée d'algorithmes de chiffrement solides (voir C17 pour en savoir plus sur ce qui constitue un algorithme de chiffrement solide)?	Politique de cryptographie – Mesures de contrôle cryptographiques
Fournisseur de DFS et fournisseurs tiers	Détection des fraudes	– Mesures de contrôle insuffisantes en matière de protection des données (DS: confidentialité)	C19: 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.	Les journaux de suivi et d'événements enregistrent-ils et conservent-ils des données sensibles des utilisateurs? (Par exemple, les codes PIN des utilisateurs sont-ils stockés dans des logiciels de type EDR, qui détectent les menaces au niveau des terminaux?)	Politique de sécurité opérationnelle – Journaux d'événements et suivi
Fournisseur de DFS et fournisseurs tiers	Confidentialité	– Exposition d'informations sensibles concernant les utilisateurs pendant les transactions ou l'utilisation d'interfaces de programmation d'application (API) (DS: confidentialité)	C20: Les fournisseurs de DFS doivent restreindre le partage des données des utilisateurs en se limitant aux informations strictement nécessaires aux transactions avec des parties tierces et d'autres fournisseurs de services.	Le partage des données sensibles des utilisateurs pendant le traitement des transactions avec des parties tierces est-il soumis à des limitations? (Par exemple, les parties tierces n'ont accès qu'aux informations strictement nécessaires au traitement des transactions.)	Politique de sécurité opérationnelle – Procédures et responsabilités opérationnelles

(continue)

Entité DFS concernée	Catégorie	Risques et vulnérabilités	Mesures de contrôle	Question de vérification de la sécurité	Politique ou procédure applicable
Fournisseur de DFS et fournisseurs tiers	Détection des fraudes	– Faiblesse du chiffrement des API (DS: confidentialité)	C21: 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.	Les transactions traitées par des API de paiement font-elles l'objet d'un suivi assuré par des mécanismes adéquats?	Politique de sécurité opérationnelle – Journaux d'événements et suivi
				Le fournisseur de DFS a-t-il conclu des accords de non-divulgation des données sensibles de ses utilisateurs avec des parties tierces?	
				Les transferts de données à des parties tierces sont-ils protégés par des algorithmes de chiffrement solides?	
MNO	Disponibilité	– Défaillance du réseau en raison de capacités insuffisantes, d'opérations de maintenance ou d'un défaut de conception (DS: disponibilité)	C22: L'opérateur de réseau mobile (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.	Des systèmes sont-ils mis en place pour garantir la disponibilité des services (la redondance des services, par exemple)?	Gestion des incidents liés à la sécurité des informations – Redondances
				Des mécanismes de suivi sont-ils en place pour mesurer le temps de réponse et le taux d'indisponibilité et générer des rapports en la matière?	
MNO	Disponibilité	– Défaillance du réseau en raison de capacités insuffisantes, d'opérations de maintenance ou d'un défaut de conception (DS: disponibilité)	C23: 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.	Des systèmes sont-ils mis en place pour mesurer la qualité de service et la qualité d'expérience?	Acquisition, développement et maintenance des systèmes d'information – Sécurité des processus de développement et d'assistance technique
				La qualité de service et la qualité d'expérience sont-elles conformes aux normes en vigueur en matière de DFS?	
Fournisseur de DFS	Sécurité des réseaux	– Suivi insuffisant du trafic du réseau et des paquets réseau individuels (DS: disponibilité, sécurité des communications)	C24: 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.	Le réseau est-il suffisamment protégé contre les attaques, par exemple à travers la mise en place de pare-feu et de filtres de trafic correctement configurés?	Politique de sécurité opérationnelle – Protection contre les logiciels malveillants
Fournisseur de DFS	Sécurité des réseaux	– Environnement favorable aux services inutiles (DS: confidentialité des données)	C25: Le trafic Internet entrant doit être limité et faire l'objet d'un suivi constant.	Le trafic des applications de DFS connectées à Internet fait-il l'objet d'un suivi adéquat?	Politique de sécurité opérationnelle – Protection contre les logiciels malveillants
Fournisseur de DFS	Sécurité des réseaux	– Environnement favorable aux services inutiles (DS: confidentialité des données)	C26: 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.	Les règles du pare-feu sont-elles correctement configurées (liste blanche des ports, filtrage de paquets, etc.)?	Politique de sécurité opérationnelle – Protection contre les logiciels malveillants
Fournisseur de DFS	Détection des fraudes	– Les opérations critiques ne font pas l'objet de mesures de contrôle interne suffisantes (DS: contrôle des accès).	C27: 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.	L'examen et l'approbation des modifications importantes apportées aux comptes font-ils l'objet de mesures de contrôle suffisantes? Par exemple, ces modifications sont-elles soumises à un processus de vérification et au principe de la double approbation?	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications

(continue)

Entité DFS concernée	Catégorie	Risques et vulnérabilités	Mesures de contrôle	Question de vérification de la sécurité	Politique ou procédure applicable
Fournisseur de DFS	Détection des fraudes	– Les données d'entrée ne font pas l'objet d'un processus de vérification suffisant (DS: intégrité des données).	C28: 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.	La réalisation d'une tâche critique au sein du système de DFS requiert-elle le concours de plus d'une personne?	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications
Fournisseur de DFS	Contrôle des accès	– Gestion insuffisante des privilèges d'accès (DS: contrôle des accès)	C29: 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 quoi cet individu a accédé, quelle est sa localisation et à quel moment la tentative a eu lieu).	L'accès à l'infrastructure du système de DFS est-il limité par des obstacles physiques et logiques suffisants?	Sécurité physique et environnementale – Zones sécurisées
Fournisseur de DFS	Sécurité des réseaux	– Ajout des données de test aux données de production (DS: intégrité des données)	C30: 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).	Le fournisseur de DFS procède-t-il à la vérification des données d'entrée?	Acquisition, développement et maintenance des systèmes d'information – Sécurité des processus de développement et d'assistance technique
Fournisseur de DFS	Détection des fraudes	– Ajout des données de test aux données de production (DS: intégrité des données)	C31: Utiliser la prise d'empreinte pour détecter toute modification ou falsification des données postérieure à leur stockage.	Des mécanismes sont-ils mis en place pour détecter la modification et la falsification de la base de données?	Politique de sécurité opérationnelle – Journaux d'événements et suivi
Fournisseur de DFS		– Ajout des données de test aux données de production (DS: intégrité des données)	C32: S'assurer que l'ensemble des données de test ont été supprimées du code avant sa migration vers l'environnement de production.	Les données de test et les comptes d'utilisateurs tests ont-ils été supprimés de l'environnement de production?	Acquisition, développement et maintenance des systèmes d'information – Données de test
Fournisseur de DFS	Détection des fraudes	– Absence de suivi, journaux d'événements exposés aux modifications et informations de suivi insuffisantes (DS: non-répudiation)	C33: 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.	Les journaux du système de DFS sont-ils stockés de manière sécurisée dans un module inviolable (un outil de gestion des informations et des événements de sécurité [SIEM], par exemple)?	Politique de sécurité opérationnelle – Journaux d'événements et suivi

(continue)

Entité DFS concernée	Catégorie	Risques et vulnérabilités	Mesures de contrôle	Question de vérification de la sécurité	Politique ou procédure applicable
Fournisseur de DFS	Sécurité des réseaux	– Horloges imprécises et non synchronisées (DS: intégrité des données)	C34: 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.	Toutes les horloges de l'écosystème des DFS sont-elles synchronisées?	Politique de sécurité opérationnelle – Procédures et responsabilités opérationnelles
MNO	Sécurité des réseaux	– Faiblesse du chiffrement « over-the-air » (DS: sécurité des communications)	C38: Cesser d'utiliser les algorithmes de chiffrement GSM A5/0, A5/1 et A5/2. Observer attentivement les résultats obtenus par la communauté en charge des questions de sécurité et de cryptographie afin de déterminer s'il est possible et facile de compromettre les algorithmes de chiffrement A5/3 et A5/4. Parallèlement, commencer à envisager l'utilisation d'algorithmes plus solides et prévoir une stratégie de déploiement.	Les algorithmes de chiffrement connus pour leur faiblesse ont-ils été abandonnés? De nouveaux algorithmes sont-ils prêts à être déployés?	Sécurité des communications: transfert des informations
MNO	Détection des fraudes	– Faiblesse du filtrage par identification des lignes téléphoniques (DS: sécurité des communications)	C39: 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.	Des mécanismes sont-ils mis en place pour détecter les tentatives d'usurpation d'identité par SMS et par téléphone (par exemple, l'identification des lignes téléphoniques)?	Sécurité des communications: transfert des informations
Fournisseur de DFS	Authentification	– Mesures de contrôle manquantes ou inadéquates pour la configuration et les autorisations des comptes (DS: authentification)	C40: 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.	Des procédures d'autorisation et d'authentification supplémentaires sont-elles mises en place pour les transactions importantes et les modifications de compte présentant un risque élevé? Par exemple, quelles vérifications complémentaires sont prévues pour l'augmentation des plafonds de transaction?	Politique de contrôle des accès – Gestion des accès des utilisateurs
Fournisseurs tiers	Confidentialité	– Faiblesse des algorithmes de chiffrement utilisés pour la transmission des données et pour les données stockées sur l'appareil (DS: confidentialité)	C41: 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.	Les données stockées sur l'appareil et les données communiquées aux systèmes internes de DFS sont-elles protégées par des algorithmes de chiffrement solides et des mécanismes de protection de l'intégrité des données tels que l'envoi de codes d'authentification (voir C17 pour en savoir plus sur la solidité des algorithmes de chiffrement)? Des politiques sont-elles mises en place pour garantir la protection des données sensibles et confidentielles des utilisateurs?	Politique de cryptographie – Mesures de contrôle cryptographiques
Fournisseurs tiers	Confidentialité	– Absence de chiffrement des communications (DS: sécurité des communications)	C42: Utiliser la signature numérique pour identifier les parties tierces connectées au système de DFS lorsque des transactions sont en cours.	Le processus de signature numérique est-il utilisé pour identifier les fournisseurs tiers connectés aux systèmes de DFS?	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications
Fournisseurs tiers	Confidentialité	– Gestion insuffisante des certificats et des clés (DS: contrôle des accès)	C43: Utiliser des clés et des certificats fiables et secrets pour permettre l'échange de données entre les fournisseurs de DFS et les parties tierces.	Des procédures sont-elles mises en place pour garantir la fiabilité et la protection des clés privées et secrètes? Les certificats et autres informations cryptographiques sont-ils protégés par les mesures de contrôle du système d'exploitation?	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications

(continue)

Entité DFS concernée	Catégorie	Risques et vulnérabilités	Mesures de contrôle	Question de vérification de la sécurité	Politique ou procédure applicable
Fournisseurs tiers	Disponibilité	– 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)	C44: – 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.	Des politiques sont-elles mises en place pour assurer la gestion du système en cas d'indisponibilité du réseau?	Politique de sécurité opérationnelle – Procédures et responsabilités opérationnelles
Fournisseur de DFS	Authentification	– Contrôle insuffisant et non sécurisé des accès aux comptes d'utilisateurs (DS: contrôle des accès)	C45: Utiliser l'authentification à facteurs multiples ou une combinaison de plusieurs modes d'authentification pour l'accès aux comptes du système de DFS.	La connexion aux comptes du système de DFS est-elle soumise à une procédure d'authentification à facteurs multiples?	Politique de contrôle des accès – Gestion des accès des utilisateurs
	Contrôle des accès	– Pratiques de restauration non testées (DS: disponibilité)	C46: – 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.	Les comptes par défaut sont-ils supprimés du système de DFS et de l'ensemble des systèmes connectés à ceux des DFS?	Politique de contrôle des accès – Gestion des accès des utilisateurs
Fournisseur de DFS	Contrôle des accès	– Pratiques de restauration non testées (DS: disponibilité)	C47: 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 comptes de l'éditeur des DFS et du système d'assistance technique sont-ils désactivés lorsqu'ils n'ont plus aucune tâche à effectuer?	Politique de contrôle des accès – Gestion des accès des utilisateurs
Fournisseur de DFS	Disponibilité	– Mesures de protection des données insuffisantes; par exemple, incapacité à mettre en œuvre l'atomicité des transactions, ouvrant ainsi la voie à des transactions en état d'achèvement partiel (DS: intégrité des données)	C48: 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.	Des tests de bout en bout sont-ils mis en œuvre lorsque les systèmes de DFS font l'objet d'une modification ou d'une mise à niveau? Les tests de bout en bout peuvent notamment inclure des tests de capacité, des tests de sécurité, des tests de la qualité de service, des tests de validation des utilisateurs, etc.	Acquisition, développement et maintenance des systèmes d'information – Sécurité des processus de développement et d'assistance technique
Fournisseur de DFS	Disponibilité	– Mesures de protection des données insuffisantes; par exemple, incapacité à mettre en œuvre l'atomicité des transactions, ouvrant ainsi la voie à des transactions en état d'achèvement partiel (DS: intégrité des données)	C49: Programmer des sauvegardes régulières des systèmes de DFS. Procéder à la vérification régulière des sauvegardes et prévoir un stockage sécurisé, hors ligne et sur un site externe, en adoptant un format chiffré.	Le fournisseur de DFS a-t-il programmé des sauvegardes régulières? Les sauvegardes sont-elles chiffrées et stockées sur un site externe?	Politique de sécurité opérationnelle – Politique de sauvegarde

(continue)

Entité DFS concernée	Catégorie	Risques et vulnérabilités	Mesures de contrôle	Question de vérification de la sécurité	Politique ou procédure applicable
Fournisseur de DFS		– Mesures de protection des données insuffisantes; par exemple, incapacité à mettre en œuvre l'atomicité des transactions, ouvrant ainsi la voie à des transactions en état d'achèvement partiel (DS: intégrité des données)	C50: 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).	Existe-t-il des transactions en attente ou en double au sein du système de DFS? La transaction a-t-elle abouti?	Politique de sécurité opérationnelle – Procédures et responsabilités opérationnelles
Fournisseur tiers	Confidentialité	– Insuffisance des mécanismes destinés à garantir l'intégrité des données et dépendance excessive à l'égard d'ancres de confiance externes (DS: non-répudiation)	C51: 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 (ICP) 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.	Les applications des DFS ou des fournisseurs tiers ont-elles recours à la signature numérique? Les signatures numériques sont-elles protégées par des algorithmes de chiffrement solides et des longueurs de clé suffisantes? La mise en œuvre des algorithmes de chiffrement est-elle sécurisée, actualisée et suffisamment aléatoire? (Les algorithmes de signature numérique les plus solides comprennent notamment les clés RSA, DSA et ECDSA. Les algorithmes de chiffrement sur courbes elliptiques peuvent garantir une sécurité équivalente aux autres algorithmes tout en s'appuyant sur des clés plus courtes.)	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications
MNO	Authentification	– Mesures de contrôle insuffisantes pour l'identification et la vérification de l'utilisateur avant tout échange ou recyclage de carte SIM (DS: authentification)	C52: 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.	Des politiques et des processus sont-ils mis en place pour vérifier l'identité des utilisateurs avant les opérations d'échange de carte SIM? Des mécanismes techniques sont-ils mis en place pour éviter les fuites ou le transfert d'informations avant la confirmation de l'échange de carte SIM?	Politique de contrôle des accès – Gestion des accès des utilisateurs
MNO	Authentification	– Mesures de contrôle insuffisantes pour l'identification et la vérification de l'utilisateur avant tout échange ou recyclage de carte SIM (DS: authentification)	C53: 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 sur son compte avant de pouvoir procéder à un échange ou un remplacement de carte SIM.	Le MNO procède-t-il à l'authentification biométrique de l'utilisateur avant l'échange ou le remplacement d'une carte SIM?	Politique de contrôle des accès – Gestion des accès des utilisateurs
MNO	Authentification	– Mesures de contrôle insuffisantes pour l'identification et la vérification de l'utilisateur avant tout échange ou recyclage de carte SIM (DS: authentification)	C54: 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.	Le fournisseur de DFS est-il en mesure de détecter un échange ou une modification de carte SIM associée à un compte d'utilisateur de DFS?	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications
MNO	Authentification	– Mesures de contrôle insuffisantes pour l'identification et la vérification de l'utilisateur avant tout échange ou recyclage de carte SIM (DS: authentification)	C55: 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).	Les données de carte SIM telles que le numéro IMSI et les valeurs Kc et Ki sont-elles stockées de manière sécurisée par le MNO?	Gestion des actifs – Traitement des différents médias

(continue)

Entité DFS concernée	Catégorie	Risques et vulnérabilités	Mesures de contrôle	Question de vérification de la sécurité	Politique ou procédure applicable
MNO	Authentification	– Mesures de contrôle insuffisantes pour l'identification et la vérification de l'utilisateur avant tout échange ou recyclage de carte SIM (DS: authentification)	C56: 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.	Le fournisseur de DFS est-il impliqué dans le processus de recyclage des cartes SIM des utilisateurs du service?	Gestion des actifs – Traitement des différents médias
	Confidentialité	– Vol d'appareil mobile (DS: confidentialité des données)	C57: 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.	L'application ou le système d'exploitation sous-jacent prennent-ils en charge la suppression à distance des données des DFS ou de l'appareil mobile, et des mécanismes sont-ils mis en place pour assurer le chiffrement des données en cas de perte ou de vol?	Politique de sécurité opérationnelle – Procédures et responsabilités opérationnelles
Fournisseur de DFS	Contrôle des accès	– Processus d'échange et de recyclage de carte SIM[ii] incorrects (DS: intégrité des données)	C58: 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:	Des procédures sont-elles mises en place pour permettre au fournisseur de DFS de détecter les cas suspects d'échange et de recyclage de carte SIM?	Politique de sécurité opérationnelle – Procédures et responsabilités opérationnelles
			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.		
			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.		
Fournisseur de DFS	Détection des fraudes	– Modifications non autorisées de la configuration du système ainsi que des données et des journaux d'événements (DS: intégrité des données)	C59: Protéger le système contre les tentatives de falsification et n'autoriser que les transactions en ligne.	L'application stocke-t-elle les transactions pour une transmission ultérieure?	Politique de sécurité opérationnelle – Procédures et responsabilités opérationnelles
			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	Authentification	– Vérification insuffisante des accès ou des données d'entrée des utilisateurs (DS: authentification)	C60: 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.	Les utilisateurs sont-ils soumis à une procédure d'authentification à facteurs multiples?	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications

(continue)

Entité DFS concernée	Catégorie	Risques et vulnérabilités	Mesures de contrôle	Question de vérification de la sécurité	Politique ou procédure applicable
Fournisseur de DFS	Authentification	– Vérification insuffisante des accès ou des données d'entrée des utilisateurs (DS: authentification)	C61: 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 une vérification de la signature XML.	Le fournisseur de DFS procède-t-il à une vérification de la signature XML des données pour les requêtes issues des API et du canal USSD? Par exemple: validation des données d'entrée, vérification des montants, détection de la présence de caractères spéciaux dans les montants, contrôle des devises, etc.	Sécurité des communications – Transfert d'informations
Fournisseur de DFS	Authentification	– Vérification insuffisante des accès ou des données d'entrée des utilisateurs (DS: authentification)	C62: 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.	Le système de DFS est-il en mesure de détecter des transactions inhabituelles en s'appuyant sur le profil de l'utilisateur? Le fournisseur de DFS procède-t-il à des vérifications fondées sur le profil de transaction de l'utilisateur (par exemple, des agents intelligents procédant à des transactions tardives ou des utilisateurs procédant à des transactions depuis deux endroits différents)?	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications
Fournisseur de DFS	Authentification	– Vérification insuffisante des accès ou des données d'entrée des utilisateurs (DS: authentification)	C63: Quelle que soit la méthode utilisée pour produire les reçus (courriers électroniques, SMS, imprimante reliée au réseau, etc.), le numéro de compte principal (de l'anglais Primary Account Number, ou 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 (de l'anglais Sensitive authentication data, ou SAD).	L'application de DFS stocke-t-elle ou transmet-elle le numéro PAN ou les données SAD en texte clair par SMS ou par courrier électronique?	Gestion des actifs – Traitement des différents médias
MNO	Sécurité des réseaux	– Vulnérabilités SS7 inhérentes [iii] (DS: sécurité des communications)	C70: 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, tant sur le réseau interne qu'au repos, afin de limiter les menaces internes auxquelles elles peuvent être exposées.	Les algorithmes et les clés de chiffrement utilisés sont-ils suffisamment solides pour protéger les codes PIN et les données des utilisateurs?	Cryptographie – Mesures de contrôle cryptographiques
MNO	Sécurité des réseaux	– Vulnérabilités SS7 inhérentes [iii] (DS: sécurité des communications)	C71: Utiliser des pare-feu pour détecter et limiter les attaques exploitant des vulnérabilités SS7.	Le MNO a-t-il mis en place un pare-feu pour détecter et se protéger contre les attaques externes exploitant des vulnérabilités SS7 (par exemple, une protection pare-feu contre l'interception du trafic d'abonné, l'accès USSD non autorisé et l'usurpation de carte SIM)?	Politique de sécurité des communications – Gestion de la sécurité des réseaux
MNO	Contrôle des accès	– Interception des transactions USSD réalisées depuis un terminal mobile (DS: sécurité des communications)	C72: 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 de l'homme du milieu, il est possible de cloner la carte SIM en utilisant un numéro IMEI différent).	Le fournisseur de DFS procède-t-il à la vérification en temps réel de l'appareil de l'utilisateur avant le traitement d'une transaction?	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications
MNO	Sécurité des réseaux	– Absence de protection du trafic sensible et faiblesse des pratiques de chiffrement (DS: sécurité des communications)	C73: 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).	Avant de traiter les transactions, le fournisseur de DFS procède-t-il à des vérifications fondées sur la détection intelligente de la géovélocité?	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications
MNO	Sécurité des réseaux	– Absence de protection du trafic sensible et faiblesse des pratiques de chiffrement (DS: sécurité des communications)	C74: 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.	Le MNO impose-t-il l'usage d'un code PUK sur les cartes SIM afin d'atténuer les risques liés au vol des cartes SIM associées à des comptes de DFS?	Sécurité des communications – Transfert d'informations

(continue)

Entité DFS concernée	Catégorie	Risques et vulnérabilités	Mesures de contrôle	Question de vérification de la sécurité	Politique ou procédure applicable
MNO	Sécurité des réseaux	– Absence de protection du trafic sensible et faiblesse des pratiques de chiffrement (DS: sécurité des communications)	C75: 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.	Le MNO a-t-il mis en place des mesures de contrôle pour limiter l'accès au suivi MAP et l'usage des analyseurs de protocole sur le réseau interne? (Dans le protocole MAP, les messages SMS et USSD sont transmis en texte clair.)	Politique de contrôle des accès – Gestion des accès des utilisateurs
MNO	Sécurité des réseaux	– Absence de protection du trafic sensible et faiblesse des pratiques de chiffrement (DS: sécurité des communications)	C76: Vérifier la légitimité de la transaction grâce à une procédure d'approbation bidirectionnelle avec envoi d'un mot de passe à usage unique au numéro de téléphone original [iv]	La validation des transactions s'opère-t-elle grâce à l'emploi d'un mot de passe à usage unique?	Politique de contrôle des accès – Gestion des accès des utilisateurs
MNO	Confidentialité	– Absence de protection du trafic sensible et faiblesse des pratiques de chiffrement (DS: sécurité des communications)	C77: 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.	Les algorithmes et les clés de chiffrement utilisés sont-ils suffisamment solides pour protéger les codes PIN et les données des utilisateurs?	Cryptographie – Mesures de contrôle cryptographiques
MNO	Contrôle des accès	– Absence de protection du trafic sensible et faiblesse des pratiques de chiffrement (DS: sécurité des communications)	C78: 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.	Des mesures de contrôle sont-elles mises en place pour empêcher les connexions simultanées à plusieurs canaux?	Politique de contrôle des accès – Contrôle des accès aux systèmes et aux applications
				Le fournisseur de DFS autorise-t-il une seule session d'utilisateur à la fois pour se connecter au réseau de DFS? (Une connexion simultanée à plusieurs canaux peut indiquer une faille de sécurité.)	
MNO	Sécurité des réseaux	– Absence de protection du trafic sensible et faiblesse des pratiques de chiffrement (DS: sécurité des communications)	C79: L'opérateur de réseau mobile doit déployer le protocole SS7 et les contrôleurs de signalisation de diamètre recommandés par la GSM Association (FS.11, FS.07, IR.82, and IR.88) afin de limiter les menaces liées à des attaques SS7 [3].	Le MNO a-t-il mis en place le protocole SS7 et les contrôleurs de signalisation de diamètre afin de limiter les menaces liées à des attaques SS7?	Politique de sécurité des communications – Gestion de la sécurité des réseaux
Fournisseur de DFS	Confidentialité	– Protection insuffisante des données d'inscription des utilisateurs des DFS (DS: authentification)	C80: 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.	Les données et les formulaires d'inscription des utilisateurs des DFS sont-ils stockés et transmis de manière sécurisée, et protégés contre les fuites de données grâce au contrôle d'accès basé sur les rôles (RBAC), au chiffrement des données, etc.?	Gestion des actifs – Traitement des différents médias
Fournisseur de DFS	Sécurité des réseaux	– Faiblesse du chiffrement (DS: sécurité des communications)	C81: Appliquer des normes de chiffrement solides aux communications avec les API, telles que le protocole TLS v1.2 et normes supérieures.	Le protocole de chiffrement TLS utilisé est-il suffisamment sûr (v1.2 ou supérieures en juillet 2020)?	Sécurité des communications – Transfert d'informations
				L'application utilise-t-elle les dernières versions du protocole TLS?	
				L'application utilise-t-elle une version obsolète du protocole TLS?	
Fournisseur de DFS	Sécurité des réseaux	– Contrôle et suivi insuffisants de l'accès des utilisateurs au système de DFS (DS: contrôle des accès)	C82: Élargir les processus de détection des menaces afin d'inclure de manière explicite les menaces liées aux API.	Des mesures de contrôle opérationnelles sont-elles mises en place pour détecter les menaces liées aux API?	Politique de sécurité opérationnelle – Gestion des vulnérabilités techniques
				Des mesures de contrôle opérationnelles sont-elles mises en place pour détecter les applications dangereuses ou malveillantes?	
Fournisseur de DFS	Contrôle des accès	– Contrôle et suivi insuffisants de l'accès des utilisateurs au système de DFS (DS: contrôle des accès)	C83: Limiter l'accès à la connexion à distance et limiter les privilèges des sessions à distance pour l'accès aux systèmes internes de DFS.	Des mesures de contrôle sont-elles mises en place pour limiter l'accès aux systèmes de DFS, en particulier pour les utilisateurs qui ont recours à une connexion à distance?	Politique de contrôle des accès – Gestion des accès des utilisateurs
Fournisseur de DFS	Confidentialité	– Contrôle et suivi insuffisants de l'accès des utilisateurs au système de DFS (DS: contrôle des accès)	C84: Limiter la durée de vie des certificats TLS à 825 jours.	Le certificat TLS est-il encore valide (il ne doit pas dater de plus de 825 jours)?	Politique de sécurité des communications – Gestion de la sécurité des réseaux

(continue)

Entité DFS concernée	Catégorie	Risques et vulnérabilités	Mesures de contrôle	Question de vérification de la sécurité	Politique ou procédure applicable
Fournisseur de DFS	Authentification	– Contrôle et suivi insuffisants de l'accès des utilisateurs au système de DFS (DS: contrôle des accès)	C85: 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.	Des mesures de contrôle sont-elles mises en place pour authentifier les utilisateurs bénéficiant de privilèges d'accès (par exemple, grâce à la vérification de l'adresse IP et de l'horaire de connexion)?	Politique de contrôle des accès – Gestion des accès des utilisateurs
Fournisseur de DFS	Sécurité des réseaux	– Contrôle et suivi insuffisants de l'accès des utilisateurs au système de DFS (DS: contrôle des accès)	C86: 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.	Les modifications du code sont-elles testées et approuvées avant d'entrer dans l'environnement de production (par exemple, avec l'émission de certificats prouvant que des tests d'acceptation utilisateur et des tests d'acceptation interne ont été menés)?	Acquisition, développement et maintenance des systèmes d'information – Sécurité des processus de développement et d'assistance technique
Fournisseur de DFS	Sécurité des réseaux	– Contrôle et suivi insuffisants de l'accès des utilisateurs au système de DFS (DS: contrôle des accès)	C87: 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.	Le fournisseur de DFS a-t-il mis en place un mécanisme permettant de stocker les clés cryptographiques de manière sécurisée?	Cryptographie – Mesures de contrôle cryptographiques
Fournisseur de DFS	Contrôle des accès	– Contrôle et suivi insuffisants de l'accès des utilisateurs au système de DFS (DS: contrôle des accès)	C88: Définir des rôles d'utilisateur afin de fixer des droits d'accès en s'appuyant sur le principe du moindre privilège.	Le fournisseur de DFS propose-t-il des mesures de contrôle des accès fondé sur les rôles?	Politique de contrôle des accès – Gestion des accès des utilisateurs
Fournisseur de DFS	Contrôle des accès	– Contrôle et suivi insuffisants de l'accès des utilisateurs au système de DFS (DS: contrôle des accès)	C89: Après le départ ou la résiliation d'un utilisateur, d'un agent ou d'un commerçant, les fournisseurs de services de paiement et les tiers doivent désactiver le compte correspondant.	Les identifiants de connexion des administrateurs, des agents et des utilisateurs qui ont quitté ou résilié le DFS sont-ils désactivés? Les comptes enregistrés sur le système de DFS sont-ils désactivés après une période d'inactivité?	Politique de contrôle des accès – Gestion des accès des utilisateurs
Fournisseur de DFS	Contrôle des accès	– Contrôle et suivi insuffisants de l'accès des utilisateurs au système de DFS (DS: contrôle des accès)	C90: Fixer un délai d'inactivité au-delà duquel les comptes seront désactivés.	Le fournisseur de DFS a-t-il prévu la désactivation des comptes d'administrateur après une période d'inactivité déterminée? Tous les comptes inactifs du personnel interne et des API sont-ils désactivés?	Politique de contrôle des accès – Gestion des accès des utilisateurs
Fournisseur de DFS	Détection des fraudes	– Contrôle et suivi insuffisants de l'accès des utilisateurs au système de DFS (DS: contrôle des accès)	C91: 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).	Le fournisseur de DFS a-t-il recours à des mesures de contrôle des accès fondé sur les rôles?	Politique de contrôle des accès – Gestion des accès des utilisateurs
Fournisseur de DFS	Détection des fraudes	– Contrôle et suivi insuffisants de l'accès des utilisateurs au système de DFS (DS: contrôle des accès)	C92: 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.	Un mécanisme est-il mis en place pour examiner les privilèges administratifs?	Politique de contrôle des accès – Gestion des accès des utilisateurs
Fournisseur de DFS	Confidentialité	– Contrôle et suivi insuffisants de l'accès des utilisateurs au système de DFS (DS: contrôle des accès)	C93: Surveiller l'utilisation des API et crypter 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.	Existe-t-il un mécanisme permettant d'assurer le suivi des données partagées par l'intermédiaire des API? Existe-t-il des mesures de contrôle permettant de prévenir les fuites de données?	Politique de sécurité des communications – Gestion de la sécurité des réseaux

(continue)

Entité DFS concernée	Catégorie	Risques et vulnérabilités	Mesures de contrôle	Question de vérification de la sécurité	Politique ou procédure applicable
Fournisseur de DFS	Sécurité des réseaux	– Surveillance insuffisante du réseau hertzien (DS: confidentialité des données)	C94: 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:	Les clés de chiffrement installées par défaut sont-elles modifiées avant leur application? Les chaînes de communauté SNMP installées par défaut sont-elles modifiées avant leur application?	Politique de sécurité des communications – Gestion de la sécurité des réseaux
			– 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.		
			– 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	Confidentialité	– Les données ne sont pas détruites ou effacées lorsqu'un appareil est mis au rebut (DS: confidentialité)	C95: Les fournisseurs de DFS 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:	La procédure de suppression des données liées aux DFS s'appuie-t-elle sur des instructions de sécurité?	Politique de sécurité opérationnelle – Protection contre les logiciels malveillants
			– 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.		
Fournisseur tiers, fournisseur de DFS	Sécurité des réseaux	– Collaboration insuffisante avec le fournisseur concernant la sécurité des appareils mobiles achetés (DS: disponibilité et confidentialité)	C99: Les commerçants et les fournisseurs de DFS doivent poser les questions suivantes à leur fournisseur:	Existe-t-il des procédures pour assurer le suivi des mises à jour logicielles et ces mises à jour ~~sont-elles~~ installées de manière sécurisée?	Politique de sécurité opérationnelle – Gestion des vulnérabilités techniques
			– 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.		

(continue)

Entité DFS concernée	Catégorie	Risques et vulnérabilités	Mesures de contrôle	Question de vérification de la sécurité	Politique ou procédure applicable
Fournisseur tiers, fournisseur de DFS	Détection des fraudes	– Vulnérabilités non détectées dans les applications du système (DS: confidentialité des données)	C100: 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 de système pour détecter d'éventuelles activités suspectes. En cas d'activité suspecte supposée ou avérée, interrompre l'accès à l'appareil mobile et à son application de paiement en attendant 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.	Les journaux d'audit offrent-ils un suivi suffisant de l'ensemble des modifications apportées au système de DFS ou du MNO et ayant un impact sur les DFS?	Politique de sécurité opérationnelle – Gestion des vulnérabilités techniques
Fournisseur tiers, fournisseur de DFS	Sécurité des réseaux	– Exposition du réseau aux attaques extérieures (DS: disponibilité)	C101: 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.	Les systèmes de DFS sont-ils soumis à des tests d'intrusion réguliers?	Politique de sécurité opérationnelle – Gestion des vulnérabilités techniques
MNO	Disponibilité	– Exposition du réseau aux attaques extérieures (DS: disponibilité)	C107: 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.	Les systèmes de DFS font-ils régulièrement l'objet d'analyses de vulnérabilité?	Politique de sécurité opérationnelle – Gestion des vulnérabilités techniques
MNO	Sécurité des réseaux	– Exposition du réseau aux attaques extérieures (DS: disponibilité)	C108: 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.	Les versions les plus récentes des systèmes de DFS sont-elles installées pour assurer la protection contre les dernières menaces?	Politique de sécurité opérationnelle – Protection contre les logiciels malveillants
MNO, fournisseurs de DFS et fournisseurs tiers	Sécurité des réseaux	– Découverte de nouveaux exploits contre les systèmes existants et incapacité à déployer des solutions pour combattre ces exploits (DS: confidentialité des données, contrôle des accès, disponibilité)	C109: 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.	Les systèmes de DFS sont-ils protégés par des correctifs contre les vulnérabilités connues?	Politique de sécurité opérationnelle – Gestion des vulnérabilités techniques
MNO, fournisseurs de DFS et fournisseurs tiers	Contrôle des accès	– Découverte de nouveaux exploits contre les systèmes existants et incapacité à déployer des solutions pour combattre ces exploits (DS: confidentialité des données, contrôle des accès, disponibilité)	C110: 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 remédiation en cas d'attaque de type zero-day. Cette stratégie repose notamment sur un usage avisé des procédures de sauvegarde.	Des politiques et des processus sont-ils mis en place pour assurer la gestion des nouvelles menaces et attaques à l'encontre des systèmes de DFS?	Politique de sécurité opérationnelle – Gestion des vulnérabilités techniques

(continue)

Entité DFS concernée	Catégorie	Risques et vulnérabilités	Mesures de contrôle	Question de vérification de la sécurité	Politique ou procédure applicable
MNO	Sécurité des réseaux	– Connexion d'appareils non sécurisés à l'infrastructure des DFS (DS: intégrité des données)	C111: 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.	L'ensemble des appareils utilisés pour se connecter aux systèmes de DFS font-ils l'objet d'une analyse des menaces et d'une vérification des derniers correctifs logiciels?	Politique de sécurité opérationnelle – Gestion des vulnérabilités techniques
	Authentification	– Accès trop permissif à l'infrastructure des DFS (DS: authentification)	C115: 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.	Le fournisseur de DFS procède-t-il à la vérification de l'IMSI pour les numéros de téléphone associés à des transactions effectuées sur le DFS, afin de se prémunir contre les échanges de carte SIM?	Politique de contrôle des accès – Gestion des accès des utilisateurs
Fournisseur tiers	Détection des fraudes	– Processus de vérification des transactions insuffisant (DS: non-répudiation)	C116: 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.	Les utilisateurs de DFS reçoivent-ils une alerte lorsqu'une transaction est réalisée sur leur compte?	Politique de contrôle des accès – Gestion des accès des utilisateurs
Fournisseur de DFS	Confidentialité	– Les environnements de test ne font pas l'objet d'une supervision et de mesures de contrôle adéquates (DS: confidentialité)	C117: Les fournisseurs de DFS doivent 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 tests ne doivent pas migrer vers l'environnement de production.	Les données associées aux environnements de test et à l'environnement de production font-elles l'objet d'une séparation nette? Existe-t-il des processus permettant de limiter l'exploitation des données des utilisateurs à des fins de test? Par exemple, l'anonymisation des données.	Gestion des actifs – Traitement des différents médias
Fournisseur tiers	Confidentialité	– Exposition d'informations sensibles concernant les utilisateurs pendant les transactions ou l'utilisation des API (DS: confidentialité)	C118: 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.	Des processus sont-ils mis en place pour limiter le partage de données avec des tiers lorsqu'une transaction est en cours?	Gestion des actifs – Traitement des différents médias
Fournisseur tiers	Confidentialité	– Mesures de contrôle insuffisantes en matière de protection des données (DS: confidentialité)	C119: 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, remplacez ces données par des caractères de remplissage dans les journaux.	Les données sensibles des utilisateurs, telles que les codes PIN, sont-elles susceptibles d'apparaître dans les journaux d'événements?	Politique de sécurité opérationnelle – Journaux d'événements et suivi

Le tableau de vérification ci-dessus [4] peut être téléchargé (en version anglaise) au format Excel à l'adresse suivante: https://itu.int/en/ITU-T/extcoop/figisymposium/Documents/Digital%20Financial%20Services%20security%20audit%20checklist.xlsm

4 LISTE DE VÉRIFICATION POUR LES AUDITS DE SÉCURITÉ

4.1 Contrôle des accès

4.1.1 Les identifiants de connexion des administrateurs, des agents et des utilisateurs qui ont quitté ou résilié le DFS sont-ils désactivés? Les comptes enregistrés sur le système de DFS sont-ils désactivés après une période d'inactivité?

4.1.2 Les comptes par défaut sont-ils supprimés du système de DFS et de l'ensemble des systèmes connectés à ceux des DFS?

4.1.3 Les comptes de l'éditeur des DFS et du système d'assistance technique sont-ils désactivés lorsqu'ils n'ont plus aucune tâche à effectuer?

4.1.4 Les sessions utilisateur des applications de DFS sont-elles soumises aux contrôles logiques suivants: i) déconnexion automatique et délai d'expiration de la session; ii) nombre maximum de tentatives de connexion infructueuses; iii) complexité du mot de passe ou du code PIN; iv) délai d'expiration du mot de passe ou du code PIN?

4.1.5 Des procédures sont-elles mises en place pour permettre au fournisseur de DFS de détecter les cas suspects d'échange et de recyclage de carte SIM?

4.1.6 Des mesures de contrôle sont-elles mises en place pour empêcher les connexions simultanées à plusieurs canaux? Le fournisseur de DFS autorise-t-il une seule session d'utilisateur à la fois pour se connecter au réseau de DFS? (Une connexion simultanée à plusieurs canaux peut indiquer une faille de sécurité.)

4.1.7 Des mesures de contrôle sont-elles mises en place pour limiter l'accès aux systèmes de DFS, en particulier pour les utilisateurs qui ont recours à une connexion à distance?

4.1.8 Des politiques et des processus sont-ils mis en place pour assurer la gestion des nouvelles menaces et attaques à l'encontre des systèmes de DFS?

4.1.9 L'accès à l'infrastructure du système de DFS est-il limité par des obstacles physiques et logiques suffisants?

4.1.10 Le fournisseur de DFS propose-t-il des mesures de contrôle des accès fondé sur les rôles?

4.1.11 Le système de DFS est-il en mesure de détecter des transactions inhabituelles en s'appuyant sur le profil de l'utilisateur? Par exemple: Le fournisseur de DFS a-t-il mis en place une procédure d'authentification des transactions fondée sur la localisation, par exemple grâce à la détection intelligente de la géovélocité?

4.1.12 Le fournisseur de DFS a-t-il restreint le nombre de connexions concurrentes autorisées et offert aux utilisateurs la possibilité d'opter pour d'autres canaux de connexion? Les utilisateurs qui ont sélectionné l'accès USSD ont-ils la possibilité d'opter pour le recours à une application pendant que le fournisseur de DFS active ce canal, par exemple?

4.1.13 Le fournisseur de DFS a-t-il prévu la désactivation des comptes d'administrateur après une période d'inactivité déterminée? Tous les comptes inactifs du personnel interne et des API sont-ils désactivés?

4.1.14 Le fournisseur de DFS a-t-il configuré la déconnexion automatique des sessions USSD et STK après une période d'inactivité déterminée?

4.1.15 Le fournisseur de DFS procède-t-il à la vérification en temps réel de l'appareil de l'utilisateur avant le traitement d'une transaction?

4.1.16 Le mot de passe est-il indiqué de manière sécurisée? L'utilisateur doit-il modifier son mot de passe après la première connexion?

4.1.17 Existe-t-il un nombre maximum de tentatives de connexion au-delà duquel le compte est verrouillé?

4.1.18 La réactivation des comptes inactifs est-elle soumise à des processus de vérification de l'identité suffisants, tels que la vérification biométrique?

4.2 Authentification

4.2.1 Des politiques et des processus sont-ils mis en place pour vérifier l'identité des utilisateurs avant les opérations d'échange de carte SIM? Des mécanismes techniques sont-ils mis en place pour éviter les fuites ou le transfert d'informations avant la confirmation de l'échange de carte SIM?

4.2.2 Les identifiants de connexion aux DFS sont-ils transmis à l'utilisateur par l'intermédiaire d'un canal distinct/hors bande? (Lorsque le compte est configuré par l'intermédiaire d'un canal USSD, par exemple, l'envoi du mot de passe à usage unique se fait-il par courrier électronique ou appel vocal?)

4.2.3 Des mesures de contrôle sont-elles mises en place pour authentifier les utilisateurs bénéficiant de privilèges d'accès (par exemple, grâce à la vérification de l'adresse IP et de l'horaire de connexion)?

4.2.4 L'application de DFS stocke-t-elle ou transmet-elle le numéro PAN ou les données SAD en texte clair par SMS ou par courrier électronique?
4.2.5 Le fournisseur de DFS applique-t-il des procédures d'authentification côté serveur pour l'ensemble des tentatives d'accès?
4.2.6 Le MNO procède-t-il à l'authentification biométrique de l'utilisateur avant l'échange ou le remplacement d'une carte SIM?
4.2.7 Les données de carte SIM telles que le numéro IMSI et les valeurs Kc et Ki sont-elles stockées de manière sécurisée par le MNO?
4.2.8 Les utilisateurs sont-ils soumis à une procédure d'authentification à facteurs multiples?
4.2.9 La connexion aux comptes du système de DFS est-elle soumise à une procédure d'authentification à facteurs multiples?
4.2.10 Le fournisseur de DFS est-il en mesure de détecter un échange ou une modification de carte SIM associée à un compte d'utilisateur de DFS?
4.2.11 Le fournisseur de DFS procède-t-il à la vérification de l'IMSI pour les numéros de téléphone associés à des transactions effectuées sur le DFS, afin de se prémunir contre les échanges de carte SIM?
4.2.12 Le fournisseur de DFS est-il impliqué dans le processus de recyclage des cartes SIM des utilisateurs du service?
4.2.13 Le fournisseur de DFS procède-t-il à une vérification de la signature XML des données pour les requêtes issues des API et du canal USSD? Par exemple: validation des données d'entrée, vérification des montants, détection de la présence de caractères spéciaux dans les montants, contrôle des devises, etc.
4.2.14 Des procédures d'autorisation et d'authentification supplémentaires sont-elles mises en place pour les transactions importantes et les modifications de compte présentant un risque élevé? Par exemple, quelles vérifications complémentaires sont prévues pour l'augmentation des plafonds de transaction?
4.2.15 Le système de DFS est-il en mesure de détecter des transactions inhabituelles en s'appuyant sur le profil de l'utilisateur? Le fournisseur de DFS procède-t-il à des vérifications fondées sur le profil de transaction de l'utilisateur (par exemple, des agents intelligents procédant à des transactions tardives ou des utilisateurs procédant à des transactions depuis deux endroits différents)?

4.3 Disponibilité
4.3.1 Des politiques sont-elles mises en place pour assurer la gestion du système en cas d'indisponibilité du réseau?
4.3.2 Des tests de bout en bout sont-ils mis en œuvre lorsque les systèmes de DFS font l'objet d'une modification ou d'une mise à niveau? Les tests de bout en bout peuvent notamment inclure des tests de capacité, des tests de sécurité, des tests de la qualité de service, des tests de validation des utilisateurs, etc.
4.3.3 Les systèmes de DFS font-ils régulièrement l'objet d'analyses de vulnérabilité?
4.3.4 Des systèmes sont-ils mis en place pour garantir la disponibilité des services (la redondance des services, par exemple)? Des rapports et des services ont-ils été mis en place pour mesurer le temps de réponse et le taux d'indisponibilité?
4.3.5 Des systèmes sont-ils mis en place pour mesurer la qualité de service et la qualité d'expérience? La qualité de service et la qualité d'expérience sont-elles conformes aux normes en vigueur en matière de DFS?
4.3.6 Le fournisseur de DFS a-t-il programmé des sauvegardes régulières? Les sauvegardes sont-elles chiffrées et stockées sur un site externe?

4.4 Détection des fraudes
4.4.1 Les journaux des DFS sont-ils stockés de manière sécurisée dans un module inviolable (un SIEM, par exemple)?
4.4.2 Des mécanismes sont-ils mis en place pour détecter la modification et la falsification de la base de données?
4.4.3 Des mécanismes sont-ils mis en place pour détecter les tentatives d'usurpation d'identité par SMS et par téléphone (par exemple, l'identification des lignes téléphoniques)?
4.4.4 L'examen et l'approbation des modifications importantes apportées aux comptes font-ils l'objet de mesures de contrôle suffisantes? Par exemple, ces modifications sont-elles soumises à un processus de vérification et au principe de la double approbation?
4.4.5 Les transactions traitées par des API de paiement font-elles l'objet d'un suivi assuré par des mécanismes adéquats? Le fournisseur de DFS a-t-il conclu des accords de non-divulgation des données sensibles de ses utilisateurs avec des parties tierces? Les transferts de données à des parties tierces sont-ils protégés par des algorithmes de chiffrement solides?

4.4.6 Les journaux d'audit offrent-ils un suivi suffisant de l'ensemble des modifications apportées au système de DFS ou du MNO et ayant un impact sur les DFS?
4.4.7 Les utilisateurs de DFS reçoivent-ils une alerte lorsqu'une transaction est réalisée sur leur compte?
4.4.8 Les journaux de suivi et d'événements enregistrent-ils et conservent-ils des données sensibles des utilisateurs? (Par exemple, les codes PIN des utilisateurs sont-ils stockés dans des logiciels de type EDR, qui détectent les menaces au niveau des terminaux?)
4.4.9 L'application stocke-t-elle les transactions pour une transmission ultérieure?
4.4.10 Le fournisseur de DFS a-t-il recours à des mesures de contrôle des accès fondé sur les rôles?
4.4.11 Un mécanisme est-il mis en place pour examiner les privilèges administratifs?
4.4.12 La réalisation d'une tâche critique au sein du système de DFS requiert-elle le concours de plus d'une personne?

4.5 Sécurité des réseaux
4.5.1 L'ensemble des appareils utilisés pour se connecter aux systèmes de DFS font-ils l'objet d'une analyse des menaces et d'une vérification des derniers correctifs logiciels?
4.5.2 Les modifications du code sont-elles testées et approuvées avant d'entrer dans l'environnement de production (par exemple, avec l'émission de certificats prouvant que des tests d'acceptation utilisateur et des tests d'acceptation interne ont été menés)?
4.5.3 Les clés de chiffrement installées par défaut sont-elles modifiées avant leur application? Les chaînes de communauté SNMP installées par défaut sont-elles modifiées avant leur application?
4.5.4 Toutes les horloges de l'écosystème des DFS sont-elles synchronisées?
4.5.5 Les systèmes de DFS sont-ils protégés par des correctifs contre les vulnérabilités connues?
4.5.6 Les versions les plus récentes des systèmes de DFS sont-elles installées pour assurer la protection contre les dernières menaces?
4.5.7 Les algorithmes et les clés de chiffrement utilisés sont-ils suffisamment solides pour protéger les codes PIN et les données des utilisateurs?
4.5.8 Les règles du pare-feu sont-elles correctement configurées (liste blanche des ports, filtrage de paquets, etc.)?
4.5.9 Le réseau est-il suffisamment protégé contre les attaques, par exemple à travers la mise en place de pare-feu et de filtres de trafic correctement configurés?
4.5.10 Des obstacles logiques sont-ils mis en place afin de limiter l'accès aux systèmes de DFS pour tous les autres systèmes? (Sur le réseau, par exemple, les systèmes de traitement des DFS sont-ils protégés par des obstacles logiques et physiques permettant d'interdire l'accès aux utilisateurs internes non autorisés?)
4.5.11 Des mesures de contrôle opérationnelles sont-elles mises en place pour détecter les menaces liées aux API? Des mesures de contrôle opérationnelles sont-elles mises en place pour détecter les applications dangereuses ou malveillantes?
4.5.12 Existe-t-il des transactions en attente ou en double au sein du système de DFS? La transaction a-t-elle abouti?
4.5.13 Existe-t-il des procédures pour assurer le suivi des mises à jour logicielles et ces mises à jour sont-elles installées de manière sécurisée?
4.5.14 Des mesures de contrôle techniques sont-elles mises en place pour limiter l'exposition des adresses internes des systèmes de DFS (telles que les adresses IP de la base de données)?
4.5.15 Le fournisseur de DFS a-t-il mis en place un mécanisme permettant de stocker les clés cryptographiques de manière sécurisée?
4.5.16 Le MNO impose-t-il l'usage d'un code PUK sur les cartes SIM afin d'atténuer les risques liés au vol des cartes SIM associées à des comptes de DFS?
4.5.17 Le MNO a-t-il mis en place un pare-feu pour détecter et se protéger contre les attaques externes exploitant des vulnérabilités SS7 (par exemple, une protection pare-feu contre l'interception du trafic d'abonné, l'accès USSD non autorisé et l'usurpation de carte SIM)?
4.5.18 Le MNO a-t-il mis en place des mesures de contrôle pour limiter l'accès au suivi MAP et l'usage des analyseurs de protocole sur le réseau interne? (Dans le protocole MAP, les messages SMS et USSD sont transmis en texte clair.)
4.5.19 Le MNO a-t-il mis en place le protocole SS7 et les contrôleurs de signalisation de diamètre afin de limiter les menaces liées à des attaques SS7?
4.5.20 Les algorithmes de chiffrement connus pour leur faiblesse ont-ils été abandonnés? De nouveaux algorithmes sont-ils prêts à être déployés?
4.5.21 Le fournisseur de DFS procède-t-il à la vérification des données d'entrée?
4.5.22 Avant de traiter les transactions, le fournisseur de DFS procède-t-il à des vérifications fondées sur la détection intelligente de la géovélocité?

4.5.23 Le trafic des applications de DFS connectées à Internet fait-il l'objet d'un suivi adéquat?
4.5.24 Les systèmes de DFS sont-ils soumis à des tests d'intrusion réguliers?
4.5.25 Le protocole de chiffrement TLS utilisé est-il suffisamment sûr (v1.2 ou supérieures en juillet 2020)? L'application utilise-t-elle les dernières versions du protocole TLS? L'application utilise-t-elle une version obsolète du protocole TLS?
4.5.26 La validation des transactions s'opère-t-elle grâce à l'emploi d'un mot de passe à usage unique?

4.6 Confidentialité

4.6.1 Les applications des DFS ou des fournisseurs tiers ont-elles recours à la signature numérique? Les signatures numériques sont-elles protégées par des algorithmes de chiffrement solides et des longueurs de clé suffisantes? La mise en œuvre des algorithmes de chiffrement est-elle sécurisée, actualisée et suffisamment aléatoire? (Les algorithmes de signature numérique les plus solides comprennent notamment les clés RSA, DSA et ECDSA. Les algorithmes de chiffrement sur courbes elliptiques peuvent garantir une sécurité équivalente aux autres algorithmes tout en s'appuyant sur des clés plus courtes.)
4.6.2 Des procédures sont-elles mises en place pour garantir la fiabilité et la protection des clés privées et secrètes? Les certificats et autres informations cryptographiques sont-ils protégés par les mesures de contrôle du système d'exploitation?
4.6.3 Le processus de signature numérique est-il utilisé pour identifier les fournisseurs tiers connectés aux systèmes de DFS?
4.6.4 Les bibliothèques cryptographiques utilisées par le système d'exploitation ou par l'application sont-elles à jour et correctement conçues et mises en œuvre? Ces bibliothèques prennent-elles en charge des suites cryptographiques solides et permettent-elles d'empêcher ou de décourager l'utilisation de suites cryptographiques faibles? Les algorithmes de hachage utilisés sont-ils toujours adaptés et prennent-ils en charge des condensés d'une longueur suffisante? (À l'heure actuelle, toute fonction de hachage antérieure à SHA512 est considérée comme obsolète. Les fonctions MD5 et SHA1 ont été compromises.) Les algorithmes de chiffrement symétrique sont-ils solides et dotés de longueurs de clé suffisantes? (L'attaque SWEET-32, par exemple, a rendu l'algorithme 3-DES obsolète et il est désormais recommandé d'adopter au plus vite la norme AES, considérée comme sûre.) Dans le cas du chiffrement à clé publique, les longueurs de clé choisies sont-elles adaptées à l'algorithme de chiffrement à clé publique utilisé? Les critères de sélection des algorithmes de chiffrement et des longueurs de clé sont-ils fondés sur des normes publiques et éprouvées? (La publication spéciale du NIST 800-57, par exemple, propose des orientations concernant les longueurs de clé minimales pour chaque algorithme et leur durée de validité.)
4.6.5 Les algorithmes et les clés de chiffrement utilisés sont-ils suffisamment solides pour protéger les codes PIN et les données des utilisateurs?
4.6.6 Des processus sont-ils mis en place pour limiter le partage de données avec des tiers lorsqu'une transaction est en cours?
4.6.7 La procédure de suppression des données liées aux DFS s'appuie-t-elle sur des instructions de sécurité?
4.6.8 Les données sensibles des utilisateurs, telles que les codes PIN, sont-elles susceptibles d'apparaître dans les journaux d'événements?
4.6.9 L'application ou le système d'exploitation sous-jacent prennent-ils en charge la suppression à distance des données des DFS ou de l'appareil mobile, et des mécanismes sont-ils mis en place pour assurer le chiffrement des données en cas de perte ou de vol?
4.6.10 L'ensemble des données sensibles des utilisateurs ont-elles été chiffrées par l'application ou le système d'exploitation? La version chiffrée des données est-elle accessible depuis l'appareil, par exemple dans la mémoire ou dans une mémoire tampon temporaire? Toutes les informations sont-elles envoyées par l'intermédiaire d'une connexion réseau dotée d'algorithmes de chiffrement solides (voir C17 pour en savoir plus sur ce qui constitue un algorithme de chiffrement solide)?
4.6.11 Les données stockées sur l'appareil et les données communiquées aux systèmes internes de DFS sont-elles protégées par des algorithmes de chiffrement solides et des mécanismes de protection de l'intégrité des données tels que l'envoi de codes d'authentification (voir C17 pour en savoir plus sur la solidité des algorithmes de chiffrement)? Des politiques sont-elles mises en place pour garantir la protection des données sensibles et confidentielles des utilisateurs?
4.6.12 Les données de test et les comptes d'utilisateurs tests ont-ils été supprimés de l'environnement de production?
4.6.13 Les données et les formulaires d'inscription des utilisateurs des DFS sont-ils stockés et transmis de manière sécurisée, et protégés contre les fuites de données grâce au contrôle d'accès basé sur les rôles (RBAC), au chiffrement des données, etc.?

4.6.14 Le certificat TLS est-il encore valide (il ne doit pas dater de plus de 825 jours)?

4.6.15 Existe-t-il un mécanisme permettant de garantir le chiffrement et la protection des données au repos stockées?

4.6.16 Existe-t-il un mécanisme permettant d'assurer le suivi des données partagées par l'intermédiaire des API? Existe-t-il des mesures de contrôle permettant de prévenir les fuites de données?

4.6.17 Le partage des données sensibles des utilisateurs pendant le traitement des transactions avec des parties tierces est-il soumis à des limitations? (Par exemple, les parties tierces n'ont accès qu'aux informations strictement nécessaires au traitement des transactions.)

4.6.18 Les données associées aux environnements de test et à l'environnement de production font-elles l'objet d'une séparation nette? Existe-t-il des processus permettant de limiter l'exploitation des données des utilisateurs à des fins de test? Par exemple, l'anonymisation des données.

5 BIBLIOGRAPHIE

[1] Kevin Butler et Vijay Mauree,*Digital Financial Service Security Assurance Framework*, disponible à l'adresse suivante (en anglais): https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/ITU_SIT_WG_Technical%20report%20on%20Digital%20Financial%20Services%20Security%20Assurance%20Framework_f.pdf

[2] "Management de la sécurité de l'information", disponible à l'adresse suivante: https://www.iso.org/fr/isoiec-27001-information-security.html

[3] Assaf Klinger, *SS7 vulnerabilities and mitigation measures for Digital Financial Services transaction*, disponible à l'adresse suivante (en anglais): https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/ITU_SIT_WG_Technical%20report%20on%20the%20SS7%20vulnerabilities%20and%20their%20impact%20on%20DFS%20transactions_f.pdf

[4] "Digital Financial Services audit checklist", disponible à l'adresse suivante (en anglais): https://itu.int/en/ITU-T/extcoop/figisymposium/Documents/Digital%20Financial%20Services%20security%20audit%20checklist.xlsm

Union internationale des télécommunications (UIT)
Place des Nations
1211 Genève 20
Suisse