ITUPublications
Recommandations

Union internationale des télécommunications
Secteur de la normalisation

Recommandation

UIT-T X.1150 (03/2024)

SÉRIE X: Réseaux de données, communication entre systèmes ouverts et sécurité

Applications et services sécurisés (I) – Sécurité des applications (I)

Cadre d'assurance de la sécurité pour les services financiers numériques

RECOMMANDATIONS UIT-T DE LA SÉRIE X

Réseaux de données, communication entre systèmes ouverts et sécurité

RÉSEAUX PUBLICS DE DONNÉES	X.1-X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200-X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300-X.399
SYSTÈMES DE MESSAGERIE	X.400-X.499
ANNUAIRE	X.500-X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600-X.699
GESTION OSI	X.700-X.799
SÉCURITÉ	X.800-X.849
APPLICATIONS OSI	X.850-X.899
TRAITEMENT RÉPARTI OUVERT	X.900-X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	X.1000-X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (I)	X.1100-X.1199
Sécurité en multidiffusion	X.1100-X.1109
Sécurité des réseaux domestiques	X.1110-X.1119
Sécurité des télécommunications mobiles	X.1120-X.1139
Sécurité de la toile (I)	X.1140-X.1149
Sécurité des applications (I)	**X.1150-X.1159**
Sécurité d'homologue à homologue	X.1160-X.1164
Protection des données (I) et sécurité des identificateurs en réseau	X.1165-X.1179
Lutte contre la fraude	X.1180-X.1189
Sécurité de la télévision par réseau IP	X.1190-X.1199
SÉCURITÉ DU CYBERESPACE	X.1200-X.1299
APPLICATIONS ET SERVICES SÉCURISÉS (II)	X.1300-X.1499
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	X.1500-X.1599
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	X.1600-X.1699
COMMUNICATIONS QUANTIQUES	X.1700-X.1729
SÉCURITÉ DES DONNÉES	X.1750-X.1799
SÉCURITÉ DES TÉLÉCOMMUNICATIONS MOBILES INTERNATIONALES (IMT)	X.1800-X.1839
SÉCURITÉ DU MÉTAVERS ET DES JUMEAUX NUMÉRIQUES	X.2000-X.2199
SÉCURITÉ DES CHAÎNES D'APPROVISIONNEMENT DES LOGICIELS	X.2150-X.2199
SÉCURITÉ DE L'INTELLIGENCE ARTIFICIELLE (IA)/DE L'APPRENTISSAGE AUTOMATIQUE (ML)	X.2200-X.2249

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1150

Cadre d'assurance de la sécurité pour les services financiers numériques

Résumé

Les services financiers numériques (SFN) impliquent un écosystème complexe avec la participation de différents acteurs tels que les banques, les fournisseurs de SFN, les opérateurs de réseaux mobiles (ORM), les fournisseurs de plates-formes de SFN, les régulateurs, les agents, les commerçants, les fournisseurs de services de paiement, les fabricants d'appareils, les développeurs d'applications, les fournisseurs de jetons, les fabricants d'équipements d'origine (OEM), et les clients. L'interconnexion de ces entités du système et la dépendance à l'égard de plusieurs parties de l'écosystème étendent les limites de la sécurité au-delà du fournisseur SFN jusqu'aux clients, aux fournisseurs de réseaux, aux fabricants de téléphones mobiles et à d'autres fournisseurs tiers de l'écosystème.

Un cadre d'assurance de la sécurité du SFN définit les menaces et les vulnérabilités en matière de sécurité auxquelles sont confrontées les parties prenantes du SFN. Les régulateurs, y compris les autorités de télécommunication, les régulateurs bancaires et les régulateurs de paiement, pourraient également utiliser le cadre d'assurance de sécurité du SFN pour établir également des lignes de base de sécurité pour les fournisseurs de SFN.

Une fois mis en œuvre, le cadre complétera les pratiques de gestion des risques et de la sécurité de l'information des parties prenantes de l'écosystème DFS. Par exemple, les contrôles de sécurité figurant dans le document peuvent être inclus dans le programme de sécurité des technologies de l'information et de la communication (TIC) du fournisseur de DFS.

La Recommandation UIT-T X.1150 décrit le cadre d'assurance de sécurité des SFN qui fournit un processus systématique de gestion des risques de sécurité pour évaluer les menaces et les vulnérabilités et identifier les contrôles de sécurité appropriés à mettre en œuvre par les parties prenantes des SFN. Les menaces liées aux commerçants, aux prestataires de services de paiement et aux autres organisations de services financiers, ainsi que les mesures spécifiques d'atténuation des menaces auxquelles ils sont confrontés, n'entrent pas dans le champ d'application de la présente Recommandation.

Le cadre d'assurance de la sécurité des SFN se compose des éléments suivants:

a) Un processus de gestion des risques de sécurité basé sur la norme ISO/IEC 27005.

b) Évaluation des menaces et des vulnérabilités de l'infrastructure sous-jacente de l'opérateur de réseau mobile et du fournisseur de SFN, des applications SFN, des services, des opérations de réseau et des fournisseurs tiers impliqués dans l'écosystème de fourniture de SFN.

c) Stratégies d'atténuation basées sur les résultats du point b) ci-dessus. Les mesures d'atténuation recensent 119 exigences de contrôles de sécurité pour les menaces de sécurité qui sont décrites dans le paragraphe 13.

Historique*

Édition	Recommandation	Approbation	Commission d'études	ID Unique
1.0	UIT-T X.1150	01-03-2024	17	11.1002/1000/15706

Mots clés

Modèle d'entreprise, contrôles, services financiers numériques, assurance de la sécurité, menaces.

* Pour accéder à la Recommandation, reporter cet URL https://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique.

AVANT-PROPOS

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

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

À la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1150

Cadre d'assurance de la sécurité pour les services financiers numériques

1 Domaine d'application

La présente Recommandation fournit le cadre d'assurance de la sécurité pour les services financiers numériques (SFN). Elle précise également un processus systématique de gestion des risques de sécurité visant à identifier et évaluer les menaces et les vulnérabilités et identifie les contrôles de sécurité appropriés pour remédier aux vulnérabilités et atténuer les risques, qui doivent être mis en œuvre par le fournisseur de services de dématérialisation et l'opérateur de réseau mobile. Elle peut être utilisée pour mettre en œuvre des contrôles de sécurité afin de protéger l'utilisateur, l'appareil mobile, l'opérateur de réseau mobile et le fournisseur SFN.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

[UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

[UIT-T X.805] Recommandation UIT-T X.805 (2003), *Architecture de sécurité pour les systèmes assurant des communications de bout en bout*.

[ISO/IEC 27005] ISO/IEC 27005:2022, *Sécurité de l'information, cybersécurité et protection de la vie privée – Préconisations pour la gestion des risques liés à la sécurité de l'information*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 contrôle d'accès [UIT-T X.800]: précaution prise contre l'utilisation non autorisée d'une ressource; cela comprend les précautions prises contre l'utilisation d'une ressource de façon non autorisée.

3.1.2 authentification [UIT-T X.800]: voir authentification de l'origine des données et authentification de l'entité homologue.

NOTE – Dans la présente Recommandation, le terme "authentification" n'est pas utilisé en relation avec l'intégrité des données; le terme "intégrité des données" est utilisé à la place.

3.1.3 autorisation [UIT-T X.800]: l'octroi de droits, qui comprend l'octroi d'un accès sur la base de droits d'accès.

3.1.4 disponibilité [UIT-T X.800]: propriété qui consiste à être accessible et utilisable à la demande d'une entité autorisée.

3.1.5 confidentialité [UIT-T X.800]: propriété selon laquelle l'information n'est pas mise à disposition ou divulguée à des personnes, entités ou processus non autorisés.

3.1.6 contrôle [b-ISO/IEC 27000]: mesure qui modifie le risque.

NOTE 1 – Les contrôles comprennent tout processus, politique, dispositif, pratique ou autre action qui modifie le risque.

NOTE 2 – Il est possible que les contrôles n'exercent pas toujours l'effet modificateur prévu ou supposé.

NOTE 3 – Ce terme peut être remplacé par "contrôle de sécurité" dans la présente Recommandation.

3.1.7 intégrité des données [UIT-T X.800]: propriété selon laquelle les données n'ont pas été modifiées ou détruites de manière non autorisée.

3.1.8 authentification de l'origine des données [UIT-T X.800]: la corroboration que la source des données reçues est conforme à la déclaration.

3.1.9 signature numérique [UIT-T X.800]: données ajoutées à une unité de données ou transformation cryptographique d'une unité de données qui permet à un destinataire de l'unité de données de prouver la source et l'intégrité de l'unité de données et de se protéger contre la falsification, par exemple, par le destinataire.

3.1.10 identité [b-UIT-T X.1408]: ensemble d'attributs permettant d'identifier le donneur d'ordre d'une information nominative.

3.1.11 répudiation [UIT-T X.800]: déni par l'une des entités impliquées dans une communication d'avoir participé à tout ou partie de la communication.

3.1.12 risque [b-ISO/IEC 27000]: effet de l'incertitude sur les objectifs.

NOTE 1 – Un effet est un écart – positif ou négatif – par rapport aux prévisions.

NOTE 2 – L'incertitude est l'état, même partiel, d'un manque d'information lié à la compréhension ou à la connaissance d'un événement, de ses conséquences ou de sa probabilité.

NOTE 3 – Le risque est souvent caractérisé par une référence à des "événements" potentiels (tels que définis dans le Guide ISO 73:2009, 3.5.1.3) et à des "conséquences" (telles que définies dans le Guide ISO 73:2009, 3.6.1.3), ou à une combinaison de ces éléments.

NOTE 4 – Le risque est souvent exprimé en termes de combinaison des conséquences d'un événement (y compris les changements de circonstances) et de la "probabilité" associée (telle que définie dans le Guide ISO 73:2009, 3.6.1.1) d'occurrence.

NOTE 5 – Dans le contexte des systèmes de gestion de la sécurité de l'information, les risques liés à la sécurité de l'information peuvent être exprimés comme l'effet de l'incertitude sur les objectifs de sécurité de l'information.

NOTE 6 – Le risque de sécurité de l'information est associé à la possibilité que des menaces exploitent les vulnérabilités d'un actif ou d'un groupe d'actifs informationnels et causent ainsi des dommages à un organisme.

3.1.13 authentification de l'entité homologue [UIT-T X.800]: la corroboration qu'une entité homologue d'une association est bien celle qui est revendiquée.

3.1.14 informations d'identification personnelle (PII) [b-UIT-T X.29100]: toute information qui a) peut être utilisée pour identifier l'entité principale des PII, ou b) est ou peut être directement ou indirectement liée à une entité principale des PII

NOTE – Pour déterminer si l'entité principale des PII peut être identifiée, il convient de tenir compte de tous les moyens qui peuvent être raisonnablement utilisés par la partie intervenant dans la protection de la vie privée et détenant les données, ou par toute autre partie, pour identifier cette personne physique.

3.1.15 hameçonnage [b-ISO/IEC 27032]: processus frauduleux consistant à tenter d'obtenir des informations privées ou confidentielles en se faisant passer pour une entité digne de confiance dans une communication électronique.

3.1.16 vie privée [UIT-T X.800]: le droit des individus de contrôler ou d'influencer les informations les concernant qui peuvent être collectées et stockées et par qui et à qui ces informations peuvent être divulguées.

NOTE – Comme ce terme se rapporte au droit des personnes, il ne peut être très précis et son utilisation devrait être évitée, sauf pour motiver l'exigence en matière de sécurité.

3.1.17 élément sécurisé [b-UIT-T X.1158]: un système à microprocesseur dédié qui contient un système d'exploitation, une mémoire, un environnement d'application et des protocoles de sécurité destinés à être utilisés pour stocker des données sensibles et exécuter des applications sensibles.

3.1.18 assurance de la sécurité [b-ISO/IEC TR 15443-1]: motifs de confiance justifiée dans le fait qu'une déclaration relative à la réalisation d'objectifs de sécurité a été ou sera effectuée.

3.1.19 politique de sécurité [UIT-T X.800]: l'ensemble des critères pour la fourniture de services de sécurité (voir aussi politique de sécurité basée sur l'identité et sur les règles).

3.1.20 service de messages courts [b-UIT-T X.1231]: le service de messages courts désigne un type de service de messagerie qui permet aux téléphones mobiles, aux téléphones et à d'autres entités de messages courts de transférer et de recevoir des messages textuels par l'intermédiaire d'un centre de services nommé dispositif, qui met en œuvre des fonctions telles que l'enregistrement et la livraison.

3.1.21 module d'identification de l'abonné [b-ISO/TR 19231]: circuit intégré qui stocke en toute sécurité l'identité internationale de l'abonné mobile (IMSI) et la clé correspondante utilisée pour identifier et authentifier les abonnés sur les appareils de téléphonie mobile (tels que les téléphones mobiles et les ordinateurs).

3.1.22 menace [UIT-T X.800]: une violation potentielle de la sécurité.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 services financiers numériques (SFN): le large éventail de services financiers accessibles et fournis par le biais de télécommunications ou d'applications numériques, notamment les paiements, le crédit, l'épargne, les transferts de fonds, l'investissement et l'assurance.

NOTE – Le concept de services financiers numériques (SFN) inclut les services financiers mobiles (SFM).

3.2.2 smartphone: un appareil qui combine un téléphone mobile et un ordinateur.

3.2.3 SOAR (*security orchestration automation and response*): technologie de cybersécurité qui rationalise et automatise le processus de détection, d'investigation et de réponse aux incidents de sécurité.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AAA	authentification, autorisation, comptabilité (*authentication, authorization, accounting)*
ACID	atomicité, cohérence, isolement, durabilité (*atomicity, consistency, isolation, durability*)
API	interface de programmation d'applications (*application programming interface*)
CAPTCHA	test public de Turing entièrement automatisé pour distinguer les ordinateurs des humains (*completely automated public turing test to tell computers and humans apart*)
CLI	identité de la ligne appelante (*caller line identity*)

DFS	services financiers numériques (*digital financial services*)
GCM	mode galois/compteur (*galois/counter mode*)
GW	passerelle (*gateway*)
HCE	émulation de la carte hôte (*host card emulation*)
HLR	accueil localisation registre (*home location register*)
HSM	module de sécurité matérielle (*hardware security module*)
ICT	technologie de l'information et de la communication (*information and communication technology*)
IMEI	identité internationale des équipements mobiles (*international mobile equipment identity*)
IMSI	identité internationale de l'abonné mobile (*international mobile subscriber identity*)
IMT	télécommunications mobiles internationales (*international mobile telecommunications*)
ISO	Organisation Internationale de Normalisation (*International Organization for Standardization*)
IVR	réponse vocale interactive (*interactive voice response*)
MAP	partie application mobile (*mobile application part*)
MFA	authentification multifactorielle (*multi-factor authentication*)
MNO	opérateur de réseau mobile (*mobile network operator*)
MSC	centre de commutation mobile (*mobile switching centre*)
MSISDN	numéro d'annuaire international d'abonné de la station mobile (*mobile station international subscriber directory number*)
MST	technologie des bandes magnétiques (*magnetic strip technology*)
MVNO	opérateur de réseau mobile virtuel (*mobile virtual network operator*)
NFC	communication en champ proche (*near field communication*)
NSDT	transfert de données quasi-sonore (*near sound data transfer*)
OEM	fabricant d'équipement d'origine (*original equipment manufacturer*)
OS	système d'exploitation (*operating system*)
OTP	mot de passe à usage unique (*one-time password*)
OWASP	projet libre de sécurité des applications web (*open web application security project*)
PA-DSS	norme de sécurité des données des applications de paiement (*payment application data security standard*)
PCI-DSS	normes de sécurité des données de l'industrie des cartes de paiement (*payment card industry data security standard*)
POS	point de vente (*pont of sale*)
QR	code QR, code de réponse rapide (*code quick response code*)
SCCP	partie contrôle de la connexion de signalisation (*signalling connection control part*)

SD	dimension de la sécurité (*security dimension*)
SE	élément de sécurité (*secure element*)
SIM	module d'identité d'abonné (*subscriber identity module*)
SMS	service de minimessages (*short messaging service*)
SOAR	orchestration, automatisation et réponse aux incidents de sécurité informatique (*security orchestration automation and response*)
STK	boîte à outils SIM (*SIM toolkit*)
TEE	environnement d'exécution de confiance (*trusted execution environment*)
TLS	sécurité de la couche transport (*transport layer security*)
TPP	prestataires tiers (services de paiement) (*third-party (payment service) providers*)
TSP	fournisseur de services de jeton (*token service provider*)
UICC	carte universelle à circuit intégré (*universal integrated circuit card*)
URL	localisateur de ressources uniformes (*uniform resource locator*)
USSD	données de service supplémentaires non structurées (*unstructured supplementary service data*)
VLR	registre de localisation des visiteurs (*visitor location register*)

5 Conventions

La présente Recommandation utilise les conventions suivantes:

La forme "**doit**" indique une exigence qui doit être strictement suivie, et par rapport à laquelle aucun écart n'est autorisé pour pouvoir déclarer la conformité à la présente Recommandation.

La forme "**devrait**" indique une exigence qui est recommandée mais qui n'est pas absolument obligatoire. Cette exigence n'est donc pas indispensable pour déclarer la conformité. Le mot-clé "**devrait**" peut être remplacé par l'expression "**il est recommandé de**" dans la présente Recommandation.

6 Introduction

La technologie numérique a favorisé l'accès financier de millions de personnes grâce à sa facilité d'utilisation par le biais des téléphones mobiles, en fournissant des services financiers centrés sur le client qui sont abordables, évolutifs et pratiques.

Cependant, comme les fournisseurs exploitent les moyens numériques pour offrir une gamme plus large de services financiers avec une plus grande portée, une meilleure efficacité et des coûts d'exploitation minimaux, la croissance rapide et l'adoption des services financiers numériques (SFN) rendent son écosystème particulièrement vulnérable à diverses menaces pour la sécurité. L'interconnexion des entités du système et la dépendance/l'implication d'un certain nombre de parties dans l'écosystème étendent les limites de la sécurité au-delà du fournisseur SFN aux clients, aux fournisseurs de réseaux, aux fabricants de téléphones mobiles et à d'autres fournisseurs tiers dans l'écosystème.

En outre, les fournisseurs de SFN doivent faire face à un écosystème mobile de plus en plus complexe, développant des applications pour de multiples versions de systèmes d'exploitation, chacune présentant des vulnérabilités spécifiques, et prenant en charge différents types d'appareils mobiles. Dans cet environnement dynamique qui évolue rapidement, les prestataires de services de SFN sont

confrontés à des défis concernant la connaissance des menaces réelles pour la sécurité et les contrôles de sécurité possibles pour atténuer les risques.

Un cadre d'assurance de la sécurité SFN vise à combler le manque de connaissances susmentionné et recommande un processus structuré de gestion des risques de sécurité que les parties prenantes de l'écosystème SFN pourraient mettre en œuvre:

- renforcer la confiance des clients dans les services financiers numériques;
- clarifier le rôle et les responsabilités de chacun des acteurs de l'écosystème;
- identifier les vulnérabilités en matière de sécurité et les menaces connexes au sein de l'écosystème;
- établir des contrôles de sécurité pour assurer une sécurité de bout en bout;
- renforcer les pratiques de gestion en ce qui concerne la gestion des risques en matière de sécurité, en tenant compte de toutes les parties prenantes du SFN.

Le cadre d'assurance de la sécurité du SFN fournit une vue d'ensemble des menaces et des vulnérabilités en matière de sécurité auxquelles sont confrontés les fournisseurs de SFN (banques, non-banques fournissant des services d'argent mobile), les opérateurs de réseaux mobiles, les clients, les fournisseurs de systèmes de paiement, les commerçants et les fournisseurs de services technologiques/de services tiers. Les régulateurs, y compris les autorités de télécommunication, les régulateurs bancaires et les régulateurs de paiement, pourraient également utiliser le cadre d'assurance de sécurité SFN pour établir des lignes de base de sécurité pour les fournisseurs SFN également.

Une fois mis en œuvre, le cadre complétera les pratiques de gestion des risques et de la sécurité de l'information établies par les parties prenantes de l'écosystème SFN. Par exemple, les contrôles de sécurité du document peuvent être inclus dans le programme de sécurité des TIC du prestataire de services de SFN.

Les organisations devraient mettre en œuvre des principes et des normes de bonne gouvernance en matière de sécurité, tels que la documentation sur la politique de sécurité de l'information, la classification des données, l'attribution des responsabilités en matière de sécurité de l'information, les politiques de confidentialité des données, la sensibilisation et la formation du personnel à la sécurité, le développement, le test et la maintenance sécurisés des infrastructures, des appareils, des applications et des processus, la gestion de la vulnérabilité, les procédures de sauvegarde, la gestion des incidents, la continuité des activités et les processus de reprise en cas de catastrophe.

7 Aperçu de la Recommandation UIT-T X.805

Le cadre d'assurance de la sécurité des services financiers numériques s'appuie sur [UIT-T X.805] – *Architecture de sécurité pour les systèmes assurant des communications de bout en bout*, pour appliquer des contrôles de sécurité afin d'assurer la sécurité du réseau de bout en bout. Il prévoit également des contrôles fondés sur les recommandations du document de référence "Aspects sécuritaires des services financiers numériques" [b-DFS-SA] du groupe de discussion UIT-T sur les services financiers numériques.

L'environnement de communication de bout en bout de l'écosystème DFS est examiné sous l'angle de [UIT-T X.805], qui fournit un cadre de référence utile pour la gestion de la sécurité. L'architecture de sécurité de [UIT-T X.805] comporte huit "dimensions de sécurité", qui sont des mesures visant à traiter un aspect particulier de la sécurité du réseau. Ces huit dimensions de la sécurité sont présentées dans la Figure 1, adaptée de [UIT-T X.805].

Les huit dimensions de la sécurité qui fournissent un moyen systématique de faire face aux menaces qui pèsent sur les réseaux sont les suivantes:

- **Contrôle d'accès**: protection contre l'utilisation non autorisée des ressources du réseau.
- **Authentification**: méthodes de confirmation de l'identité des entités communicantes.

- **Non-répudiation**: méthodes visant à empêcher une personne ou une entité de nier la cause d'un événement ou d'une action.
- **Confidentialité des données**: protection des données contre la divulgation non autorisée.
- **Sécurité des communications**: assurance que l'information ne circule qu'entre les points d'extrémité autorisés, sans être détournée ou interceptée.
- **Intégrité des données**: protection de l'exactitude et de la précision des données.
- **Disponibilité**: prévention du refus d'accès autorisé aux éléments du réseau et aux données.
- **Vie privée**: protection des données susceptibles d'être obtenues par l'observation de l'activité du réseau.

[UIT-T X.805] définit une hiérarchie d'équipements de réseau et de regroupements d'installations en trois couches de sécurité. Ces couches de sécurité fournissent des solutions de sécurité complètes, de bout en bout, et identifient où la sécurité doit être abordée dans les produits et les solutions, car chaque couche peut être exposée à différents types de menaces et d'attaques.

Les couches de sécurité sont les suivantes:

- **Couche de sécurité de l'infrastructure**: il s'agit des éléments de base utilisés pour construire les réseaux, les services et les applications de télécommunications, ainsi que des liaisons de transmission et des éléments de réseau individuels, y compris leurs plates-formes matérielles et logicielles sous-jacentes.
- **Couche de sécurité des services**: elle se compose des services que les clients/utilisateurs finaux reçoivent des réseaux. Ces services vont du transport et la connectivité de base aux facilitateurs de services comme ceux qui sont nécessaires pour fournir un accès à l'internet, comme les services d'authentification, d'autorisation et de comptabilité (AAA), les services de configuration dynamique des hôtes, les services de noms de domaine, etc., et les services à valeur ajoutée tels que les services de téléphonie gratuite, la qualité de service (QoS), les réseaux privés virtuels (VPN), les services de localisation, la messagerie instantanée, etc.
- **Couche de sécurité des applications**: elle se concentre sur les applications basées sur le réseau auxquelles accèdent les clients/utilisateurs finaux.

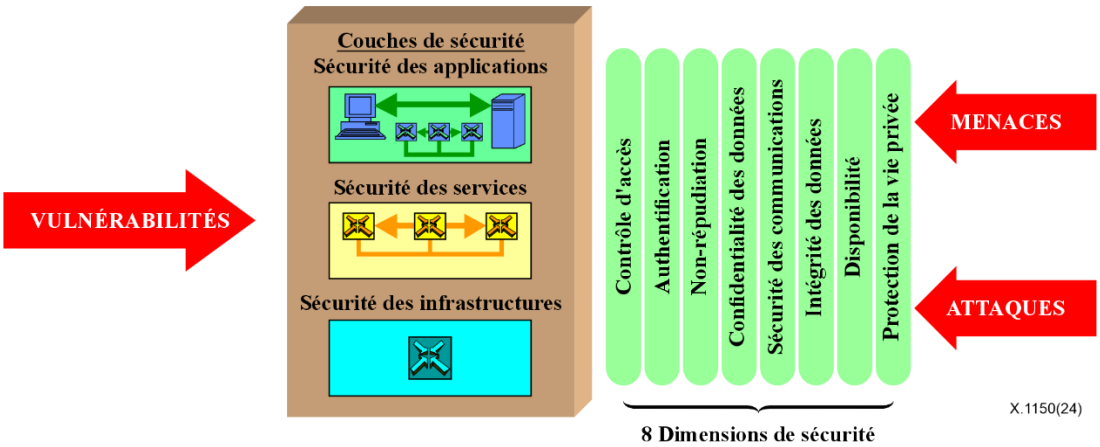

Figure 1 – Dimensions de sécurité de la Recommandation UIT-T X.805

8 Modèles d'entreprise des fournisseurs de services financiers numériques

Sept acteurs principaux de l'écosystème SFN sont pris en compte: 1) utilisateur SFN, 2) commerçant, 3) institution gouvernementale ou non gouvernementale, etc., 4) opérateur de réseau mobile (MNO), 5) banque, 6) tiers et 7) opérateur de réseau mobile virtuel (MVNO). Ce paragraphe prend également en compte les cinq fonctions principales de la chaîne de valeur des services de dépôt et de ompensation pour ces parties prenantes: détenteur de dépôts, émetteur de monnaie électronique,

prestataire de services de paiement, gestionnaire de réseau d'agents et fournisseur de communications mobiles.

En fonction des rôles joués par chacune des parties prenantes, ce paragraphe envisage les quatre modèles d'entreprise les plus courants des prestataires de services de dépôt de documents:

- modèle d'entreprise dirigé par la banque;
- modèle d'entreprise dirigé par les ORM;
- modèle MVNO;
- modèle hybride.

8.1 Modèle d'entreprise dirigé par la banque

Dans ce modèle, les services financiers proposés par la banque sont étendus aux utilisateurs mobiles, le processus d'inscription pouvant se faire à la banque ou par l'intermédiaire d'un réseau d'agents. Dans ce modèle, la banque joue les rôles financiers clés, c'est-à-dire qu'elle est le détenteur des dépôts, l'émetteur de monnaie électronique et le prestataire de services de paiement. Le réseau de communication permettant de fournir ces services financiers à l'utilisateur est fourni par l'ORM, par le biais de ses différents canaux, qui peuvent être des données de service supplémentaires non structurées (USSD), un service de minimessage (SMS), une réponse vocale interactive (IVR) ou la boîte à outils de l'application SIM (STK).

La Figure 2 illustre le modèle dirigé par les banques.

Figure 2 – Modèle d'entreprise piloté par la banque

8.2 Modèle d'entreprise dirigé par les ORM

Dans un modèle dirigé par un ORM, parallèlement au rôle traditionnel de fournisseur du réseau de communication, l'ORM assume également l'essentiel des rôles financiers et émet donc la monnaie électronique, gère le réseau d'agents et les relations avec les clients et est le fournisseur de services de paiement. L'ORM gère un vaste réseau d'agents SFN qui enregistrent les utilisateurs SFN et reçoivent d'eux des espèces physiques en échange de monnaie électronique pour le compte de l'ORM. En fonction du régime financier, l'ORM peut être tenu de collaborer avec une banque partenaire dans laquelle les agents du SFN déposeront les fonds physiques collectés auprès des clients pour le compte de l'ORM. La monnaie électronique émise par l'ORM est garantie par les fonds qui se trouvent sur le compte fiduciaire de la banque partenaire. La Figure 3 illustre le modèle d'entreprise dirigé par l'ORM.

Figure 3 – Modèle d'entreprise piloté par l'ORM

8.3 Modèle MVNO

Dans certains cas, un opérateur de réseau mobile virtuel (MVNO) fournit les services de télécommunications requis pour le SFN. Le MVNO peut être indépendant ou appartenir à une banque. Le MVNO utilise l'infrastructure fournie par un MNO, mais offre à ses clients une gamme différente de services de télécommunications, y compris des services financiers numériques. La Figure 4 illustre le modèle MVNO.

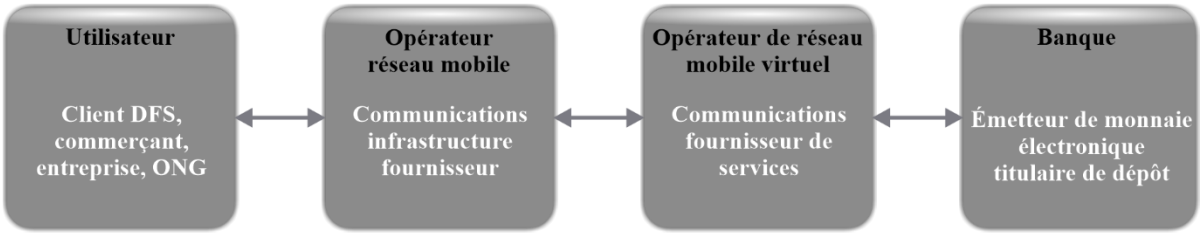

Figure 4 – Modèle MVNO

8.4 Modèle hybride

Dans un modèle hybride, les rôles essentiels sont partagés entre la banque et l'ORM. Elles peuvent impliquer un tiers dans l'écosystème qui fournit des services qui ne sont fournis ni par l'ORM ni par la banque. Par exemple, un tiers pourrait posséder le réseau d'agents et jouer également le rôle de prestataire de services de paiement. La Figure 5 présente le modèle hybride.

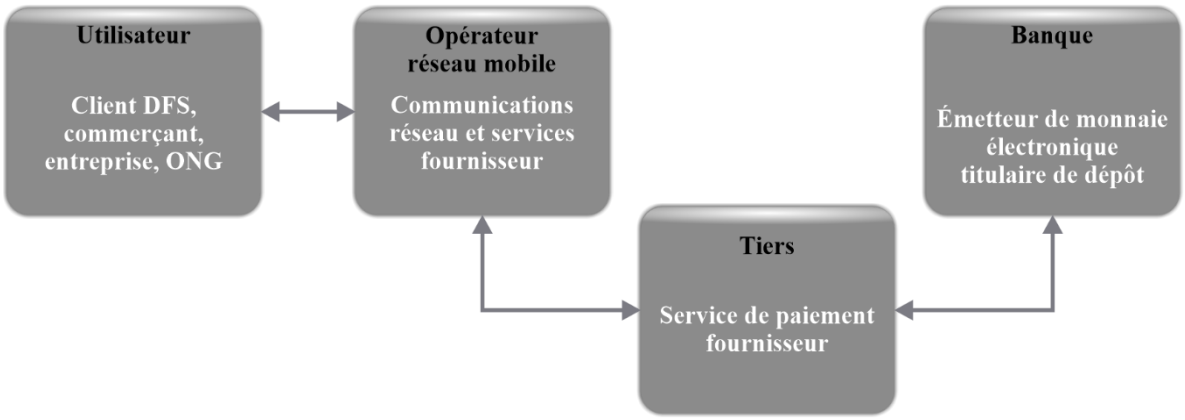

Figure 5 – Modèle hybride

9 L'écosystème DFS

L'écosystème DFS se compose des éléments suivants:

- Transfert d'argent par téléphone mobile en utilisant les canaux de l'ORM (par exemple, SMS, USSD, téléphonie vocale) sans application de paiement spécifique téléchargée sur l'appareil mobile du client, qui serait un featurephone.
- Application de paiement mobile sur l'appareil mobile de l'utilisateur lié à un compte bancaire, une carte de débit ou une carte de crédit.
- Technologies de paiement sans contact: les technologies de paiement sans contact impliquent l'utilisation d'un portefeuille numérique, qui peut utiliser différents types de technologies de communication pour envoyer les données de paiement de l'appareil mobile de l'utilisateur au point de vente du commerçant (POS). Parmi les technologies de communication utilisées pour transmettre les informations au point de vente figurent la communication en champ proche (NFC), le code QR, la transmission magnétique sécurisée (MST), le Bluetooth, les

SMS et l'internet. Le portefeuille numérique peut être stocké sur l'appareil mobile de l'utilisateur ou dans le cloud.

- Les paiements par transfert de données quasi-sonore (NSDT): le NSDT utilise le canal audio du téléphone mobile pour crypter les données des transactions de paiement.
- Paiements à distance: il s'agit notamment des paiements par Internet (par carte de crédit sur un site web de commerce électronique ou par carte sur fichier), de la facturation directe à l'opérateur, des paiements de primes par SMS et des services bancaires mobiles.

Les portefeuilles de monnaies numériques n'entrent pas dans le champ d'application de la présente Recommandation.

Dans les paragraphes 9.1 et 9.2, les éléments de l'écosystème SFN sont examinés:

- Paiement mobile par données de service supplémentaires non structurées (USSD), SMS, réponse vocale interactive (IVR) et boîte à outils SIM (STK).
- Applications de paiement mobile et portefeuilles numériques.

9.1 Éléments d'un écosystème DFS pour USSD, SMS, IVR, STK et NSDT

La Figure 6 présente les principales composantes du SFN et de l'écosystème du SFN. Tous les éléments ne seront pas utilisés dans tous les déploiements; par exemple, dans les cas où il n'y a pas d'accès WiFi ou d'application pour smartphone disponible pour un service SFN, les communications de l'utilisateur seraient limitées aux interactions via le réseau mobile, plutôt que par des passerelles Internet externes ou en s'appuyant sur un service en nuage.

Les constituants de l'écosystème sont composés des éléments décrits dans les § 9.1.1 à 9.1.7.

9.1.1 Utilisateur/client

Le client est le public cible d'un service SFN, qui utilise une application d'argent mobile pour interagir avec le service. Cette interaction peut se faire directement, par le biais du réseau mobile ou de l'internet (en fonction des caractéristiques de la plate-forme mobile sous-jacente et de l'application d'argent mobile); un agent SFN qui interagit avec le service SFN pour le compte du client peut également servir de médiateur. L'agent peut soit s'interfacer directement avec le réseau, soit utiliser une passerelle web pour fournir ces services.

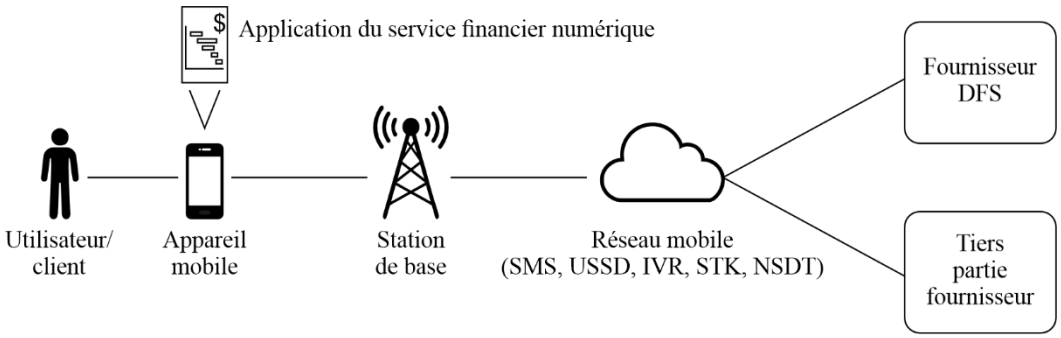

Figure 6 – Principaux éléments de l'écosystème SFN

9.1.2 Appareil mobile

L'appareil mobile fournit une plate-forme pour le déploiement d'une application d'argent mobile. Il s'agit du principal canal par lequel le client (ou l'agent interagissant pour le compte du client; pour faciliter l'exposé, on suppose que toutes les interactions ultérieures avec le service se font par l'intermédiaire du client, sauf si des actions sont spécifiquement demandées à l'agent) s'interface avec le service SFN. Les appareils mobiles peuvent être des téléphones fonctionnels ou des smartphones. Les téléphones ordinaires contiennent souvent des ressources limitées et prennent en charge des

interfaces limitées pour les applications ainsi que des options de connectivité limitées (par exemple, les services GSM 2G). Les smartphones, quant à eux, peuvent prendre en charge des services très puissants grâce à des éléments matériels sécurisés et à la prise en charge de réseaux avancés et de la connectivité WiFi. Les téléphones ordinaires et les smartphones contiennent des cartes SIM, dont certaines contiennent des éléments sécurisés qui peuvent être exploités par des applications. L'appareil mobile est doté d'un système d'exploitation dont les capacités dépendent des ressources dont il dispose.

9.1.3 Station de base

Le lien de communication entre la station de base et le combiné mobile est le principal canal de transmission des informations entre l'utilisateur et le fournisseur SFN. Notamment, dans les systèmes où les applications ne sont pas fournies aux téléphones, mais où des réseaux ouverts sont utilisés (par exemple, SMS, STK, IVR et communication basée sur USSD), ce lien est la seule partie de l'architecture globale où le cryptage est en place sur les données transmises vers le consommateur et à partir de celui-ci – une fois que les données sont reçues par la station de base, elles sont envoyées en clair via les réseaux du fournisseur. Il est essentiel pour la durabilité et la faisabilité d'un système SFN que ce lien soit robuste, fiable et pratiquement omniprésent.

9.1.4 Réseau mobile

Le réseau de l'opérateur fournit une connectivité de transit pour les informations provenant du combiné du client. Il est composé de différents nœuds qui permettent la communication entre les différentes passerelles vers les fournisseurs externes et vers les fournisseurs SFN, qui peuvent être associés au transporteur ou être des entités externes nécessitant une communication Internet. Au sein de ce réseau réside des passerelles (GW) pour USSD, IVR, STK et SMS, des bases de données internes telles que les registres de localisation des foyers (HLR) et les registres de localisation des visiteurs (VLR), et des passerelles Internet qui peuvent servir de points de connexion avec le fournisseur SFN. Dans les cas où l'opérateur de réseau mobile fournit également les services SFN les passerelles vers ces services seront maintenues dans leur réseau interne. Le centre de commutation mobile (MSC) est au cœur des différents nœuds du réseau mobile pour faciliter l'acheminement des communications à l'aide des données de l'utilisateur HLR ou VLR. L'Annexe A décrit les nœuds du réseau mobile, la passerelle SMSC (Short Message Service Center), la passerelle SAT (SIM Application Toolkit), la passerelle USSD, la passerelle IVR et la passerelle Internet qui permettent à l'utilisateur d'utiliser les modes d'accès respectifs; ce paragraphe indique également que le système de facturation de l'ORM est utilisé dans certains déploiements par l'ORM pour les frais liés aux SMS, à l'IVR ou à l'Internet. Un opérateur de réseau mobile virtuel (MVNO) peut fournir les services de l'ORM au fournisseur SFN et au client, mais l'infrastructure du réseau sans fil est toujours fournie par un opérateur de réseau ou un facilitateur.

9.1.5 Fournisseur SFN

Le fournisseur SFN assure l'interface entre le contenu de l'application provenant des réseaux d'opérateurs mobiles et les fournisseurs de services financiers d'arrière-plan; il est utilisé pour gérer les informations des clients de manière sécurisée et pour permettre des services tels que les audits. Pour que ces opérations soient sûres, le fournisseur de SFN doit avoir la certitude que la personne qui accède aux données est bien celle qu'elle prétend être. Les journaux d'audit doivent également être activés pour permettre l'évaluation du contenu des données au sein du réseau et des commandes émises par l'intermédiaire de l'application SFN. La détermination de l'identité du client, l'accréditation, le stockage des données de transaction du client, la fourniture d'interfaces d'habilitation telles que les interfaces de programmation d'applications (API) pour les tiers, et le traitement des transactions provenant des différentes sources, sont également des rôles assumés par le fournisseur de services SFN.

9.1.6 Fournisseurs tiers

Les fournisseurs externes permettent l'interface entre les systèmes d'argent mobile basés sur les opérateurs et fournissent la base pour la connexion avec les réseaux financiers dorsaux tels que l'infrastructure bancaire. D'autres rôles pouvant être assumés par ces prestataires externes comprennent l'exploitation de l'infrastructure informatique ou l'assistance à la clientèle l'assistance à la clientèle, et, dans certains cas, ils peuvent assurer l'interface directement entre les systèmes SFN ou agir en tant qu'agrégateurs de services et de transactions.

9.1.7 Application de services financiers numériques

L'application constitue l'interface par laquelle le client interagit avec l'écosystème SFN. Les applications peuvent varier considérablement en termes d'interfaces et de richesse de l'expérience qu'elles offrent au client, qu'il s'agisse de systèmes à base de menus sur des téléphones fonctionnels, conçus pour communiquer par USSD, STK ou SMS, de conceptions vocales qui utilisent la réponse vocale interactive (IVR), ou d'interfaces graphiques riches sur des smartphones avec une sécurité de transport de bout en bout assurée par des algorithmes cryptographiques conformes aux normes de l'internet. Les interactions peuvent utiliser des menus d'application spéciaux activés par code, mot de passe, empreinte digitale, etc., permettant aux utilisateurs d'envoyer de l'argent, de payer des factures, de recharger le temps de communication et de vérifier le solde de leur compte.

9.2 Éléments de l'écosystème SFN basés sur les applications et les portefeuilles numériques

Il existe différents éléments dans les écosystèmes basés sur des modèles de portefeuilles numériques, parmi lesquels les principaux modèles sont le portefeuille mobile de proximité centré sur l'appareil, le portefeuille mobile in-app centré sur l'appareil, le portefeuille de carte absente, le code QR et le portefeuille de paiement numérique. Tous ceux-ci ont des plates-formes technologiques différentes et utilisent des modèles de sécurité différents.

Cette clause décrit chacune des composantes de l'écosystème SFN. La Figure 7 montre l'écosystème basé sur les applications et les portefeuilles numériques.

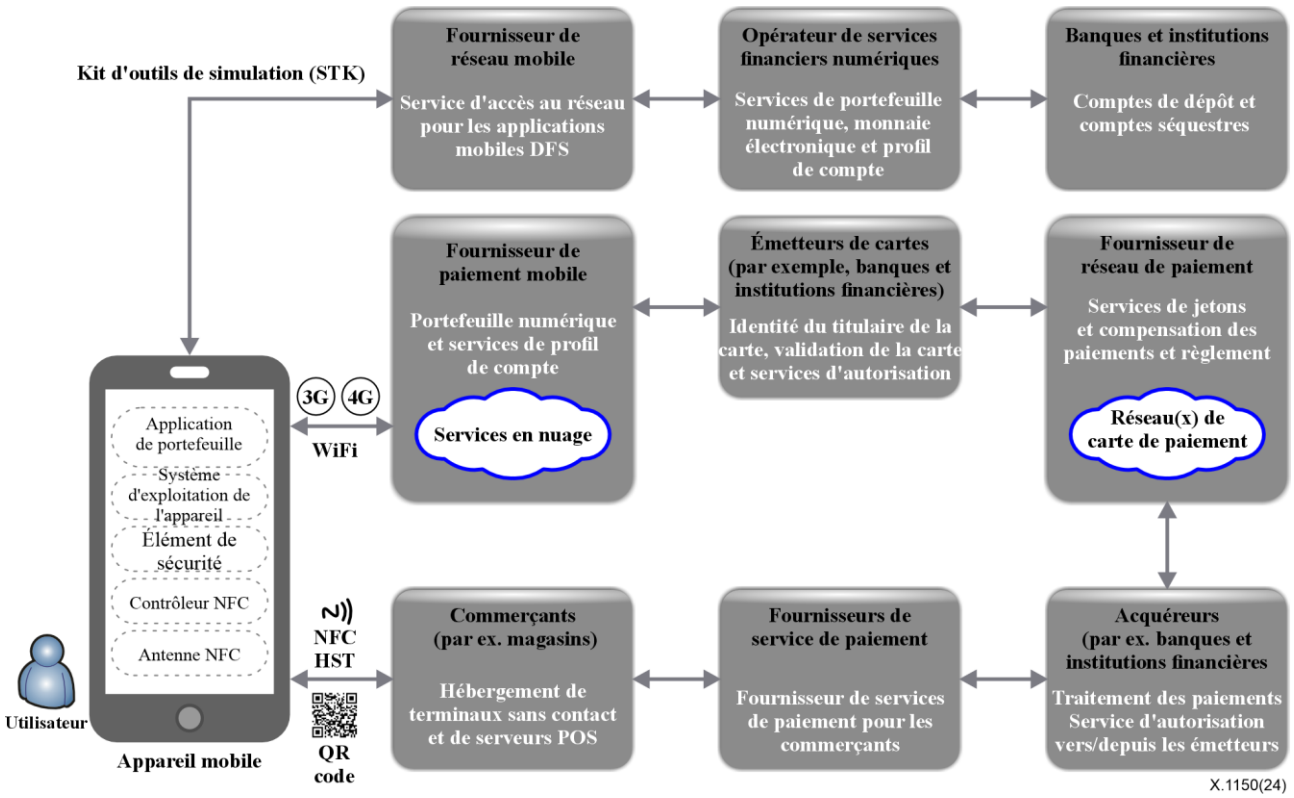

Figure 7 – L'écosystème SFN basé sur les applications et le portefeuille numérique

9.2.1 Appareil mobile

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

La Figure 8 illustre certains des composants de l'appareil mobile de l'utilisateur.

- **Le contrôleur NFC et l'antenne NFC**: le contrôleur NFC gère les protocoles de communication en champ proche et achemine la communication entre l'application et l'élément sécurisé (SE), et entre le SE et le terminal du point de vente. L'antenne NFC relaie les signaux entre le contrôleur et le terminal POS.
- **L'élément sécurisé (SE)**: l'élément sécurisé (SE) est une plate-forme inviolable, généralement un microcontrôleur sécurisé à puce conçu pour héberger en toute sécurité des applications et leurs données confidentielles et cryptographiques. L'utilisation du SE dépend du type d'application de portefeuille mobile et du type de mode de paiement mobile. Les SE existent sous différentes formes pour répondre aux exigences des diverses applications de paiement ou des portefeuilles numériques et aux besoins du marché. Le SE peut être incorporé et intégré dans le matériel de l'appareil mobile, comme le SE dans l'iPhone. Le SE peut également être un SIM/UICC, les réseaux utilisant la norme GSM préfèrent cela plus souvent sous la forme d'applications SIM toolkit (STK) qui s'appuient sur la SIM en tant qu'élément sécurisé pour offrir une application sécurisée d'argent mobile. Le SE peut également être une carte à mémoire sécurisée qui peut être insérée dans l'appareil mobile.
- **Émulation de carte hôte**: les appareils mobiles peuvent émuler une carte sans contact à l'aide de l'émulation de carte hôte (HCE), qui ne repose pas sur un élément matériel sécurisé pour le stockage de données sensibles telles que les données des cartes de paiement. Le HCE est une solution d'infrastructure logicielle qui permet à une application de portefeuille mobile de communiquer en toute sécurité via le contrôleur NFC pour transmettre les informations d'identification de la carte de paiement ou les jetons de paiement à un terminal de point de

vente ou à un lecteur NFC sans contact, éliminant ainsi la nécessité d'utiliser un élément sécurisé (SE).

- **Application de portefeuille**: les portefeuilles sont des applications/services accessibles via l'appareil qui permettent au détenteur du portefeuille d'accéder, de gérer et d'effectuer des transactions financières, comme des paiements, en toute sécurité. Les portefeuilles sont spécifiques à l'appareil et au logiciel et peuvent remplacer les cartes de crédit et de débit. D'autre part, d'autres portefeuilles mobiles/numériques ne dépendent d'aucun appareil et stockent en toute sécurité les informations de paiement et les mots de passe de l'utilisateur pour de nombreuses méthodes de paiement et sites web, ce qui permet d'effectuer des transactions facilement et rapidement et d'utiliser des moyens d'authentification plus forts tels que la biométrie.

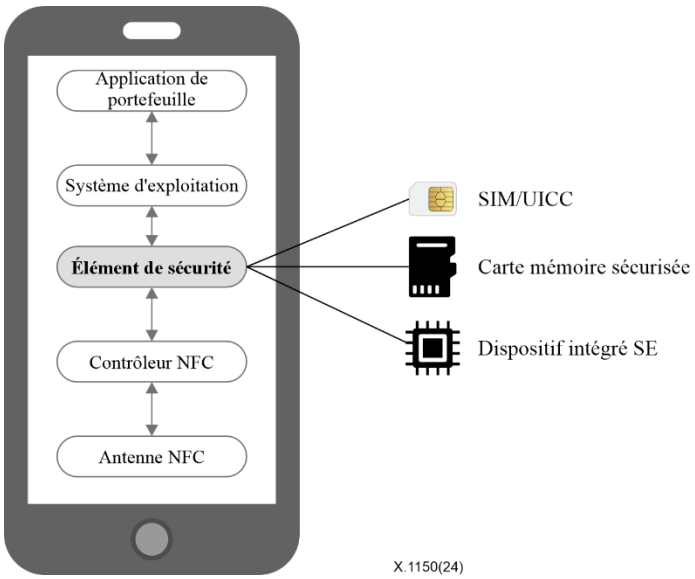

Figure 8 – Composants de l'appareil mobile

9.2.2 Commerçants

Les commerçants acceptent les paiements des clients pour des biens ou des services, par le biais d'un terminal de point de vente (POS) ou par d'autres moyens tels que le balayage d'un code QR par le client ou la saisie du numéro du commerçant dans leur application de paiement. Les appareils mobiles sont également utilisés par les commerçants pour les paiements, ce qui constitue donc une autre source inhérente de vulnérabilités.

9.2.3 Terminaux de point de vente

Un terminal de point de vente (POS) est un appareil électronique utilisé pour traiter les paiements mobiles chez le commerçant. Les canaux de communication entre le terminal de point de vente et l'appareil mobile pour les paiements de proximité sont la communication sans contact en champ proche (NFC), les codes de réponse rapide (QR) ou la technologie de la bande magnétique (MST). Les IMT-2000, les IMT évoluées, les IMT-2020 et le WiFi sont principalement utilisés pour les portefeuilles mobiles. Tout risque existant sur un ordinateur de bureau ou portable standard peut également exister sur un appareil mobile.

Outre les méthodes de communication standard des ordinateurs de bureau et des ordinateurs portables traditionnels, les appareils mobiles peuvent également être dotés de plusieurs technologies cellulaires (par exemple, LTE et GSM), de GPS, de Bluetooth, d'infrarouges (IR) et de capacités de communication en champ proche (NFC). Le risque est encore accru par les supports amovibles (par exemple, la carte SIM et la carte SD), l'électronique interne utilisée pour les tests par le fabricant, les capteurs intégrés et les lecteurs biométriques.

- **Communication en champ proche (NFC)**: la NFC est un protocole de communication sans fil basé sur la technologie des radiofréquences qui permet l'échange de données entre des appareils distants de quelques centimètres. Un portefeuille sur un appareil mobile doté de la technologie NFC est une application logicielle stockée sur le téléphone mobile qui gère et initie les paiements. Le portefeuille mobile accède aux informations de paiement telles que les cartes de paiement à jetons, les comptes bancaires, les coupons de fidélité ou les informations financières stockées sur le téléphone mobile dans un environnement d'exécution de confiance (TEE). Le téléphone physique est utilisé pour initier une transaction de paiement en mettant en contact ou en tenant l'appareil mobile près d'un terminal de point de vente sans contact.
- **Technologie de la bande magnétique (MST)**: la technologie de la bande magnétique génère un signal magnétique semblable à celui d'une carte de paiement traditionnelle lorsqu'elle est glissée dans le lecteur. Le signal magnétique est alors envoyé de l'appareil au terminal POS. La MST est activée sur certains téléphones mobiles.
- **Codes QR**: les codes QR offrent une alternative de paiement sans contact de deux manières:
  - Le payeur scanne le code QR du commerçant, le commerçant génère un code QR de transaction ou affiche le code QR statique qui lui a été attribué, le payeur scanne alors le code à l'aide de l'appareil photo de son téléphone et l'application de paiement interprète les détails du paiement ou du commerçant pour lancer la transaction qui peut être complétée par la saisie d'un code PIN.
  - Le commerçant scanne le code QR du payeur; le client, par le biais de son application de paiement, génère pour le commerçant un code QR unique spécifique à la transaction; le commerçant scanne le code par le biais de son application de paiement à l'aide d'un scanner QR pour initier la transaction qui peut être complétée par la saisie d'un code PIN.
- **IMT-2000/IMT évoluées/IMT-2020 et WiFi**

Outre les réseaux cellulaires IMT-2000/IMT évoluées/IMT-2020, les appareils mobiles peuvent également se connecter à des réseaux sans fil (WiFi). Ces réseaux permettent à l'application mobile de l'appareil d'interagir avec les fournisseurs de services de paiement. Les réseaux IMT-2000/IMT évoluées/IMT-2020 et WiFi sont généralement fournis par l'opérateur de réseau mobile.

9.2.4 Fournisseur de services de jetons (TSP)

La TSP gère le cycle de vie des jetons. Les services supplémentaires comprennent généralement la création et le stockage de jetons, la gestion du cycle de vie des jetons, le traitement des transactions par jetons, la mise en correspondance des jetons avec le PAN, la validation du titulaire de la carte, y compris les services de provisionnement, la gestion des clés pour les portefeuilles basés sur l'appareil utilisant le HCE, les services de vérification de la transaction et de la validité de l'appareil.

9.2.5 Acquéreur

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

9.2.6 Émetteur

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

9.2.7 Fournisseur de services de portefeuille (WSP)

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

9.2.8 Prestataire de services de paiement (PSP)

Les PSP fournissent les différentes méthodes qui permettent à un commerçant d'accepter des paiements à partir de portefeuilles mobiles et numériques. Le PSP peut se connecter à plusieurs acquéreurs, ainsi qu'à des systèmes de paiement et de cartes, ainsi qu'aux réseaux de paiement et de cartes. En faisant appel aux services d'un PSP, le commerçant devient moins dépendant des institutions financières pour la gestion des transactions, puisque le PSP peut gérer les comptes bancaires ainsi que les relations avec le réseau externe.

10 Menaces pour la sécurité

10.1 Menaces pour les SFN utilisant USSD, SMS, IVR, STK et NSDT

La Figure 9 résume les menaces des applications SFN basées sur USSD, SMS, IVR, STK et NSDT.

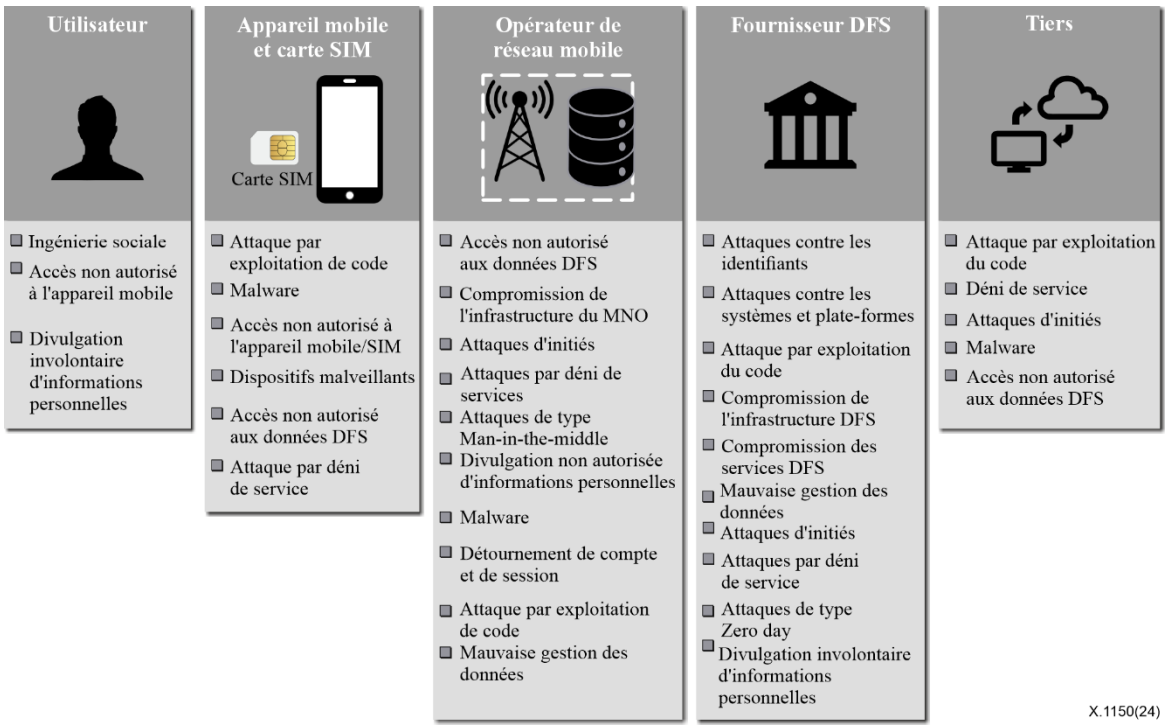

Figure 9 – Menaces pour les systèmes SFN utilisant USSD, SMS, IVR et NSDT

10.2 Menaces pour l'écosystème SFN basé sur les applications et les portefeuilles numériques

Les applications/portefeuilles de paiement mobile permettent d'offrir des services financiers numériques par le biais d'applications installées sur l'appareil mobile. La nature des applications financières et des canaux utilisés dépend des capacités de l'appareil. Le Tableau 1 résume les menaces qui pèsent sur les écosystèmes SFN en fonction des applications et des portefeuilles numériques.

Tableau 1 – Synthèse des menaces pesant sur l'écosystème des services SFN en fonction des applications et des portefeuilles numériques

Élément	Menaces
Application de paiement mobile	• Rétro-ingénierie du code source de l'application. • Falsification de l'application de paiement mobile. • Exploitation des vulnérabilités des applications de paiement mobile.

Tableau 1 – Synthèse des menaces pesant sur l'écosystème des services SFN en fonction des applications et des portefeuilles numériques

Élément	Menaces
	• Installation de rootkits/malwares. • système d'exploitation mobile Autorisations d'accès.
Appareil mobile	• Installation d'applications malveillantes et de logiciels malveillants. • Accès non autorisé à un appareil mobile perdu ou volé. • Installation de logiciels malveillants sur l'appareil.
Commerçant	• Malware d'OS: les attaquants peuvent télécharger des logiciels malveillants sur les terminaux de paiement qui pourraient être utilisés pour accéder à distance aux données de paiement. • Compromission du code QR: les codes QR présentent des menaces inhérentes car ils ne sont pas facilement lisibles par l'œil humain. Les pirates pourraient facilement remplacer le code QR d'un commerçant par des codes malveillants qui pourraient être incorporés avec un contenu malveillant. Le contenu malveillant peut être des URL d'hameçonnage, des applications mobiles malveillantes. • Attaques de type "Man-in-the-Middle" contre les terminaux sans contact et les serveurs des points de vente: les attaquants peuvent exploiter les faiblesses de la sécurité du réseau, telles que l'absence de pare-feu pour protéger le réseau interne des commerçants. • Attaques par relais contre les terminaux sans contact des points de vente équipés de la technologie NFC: le logiciel relais installé sur un appareil mobile peut relayer les commandes et les réponses entre l'élément sécurisé (SE) et un émulateur de carte installé en tant que proxy sur le POS mobile via un réseau sans fil. • Utilisation de codes PIN par défaut pour accéder aux terminaux de paiement, par exemple 166816 et Z66816.
Acquéreurs	• Compromission des systèmes de traitement des paiements: en demandant des jetons et des cryptogrammes au réseau de paiement de l'émetteur, un pirate peut obtenir une grande quantité de données sur les titulaires de cartes en installant des logiciels malveillants et des outils d'accès à distance sur n'importe lequel des serveurs de traitement des paiements du réseau interne. • Compromission de la sécurité du réseau et de l'interface: les attaquants peuvent exploiter des connexions point à point non sécurisées entre l'acquéreur et l'émetteur en compromettant le fournisseur de réseau; les attaquants peuvent alors utiliser ce niveau d'accès pour être en mesure de surveiller et de manipuler les appels API.
Fournisseur de services Internet	• Compromission des passerelles de paiement: les passerelles de paiement peuvent être la cible d'attaquants désireux d'accéder aux données de transaction en transit entre les commerçants et les banques acquéreuses et de les compromettre. • Compromission des vulnérabilités logicielles dans les terminaux sans contact des points de vente qui sont fournis aux commerçants par les PSP et qui peuvent traiter des données provenant de différents canaux, y compris la carte présente, les paiements sans contact et la carte non présente. • Compromission des réseaux non sécurisés; les attaquants pourraient effectuer des attaques de type "Man in the middle" pour usurper des données sensibles en transit entre le PSP et l'acquéreur si le fournisseur utilise des connexions faibles ou non sécurisées telles que des versions inférieures de TLS et SSL.

Tableau 1 – Synthèse des menaces pesant sur l'écosystème des services SFN en fonction des applications et des portefeuilles numériques

Élément	Menaces
	• Défauts de conception et vulnérabilités logicielles non corrigées dans les terminaux de paiement, les systèmes POS et les passerelles de paiement vers/depuis les acquéreurs.
Émetteurs	• Compromission des systèmes de traitement des paiements: en demandant des jetons et des cryptogrammes au réseau de paiement de l'émetteur, un pirate peut obtenir une grande quantité de données sur les titulaires de cartes en installant des logiciels malveillants et des outils d'accès à distance sur n'importe lequel des serveurs de traitement des paiements du réseau interne. • Compromission de la sécurité du réseau et de l'interface: les attaquants peuvent exploiter des connexions point à point non sécurisées entre l'acquéreur et l'émetteur en compromettant le fournisseur de réseau; les attaquants peuvent alors utiliser ce niveau d'accès pour être en mesure de surveiller et de manipuler les appels API.

La communication entre l'appareil/l'application et le prestataire de services de paiement repose principalement sur le canal Internet via les réseaux WiFi, IMT-2000, IMT évoluées et IMT-2020, et/ou un paiement peut être affecté à un dispositif de point de vente du commerçant par transmission magnétique sécurisée, par balayage d'un code QR ou par NFC. L'utilisation de ces canaux présente d'autres menaces et éléments (points de vente, acquéreurs, fournisseurs de réseaux de paiement, émetteurs de cartes, fournisseurs de paiements mobiles). Sur la base de ces éléments, ce paragraphe identifie les menaces suivantes pour l'écosystème DFS basé sur les applications mobiles et les portefeuilles.

Sur la base des parties prenantes de l'écosystème DFS, ce paragraphe considère les commerçants, les acquéreurs, les prestataires de services de paiement et les émetteurs comme des fournisseurs tiers dans la Figure A.1. Bien que ce paragraphe énumère les menaces générales auxquelles ces entités sont confrontées, les mesures d'atténuation spécifiques pour faire face aux menaces auxquelles elles sont confrontées n'entrent pas dans le champ d'application du présent document.

11 Cadre d'assurance de la sécurité du SFN

Le cadre d'assurance de la sécurité du SFN suit des principes similaires à ceux de la famille ISO/IEC 27000 – Systèmes de gestion de la sécurité de l'information, [b-ISO/IEC 27000], Payment Card Industry Data Security Standard (PCI-DSS) v3.2, Payment Applications Data Security Standards (PA-DSS), [b-pci-dss], National Institute of Standards and Technology Special Publication 800-53, Revision [b-nist-800-63], [b-REPORT]. Lignes directrices techniques du Centre for Internet Security (CIS controls Version 7) [b-cis], et de l'Open Web Security Application Project (OWASP), communément appelées OWASP Top 10 [b-OWASP]. Ces normes servent de référence pour identifier les contrôles propres à l'écosystème des services financiers numériques.

Ce cadre se compose des éléments suivants:

- une évaluation des risques de sécurité basée sur la norme [ISO/IEC 27005], décrite dans le paragraphe 12;
- une évaluation des menaces et des vulnérabilités de l'infrastructure sous-jacente, des applications SFN, des services, des opérations de réseau et des fournisseurs tiers impliqués dans l'écosystème pour la fourniture de SFN, décrite dans le paragraphe 13;
- des stratégies d'atténuation basées sur les résultats de l'évaluation des menaces et des vulnérabilités ci-dessus, qui est décrite dans le paragraphe 13.

Ce cadre permet d'identifier:

- les différentes menaces de sécurité pesant sur les actifs SFN dans chacune des huit dimensions de sécurité [UIT-T X.805];
- les vulnérabilités associées qui peuvent être exploitées par ces menaces;
- des contrôles de sécurité pouvant être mis en œuvre par les parties prenantes du SFN contre les menaces et les vulnérabilités sont proposés. La mesure de contrôle de la sécurité peut relever d'une ou de plusieurs des huit dimensions de la sécurité.

12 Processus de gestion des risques de sécurité

Afin de garantir un modèle de sécurité durable et d'améliorer continuellement la sécurité de la SFN, ce cadre utilise le modèle de qualité en quatre étapes présenté en Figure 10. Il est divisé en quatre phases: planifier, faire, vérifier et agir (PDCA). Dans le processus de gestion basé sur le PDCA, les activités et les résultats qui doivent être atteints dans chacune des quatre phases sont identifiés. Dans l'écosystème SFN, de multiples parties prenantes sont impliquées et le PDCA est conçu avec des activités qui assurent la sécurité globale de bout en bout de l'écosystème SFN. La Figure 10 montre le modèle de cadre de sécurité SFN basé sur le PDCA.

Le suivi et l'examen de l'environnement SFN peuvent prendre différentes formes en fonction de la partie prenante, par exemple l'autorité de régulation examinant les contrôles de sécurité mis en place par le fournisseur SFN pour assurer la sécurité des utilisateurs SFN ou les examens internes et externes de l'environnement SFN par les auditeurs. Ainsi, la phase de suivi traite également de l'escalade et de la notification des risques aux parties prenantes concernées.

La communication avec la direction durant toutes les phases du processus de gestion des risques permet de comprendre et de s'approprier les rôles et les responsabilités, ce qui est essentiel pour établir le contexte de manière appropriée, l'identification adéquate des risques, l'analyse et l'évaluation des risques par les différentes parties prenantes. La communication avec la direction constitue une plate-forme pour une consultation plus large et un examen du processus avec toutes les parties prenantes du SFN, ce qui permet d'obtenir l'approbation et le soutien des plans de traitement des risques sur la base d'une vision pertinente et précise des risques au sein de l'écosystème.

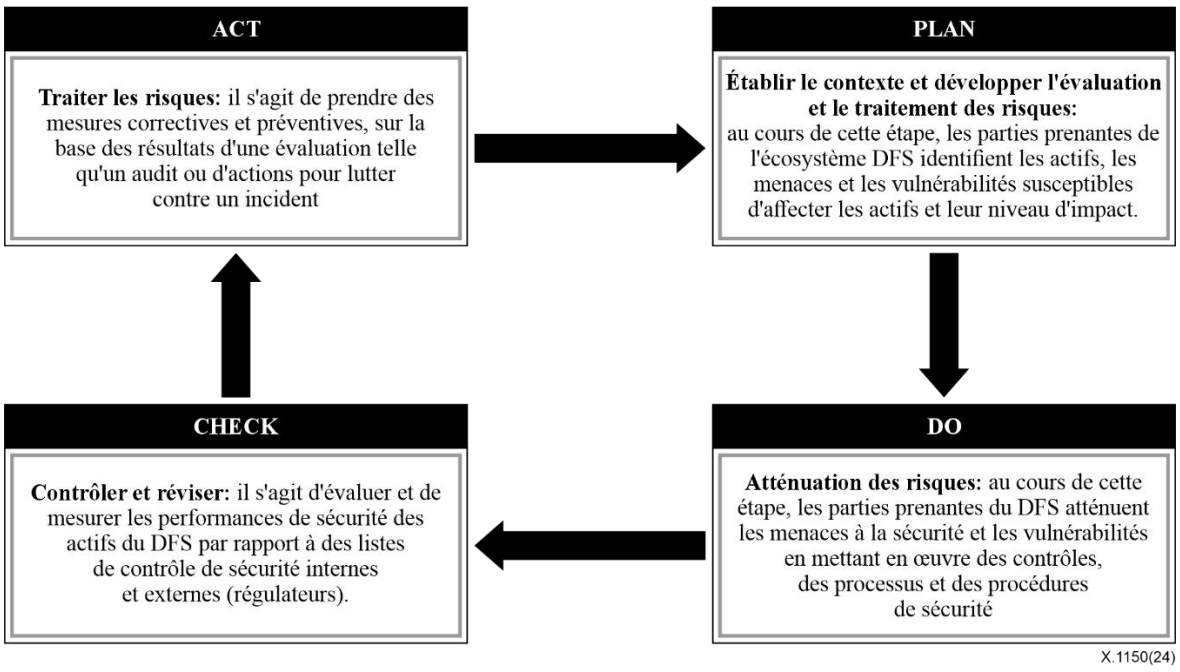

Figure 10 – Planifier, faire, vérifier, agir (PDCA)

La Figure 11 présente un plan de processus de gestion des risques de haut niveau, qui englobe les quatre phases du PDCA.

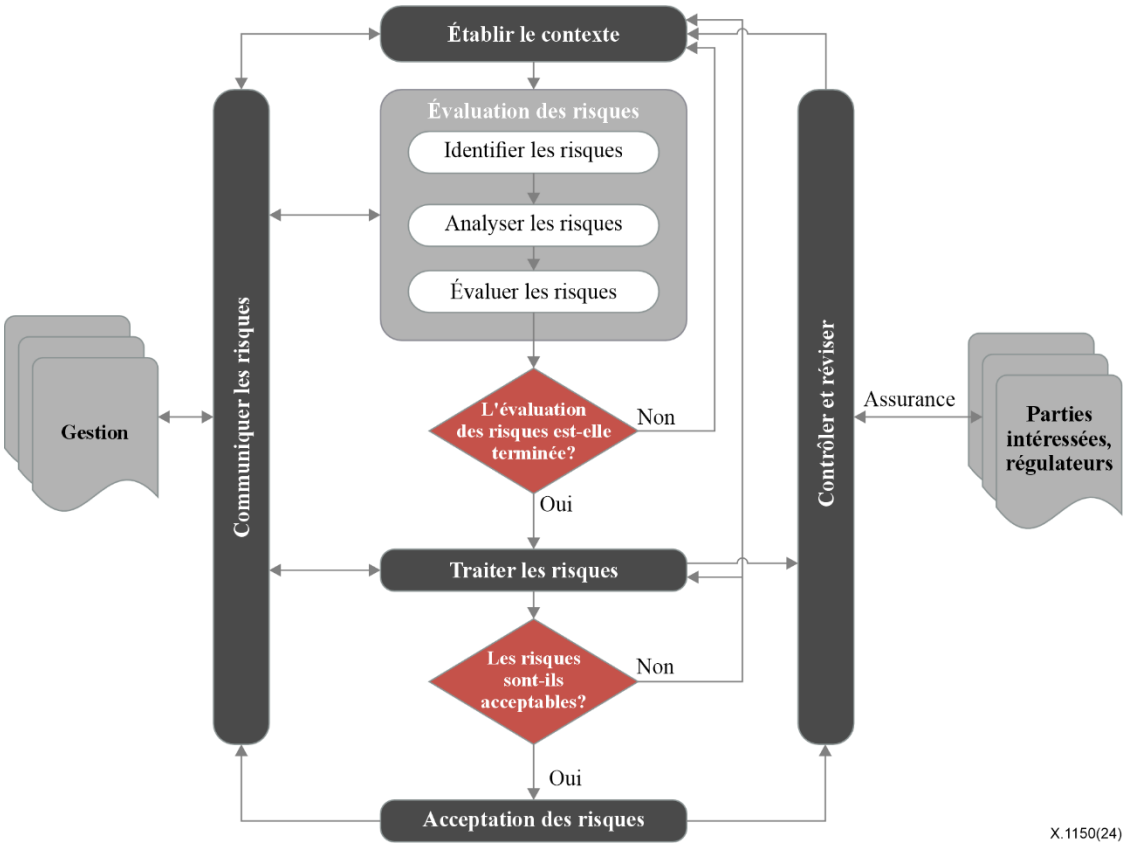

Figure 11 – Processus de gestion des risques de sécurité

12.1 Vue d'ensemble

Le cadre d'assurance de la sécurité SFN s'applique aux parties prenantes de l'écosystème SFN. Il définit les contrôles de sécurité à adopter par les utilisateurs de services financiers numériques, les opérateurs de réseaux mobiles, les fournisseurs, y compris les banques et les autres institutions financières non bancaires agréées, qui fournissent des produits et des services financiers par voie numérique.

Pour l'utilisateur, le cadre se concentre sur les contrôles de sécurité des appareils tels que les téléphones mobiles utilisés pour accéder aux services financiers numériques. Les moyens et la technologie sont généralement fournis par un opérateur de réseau mobile qui permet la communication entre l'utilisateur et le fournisseur SFN. Le cadre se concentre sur ce que le fournisseur de réseau de communication doit faire pour sécuriser l'écosystème.

Ce cadre comprend également les contrôles à mettre en place par le fournisseur de services financiers numériques, qui peut être une institution financière telle qu'une banque ou un fournisseur non bancaire; dans certains cas, le fournisseur de réseau de communication est également le fournisseur de services financiers numériques.

12.2 Établir un contexte

Il s'agit de l'étape initiale du processus de gestion des risques, dont l'objectif est de permettre à la partie prenante de comprendre l'environnement opérationnel du SFN. Il s'agit d'identifier les événements internes et externes qui affectent la capacité à assurer la sécurité de bout en bout. Il est donc important pour la partie prenante de comprendre et d'évaluer le contexte interne et externe dans

lequel les services financiers numériques opèrent, ce qui permet également de délimiter le champ d'application de l'évaluation des risques.

Afin d'établir le contexte interne, les points suivants doivent être formulés:

- le système de gestion de la sécurité de l'information fondé sur les documents normatifs [b-ISO/IEC 27001] doit être pris en compte ou mis en œuvre;
- la structure globale de l'organisation des parties prenantes du SFN et la manière dont le SFN s'inscrit dans cette structure des organisations et de ses objectifs;
- les actifs du SFN comprennent la technologie de soutien et les systèmes d'information, l'infrastructure physique, les applications logicielles, le matériel, les réseaux d'agents, les dispositifs des clients/agents/commerçants qui sont utilisés pour accéder au SFN;
- contrôles internes existants, événements antérieurs liés aux risques de sécurité, incidents de fraude antérieurs, rapports d'audit antérieurs et documents relatifs au projet SFN;
- exigences réglementaires;
- la tolérance et l'appétence au risque.

Le contexte externe prend en compte, entre autres, les éléments suivants:

- lois et réglementations relatives aux services financiers numériques;
- principales parties prenantes du SFN;
- l'environnement politique et social, qui comprend des données démographiques telles que le niveau d'éducation de la population, l'utilisation d'appareils mobiles et le niveau de pénétration des téléphones intelligents dans la population cible;
- les alternatives concurrentes et les services complémentaires aux services financiers numériques;
- les risques émergents et leur influence, tant sur le service financier que sur les parties prenantes.

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

12.3 Évaluation des risques

L'évaluation des risques aide les parties prenantes à obtenir des mesures indicatives du niveau de sécurité actuel dans l'écosystème SFN. Le processus d'évaluation des risques de sécurité comprend l'identification, l'analyse et l'évaluation des risques. L'évaluation des risques SFN doit être effectuée périodiquement et les résultats doivent être communiqués à la direction.

La Figure 12 donne un aperçu du déroulement du processus.

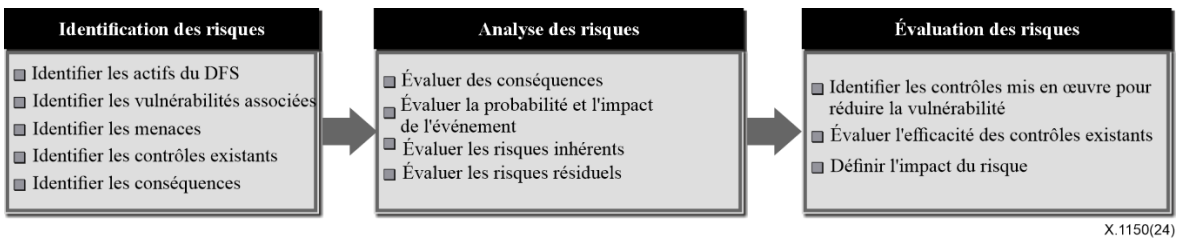

Figure 12 – Déroulement du processus d'évaluation des risques

12.3.1 Identification des risques

L'identification des risques consiste à déterminer quoi, comment, où et pourquoi les vulnérabilités du SFN pourraient être exploitées, ce qui implique d'identifier les actifs critiques du SFN, les menaces et vulnérabilités associées, la probabilité d'occurrence, les faiblesses des contrôles existants, l'impact

ou les conséquences des menaces et vulnérabilités lorsqu'elles sont exploitées. Dans le cadre du processus d'identification des risques, la partie prenante doit prendre connaissance des considérations internes et externes décrites au § 7.2.

Lors de l'identification des risques, les parties prenantes du SFN doivent prendre en compte cinq actions essentielles:

- **Identification des actifs**: il s'agit de dresser la liste de tous les actifs de l'écosystème SFN et de déterminer qui en est responsable. Les actifs SFN comprennent, entre autres, l'infrastructure physique, les applications logicielles, le matériel, l'équipement des agents, les appareils des clients/agents/commerçants utilisés pour accéder aux services SFN et les appareils du réseau de communication. L'identification permet à la partie prenante de classer les actifs SFN en fonction de l'impact qu'un incident sur l'actif aura sur l'écosystème SFN, la classification vise à classer les actifs en fonction de leur valeur et de leur criticité pour l'écosystème SFN.
- **Identification des vulnérabilités**: une vulnérabilité est une faiblesse ou un défaut qui permet à une menace d'attaquer un bien. Il peut s'agir, entre autres, de faiblesses au niveau de l'agencement physique, des procédures d'organisation, du personnel, de la gestion, du matériel, des logiciels, du réseau, etc. Ils peuvent être exploités par une menace, ce qui peut nuire au système ou l'endommager. Les vulnérabilités identifiées doivent être mises en évidence dans l'évaluation des risques, au même titre que les menaces qui pèsent sur un actif.
- **Identification des menaces**: une menace est la possibilité pour une source d'exploiter (accidentellement ou intentionnellement) une vulnérabilité spécifique. Les menaces qui pèsent sur les actifs du SFN peuvent être naturelles, par exemple les tremblements de terre et les inondations, humaines, par exemple le vol et la fraude ou les menaces techniques par exemple les logiciels malveillants ou les pannes de serveur. Une fois la menace identifiée, tous les actifs informationnels doivent être analysés afin de découvrir toute vulnérabilité présente susceptible d'être exploitée par la menace.
- **Identification des contrôles existants**: une liste de tous les contrôles existants et prévus, leur état de mise en œuvre et d'utilisation.
- **Identification conséquente**: l'ampleur des dommages qui pourraient être causés par un incident ou une menace réussissant à exploiter une vulnérabilité. Ce processus permet d'identifier les actifs susceptibles d'être affectés et la gravité de l'impact. Dans la plupart des cas, l'ampleur des dommages subis par un actif du SFN est supérieure au simple coût de remplacement. Il existe diverses considérations relatives aux dommages, qui peuvent être d'ordre monétaire, technique, humain et réglementaire.

12.3.2 Analyse des risques

L'analyse des risques permet de comprendre la probabilité et l'impact de la menace sur un actif. Ces deux éléments sont importants pour la prise de décision et pour la hiérarchisation des actions visant à faire face aux risques les plus critiques et aux risques significatifs (risques ayant l'impact le plus important). Le résultat de l'analyse des risques est un registre des risques mis à jour qui comprend les évaluations de la probabilité et de l'impact de chaque risque, L'analyse des risques peut être effectuée de manière quantitative ou qualitative, ou une combinaison des deux.

Le processus suivant devrait être le résultat de la phase d'analyse des risques:

- Évaluation des conséquences: il convient d'évaluer l'impact sur l'activité de l'organisation qui pourrait résulter d'incidents possibles ou réels en matière de sécurité de l'information, en tenant compte des conséquences d'une violation de la sécurité de l'information, telles que la perte de confidentialité, d'intégrité ou de disponibilité des actifs. Les conséquences en matière de sécurité pour les SFN peuvent notamment se traduire par des pertes financières, une atteinte à la réputation, une perte de clientèle, des interdictions réglementaires et des amendes.

- Évaluation de la probabilité d'occurrence d'une menace potentielle susceptible d'exploiter la vulnérabilité et de son impact en cas de succès. La probabilité d'occurrence doit tenir compte des contrôles préventifs et de détection en place, de leur efficacité, de leur mise en œuvre et de leur utilisation.
- Définition de l'évaluation du risque inhérent en tant que produit de la probabilité et de l'impact. L'objectif de l'évaluation du risque inhérent est d'aider la direction à hiérarchiser les mesures de gestion pour faire face aux risques les plus importants.
- Définition du risque résiduel par l'évaluation de l'efficacité des contrôles existants pour traiter le risque. Les contrôles mis en œuvre doivent permettre de ramener les risques à un niveau acceptable en fonction de l'appétence au risque des parties prenantes du SFN.

12.3.3 Évaluation des risques

Au cours du processus d'évaluation des risques, la partie prenante du SFN comparera les risques identifiés et les évaluera par rapport à des critères de risque prédéterminés afin de déterminer l'effet net des risques sur l'écosystème SFN. Il s'agit également de déterminer l'efficacité des contrôles existants, c'est-à-dire d'analyser la probabilité et l'impact des risques après avoir pris en compte les contrôles existants, puis d'estimer les risques résiduels. Ce processus permet d'établir des priorités et de prendre des décisions concernant le traitement et la mise en œuvre des risques.

Lors de l'évaluation des risques, les éléments suivants doivent être pris en compte:

- déterminer l'efficacité des contrôles en place pour chaque combinaison de menaces et de vulnérabilités pour une catégorie d'actifs, c'est-à-dire l'efficacité des contrôles en place qui permettraient d'atténuer la combinaison de menaces et de vulnérabilités;
- déterminer l'impact du risque;
- déterminer l'évaluation du risque résiduel en tant que produit de la probabilité d'occurrence et de l'impact.

13 Évaluation des vulnérabilités, des menaces et des exigences de contrôles d'atténuation dans le cadre de la sécurité du SFN

Afin de contrer systématiquement les menaces et les vulnérabilités de l'écosystème SFN décrites dans les paragraphes ci-dessus, ce paragraphe prévoit des contrôles pour chacune des entités de l'écosystème sur la base des huit dimensions de sécurité visant à assurer une sécurité de bout en bout.

Parce qu'il y a souvent des points communs dans les menaces auxquelles sont confrontées des entités dans l'ensemble de l'écosystème DFS, pour faciliter la discussion, cette clause examine d'abord une menace standardisée qui est identifiée, l'entité affectée par la menace générale, les vulnérabilités, les risques et les mesures d'atténuation et de contrôle proposées qui peuvent être déployées par cette entité particulière. Ce paragraphe identifie les vulnérabilités dans le contexte de leur impact sur les dimensions de sécurité [UIT-T X.805].

La Figure 13 montre comment les menaces pour la sécurité identifiées précédemment dans la Figure 9 sont mises en correspondance avec les 119 contrôles de sécurité décrits dans les § 13.1 à 13.17.

NOTE – Le numéro de paragraphe de la présente Recommandation dans la Figure 13 apparaît entre parenthèses pour indiquer l'endroit où le contrôle pertinent est abordé.

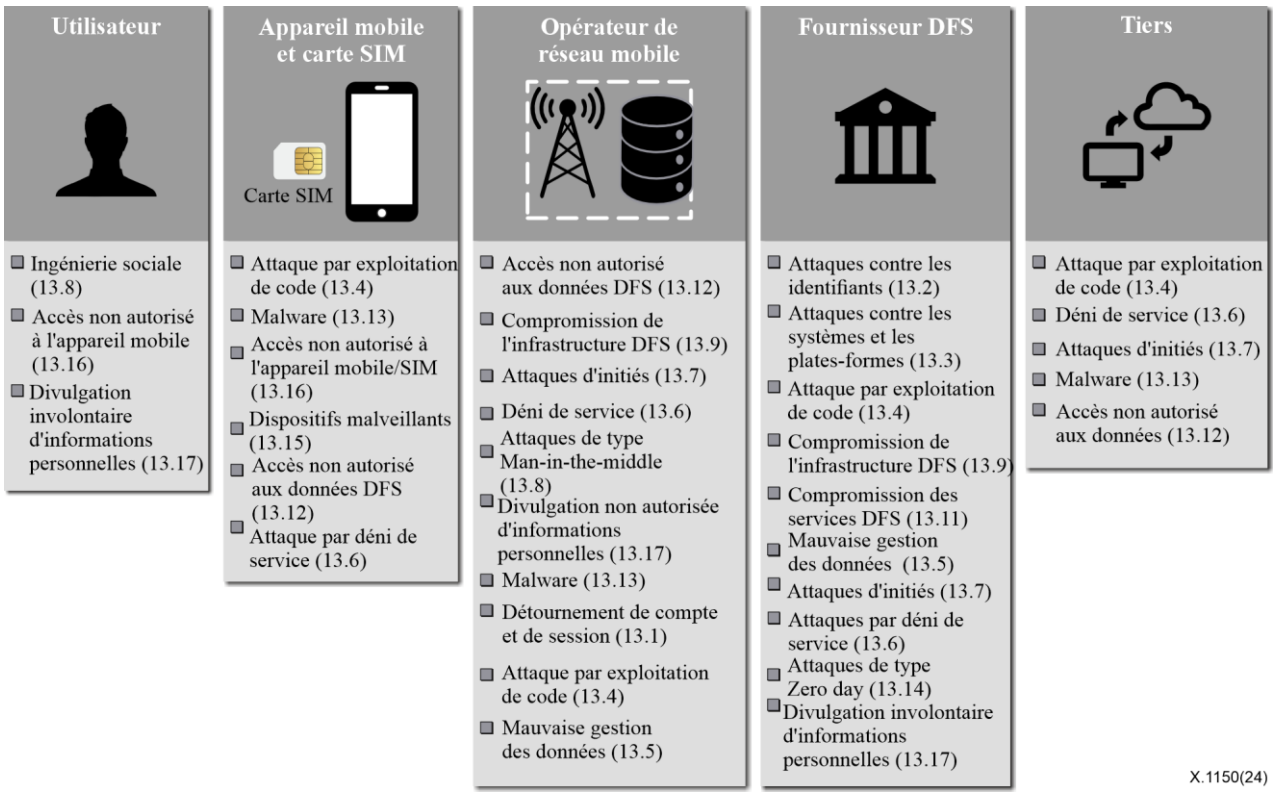

Figure 13 – Correspondance entre les menaces et les contrôles de sécurité

13.1 Menace: détournement de compte et de session

La menace générale ici est la capacité d'un attaquant à prendre le contrôle d'un compte ou d'une session de communication. Les vulnérabilités se manifestent de différentes manières au niveau du fournisseur de services de téléphonie mobile et de l'opérateur de réseau mobile. Le Tableau 2 résume les risques, les vulnérabilités et les contrôles pour le fournisseur SFN et l'ORM.

Tableau 2 – Synthèse des risques, des vulnérabilités et des contrôles pour le fournisseur de services SFN et l'ORM

Entité concernée	Risques et vulnérabilités	Exigences de contrôles
Prestataire SFN	Le risque ***d'exposition et de modification des données*** est dû à la vulnérabilité suivante: – Contrôles inadéquats des sessions d'utilisateurs (SD: access control).	**C1**: le système SFN devrait définir les délais d'attente et la déconnexion automatique des sessions utilisateur sur les applications SFN (sessions logiques). Dans l'application, assurer la prise en charge de la complexité du mot de passe (appliquée par le serveur), fixer le nombre maximal de tentatives de connexion infructueuses, l'historique du mot de passe et les périodes de réutilisation, les périodes de verrouillage du compte à une valeur minimale raisonnable afin de réduire au minimum le potentiel d'attaque hors ligne.
	Le risque de ***prise de contrôle non autorisée d'un compte*** est dû à la vulnérabilité suivante: – Contrôles inadéquats sur les comptes dormants (SD: authentification).	**C2**: le système SFN devrait exiger la validation de l'identité de l'utilisateur pour les comptes SFN dormants avant de réactiver les comptes.
	Le risque qu'un ***attaquant se fasse passer pour un utilisateur autorisé*** est dû aux vulnérabilités suivantes:	

Tableau 2 – Synthèse des risques, des vulnérabilités et des contrôles pour le fournisseur de services SFN et l'ORM

Entité concernée	Risques et vulnérabilités	Exigences de contrôles
	– Absence de validation de la localisation géographique (SD: sécurité des communications).	**C3**: le système SFN devrait limiter l'accès aux services SFN en fonction de la localisation de l'utilisateur (par exemple, désactiver l'accès aux codes USSD SFN en itinérance, aux STK et aux SMS pour les commerçants et les agents), si possible restreindre l'accès par région pour les agents SFN, si possible vérifier que l'agent et le numéro effectuant un dépôt ou un retrait se trouvent dans la même zone de desserte.
	– Vérification inadéquate par l'utilisateur des canaux de communication préférés de l'utilisateur pour les services SFN (SD: sécurité des communications).	**C4**: le système SFN devrait restreindre les services SFN en fonction des canaux de communication (lors de l'enregistrement, les clients doivent choisir le canal d'accès au service, USSD uniquement, STK uniquement, application uniquement, ou une combinaison); les tentatives d'accès SFN par des canaux autres que ceux choisis doivent être bloquées et signalées par un drapeau rouge.
	Le risque ***d'accès non autorisé aux données et aux informations d'identification de l'utilisateur*** est dû aux vulnérabilités suivantes:	
	– Reprise de la session sur la base des jetons interceptés (SD: sécurité des communications).	**C5**: le système SFN ne doit pas faire confiance aux jetons d'authentification ou d'autorisation côté client; la validation des jetons d'accès doit être effectuée côté serveur.
	– Algorithmes de cryptage faibles pour le stockage des mots de passe (SD: confidentialité des données).	**C6**: le système SFN devrait stocker les mots de passe SFN à l'aide d'algorithmes de hachage cryptographique fortement salés.
MNO	Le risque d'***usurpation d'identité des utilisateurs autorisés*** est dû à la vulnérabilité suivante: – Délais de session non spécifiés pour les services SFN.	**C7**: le système SFN devrait ajouter des délais de session pour l'accès aux services SFN par USSD, SMS, application et web.
	Le risque d'***accès non autorisé aux données et aux informations d'identification de l'utilisateur*** est dû à la vulnérabilité suivante: – Les informations d'identification de l'utilisateur pour l'application SFN sont envoyées par des moyens intrinsèquement peu sûrs tels que les SMS ou par l'intermédiaire d'agents (SD: confidentialité des données).	**C8**: dans la mesure du possible, les utilisateurs du système SFN doivent définir leurs propres mots de passe lors de l'enregistrement et ceux-ci doivent être cryptés tout au long de la transmission au système SFN. Lorsque les identifiants sont envoyés pour la première fois aux utilisateurs, s'assurer que les identifiants de l'application SFN sont envoyés aux utilisateurs directement, sans tiers/agents. Les utilisateurs devraient alors être tenus de définir de nouveaux mots de passe après la première connexion.

13.2 Menace: attaques contre les informations d'identification

Ces menaces sont généralement caractérisées comme étant celles conçues pour voler ou falsifier les informations d'identification des utilisateurs des systèmes SFN et des appareils mobiles. Le Tableau 3 résume les risques, les vulnérabilités et les contrôles pour le dispositif mobile et le fournisseur SFN.

Tableau 3 – Résumé des risques, des vulnérabilités et des contrôles pour les appareils mobiles et le fournisseur SFN

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
Appareil mobile	Le risque d'***accès non autorisé et de prise de contrôle du compte SFN d'un utilisateur*** est dû aux vulnérabilités suivantes:	
	– Utilisation de mots de passe/PIN faibles au niveau de l'application, rendant ces informations d'identification susceptibles d'être soumises à des attaques par force brute (SD: authentification).	**C9**: les applications SFN devraient exiger l'utilisation de PIN/mots de passe plus longs et difficiles à deviner dans les applications d'argent mobile. Il convient d'être prudent avant d'imposer l'utilisation de codes PIN complexes; il faut veiller à ce que l'adoption de ces codes aille de pair avec la formation des utilisateurs, car les codes PIN trop complexes sont susceptibles d'être écrits ou saisis par d'autres personnes, ce qui nuit à leur sécurité.
	– Utilisation de simples codes PIN pour accéder à l'appareil mobile (SD: authentification).	**C10**: les applications SFN devraient utiliser des mécanismes d'authentification robustes pour démontrer la propriété du dispositif. Étant donné que l'espace de clés des codes PIN les rend sensibles à une attaque par force brute, envisagez d'utiliser des codes PIN plus longs ou alphanumériques, tels que des phrases de passe faciles à mémoriser.
	Le risque de ***vol d'informations d'identification par le biais d'attaques de type* "man in the middle"** est dû à la vulnérabilité suivante: – Mauvaise configuration du serveur (SD: authentification).	**C11**: les applications SFN doivent être conçues pour vérifier le nom du serveur auquel elles se connectent.
Prestataire SFN	Le risque de ***compromission du système SFN*** est dû à la vulnérabilité suivante: – Absence de contrôle des connexions, ce qui rend les systèmes vulnérables aux attaques par force brute (DS: contrôle d'accès).	**C12**: les applications SFN devraient appliquer un nombre maximum de tentatives de connexion aux comptes SFN pour les utilisateurs du système dorsal, les commerçants, les agents et les clients SFN sur les systèmes SFN (base de données, système d'exploitation, application).

13.3 Menace: attaques contre les systèmes et les plates-formes

Ces attaques sont caractérisées par le fait qu'un adversaire distant peut espionner ou modifier des informations sans disposer d'identifiants d'initiés ou d'autres accès privilégiés. Le Tableau 4 résume les risques, les vulnérabilités et les contrôles pour l'appareil mobile, l'ORM et le fournisseur SFN.

Tableau 4 – Résumé des risques, des vulnérabilités et des contrôles pour l'appareil mobile, l'ORM et le fournisseur SFN

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
Utilisateur mobile	Le risque d'***espionnage et de vol à distance d'informations d'identification sur les appareils des utilisateurs*** est dû aux vulnérabilités suivantes:	
	– Mises à jour de SIM par SMS binaires malveillants non vérifiés (SD: authentification).	**C13**: les fournisseurs de SFN devraient fournir à l'utilisateur mobile la possibilité de faire confiance ou de se méfier des messages SMS binaires individuels. Cela pourrait empêcher les mises à jour malveillantes de la carte SIM.
MNO	– Transfert non sécurisé des données d'identification des clients (SD: contrôle d'accès).	**C14**: les fournisseurs de SFN doivent transmettre les informations d'authentification de l'utilisateur de manière sécurisée sur un canal différent (hors bande).
	Les risques d'***accès et de compromission des comptes et de déni de service*** sont dus à la vulnérabilité suivante: – Exposition du réseau interne à des adversaires externes (SD: contrôle d'accès).	**C15**: les fournisseurs de SFN devraient utiliser la traduction d'adresses réseau pour limiter l'exposition externe de l'adresse IP du SFN et les informations de routage.
Prestataire SFN	Les risques d'***accès au compte, de compromission et de déni de service*** sont dus à la vulnérabilité suivante: – Protection insuffisante des systèmes internes contre les adversaires extérieurs (SD: contrôle d'accès).	**C16**: les fournisseurs de SFN devraient éviter l'accès direct des systèmes externes aux systèmes dorsaux SFN en mettant en place une zone démilitarisée (DMZ) qui sépare logiquement le système SFN de tous les autres systèmes internes et externes.

13.4 Menace: attaques par exploitation de code

Ces attaques sont caractérisées par le fait qu'elles visent le code des applications SFN compromettantes. Le Tableau 5 résume les risques et les vulnérabilités ainsi que les contrôles pour le prestataire SFN.

Tableau 5 – Synthèse des risques, des vulnérabilités et des contrôles pour le prestataire SFN

Entité concernée	Risques et vulnérabilités	Exigences de contrôles
Prestataire SFN	Le risque de ***compromission de l'application SFN*** est dû à la vulnérabilité suivante: – Dépendance de l'application SFN à l'égard des bibliothèques de sécurité offertes par les systèmes d'exploitation (SD: sécurité des communications)	**C17**: les fournisseurs de SFN devraient s'assurer que les bibliothèques de sécurité proposées par le système d'exploitation sont correctement conçues et mises en œuvre et que les suites de chiffrement qu'elles prennent en charge sont suffisamment solides.

13.5 Menace: utilisation abusive des données

Cette menace est caractérisée comme étant liée à la mauvaise manipulation des données sensibles des clients [b-REPORT]. Le Tableau 6 résume les risques, les vulnérabilités et les contrôles pour l'ORM, le fournisseur SFN et les fournisseurs tiers.

Tableau 6 – Résumé des risques, des vulnérabilités et des contrôles pour l'ORM, le fournisseur SFN et les fournisseurs tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
MNO	Les risques d'***accès non autorisé*** *aux données des utilisateurs et d'****interception des données en transit*** sont dus à la vulnérabilité suivante: – Faibles pratiques de cryptage ou envoi d'informations sensibles en texte clair sur des canaux de communication non sécurisés tels que les SMS et les USSD (SD: sécurité des communications).	**C18**: les fournisseurs de SFN devraient veiller à ce que toutes les données sensibles des consommateurs, telles que les codes PIN et les mots de passe, soient cryptées lorsqu'elles traversent le réseau et lorsqu'elles sont au repos.
Prestataire SFN et prestataires tiers	Le risque ***d'exposition des données sensibles*** est dû aux vulnérabilités suivantes:	
	– Contrôles inadéquats de la protection des données (SD: vie privée).	**C19**: les fournisseurs de SFN devraient supprimer les données sensibles des clients des journaux de suivi. Les codes des bons de retrait, les numéros de compte bancaire et les informations d'identification sont des exemples de données qui doivent être supprimées. Au lieu de cela, utiliser, dans la mesure du possible, des caractères de remplacement pour représenter ces données dans les journaux.
	– Exposition d'informations sensibles sur les clients lors de transactions ou par le biais d'API (SD: vie privée).	**C20**: les prestataires de services SFN devraient limiter le partage d'informations au minimum requis pour les transactions avec les tiers et les prestataires de services.
	– Faible cryptage des interfaces API (SD: vie privée).	**C21**: les fournisseurs de SFN devraient contrôler l'utilisation des API et crypter toutes les données partagées avec des tiers. En outre, mettre en place des procédures de gestion des données et des contrôles tels que la signature d'accords de non-divulgation avec les prestataires de services de paiement afin d'éviter les fuites d'informations ou de données.

13.6 Menace: attaques par déni de service (DoS)

Ces attaques sont caractérisées par le fait qu'elles sont conçues pour empêcher l'offre de services au sein de l'écosystème SFN. Le Tableau 7 résume les risques et les vulnérabilités ainsi que les contrôles pour les ORM et les fournisseurs SFN.

Tableau 7 – Résumé des risques, des vulnérabilités et des contrôles pour les ORM et les prestataires SFN

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
MNO	Les risques d'***incapacité à effectuer une transaction en raison d'une panne de service*** et d'***échec de la transaction en raison de retards importants*** sont dus aux vulnérabilités suivantes:	

Tableau 7 – Résumé des risques, des vulnérabilités et des contrôles pour les ORM et les prestataires SFN

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
	– Défaillance du réseau due à une capacité insuffisante, à la maintenance ou à la conception (DS: disponibilité).	**C22**: l'opérateur de réseau mobile doit prendre des mesures pour assurer la haute disponibilité du réseau afin de permettre l'accès aux services SFN par USSD, SMS et Internet.
		C23: l'ORM doit effectuer des tests de capacité technique en simulant différentes transactions sur la base du nombre de clients, de la croissance prévue, du nombre de transactions prévues et des périodes de pointe prévues, afin de garantir la continuité des performances du système.
Prestataire SFN	– Absence de surveillance du trafic réseau et des paquets réseau individuels (SD: disponibilité, sécurité des communications).	**C24**: le fournisseur SFN doit se protéger contre les attaques du réseau en utilisant des pare-feu et des filtres de trafic et se protéger contre les menaces de l'infrastructure SFN en contestant le trafic suspect par des techniques d'admission au réseau et des mécanismes tels que les CAPTCHA.
	Les risques d'***accès non autorisé*** *aux données des utilisateurs sont* également dus à la vulnérabilité suivante: – Permettre des services inutiles (SD: confidentialité des données).	**C25**: le trafic internet entrant doit être limité et contrôlé en permanence.
		C26: les fournisseurs de SFN devraient définir des règles de pare-feu restrictives par défaut, utiliser la liste blanche des ports, utiliser des filtres de paquets et surveiller en permanence l'accès aux ports et aux IP figurant sur la liste blanche/autorisés.

13.7 Menace: attaques d'initiés

Ces attaques sont caractérisées par le fait qu'elles sont menées par des adversaires à l'intérieur du périmètre de l'organisation, qui disposent souvent d'un accès et de privilèges élevés aux ressources. Le Tableau 8 résume les risques, les vulnérabilités et les contrôles pour les prestataires SFN.

Tableau 8 – Résumé des risques, des vulnérabilités et des contrôles pour les prestataires SFN

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
Prestataire SFN	Le risque d'***exposition et de modification des données*** est dû aux vulnérabilités suivantes:	
	– Contrôles internes insuffisants sur les opérations critiques (SD: contrôle d'accès).	**C27**: dans la mesure du possible, limiter les changements critiques en appliquant le principe des quatre yeux (règle de l'auteur, du vérificateur et des deux personnes) pour les actions critiques, notamment (mais pas exclusivement) la création, la modification ou la suppression par un administrateur d'un autre compte d'administrateur, la modification, l'attachement et le détachement d'un compte SFN d'un numéro de téléphone mobile/d'un identifiant d'utilisateur et l'annulation d'une transaction.
	– Absence de validation des données saisies (SD: intégrité des données).	**C28**: les fournisseurs de SFN doivent garantir une séparation suffisante des tâches entre le créateur et l'approbateur; par exemple, un administrateur ne peut pas avoir les droits d'accès pour créer et activer un compte SFN.

Tableau 8 – Résumé des risques, des vulnérabilités et des contrôles pour les prestataires SFN

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
	– Gestion insuffisante des privilèges (SD: contrôle d'accès).	**C29**: les fournisseurs de SFN devraient limiter, contrôler et surveiller l'accès physique à l'infrastructure SFN sensible. Isoler physiquement et mettre en place des mesures de dissuasion/barrières logiques et physiques entre l'infrastructure SFN et les autres infrastructures. Employer des techniques de moindre privilège, de sorte que l'accès préventif n'est autorisé qu'aux personnes autorisées, remplacé par la détection et l'exécution (par exemple, alarmes en cas d'accès forcé). Contrôler l'activité du système en enregistrant tous les accès (par exemple, qui a accédé, à quoi il a accédé, d'où il a accédé et quand il a accédé).
	Les vulnérabilités suivantes entraînent un risque d'inexactitude et d'incohérence des données:	**C30**: le fournisseur SFN doit utiliser des routines de validation d'entrée robustes sur les services externes en vérifiant les valeurs hors plage et les caractères non autorisés dans les champs, ainsi qu'en contraignant et en assainissant les entrées. La validation des entrées doit intervenir le plus tôt possible et doit être effectuée à la fois du côté du client et du côté du serveur, mais le serveur ne doit pas s'appuyer uniquement sur la validation du côté du client. En outre, il bloque, consigne et examine toutes les demandes qui ne respectent pas le langage de description des services web (WSDL) et les schémas.
	– Ajout de données de test aux données de production (SD: intégrité des données).	**C31**: les fournisseurs de SFN devraient utiliser l'empreinte digitale de la base de données pour détecter l'altération et la modification des données après leur stockage. Des techniques telles que les signatures numériques sur les colonnes de la base de données peuvent être utilisées pour détecter la modification des données de l'utilisateur.
		C32: les fournisseurs de SFN devraient s'assurer que toutes les données de test sont retirées du code avant qu'il ne soit transféré dans l'environnement de production.
	– Absence de journalisation, possibilité de modifier les journaux et informations insuffisantes dans les journaux (SD: non-répudiation).	**C33**: les systèmes SFN doivent utiliser des mécanismes de journalisation, y compris la capture de la provenance des actions de l'utilisateur ou la journalisation des actions critiques dans un stockage inviolable, sécuriser les journaux du système SFN contre la falsification, l'édition, la suppression, l'arrêt. Utiliser les signatures numériques attachées aux actions, en particulier celles qui arrivent par le biais d'une connexion réseau.
	– Imprécis et horloges non synchronisées (SD: intégrité des données).	**C34**: Assurer la synchronisation de la précision de l'horloge sur tous les systèmes connectés au système SFN. NTP et SNTP sont quelques-uns des protocoles utilisés pour synchroniser l'heure avec précision, mais ils doivent être déployés de manière sécurisée.

13.8 Menace: attaques de type "Man-in-the-middle" et d'ingénierie sociale

Ces deux types d'attaques sont regroupés parce qu'ils impliquent tous deux qu'un adversaire s'interpose activement dans la communication ou l'interaction (par exemple, entre un utilisateur et un appareil ou un ORM, ou une interposition de communication entre les parties). Le Tableau 9 résume les risques, les vulnérabilités et les contrôles pour les utilisateurs mobiles, les ORM, les fournisseurs de services SFN et les fournisseurs tiers.

Tableau 9 – Résumé des risques, des vulnérabilités et des contrôles pour l'utilisateur mobile, l'opérateur de réseau mobile, les fournisseurs de services SFN et les fournisseurs tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
Utilisateur mobile	Le risque d'***exposition et de modification des données*** est dû aux vulnérabilités suivantes:	
	– Applications non vérifiées et non signées (SD: vie privée, intégrité des données).	**C35**: il est essentiel de guider le client pour qu'il accède aux applications SFN et les télécharge par l'intermédiaire des canaux officiels de diffusion des applications afin de réduire le risque d'exécution d'applications infectées par des logiciels malveillants.
	– Entrées non vérifiées telles que les messages SMS non sollicités, les publicités "in-app" ou les courriels (SD: intégrité des données).	**C36**: les ORM et les fournisseurs de services de téléphonie mobile devraient lancer des campagnes actives de sensibilisation des consommateurs et du personnel interne aux messages malveillants, aux attaques par hameçonnage et à l'usurpation d'identité (spoofing).
	– Protection insuffisante des données d'identification (SD: contrôle d'accès).	**C37**: les ORM et les fournisseurs de SFN devraient masquer les mots de passe et les codes PIN des utilisateurs, éduquer activement les clients sur le "shoulder surfing" et l'utilisation sûre des codes PIN et des mots de passe afin d'éviter l'espionnage par-dessus l'épaule et l'écriture des mots de passe.
MNO	Le risque d'***accès non autorisé aux données de l'utilisateur*** est dû à la vulnérabilité suivante: – Faiblesse du cryptage en direct (SD: sécurité des communications).	**C38**: les ORM devraient cesser d'utiliser les codes de chiffrement GSM A5/0, A5/1 et A5/2. Suivre de près les résultats de la communauté de la sécurité et de la cryptographie concernant la faisabilité et la facilité de compromettre A5/3 et A5/4 et commencer à envisager des algorithmes de chiffrement plus puissants. Préparer une stratégie de déploiement pour ces nouveaux algorithmes de chiffrement.
	Le risque d'***usurpation d'identité*** est dû à la vulnérabilité suivante: – Filtrage faible de l'identification de la ligne d'appel (SD: sécurité des communications).	**C39**: les ORM doivent procéder à une analyse CLI des appels/SMS afin de détecter les appels et les SMS susceptibles d'être usurpés pour ressembler à des appels de fournisseurs SFN.
Prestataire SFN	Le risque de ***prise de contrôle d'un compte d'utilisateur*** est dû à la vulnérabilité suivante: – Contrôles de configuration et d'autorisation des comptes manquants/insuffisants (SD: authentification).	**C40**: les fournisseurs de SFN devraient exiger l'authentification et l'autorisation de l'utilisateur pour les modifications de compte et les transactions à haut risque et refuser d'effectuer des transactions même lorsque l'appareil est connecté tant que la connaissance du code PIN ou du mot de passe n'a pas été démontrée.
Fournisseurs tiers	Le risque d'***exposition d'informations sensibles*** est dû aux vulnérabilités suivantes: – Faiblesse des algorithmes de cryptage utilisés pour les données stockées dans l'appareil et les données transmises (SD: vie privée).	**C41**: un cryptage suffisamment sûr doit être utilisé à la fois pour la protection des données au sein de l'application mobile et pour la communication avec les systèmes SFN dorsaux et, dans la mesure du possible, masquer, tronquer ou expurger les informations confidentielles des clients.

Tableau 9 – Résumé des risques, des vulnérabilités et des contrôles pour l'utilisateur mobile, l'opérateur de réseau mobile, les fournisseurs de services SFN et les fournisseurs tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
	– Absence de cryptage des communications (SD: sécurité des communications).	**C42**: les systèmes SFN devraient utiliser des signatures numériques pour identifier les tiers connectés au système SFN lorsque des transactions sont effectuées.
	– Gestion insuffisante des certificats ou des clés (SD: contrôle d'accès).	**C43**: seuls des clés et des certificats de confiance doivent être acceptés pour permettre l'échange de données entre les fournisseurs SFN et les tiers, et ils doivent être protégés contre la divulgation.
	Le risque d'***usurpation d'identité et d'échec des transactions*** est dû à la vulnérabilité suivante: – Défaillance du système du fournisseur SFN ou de l'ORM entraînant le retour à des processus hors ligne pour les agents/tiers (SD: disponibilité).	**C44**: les systèmes SFN devraient mettre en place des contrôles procéduraux et techniques pour une gestion efficace pendant les temps d'arrêt du système avec les prestataires de services concernés. Par exemple, mettre en place des contrôles pour gérer les transactions hors ligne (par exemple, les échanges de cartes SIM) lorsque l'accès au système SFN est intermittent. Effectuer des contrôles supplémentaires pour les remises et les paiements de tiers lorsque l'accès au système SFN ou au système de tiers est intermittent.

13.9 Menace: compromission de l'infrastructure SFN

Ces attaques visent l'infrastructure sous-jacente de l'écosystème SFN. Le Tableau 10 résume les risques, les vulnérabilités et les contrôles pour les fournisseurs SFN mobiles et les fournisseurs tiers.

Tableau 10 – Résumé des risques, des vulnérabilités et des contrôles pour les fournisseurs de services de dépôt de documents mobiles et les fournisseurs tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
Prestataire SFN	Le risque de ***compromission de l'infrastructure et des données*** est dû à la vulnérabilité suivante: – Contrôles d'accès non sécurisés et inadéquats sur les comptes d'utilisateurs (SD: contrôle d'accès).	**C45**: le système SFN devrait utiliser l'authentification multi-facteurs ou multi-modèles pour l'accès aux comptes SFN.
	Le risque d'***interruption de service et d'incapacité à effectuer des transactions*** est dû à la vulnérabilité suivante: – Pratiques de restauration non testées (SD: disponibilité).	**C46**: désactiver et supprimer les comptes et identifiants par défaut des bases de données, applications, systèmes d'exploitation et autres interfaces d'accès qui interagissent avec le système SFN de production.
		C47: le système SFN devrait examiner l'installation, le fournisseur, les comptes d'assistance et les points d'accès aux systèmes et à l'infrastructure SFN. Tous ces comptes doivent être désactivés ou attribués à des profils d'utilisateurs appropriés.
	Les risques ***d'exfiltration et de modification des données, de compromission de l'intégrité des transactions et d'interruption de***	**C48**: le fournisseur de SFN devrait effectuer des tests de bout en bout après toute modification apportée aux systèmes SFN, MNO, SP et tiers, et inclure des tests de régression et de capacité dans les tests d'acceptation.

Tableau 10 – Résumé des risques, des vulnérabilités et des contrôles pour les fournisseurs de services de dépôt de documents mobiles et les fournisseurs tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
	service sont dus à la vulnérabilité suivante:	Veiller également à ce qu'il y ait un plan de secours ou d'extinction.
	– Contrôles inadéquats des données, comme l'absence de mise en œuvre de l'atomicité des transactions, ce qui permet à celles-ci d'exister dans un état partiellement achevé (SD: intégrité des données).	**C49**: le fournisseur de SFN devrait effectuer des sauvegardes régulières et planifiées des systèmes SFN. Tester régulièrement les sauvegardes et les stocker en toute sécurité hors ligne et hors site sous une forme cryptée.
		C50: le fournisseur de SFN devrait utiliser la fonction ACID (atomicité, cohérence, isolation, durabilité) standard de la base de données pour garantir l'intégrité des transactions. Les opérations SFN doivent soit réussir complètement, soit échouer complètement. Le fournisseur SFN doit également veiller à ce que des contrôles soient effectués pour éviter les transactions en double (identifiants de transaction uniques, horodatage et utilisation d'un nonce cryptographique).
Fournisseur tiers	Le risque d'***incapacité de l'utilisateur à effectuer des transactions*** est dû à la vulnérabilité suivante: – Mécanismes inadéquats pour garantir l'intégrité des données et dépendance excessive à l'égard des points d'ancrage de confiance externes (SD: non-répudiation).	**C51**: les applications SFN et les tiers doivent prendre en charge l'utilisation de signatures numériques. Une signature numérique sécurisée fournit une preuve irréfutable de l'origine de la transaction. Les signatures numériques ne sont valables que tant que l'ICP n'a pas été compromise et doivent être testées dans le cadre de plans visant à garantir l'agilité. En démontrant que les clés de signature sont protégées de manière adéquate jusqu'à la clé racine, le fournisseur SFN peut résister aux contestations juridiques concernant l'authenticité d'un utilisateur spécifique et les transactions litigieuses.

13.10 Menace: attaques SIM

La menace générale est la capacité d'un attaquant à obtenir un accès non autorisé à la carte SIM d'un utilisateur SFN. Les vulnérabilités se manifestent de différentes manières au niveau de l'opérateur de réseau mobile, du fournisseur SFN et de l'utilisateur mobile. Le Tableau 11 résume les risques, les vulnérabilités et les contrôles pour l'ORM, les utilisateurs mobiles et les fournisseurs tiers.

Tableau 11 – Résumé des risques, des vulnérabilités et des contrôles pour les ORM, les utilisateurs de téléphones mobiles et les fournisseurs tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
MNO	Les risques de ***prise de contrôle d'un compte et de transactions non autorisées*** sont dus aux vulnérabilités suivantes: – Contrôles inadéquats de l'identification et de la vérification de	**C52**: les ORM doivent s'assurer qu'un processus de vérification de l'identité est en place avant de procéder à des échanges de cartes SIM.
		C53: l'identité de l'utilisateur doit être vérifiée en combinant ce qu'il est, ce qu'il détient ou ce qu'il sait. Par exemple, la présentation d'une pièce d'identité valide, la vérification biométrique et la connaissance des détails du compte SFN avant l'échange ou le remplacement de la carte SIM.

Tableau 11 – Résumé des risques, des vulnérabilités et des contrôles pour les ORM, les utilisateurs de téléphones mobiles et les fournisseurs tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
	l'utilisateur avant l'échange et le recyclage des cartes SIM (SD: authentification).	**C54**: les prestataires de services SFN et de paiement devraient être en mesure de détecter en temps réel tout échange ou remplacement d'une carte SIM avec des services SFN et effectuer des vérifications supplémentaires avant d'autoriser toute transaction de grande valeur ou tout changement de compte à l'aide de la nouvelle carte SIM.
	Les risques de ***prise de contrôle d'un compte et de transactions non autorisées*** sont dus aux vulnérabilités suivantes: – Contrôles inadéquats de l'identification et de la vérification de l'utilisateur avant l'échange et le recyclage des cartes SIM (SD: authentification).	**C55**: l'opérateur mobile doit sauvegarder et stocker en toute sécurité les données SIM telles que l'IMSI et les valeurs de la clé secrète SIM (valeurs KI).
		C56: il convient de mettre en place un processus de recyclage des numéros mobiles qui implique de communiquer avec les fournisseurs SFN sur les numéros d'identification d'abonné mobile (MSIDN) en cours de renouvellement ou de recyclage (dans ce contexte, on parle de recyclage des numéros lorsque l'ORM réattribue un numéro d'identification d'abonné mobile dormant/inactif (MSISDN) à un nouveau client). Lorsqu'une carte SIM est recyclée, l'opérateur mobile signale un nouvel IMSI pour le numéro de téléphone du compte correspondant. Le prestataire SFN doit bloquer le compte jusqu'à ce que l'identité de la nouvelle personne détenant la carte SIM soit vérifiée en tant que titulaire du compte.
Utilisateur mobile	Le risque d'***accès non autorisé aux données mobiles de l'utilisateur*** est dû à la vulnérabilité suivante: – Vol d'appareils mobiles (SD: confidentialité des données).	**C57**: les utilisateurs du SFN doivent avoir la possibilité d'effacer leurs données à distance sur un appareil mobile et de les crypter en cas de perte ou de vol de l'appareil.
Prestataire SFN	Le risque de ***perte d'accès aux comptes ou d'atteinte à la réputation*** est dû à la vulnérabilité suivante: – Insuffisances dans le processus d'échange et de recyclage des cartes SIM [b-ss7-12.5] (SD: intégrité des données).	**C58**: les fournisseurs SFN doivent s'assurer qu'ils ont mis en place des procédures permettant de détecter et d'éviter les échanges et les recyclages suspects de SIM en: – vérifiant si l'IMSI associé au numéro de téléphone a changé, ce qui indique un échange de cartes SIM. S'il y a une indication d'échange de carte SIM, vérifier l'IMEI du téléphone contenant la carte SIM. Si l'IMEI a également changé, il est fort probable que la carte SIM ait été échangée. Dans ce cas, le prestataire SFN doit bloquer le compte jusqu'à ce qu'il effectue les procédures de vérification du compte, par exemple, via un appel vocal ou un agent.

13.11 Menace: compromission des services DFS

La menace générale réside dans la capacité d'un pirate à pénétrer dans un service financier sans être détecté. Les vulnérabilités se manifestent de différentes manières chez le fournisseur SFN. Le Tableau 12 résume les risques et les vulnérabilités ainsi que les contrôles pour les prestataires SFN.

Tableau 12 – Synthèse des risques, des vulnérabilités et des contrôles pour les prestataires SFN

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
Prestataire SFN	Les risques de ***défaillance du service et de compromission des services et des données SFN*** sont dus aux vulnérabilités suivantes:	
	– Modifications non autorisées de la configuration du système, des fichiers journaux et des données (SD: intégrité des données).	**C59**: le système SFN devrait protéger contre la falsification et n'autoriser que les transactions en ligne. a) Protéger et surveiller les fichiers d'application SFN contre les altérations et les modifications à l'aide de moniteurs d'intégrité de fichiers, par exemple en calculant les sommes de contrôle ou en validant les signatures numériques. b) Par principe, le prestataire de services de paiement direct ou le commerçant ne doit pas utiliser la solution de paiement mobile pour autoriser des transactions hors ligne ou pour stocker des transactions en vue d'une transmission ultérieure.
Prestataire SFN	– Validation inadéquate de l'accès de l'utilisateur ou de l'entrée de l'utilisateur (SD: authentification).	**C60**: le système SFN devrait utiliser une authentification forte à plusieurs facteurs pour l'accès des utilisateurs et des fournisseurs tiers aux systèmes SFN, par exemple à l'aide de jetons ou de données biométriques; l'utilisation d'une authentification à plusieurs facteurs pour vérifier les utilisateurs du système augmente la non-répudiation de l'origine.
		C61: le système SFN devrait vérifier les données entrantes par rapport aux valeurs attendues dans le schéma de données lié à l'API, pour l'USSD, effectuer la validation XML des requêtes HTTP.
		C62: le système SFN devrait utiliser des systèmes d'analyse pour vérifier la vélocité des utilisateurs entre les transactions, le suivi de l'accès à l'heure de la journée pour des contrôles supplémentaires de validation des autorisations.
		C63: quelle que soit la méthode utilisée pour produire les reçus (par exemple, courrier électronique, SMS ou imprimante jointe), celle-ci doit masquer le numéro de compte primaire (PAN) conformément aux lois, réglementations et politiques applicables en matière de cartes de paiement. Par politique et par pratique, le prestataire SFN/le commerçant ne doit pas autoriser l'utilisation de canaux non sécurisés tels que le courrier électronique et les SMS pour envoyer le PAN ou des données d'authentification sensibles (DAS).

13.12 Menace: accès non autorisé aux données SFN

La menace générale est la capacité d'un attaquant à obtenir un accès non autorisé aux données SFN des utilisateurs SFN. Les vulnérabilités se manifestent de différentes manières au niveau de l'opérateur de réseau mobile, du fournisseur SFN et de l'utilisateur mobile. Le Tableau 13 résume les risques, les vulnérabilités et les contrôles pour les utilisateurs de téléphones mobiles, les ORM, les fournisseurs de services SFN et les tiers.

Tableau 13 – Résumé des risques, des vulnérabilités et des contrôles pour les utilisateurs de téléphones mobiles, les ORM, les fournisseurs de services SFN et les tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
Utilisateur mobile	Le risque d'***accès non autorisé aux données mobiles des utilisateurs SFN*** est dû aux vulnérabilités suivantes:	
	– Mécanismes de contrôle d'accès aux comptes d'utilisateurs inadéquats (SD: contrôle d'accès).	**C64**: les utilisateurs de SFN doivent définir le code PIN de leur compte. Lorsque le code PIN saisi pour la première fois est défini par le système du prestataire SFN ou ses agents, le code PIN est unique pour chaque utilisateur et doit être modifié lors de la première connexion.
	– Contrôles limités pour l'accès aux données sensibles sur l'appareil (SD: contrôle d'accès).	**C65**: les utilisateurs de SFN doivent définir des mots de passe forts et éviter les codes PIN facilement devinables pour leurs appareils, comme les dates d'anniversaire.
		C66: les utilisateurs de SFN devraient veiller à ce que les informations sensibles du SFN soient stockées dans des parties sécurisées de l'appareil mobile.
		C67: les développeurs d'applications doivent s'assurer que l'authentification de l'utilisateur est requise avant l'installation de l'application sur l'appareil.
		C68: les développeurs d'applications doivent veiller à ce que l'accès à l'infrastructure, aux applications et aux services SFN ne soit autorisé qu'après authentification de l'identité. Utiliser l'authentification à plusieurs facteurs: quelque chose que l'utilisateur connaît (comme un code PIN), quelque chose qu'il détient (comme une carte SIM), quelque chose qu'il incarne (comme une empreinte digitale ou une autre méthode biométrique).
		C69: les développeurs d'applications doivent s'assurer que les applications SFN gèrent de manière sécurisée les identifiants d'accès.
MNO	Le risque d'***interception des données SFN en transit*** est dû aux vulnérabilités suivantes:	**C70**: le système SFN devrait veiller à ce que toutes les données sensibles des consommateurs, telles que les codes PIN et les mots de passe, soient stockées en toute sécurité au moyen d'un cryptage puissant – dans le réseau interne et au repos – afin d'atténuer les menaces internes qui pèsent sur ces données.
	– Faiblesse inhérente à la sécurité SS7 [b-ss7-8/9] (SD: sécurité des communications).	**C71**: le système SFN devrait utiliser les pare-feu pour détecter et limiter les attaques basées sur les failles de sécurité du SS7.
	– Interception des transactions MO-USSD (SD: sécurité des communications).	**C72**: le système SFN devrait vérifier si l'IMEI de l'appareil effectuant la transaction correspond à l'IMEI enregistré du téléphone du titulaire du compte (un système MITM peut cloner la carte SIM avec un IMEI différent).
	– Trafic sensible non protégé et pratiques de cryptage insuffisantes (SD: sécurité des communications).	**C73**: les ORM devraient contrôler la vélocité de l'utilisateur en comparant la localisation du téléphone utilisé pour effectuer des transactions à la dernière localisation signalée du téléphone (dernier SMS ou appel entrant/sortant).
		C74: les ORM devraient imposer l'utilisation de la clé de déverrouillage personnelle (PUK) sur la carte SIM pour une sécurité supplémentaire en cas de perte ou de vol de l'appareil mobile.

Tableau 13 – Résumé des risques, des vulnérabilités et des contrôles pour les utilisateurs de téléphones mobiles, les ORM, les fournisseurs de services SFN et les tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
		C75: les ORM devraient contrôler et surveiller l'utilisation d'analyseurs de protocole et de traçage MSC MAP sur l'infrastructure USSD et SMS afin de limiter l'accès interne aux SMS en texte clair et au trafic USSD en transit.
		C76: les ORM devraient utiliser le protocole SecureOTP bidirectionnel vers le numéro de téléphone d'origine pour vérifier la légitimité de la transaction [b-ss7-12.1].
		C77: les ORM devraient utiliser des pratiques de cryptographie rigoureuses pour garantir la confidentialité et l'intégrité des données lorsqu'elles pénètrent dans le réseau des prestataires de services de santé publique et lorsqu'elles sont traitées et stockées dans cet environnement.
		C78: les ORM devraient limiter le nombre de sessions SFN par utilisateur. Autoriser une seule session par utilisateur à la fois, quel que soit le canal d'accès (STK, USSD ou https); un compte d'utilisateur SFN ne doit pas être accessible par plusieurs canaux simultanément.
		C79: l'opérateur mobile doit déployer les contrôles de sécurité de la signalisation SS7 et du diamètre spécifiés par la GSMA (FS.11, FS.07, IR.82, et IR.88) pour limiter les menaces dues aux attaques SS7 [b-ss7-10].
Prestataire SFN	Le risque d'***exposition des données sensibles des clients est*** dû aux vulnérabilités suivantes:	
	– Protection insuffisante des données d'enregistrement des clients du SFN. (SD: authentification).	**C80**: le système SFN devrait protéger et conserver les données des clients utilisées pour l'inscription au SFN, lorsque des formulaires physiques sont utilisés, stocker et transmettre les données en toute sécurité. **C81**: le système SFN devrait utiliser des normes de cryptage solides telles que le cryptage TLS v1.2 ou supérieur pour la communication API.
	– Utilisation d'un cryptage faible. (SD: sécurité des communications).	
	– Contrôle et surveillance inadéquats de l'accès des utilisateurs SFN (SD: contrôle d'accès).	**C82**: le système SFN devrait étendre la détection des menaces pour intégrer explicitement les menaces associées aux API.
		C83: le système SFN devrait limiter l'accès à la connexion à distance et minimiser les privilèges des sessions de connexion à distance aux systèmes SFN dorsaux.
		C84: le système SFN devrait limiter la durée de vie des certificats TLS à 825 jours.
		C85: le système SFN devrait authentifier l'IP de l'utilisateur, l'appareil et l'heure de connexion pour tous les utilisateurs privilégiés, les agents et les commerçants qui se connectent au système SFN. Par exemple, configurer l'accès d'un commerçant et d'un agent au système SFN de manière à ce qu'il ne soit accessible que pendant les heures d'ouverture.

Tableau 13 – Résumé des risques, des vulnérabilités et des contrôles pour les utilisateurs de téléphones mobiles, les ORM, les fournisseurs de services SFN et les tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
		C86: le code et les modifications doivent être testés dans l'environnement de test avant d'être transférés sur la plate-forme de production; l'environnement de test doit être physiquement et logiquement séparé de l'environnement de production.
		C87: pour améliorer la sécurité, il devrait utiliser un dispositif fiable et inviolable, tel qu'un module de sécurité matériel (HSM), pour gérer en toute sécurité le processus et stocker des clés cryptographiques afin de protéger les codes PIN des utilisateurs, les transactions, les jetons et les bons d'achat.
		C88: le système SFN devrait définir les rôles des utilisateurs pour définir les droits d'accès sur la base du principe du moindre privilège.
		C89: après la résiliation du contrat d'un utilisateur, l'agent, le commerçant, les prestataires de services de paiement ou les tiers désactivent leurs comptes respectifs.
		C90: le système SFN devrait définir la période d'inactivité des comptes et désactiver les comptes inactifs à l'échéance de la période d'inactivité.
		C91: le système SFN devrait définir des horaires pour les connexions et les limitations de session en fonction des rôles SFN (les limitations de session peuvent inclure le nombre maximum d'annulations par jour en fonction du rôle).
		C92: le système SFN devrait limiter le contrôle, surveiller et examiner périodiquement l'accès privilégié aux systèmes SFN, y compris l'ajout, la modification et la suppression d'utilisateurs.
		C93: le système SFN devrait surveiller l'utilisation des API et crypter toutes les données partagées avec des tiers, mettre en place des procédures de gestion des données et des contrôles tels que des accords de non-divulgation signés avec les fournisseurs de services de paiement afin d'éviter les fuites d'informations/de données.
	– Surveillance inadéquate du réseau sans fil (SD: confidentialité des données).	**C94**: le système SFN devrait protéger les transmissions sans fil conformément aux exigences de la norme PCI DSS. Les contrôles doivent comprendre, sans s'y limiter, les éléments suivants: – Assurez-vous que les clés de cryptage, les mots de passe et les chaînes de communauté SNMP par défaut du fournisseur sont modifiés. – Faciliter l'utilisation des meilleures pratiques du secteur pour mettre en œuvre un cryptage fort pour l'authentification et la transmission. Le système SFN devrait veiller à ce que les données de compte en clair ne soient pas stockées sur un serveur connecté à l'internet.

Tableau 13 – Résumé des risques, des vulnérabilités et des contrôles pour les utilisateurs de téléphones mobiles, les ORM, les fournisseurs de services SFN et les tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
Tiers	– Défaut de destruction/effacement des données avant la mise au rebut des dispositifs (SD: vie privée).	**C95**: les prestataires SFN/commerçants doivent systématiquement se débarrasser de leurs anciens appareils. Lorsque le fournisseur de la solution émet des conseils, le commerçant doit les suivre. Voici quelques éléments à prendre en compte: – Supprimer toutes les étiquettes et tous les identificateurs d'entreprise. – Dans la mesure du possible, passer un contrat avec un fournisseur agréé qui peut vous aider à éliminer en toute sécurité les matériaux et les composants électroniques. Ne pas jeter les appareils dans les conteneurs à déchets ou les bennes à ordures de votre entreprise.

13.13 Menace: logiciels malveillants

Cette menace générale est caractérisée par le fait que des éléments du SFN sont susceptibles d'être infectés par des logiciels malveillants. Le Tableau 14 résume les risques, les vulnérabilités et les contrôles pour les utilisateurs de téléphones mobiles, les ORM, les fournisseurs de services SFN et les tiers.

Tableau 14 – Résumé des risques, des vulnérabilités et des contrôles pour les utilisateurs de téléphones mobiles, les ORM, les fournisseurs de services SFN et les tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
Tierce partie, fournisseur SFN	Les risques liés aux ***attaques de logiciels malveillants et à l'impossibilité d'effectuer des transactions, aux interruptions de service et à l'accès non autorisé aux données*** se produisent chez le commerçant ou le prestataire SFN en raison des vulnérabilités suivantes:	
	– Manquement à utiliser un logiciel anti-malware ou anti-virus ou à réaliser une mise à jour régulièrement (SD: disponibilité).	**C96**: le système SFN devrait déployer des logiciels de sécurité sur tous les appareils mobiles, y compris des antivirus, des logiciels anti-spyware et des produits d'authentification logicielle pour protéger les systèmes contre les menaces actuelles et évolutives des logiciels malveillants. Tous les logiciels doivent être installés à partir d'une source fiable.
		C97: si aucun logiciel anti-malware n'est disponible, utiliser des solutions de gestion des applications mobiles (MAM) ou des solutions MDM qui peuvent contrôler, évaluer et supprimer les logiciels et applications malveillants de l'appareil. En outre, si possible, il est idéal de déployer à la fois des solutions anti-malware et des solutions MDM (mentionnées ci-dessus) pour protéger l'appareil contre les logiciels et applications malveillants.
		C98: le système SFN devrait désactiver les fonctions inutiles de l'appareil et n'installer que des logiciels fiables.

Tableau 14 – Résumé des risques, des vulnérabilités et des contrôles pour les utilisateurs de téléphones mobiles, les ORM, les fournisseurs de services SFN et les tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
		Les commerçants et les fournisseurs SFN doivent désactiver toutes les capacités de communication qui ne sont pas nécessaires au fonctionnement de la solution de paiement. Pour éviter d'introduire de nouveaux vecteurs d'attaque sur un appareil mobile, il ne devrait autoriser que la communication avec des logiciels de confiance que dans la mesure où elle est nécessaire pour appuyer les activités de l'entreprise et pour faciliter les paiements.
	– Collaboration insuffisante avec le fournisseur de solutions sur la sécurité des appareils mobiles achetés (SD: disponibilité et confidentialité).	**C99**: les commerçants et les fournisseurs SFN doivent exiger les éléments suivants de leur fournisseur de solutions: – Le fournisseur de la solution doit régulièrement mettre à jour son application de paiement et indiquer au commerçant lorsque des mises à jour sont disponibles et peuvent être installées en toute sécurité. – Le fournisseur de la solution doit imposer des restrictions à son application de paiement afin qu'elle ne fonctionne que sur un appareil doté d'un micrologiciel approuvé. – Le fournisseur de la solution doit fournir une documentation détaillant les procédures de mise à jour qui selon le commerçant doivent être suivies. – Le fournisseur de la solution SFN doit communiquer avec le fournisseur SFN et l'informer des vulnérabilités récemment découvertes dans sa solution d'acceptation des paiements. En outre, le fournisseur de la solution doit guider les commerçants lorsque de nouvelles vulnérabilités sont découvertes, et fournir des correctifs testés pour chacune de ces vulnérabilités.
	– Ouvrir des faiblesses non détectées dans les applications du système (SD: confidentialité des données).	**C100**: le commerçant doit travailler avec son fournisseur de solutions pour s'assurer que toute capacité d'audit ou d'enregistrement est activée. Le fournisseur de la solution doit s'assurer qu'il existe des capacités de journalisation avec une granularité suffisante pour détecter les événements anormaux. Le fournisseur de la solution doit informer le commerçant de la responsabilité qui lui incombe d'examiner les journaux. En outre, inspecter régulièrement les journaux et les rapports du système pour détecter toute activité anormale. Si une activité anormale est suspectée ou découverte, interrompre l'accès à l'appareil mobile et à son application de paiement jusqu'à ce que le problème soit résolu. Les activités anormales comprennent, entre autres, les tentatives d'accès non autorisé, les élévations de privilèges et les mises à jour non autorisées de logiciels ou de microprogrammes.
	– Exposition du réseau aux attaques extérieures (SD: disponibilité)	**C101**: les applications SFN doivent faire l'objet d'analyses et de tests de pénétration réguliers. En particulier, les applications doivent être conçues pour résister aux logiciels d'hameçonnage.

Tableau 14 – Résumé des risques, des vulnérabilités et des contrôles pour les utilisateurs de téléphones mobiles, les ORM, les fournisseurs de services SFN et les tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
Utilisateur mobile	Les risques d'***installation de logiciels malveillants tels que les logiciels espions et les chevaux de Troie*** sont dus à la vulnérabilité suivante: – Aucun logiciel anti-malware ou anti-virus n'est utilisé ou mis à jour régulièrement (SD: disponibilité).	**C102**: le système SFN devrait maintenir le système d'exploitation de l'appareil mobile à jour régulièrement; ne pas autoriser l'installation de programmes sans la validation de l'utilisateur.
	Le risque d'***exécution de code à distance*** est dû aux vulnérabilités suivantes:	
	– Logiciel obsolète (SD: confidentialité des données).	**C103**: les utilisateurs de téléphones portables devraient être encouragés à effectuer des mises à jour de sécurité régulières sur leurs appareils mobiles utilisés pour les transactions SFN et à s'assurer qu'ils disposent des derniers correctifs de sécurité fournis par les fabricants d'appareils et les fournisseurs d'applications.
	– Aucun logiciel anti-malware ou anti-virus n'est utilisé ou mis à jour régulièrement (SD: disponibilité).	**C104**: le système SFN devrait installer sur les appareils mobiles des logiciels de sécurité provenant de sources fiables, notamment des antivirus, des anti-logiciels espions et des produits d'authentification logicielle, afin de protéger les appareils contre les menaces actuelles et évolutives de logiciels malveillants.
	– Falsification de l'appareil de l'utilisateur et débridage (SD: intégrité).	**C105**: parce qu'un appareil altéré ou débridé peut potentiellement compromettre la confidentialité, l'intégrité et la vie privée des données de l'utilisateur.
		C106: le développeur d'applications mobiles doit veiller à ce que les applications SFN soient placées dans un bac à sable, de sorte que d'autres applications non fiables sur l'appareil mobile ne puissent pas interagir avec l'application SFN, et que l'interaction avec le système d'exploitation soit limitée.
MNO	Les risques d'***incapacité à effectuer des transactions et de compromission des services*** sont dus à la vulnérabilité suivante: – Exposition du réseau aux attaques extérieures (SD: disponibilité).	**C107**: le système SFN devrait effectuer régulièrement des analyses de vulnérabilité et des tests de pénétration sur l'infrastructure de l'ORM afin de vérifier l'exposition à des attaques susceptibles d'affecter la disponibilité du système.
		C108: le système SFN devrait installer et mettre à jour régulièrement le dernier logiciel anti-malware (si disponible) et le mettre à la disposition des utilisateurs finaux. Envisager l'enveloppement des applications, qui peut être utilisé avec des solutions de gestion des appareils mobiles (MDM) pour prévenir et supprimer les logiciels et applications malveillants.

13.14 Menace: attaques de type "0 day"

Ce sous-ensemble de menaces liées aux logiciels malveillants est pris en compte spécifiquement parce que les moyens traditionnels de défense contre les logiciels malveillants sont inefficaces contre une

menace qui n'a jamais été observée auparavant. Le Tableau 15 résume les risques, les vulnérabilités et les contrôles pour l'ORM, les fournisseurs SFN et les tiers.

Tableau 15 – Résumé des risques, des vulnérabilités et des contrôles pour les ORM, les fournisseurs FSN et les tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
ORM, fournisseurs SFN et tiers	Les risques d'***accès non autorisé aux données confidentielles de l'utilisateur et de modification non autorisée des données de l'utilisateur*** sont dus à la vulnérabilité suivante: – Découverte de nouvelles vulnérabilités face aux systèmes déployés et incapacité à déployer des solutions contre ces vulnérabilités (SD: confidentialité des données, contrôle d'accès, disponibilité).	**C109**: les ORM, les fournisseurs SFN et les fournisseurs de services de paiement devraient patcher les systèmes avec les dernières versions fournies par le vendeur pour se défendre contre les attaques qui ont été développées à partir de vulnérabilités plus anciennes.
		C110: les fournisseurs et les ORM devraient mettre en place des plans d'urgence avec les vendeurs afin d'acquérir rapidement des correctifs et de remédier au système si une attaque de type "0-day" a été découverte. Une partie de cette stratégie implique l'utilisation correcte des sauvegardes.

13.15 Menace: dispositifs malveillants

La menace que les dispositifs non autorisés peuvent représenter pour l'infrastructure du réseau SFN est examinée ici. Le Tableau 16 résume les risques, les vulnérabilités et les contrôles pour l'ORM.

Tableau 16 – Résumé des risques, des vulnérabilités et des contrôles pour l'ORM

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
MNO	Les risques de ***fraude et de modification des données*** sont dus à la vulnérabilité suivante: – Dispositifs non sécurisés connectés à l'infrastructure SFN (SD: intégrité des données).	**C111**: les ORM doivent surveiller les appareils utilisés pour se connecter au système SFN ou y accéder d'une autre manière, afin de s'assurer que ces appareils disposent des derniers correctifs, d'un logiciel antivirus mis à jour, qu'ils sont analysés pour détecter les rootkits et les enregistreurs de clés, et qu'ils ne prennent pas en charge les extensions de réseau.

13.16 Menace: accès non autorisé aux appareils mobiles

Il s'agit d'un ensemble de menaces sous forme d'attaques spécifiques contre les appareils mobiles de la part d'adversaires. Le Tableau 17 résume les risques, les vulnérabilités et les contrôles pour les utilisateurs/dispositifs mobiles, les fournisseurs SFN et les fournisseurs tiers.

Tableau 17 – Résumé des risques, des vulnérabilités et des contrôles pour les utilisateurs/appareils mobiles, les fournisseurs SFN et les fournisseurs tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
	Le risque d'***usurpation d'identité et de perte de données/transactions frauduleuses*** est dû aux vulnérabilités suivantes:	
Utilisateur mobile/appareil	– Authentification inadéquate de l'utilisateur sur l'appareil (SD: confidentialité des données).	**C112**: les appareils mobiles doivent se verrouiller automatiquement après une période d'inactivité, ce qui oblige à procéder à une authentification de l'appareil pour le déverrouiller avant de l'utiliser pour des transactions SFN.
		C113: utiliser des codes PIN forts, l'effacement des données à distance, le verrouillage par code PIN, l'authentification biométrique (par exemple, empreinte digitale, iris) lorsque de telles fonctions sont disponibles sur l'appareil.
	– Les versions obsolètes des logiciels d'application rendent les appareils vulnérables aux logiciels malveillants (SD: confidentialité des données).	**C114**: les fabricants d'appareils veillent à ce que les consommateurs puissent acquérir directement les mises à jour critiques ou qu'elles soient mises à la disposition des fournisseurs de réseau pour être transmises aux utilisateurs.
Prestataire SFN	Le risque de ***prise de contrôle d'un compte d'utilisateur SFN*** est dû à la vulnérabilité suivante: – Accès trop permissif à l'infrastructure SFN (SD: authentification).	**C115**: avant d'authentifier les utilisateurs SFN, il convient, dans la mesure du possible, de valider l'IMSI, l'appareil, la localisation et l'adresse IP de l'utilisateur afin d'établir son identité et d'empêcher tout accès non autorisé à l'infrastructure du réseau.
Fournisseur tiers	Le risque de ***transactions refusées*** est dû à la vulnérabilité suivante: – Vérification inadéquate des transactions (SD: non-répudiation).	**C116**: les prestataires de services de paiement doivent veiller à ce que les cartes rechargeables à usage général liées aux comptes SFN exigent l'utilisation de puces EMV avec des méthodes de vérification du titulaire de la carte, telles que le code PIN ou la biométrie, lorsque c'est possible, et à ce que toutes les transactions donnent lieu à une alerte pour les clients.

13.17 Menace: divulgation involontaire d'informations personnelles identifiables

Cet ensemble de menaces se caractérise par le fait que les données de l'utilisateur sont exposées par inadvertance. Le Tableau 18 résume les risques, les vulnérabilités et les contrôles pour les fournisseurs SFN et les fournisseurs tiers.

Tableau 18 – Synthèse des risques, des vulnérabilités et des contrôles pour les fournisseurs SFN et les fournisseurs tiers

Entités concernées	Risques et vulnérabilités	Exigences de contrôles
Prestataire SFN	Le risque d'***exposition d'informations personnelles identifiables*** est dû à la vulnérabilité suivante: – Surveillance et contrôles inadéquats dans les environnements de test (SD: vie privée).	**C117**: les fournisseurs SFN doivent veiller à ce que les données des clients dans les environnements de production ne soient pas utilisées dans les environnements de test, à moins qu'elles ne soient rendues anonymes conformément aux meilleures pratiques. Inversement, les données de test ne doivent pas être migrées vers le produit.
Fournisseur tiers	Le risque d'exposition d'informations sensibles est dû aux vulnérabilités suivantes:	
	– Exposition d'informations sensibles pour le client dans les transactions ou par le biais d'API (SD: vie privée).	**C118**: les fournisseurs tiers doivent limiter le partage d'informations avec d'autres parties telles que les fournisseurs de services de paiement et les fournisseurs SFN au minimum requis pour garantir l'intégrité de la transaction.
	– Contrôles insuffisants de la protection des données (SD: vie privée).	**C119**: les fournisseurs doivent veiller à ce que les données sensibles des clients soient supprimées des environnements tels que les journaux de suivi (par exemple, les codes des bons de retrait, les numéros de compte bancaire et les informations d'identification). Utiliser autant que possible des caractères de remplacement pour représenter ces données dans les fichiers journaux.

14 Gestion des incidents de sécurité SFN

Souvent, même après l'application des contrôles appropriés les incidents de sécurité se produisent, en particulier dans les services financiers où les attaquants ont une motivation financière pour contourner les systèmes, ce qui entraîne une perturbation, l'altération ou la divulgation des données de ces derniers. Les organisations et les parties prenantes qui proposent des services financiers numériques ou qui y participent doivent élaborer des procédures, des rapports, des collectes de données, des responsabilités de gestion, des protocoles juridiques et des stratégies de communication qui leur permettront de comprendre et de gérer les incidents de sécurité et de s'en remettre. Un fournisseur SFN qui ne dispose pas d'un plan de gestion des incidents peut ne pas découvrir une attaque ou, si l'attaque est détectée, le fournisseur peut ne pas avoir de procédures en place pour limiter rapidement les dommages, éradiquer et répondre à la présence de l'attaquant, et récupérer ses actifs avec un impact minimal.

Un plan de gestion des incidents de sécurité définit des procédures cohérentes à suivre pour signaler, réagir, analyser, enquêter et récupérer de manière ordonnée, rapide et efficace les incidents de sécurité qui compromettent l'une des dix dimensions de la sécurité.

La norme [b-ISO/IEC27035] reconnaît que les contrôles de la sécurité de l'information sont imparfaits et prévoit des processus détaillés pour la gestion des incidents.

Le Center for Internet Security [b-CIS] propose les lignes directrices suivantes pour la gestion des incidents, que les opérateurs de réseaux de systèmes SFN, les fournisseurs SFN et les fournisseurs de services pourraient adopter:

- S'assurer qu'il existe des plans écrits de réponse aux incidents qui définissent les rôles du personnel ainsi que les phases de traitement/gestion des incidents.

- Attribuer des titres de poste et des tâches à des personnes spécifiques pour le traitement des incidents informatiques et de réseau et assurer le suivi et la documentation tout au long de l'incident jusqu'à sa résolution.
- Désigner le personnel d'encadrement, ainsi que les remplaçants, qui soutiendront le processus de traitement de l'incident en jouant un rôle clé dans la prise de décision.
- Établir des normes à l'échelle de l'organisation concernant le temps nécessaire aux administrateurs de système et aux autres membres du personnel pour signaler les événements anormaux à l'équipe chargée du traitement des incidents, les mécanismes de ce signalement et le type d'informations à inclure dans la notification de l'incident.
- Rassembler et conserver des informations sur les coordonnées de tiers à utiliser pour signaler un incident de sécurité, tels que les forces de l'ordre, les services gouvernementaux compétents, les vendeurs et les fabricants d'appareils.
- Publier, à l'intention de tous les membres du personnel, des informations concernant le signalement d'anomalies et d'incidents informatiques à l'équipe chargée du traitement des incidents. Ces informations devraient être incluses dans les activités courantes de sensibilisation des employés.
- Planifier et réaliser des exercices et des scénarios de réponse aux incidents pour le personnel impliqué dans la réponse aux incidents afin de maintenir le niveau de sensibilisation et d'aisance dans la réponse aux menaces du monde réel. Les exercices doivent permettre de tester les canaux de communication, la prise de décision et les capacités techniques des intervenants en cas d'incident en utilisant les outils et les données dont ils disposent.
- Créer un schéma de notation et de hiérarchisation des incidents en fonction de l'impact connu ou potentiel sur votre organisation. Utiliser le score pour définir la fréquence des mises à jour de l'état d'avancement et les procédures d'escalade.
- Mettre en place un système de reprise après sinistre afin de prévenir les interruptions d'activité telles que les catastrophes naturelles ou les cyberattaques contre les systèmes SFN.
- Répondre aux incidents de sécurité à l'aide d'une plate-forme d'orchestration, automatisation et réponse aux incidents de sécurité informatique (SOAR) qui recueille les données relatives aux menaces et automatise les réponses à ces dernières.

Annexe A

Infrastructure détaillée de l'écosystème SFN et des menaces

(Cette annexe fait partie intégrante de la présente Recommandation.)

Il existe de nombreux points d'interaction entre les différentes parties au sein de l'écosystème SFN. Par conséquent, il existe également un certain nombre de moyens par lesquels les attaquants peuvent tirer parti de ces interfaces pour attaquer le système, l'exploitation de vulnérabilités réussie ayant souvent des conséquences qui affectent non seulement les parties prenantes exploitées mais aussi d'autres au sein de l'écosystème. La Figure A.1 montre les différents points vulnérables de l'infrastructure SFN. Les chiffres seront utilisés pour décrire la surface de vulnérabilité qui se produit à ce point d'interaction.

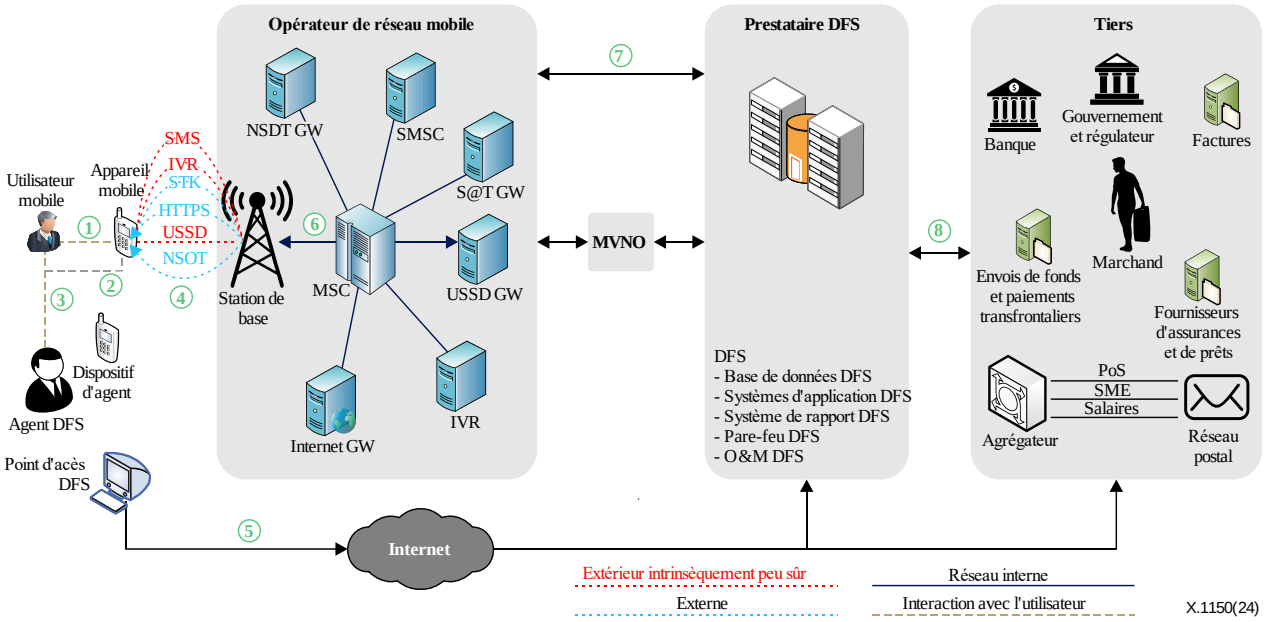

Figure A.1 – Correspondance entre les menaces et les contrôles de sécurité

A.1 Client – Appareil mobile

Ce paragraphe identifie les menaces liées à l'appareil mobile et au client:

- Exposition d'informations sensibles sur le client si celui-ci partage l'appareil avec d'autres personnes, s'il le perd, le vole ou le saisit, ou si un adversaire surfe sur les informations d'identification de l'utilisateur.
- Accès non autorisé à l'appareil par un pirate devinant le code PIN ou le mot de passe de l'appareil ou déjouant les mécanismes d'authentification, s'ils sont mis en place, sur l'appareil mobile.
- La manipulation de l'appareil afin de compromettre la sécurité de la plate-forme sous-jacente, par exemple en installant des logiciels malveillants sur le stockage sous-jacent ou en extrayant des secrets de la mémoire de l'appareil par le biais de sa manipulation.
- Modification des paramètres d'appel par un attaquant malveillant non autorisé pour définir le renvoi des appels et des SMS, ce qui permet à l'attaquant d'accéder aux informations SFN envoyées par le biais de messages, comme un mot de passe à usage unique (OTP).

A.2 Appareil mobile – Application mobile

Ce paragraphe identifie les menaces liées aux appareils mobiles et aux applications mobiles:

- Les vulnérabilités du code de l'application mobile peuvent être exploitées par des attaquants qui obtiennent l'accès à l'appareil mobile, par exemple par le biais de sur-applications. Il peut en résulter une compromission des données des clients, une violation de la vie privée et une perte d'intégrité.
- La compromission de la plate-forme mobile sous-jacente peut introduire des virus, des chevaux de Troie, des vers, des ransomwares et d'autres logiciels malveillants/rootkits qui peuvent compromettre les informations du client ou rendre l'utilisateur plus vulnérable aux tentatives d'hameçonnage pour obtenir des informations d'identification pour l'application, ce qui permet au pirate d'obtenir un accès non autorisé au compte du client.
- Des contrôles d'accès insuffisants au sein de l'application, par exemple un mécanisme d'authentification requis avant l'exécution d'opérations sensibles (par exemple l'enregistrement, le transfert de paiement) basé sur des hypothèses de confiance, peuvent conduire à la compromission de l'application et à l'exfiltration consécutive des données du client ou à un transfert d'argent non autorisé.
- L'absence de capacités d'enregistrement et d'audit dans l'application et l'absence de stockage de ces données dans une partie protégée de l'appareil peuvent empêcher les garanties de non-répudiation et exposer l'utilisateur à l'impossibilité de prouver qu'il a été victime d'une attaque.
- L'absence ou la mauvaise utilisation du chiffrement au sein de l'application, de sorte que les informations sont écrites de manière non sécurisée dans les journaux d'application ou stockées dans des bases de données dont le chiffrement est faible ou inexistant, peut également permettre à un adversaire d'exposer ces informations.
- Si l'application permet la négociation de suites de chiffrement faibles, elle peut faire l'objet d'attaques par rétrogradation vers des versions plus anciennes contenant des chiffrements potentiellement faibles. Si les clés de session ne sont pas renégociées périodiquement, l'accumulation de matériau chiffré peut rendre la clé vulnérable à une attaque.
- Accès non autorisé à un appareil mobile perdu ou volé.
- Falsification d'applications mobiles.

A.3 Client – Agent SFN

Ce paragraphe identifie les menaces liées au client et à l'agent SFN:

- Les clients peuvent être vulnérables aux attaques par échange de cartes SIM, où l'attaquant se présente à l'agent comme étant le client afin d'obtenir une nouvelle carte SIM qui donne accès au compte SFN.
- Des vulnérabilités similaires peuvent être exposées contre les cartes compagnon liées aux comptes SFN si l'authentification des informations d'identification du client est insuffisante par l'agent ou si l'agent est de connivence avec l'adversaire.

A.4 Appareil mobile – Station de base

Ce paragraphe identifie les menaces liées à l'appareil mobile et à la station de base:

- Les anciens réseaux GSM où les applications SFN utilisent principalement des SMS, des USSD ou des IVR s'appuient sur la sécurité fournie par le réseau, qui est basée sur les algorithmes de cryptage des réseaux GSM tels que A5/1 et A5/2. La vulnérabilité de ces algorithmes a été démontrée. Des travaux récents ont démontré que des approches similaires peuvent être utilisées pour compromettre le code A5/3. Dans certains systèmes,

l'algorithme A5/0 est spécifié, ce qui fournit un chiffrement nul et donc aucune protection de la confidentialité des données, ce qui permet à un attaquant d'exfiltrer des informations sensibles via l'interface aérienne. Indépendamment des menaces qui pèsent sur la sécurité du réseau de transport sous-jacent, STK et https fournissent un cryptage de bout en bout.

- Les réseaux traditionnels reposant sur le cryptage GSM (STK, USSD et IVR) sont également sujets à des attaques de type "man in the middle" de la part de stations de base malhonnêtes placées par un attaquant, prétendant malicieusement être des tours de fournisseurs légitimes (c'est-à-dire une fausse station de base, souvent appelée "IMSI-catcher") et décryptant la communication avant de la renvoyer dans le réseau de l'opérateur de téléphonie mobile. Un tel système peut permettre à l'attaquant d'obtenir un accès complet à toutes les informations communiquées, y compris les données transactionnelles et financières.

A.5 Appareil mobile – Internet

Ce paragraphe identifie les menaces liées aux appareils mobiles et à l'Internet:

- La sécurité du lien de communication dépend de la suite de chiffrement négociée entre l'application et les services d'arrière-plan dans les systèmes de bout en bout sur l'internet. Il a été démontré que les informations contenues dans les applications sont acheminées vers divers puits en dehors du point final autorisé, notamment vers des journaux et des bases de données. Par conséquent, seuls des mécanismes de cryptage puissants comme TLS garantissent la sécurité des données dans les réseaux de télécommunications publics.
- Il est également important de veiller à ce que les suites de chiffrement utilisées ne fassent pas l'objet d'attaques par rétrogradation vers des versions plus anciennes contenant des chiffrages potentiellement faibles. Si les clés de session ne sont pas périodiquement renégociées, l'accumulation de données chiffrées peut rendre la clé vulnérable à une attaque. Les protocoles comme les SSL et TLS (transport layer security) peuvent être configurés pour renégocier les algorithmes de chiffrement, mais il est important que les protocoles soient résistants aux attaques de renégociation menées par des attaquants qui injectent du trafic dans des échanges client-serveur légitimes. Négociation de suites de chiffrement faibles qui réduisent la sécurité peut permettre à un adversaire de modifier les transactions et, par conséquent, l'intégrité des données financières.
- En l'absence d'un cryptage approprié des informations transitant par les connexions Internet, les informations peuvent être écoutées sur la liaison WiFi entre l'appareil mobile et le point d'accès. Des attaques récentes contre la négociation de la clé TLS montrent que même des protocoles WiFi solides tels que le WPA2 peuvent potentiellement être compromis.

A.6 Station de base – Station de commutation mobile – Passerelles

Ce paragraphe identifie les menaces liées à la station de base, à la station de commutation mobile et aux passerelles:

- Des contrôles internes insuffisants peuvent permettre à des initiés d'accéder aux données des clients. Ceci est particulièrement important pour les solutions SMS et USSD qui n'offrent pas de cryptage au sein du réseau du fournisseur.
- Un acteur malveillant ayant accès au réseau SS7 pourrait envoyer des messages de gestion de la partie de transfert de messages (MTP) pour simuler une congestion du réseau, réacheminer les messages ou refuser la disponibilité du service/de la liaison.
- Les réseaux mobiles sont également sensibles aux menaces de déni de service (DoS) qui peuvent être exécutées en surchargeant les liaisons SS7. Un pirate envoie un grand nombre de requêtes SCCP (signalling connection control part) qui nécessitent un traitement important.

- Les informations peuvent être falsifiées par des initiés, en particulier dans les protocoles qui ne prévoient aucune notion d'intégrité des messages.
- La facilité d'accès accrue au réseau SS7 permet à un pirate d'utiliser les opérations MAP (mobile application part) pour insérer ou modifier les données de l'abonné, intercepter les communications mobiles ou identifier l'emplacement de l'abonné.
- La liaison de communication entre la station de base mobile et le réseau du fournisseur est une liaison filaire dans certains scénarios, tandis que dans d'autres, en fonction de la topographie du réseau mobile, les stations de base peuvent être connectées au réseau du fournisseur sans fil, par exemple au moyen d'une liaison micro-ondes. Si cette communication n'est pas cryptée, alors, en particulier pour les transactions par SMS et USSD où le cryptage est strictement assuré par les algorithmes GSM entre le combiné et la station de base, ces données pourraient être renvoyées au réseau en clair, facilitant ainsi une violation de la confidentialité.
- Dans le contexte SFN, un acteur malveillant disposant d'un accès au niveau du réseau SS7 peut usurper ("spoof") l'identité de la ligne appelante (CLI) d'une personne ou d'une entité de confiance et appeler le client SFN pour tenter de lui soutirer ses informations d'identification SFN et bancaires, ce qui entraînerait finalement des pertes financières.
- Les clients des ORM peuvent être victimes d'échanges de cartes SIM non autorisés, et les attaquants peuvent tirer parti des informations sur les abonnés obtenues lors d'attaques SS7 pour obtenir des informations qui peuvent être utilisées pour mener à bien l'échange de cartes SIM ou en collaboration avec le personnel interne de l'ORM.
- Les utilisateurs privilégiés au sein de l'ORM peuvent abuser de leur accès aux nœuds centraux tels que le HLR et le MSC pour effectuer des activités telles que les transferts d'appels et de SMS, le renvoi d'appels, l'interception non autorisée et la collecte d'enregistrements de données d'appels d'abonnés SFN.

A.7 Réseau mobile – Opérateur SFN

Ce paragraphe identifie les menaces liées au réseau mobile et à l'opérateur SFN:

- La protection des données est souvent limitée, notamment le cryptage des données, une fois que l'information est transmise au réseau du fournisseur. Il y a de nombreuses raisons à cela, notamment le coût de calcul et les frais généraux nécessaires pour maintenir des connexions cryptées à grande largeur de bande au sein du réseau. On part également souvent du principe que les menaces qui pèsent sur le réseau proviennent essentiellement de l'extérieur plutôt que de l'intérieur. Il en résulte des vulnérabilités dues à des adversaires internes et à des menaces externes capables de pénétrer dans le réseau.
- Les données contenues dans le réseau de l'opérateur sont menacées en raison de l'absence de protection de l'intégrité au sein de ces réseaux. Ces informations peuvent être modifiées arbitrairement par un adversaire capable d'accéder au réseau (par exemple, en compromettant les défenses périmétriques) ou par un initié malveillant.
- Les fournisseurs SFN qui utilisent la carte SIM comme élément de sécurité et les numéros SIM/mobiles comme compte financier risquent de perdre leurs comptes lors du recyclage de la carte SIM. Les opérateurs de téléphonie mobile qui effectuent des recyclages SIM périodiques dans le cadre desquels les numéros de téléphone mobile sont réattribués à de nouveaux utilisateurs s'ils sont restés inactifs pendant une période déterminée sur le réseau GSM; le processus de recyclage SIM peut créer des risques de perte d'accès à un compte financier ou de transfert illicite de ce dernier à un autre utilisateur.
- Les limitations de configuration et de capacité de l'équipement de l'ORM pourraient limiter le service et la disponibilité des services financiers numériques, les limitations de la durée des sessions USSD pourraient interrompre les transactions SFN.

- L'étendue du réseau et de l'infrastructure physique de l'opérateur mobile le rend vulnérable à la compromission de l'accès par la plantation de dispositifs malveillants qui peuvent permettre un accès à distance non autorisé, l'interconnexion de l'écosystème SFN peut permettre à une personne ayant un accès malveillant d'accéder aux différentes parties prenantes au-delà de l'opérateur mobile.
- Interface aérienne et interceptions MSC: Le MSC a des capacités qui permettent une interception légale. Un accès privilégié au MSC signifie que l'on peut intercepter des communications. Cet accès pourrait être utilisé à des fins financières frauduleuses en surveillant ou en refusant l'activité SFN.
- Attaques par déni de service sur les réseaux mobiles. Ce risque est accru par le fait que les nœuds des opérateurs tels que les passerelles MSC se connectent à d'autres opérateurs de réseau en utilisant l'IP, ce qui augmente le risque d'inondation et d'attaques de ressources qui augmentent généralement la quantité de trafic entrant et peuvent surcharger la pile IP et les processeurs des nœuds, ce qui forcera le nœud à s'arrêter ou à redémarrer, ce qui affectera directement la disponibilité.
- Réacheminement et transfert des appels: un pirate externe pourrait accéder à l'équipement du réseau ou y avoir accès et réacheminer les communications SFN vers un autre numéro, en modifiant le profil de localisation de l'abonné mobile, ce qui permettrait au pirate d'avoir accès à des informations SFN confidentielles.

A.8 Opérateur SFN – Tiers

Ce paragraphe identifie les menaces liées à l'opérateur SFN et au tiers:

- Les données peuvent être exposées si le cryptage n'est pas rigoureusement utilisé au sein des réseaux de fournisseurs et entre eux. Les menaces proviennent d'informations récupérées à l'extérieur du périmètre du réseau du fournisseur (c'est-à-dire le réseau externe), tandis que la menace interne existe à l'intérieur du périmètre du réseau (c'est-à-dire le réseau interne). En outre, les données peuvent être exposées si les systèmes du réseau du fournisseur sont infectés par des logiciels malveillants, qui peuvent être transmis à la fois sur le réseau et par des périphériques malveillants connectés aux systèmes hôtes (par exemple, des clés USB malveillantes ou des enregistreurs de frappe installés sur un clavier). Ces appareils peuvent exfiltrer des données de l'environnement du fournisseur vers l'adversaire.
- Un attaquant capable d'accéder aux bases de données des fournisseurs externes, par exemple en compromettant les vulnérabilités d'un logiciel, a la possibilité d'altérer les données financières et les informations sensibles des fournisseurs. En particulier, les interfaces entre les réseaux constituent un point d'entrée potentiel pour un adversaire et doivent être étroitement surveillées. En outre, les données au repos ne sont qu'aussi sûres que les protections mises en place sur les hôtes et les serveurs qui stockent ces informations.
- Un serveur SFN sur lequel les mises à jour de sécurité ne sont pas rigoureusement mises à jour peut être victime de logiciels malveillants et de rootkits. Toutes les machines faisant face à une interface de réseau public sont potentiellement sujettes à des vulnérabilités basées sur le réseau, y compris des attaques "0-day" qui n'ont jamais été vues auparavant. Les systèmes peuvent également être compromis par d'autres interfaces d'E/S telles que les lecteurs CD/DVD, les ports USB et d'autres interfaces périphériques où les dispositifs peuvent potentiellement injecter des codes et des données malveillants.
- Insuffisance du renforcement du système d'exploitation SFN, comme les paramètres d'accès et de mot de passe par défaut, les services non essentiels actifs, les protocoles non sécurisés actifs tels que telnet et ftp, les autorisations d'accès aux fichiers, les configurations réseau par défaut et les droits des utilisateurs, comme ceux qui sont autorisés à procéder à un arrêt.

- L'accès non contrôlé aux périphériques de démarrage externes tels que les CD, DVD et USB, qui permettent d'accéder au BIOS sans mot de passe, constitue une surface d'attaque pour le système SFN.

Annexe B

Éléments clés et recommandations additionnels pour les travaux futurs

(Cette annexe fait partie intégrante de la présente Recommandation.)

Un cadre d'assurance de la sécurité pour les services financiers numériques (SFN) devrait aussi englober un ensemble de principes, de procédures et de contrôles afin de garantir la sécurité, l'intégrité et la fiabilité des transactions et services financiers numériques. Certains éléments clés et recommandations additionnels pourraient être examinés lors de futurs travaux sur le cadre d'assurance de la sécurité pour les services financiers numériques (SFN):

– Politique et gouvernance en matière de sécurité: pour définir les grandes lignes des objectifs de sécurité, des responsabilités et des exigence de conformité de l'organisation dans le contexte des SFN.
– Procédures d'authentification et d'autorisation: définir une autorisation et des permissions claires afin de contrôler l'accès aux comptes et aux transactions financières et, en outre, garantir l'intégrité et la non-répudiation des transactions et des relevés financiers.
– Procédures de protection et de confidentialité des données: se conformer aux réglementations en matière de confidentialité des données et gérer le consentement des clients relatif à l'utilisation de leurs données.
– Procédures d'API sécurisées et d'utilisation de l'interopérabilité: mettre en œuvre des mesures de sécurités renforcées pour les points d'accès API.
– Procédures de prévention et de détection des fraudes: détecter et empêcher les activités frauduleuses.
– Procédures dédiées à l'innovation et aux technologies émergentes: réaliser des évaluation des risques sur les nouvelles technologies et innovations dans le secteur financier.
– Procédures d'amélioration et d'adaptation permanentes: aborder les technologies en constante évolution, les réglementations et les menaces de sécurité émergentes.
– Prise en compte des chaînes de blocs et des crypto-monnaies (le cas échéant): si le SFN comprend des services de chaînes de blocs ou de crypto-monnaie, aborder la conformité réglementaire et la sécurité dans ce contexte.

Appendice I

Modèle de bonnes pratiques en matière de sécurité des applications

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Cet appendice fournit un modèle de cadre de sécurité pour les applications mobiles. L'accent est mis sur les meilleures pratiques générales et non sur des technologies spécifiques, sauf lorsqu'elles sont explicitement décrites. Ce modèle est basé sur des travaux récents portant sur l'examen des applications de services financiers numériques du point de vue de l'espace d'application de l'argent mobile, notamment l'étude de la GSMA sur les meilleures pratiques en matière de sécurité des applications d'argent mobile [b-GSMA], les lignes directrices pour un développement sécurisé des smartphones [b-ENISA], et un cadre de sécurité des applications de paiement mobile développé dans le [b-sbp]. Ce modèle peut également être utilisé par les fournisseurs SFN dans le cadre d'une politique de sécurité des applications.

Cet appendice résume les recommandations comme point de départ pour les régulateurs ou les examinateurs de la sécurité des applications pour effectuer des évaluations de la sécurité. Le modèle prend strictement en compte l'application mobile sur l'appareil, sauf indication contraire, et les paragraphes décrivant les recommandations traitent de divers aspects du fonctionnement ou de la politique sous-jacente relative à l'application mobile. L'accent est mis principalement sur les applications mobiles, bien que de nombreuses recommandations soient applicables à tous les systèmes d'exploitation mobiles. Le respect de la vie privée est également un facteur important à prendre en compte, mais ces recommandations se concentrent sur la sécurité.

I.1 Intégrité des appareils et des applications

Ce paragraphe contient les recommandations relatives à l'intégrité des appareils et des applications:

- Les dispositifs les plus sûrs pour effectuer des transactions financières sont ceux qui n'ont pas été débridés car il peut être difficile, voire impossible, d'évaluer la sécurité du système d'exploitation sous-jacent lorsqu'il a été remplacé ou exploité. Les applications doivent donc utiliser les services de la plate-forme mobile pour déterminer qu'elles et la plate-forme sous-jacente n'ont pas été modifiées.
- Supprimer tout code étranger qui aurait pu être ajouté à l'application au cours du développement, comme des fonctions qui ne sont pas conçues pour les plates-formes d'appareils sur lesquelles l'application doit être déployée ou des fonctions de développement/débogage afin de réduire la surface d'attaque du code de production déployé.
- Côté serveur, déterminer si l'application est exécutée dans un état d'intégrité élevé grâce à la validation de la signature ou au hachage de l'application ou de certains blocs fonctionnels du programme.

I.2 Sécurité des communications et gestion des certificats

Ce paragraphe contient les recommandations relatives à la sécurité des communications et à la gestion des certificats:

- Les applications doivent utiliser des bibliothèques cryptographiques normalisées et, pour la communication avec les services dorsaux, elles doivent utiliser le chiffrement de bout en bout avec des protocoles normalisés, en particulier la sécurité de la couche de transport (TLS). La version minimale recommandée de TLS à utiliser est la version 1.2.
- Les certificats TLS ne doivent pas avoir expiré et doivent présenter des suites de chiffrement solides, en particulier le chiffrement AES-128 et SHA-256 pour le hachage. Les modes d'opération de cryptage authentifiés tels que le mode Galois/compteur (GCM) sont encouragés.

- Limiter la durée de vie des certificats émis à 825 jours conformément aux meilleures pratiques du CA/Browser Forum.
- S'assurer de la fiabilité de l'autorité de certification et envisager un plan d'urgence pour le cas où l'autorité de certification ne serait plus digne de confiance.
- Veiller à ce que la configuration de TLS soit effectuée de manière sécurisée et éviter les problèmes de mauvaise configuration qui pourraient entraîner un échec de l'authentification ou une mauvaise sélection d'algorithme.
- L'épinglage des certificats doit empêcher le remplacement des certificats lorsqu'il s'agit d'associer un hôte à son certificat de clé publique ou à sa clé publique attendue. Une fois qu'un certificat ou une clé publique est connu ou vu pour un hôte, le certificat ou la clé publique est associé ou "épinglé" à l'hôte.
- Les dispositifs clients doivent s'assurer qu'ils valident correctement les certificats des serveurs.

I.3 Authentification de l'utilisateur

Ce paragraphe contient les recommandations relatives à l'authentification de l'utilisateur:

- Les codes PIN et les mots de passe ne doivent pas être faciles à deviner et les identifiants faibles doivent être interdits; toutefois, les utilisateurs ne doivent pas être obligés de changer régulièrement de mot de passe.
- L'authentification multifactorielle avant l'exécution de fonctions financières ou d'autres fonctions sensibles devrait être fortement encouragée. Il convient d'utiliser une forme d'authentification multifactorielle résistante à l'hameçonnage [b-UIT-T X.1277] [b-UIT-T X.1278].
- Les applications d'authentification pour smartphone devraient être utilisées pour envoyer des mots de passe à usage unique plutôt que des SMS en raison de la possibilité de détournement du SS7 et d'autres insécurités.
- Si des informations biométriques sont utilisées pour l'authentification, elles doivent être stockées avec des mesures de sécurité appropriées, telles que le cryptage dans la base de données Android Keystore ou l'utilisation d'un matériel de confiance.

I.4 Traitement sécurisé des données

Ce paragraphe contient les recommandations relatives au traitement sécurisé des données:

- Les appareils mobiles doivent stocker les informations confidentielles en toute sécurité.
- Du matériel de confiance doit être utilisé pour le stockage d'informations sensibles s'il est disponible sur les smartphones des clients.
- Éviter de stocker des informations sur un support externe et, le cas échéant, veiller à ce qu'une validation solide des entrées soit effectuée avant d'utiliser ces données.
- Supprimer les données confidentielles des caches et de la mémoire après leur utilisation et éviter l'exposition générale des informations (par exemple, placer la clé secrète sur la pile). Assurer le nettoyage de la mémoire avant la sortie de l'application.
- Restreindre les données partagées avec d'autres applications grâce à des autorisations précises. Minimiser le nombre d'autorisations demandées par l'application et s'assurer que les autorisations correspondent aux fonctionnalités nécessaires au fonctionnement de l'application.
- Ne pas coder en dur des informations sensibles telles que des mots de passe ou des clés dans le code source de l'application.

- Valider toute entrée provenant du client et devant être stockée dans les bases de données afin d'éviter les attaques par injection SQL.

I.5 Développement d'applications sécurisées

Ce paragraphe fournit les recommandations relatives au développement d'applications sécurisées:

- Développer des applications conformément aux pratiques et aux normes de codage sécurisées acceptées par l'industrie.
- Garantir un moyen de mettre à jour les applications en toute sécurité et s'assurer que toutes les bibliothèques et tous les modules dépendants sont sécurisés; fournir des mises à jour pour ces derniers lorsque c'est nécessaire.
- Faire évaluer et tester le code de manière indépendante par des équipes d'examen du code internes ou externes.

Bibliographie

[b-UIT-T X.1158] Recommandation UIT-T X.1158 (2014), *Mécanismes d'authentification à plusieurs facteurs utilisant un dispositif mobile*.

[b-UIT-T X.1231] Recommandation UIT-T X.1231 (2008), *Stratégies techniques de lutte contre le spam*.

[b-UIT-T X.1277] Recommandation UIT-T X.1277 (2018), *Cadre d'authentification universel*.

[b-UIT-T X.1278] Recommandation UIT-T X.1278 (2018), *Protocole client-authentificateur/cadre universel à 2 facteurs*.

[b-UIT-T X.1408] Recommandation UIT-T X.1408 (2021), *Menaces et exigences de sécurité pour l'accès aux données et leur partage sur la base du dispositif d'enregistrement électronique partagé*.

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Vue d'ensemble et vocabulaire*.

[b-ISO/IEC 27001] ISO/IEC 27001:2022, *Sécurité des systèmes d'information*.

[b-ISO/IEC 27032] ISO/IEC 27032:2012, *Technologies de l'information – Techniques de sécurité – Lignes directrices pour la cybersécurité*.

[b-ISO/IEC 27035] ISO/IEC 27035-1:2016, *Technologies de l'information – Techniques de sécurité – Gestion des incidents de sécurité de l'information – Partie 1: Principes de gestion des incidents*.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Technologies de l'information – Techniques de sécurité – Cadre de protection de la vie privée*.

[b-ISO/IEC TR 15443-1] ISO/IEC TR 15443-1:2012, *Technologies de l'information – Techniques de sécurité – Assurance de la sécurité Cadre – Partie 1: Introduction et concepts*.

[b-ISO/TR 19231] ISO/TR 19231:2014, *Informatique de santé – Étude de projets de santé mobile dans les pays à revenu bas et moyen*.

[b-CIS] CIS, *CIS Critical Security Control 17: Incident Response and Management*.
https://www.cisecurity.org/controls/incident-response-and-management/

[b-cis] CIS Critical Security Controls v7.1, *Center for Internet Security*
https://www.cisecurity.org/controls/v7

[b-ENISA] Agence de l'Union européenne pour la cybersécurité (ENISA), *Smartphone Secure Development Guidelines*, 10 février 2017.
https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016

[b-DFS-SA] Groupe de réflexion de l'UIT-T sur les services financiers numériques (2017), *Security Aspects of Digital Financial Services*.
https://www.itu.int/en/ITU-T/studygroups/2017-2020/09/Documents/ITU_FGDFS_SecurityReport.pdf

[b-GSMA] GSM Association, Official Document MM.01 – *MM App Security Best Practices*, version 1.0, 28 juin 2018.
https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/08/Mobile-money-app-security-best-practices.pdf

[b-pci-dss] Payment Card Industry (PCI) *Data Security Standard Requirements and Security Assessment Procedures*, version 3.2.1, mai 2018, PCI Security Standards Council, LLC.
https://www.pcisecuritystandards.org/document_library/?category=pcidss&document=pci_dss

[b-nist-800-63] NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, 10 décembre, 2020.
https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[b-OWASP] OWASP Top Ten, OWASP
https://owasp.org/www-project-top-ten/

[b-REPORT] Le rapport sur les big data ML et la protection de la vie privée des consommateurs met en évidence les risques et la manière dont les données financières et de télécommunications des consommateurs peuvent être utilisées à mauvais escient.
https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/Big%20data%2C%20Machine%20learning%2C%20Consumer%20protection%20and%20Privacy.pdf

[b-sbp] State Bank of Pakistan, *Mobile Payment Applications (App) Security Framework* (DRAFT version 1.0), avril 2019.
https://www.sbp.org.pk/psd/2022/C1-Annex.pdf

[b-SOAR] SOAR (Orchestration, automatisation et réponse aux incidents de sécurité informatique), *Rapid7*.
https://www.rapid7.com/solutions/security-orchestration-and-automation/

[b-ss7-8/9] Voir le rapport technique sur les vulnérabilités du SS7 et les mesures d'atténuation pour le SFN – Se référer aux points 8 et 9 du rapport.
https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/Technical%20report%20on%20SS7%20vulnerabilities%20and%20mitigation%20measures%20for%20Digital%20Financial%20Services%20transactions.pdf articles 8 et 9 du rapport.

[b-ss7-12.1] Voir le rapport technique sur les vulnérabilités du SS7 et les mesures d'atténuation pour le SFN – article 12.1 Détection et atténuation de la prise de contrôle d'un compte à l'aide d'un SMS OTP intercepté.
https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/Technical%20report%20on%20SS7%20vulnerabilities%20and%20mitigation%20measures%20for%20Digital%20Financial%20Services%20transactions.pdf

[b-ss7-10] Voir le rapport technique sur les vulnérabilités du SS7 et les mesures d'atténuation pour le SFN – Voir l'article 10 Stratégies d'atténuation pour les opérateurs de téléphonie mobile. https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/Technical%20report%20on%20SS7%20vulnerabilities%20and%20mitigation%20measures%20for%20Digital%20Financial%20Services%20transactions.pdf

[b-ss7-12.5] Voir le rapport technique sur les vulnérabilités du SS7 et les mesures d'atténuation pour le SFN – article 12.5 Détection, prévention et atténuation du recyclage des cartes SIM.
https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/Technical%20report%20on%20SS7%20vulnerabilities%20and%20mitigation%20measures%20for%20Digital%20Financial%20Services%20transactions.pdf

[b-TR-SAF-FIGI] FIGI, *cadre d'assurance de la sécurité des services financiers numériques*, avril 2021.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Publié en Suisse
Genève, 2024