Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1812

(05/2022)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité des réseaux IMT-2020

Cadre de sécurité fondé sur des relations de confiance pour l'écosystème des IMT-2020

Recommandation UIT-T X.1812

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	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
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 (1)	X.1140–X.1149
Sécurité des applications (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1350–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1399
Sécurité de la technologie des registres distribués (DLT)	X.1400–X.1429
Sécurité des applications (2)	X.1450–X.1459
Sécurité de la toile (2)	X.1470–X.1489
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
Cyberdéfense	X.1590–X.1599
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
Protection des données	X.1770–X.1789
SÉCURITÉ DES RÉSEAUX IMT-2020	**X.1800–X.1819**

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

Recommandation UIT-T X.1812

Cadre de sécurité fondé sur des relations de confiance pour l'écosystème des IMT-2020

Résumé

La Recommandation UIT-T X.1812 vise à identifier les parties prenantes présentes dans un écosystème des télécommunications mobiles internationales 2020 (IMT-2020, également dites de cinquième génération), à analyser les relations de confiance entre elles, à recenser les menaces et à préciser les responsabilités qui incombent à chaque partie prenante en matière de sécurité, à définir les limites de sécurité entre les parties prenantes et à établir un cadre de sécurité fondé sur ces relations de confiance.

Historique

Édition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1812	20-05-2022	17	11.1002/1000/14808

Mots clés

Écosystème, cadre, IMT-2020, confiance.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

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.

A 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

Introduction

L'éventail de parties prenantes d'un système de télécommunications mobiles internationales 2020 (IMT-2020, également dites de cinquième génération (5G)) est plus large et plus varié que dans les systèmes de communication des générations précédentes. Concernant les deuxième, troisième et quatrième générations (2G, 3G et 4G), les principales parties prenantes se résument aux fournisseurs de services, aux opérateurs de réseau, aux distributeurs d'équipements et aux abonnés. Toutefois, dans un écosystème des IMT-2020, des acteurs des secteurs verticaux interviennent également, notamment des entreprises industrielles et commerciales. En outre, les fournisseurs de services comprennent les opérateurs des plates-formes en nuage, les sociétés d'analyse de données, les fournisseurs d'applications, etc. Par ailleurs, au niveau du terminal, les abonnés ne sont pas uniquement des utilisateurs finals comme c'était le cas pour les générations précédentes. Les abonnés peuvent englober de nombreux types différents de parties prenantes, en particulier pour ce qui est des terminaux commerciaux, par exemple dans le cas de la communication entre les véhicules. Ces changements complexifient les relations entre les différentes parties prenantes et soulèvent plusieurs questions inédites pour ce qui est de la sécurité des écosystèmes des IMT-2020.

Les réseaux IMT-2020 introduisent également de nouvelles fonctionnalités. Par exemple, la virtualisation des fonctions des réseaux IMT-2020 permet de s'affranchir des limites des connexions fixes entre les entités de réseau et de piloter les réseaux par logiciel. Un autre exemple est celui de l'architecture fondée sur les services. Grâce à une telle architecture, davantage de fonctions liées à l'informatique en nuage pourraient être intégrées dans les réseaux IMT-2020. En outre, le découpage de réseau peut permettre une coopération plus efficace entre un réseau IMT-2020 et des services.

Au fil du temps, de plus en plus de techniques informatiques seront appliquées aux systèmes IMT-2020, non seulement au niveau des services, mais également au niveau des réseaux. Les réseaux IMT-2020 reposent intégralement sur le protocole Internet. Leur architecture se définit par des services plutôt que par des points de référence, comme c'était le cas pour l'architecture des réseaux des générations précédentes. De plus en plus, les signaux sont transférés par le biais de l'Internet plutôt que sur des réseaux dédiés. Le protocole de transport utilisé dans les réseaux IMT-2020 est modifié par rapport au protocole Diameter défini dans [b-IETF RFC 6733], qui est moins répandu que le protocole de transfert hypertexte, très utilisé à l'échelle mondiale. Tous ces changements seront bénéfiques pour le déploiement et l'exploitation des réseaux et des services IMT-2020.

Toutefois, l'utilisation de protocoles répandus et d'un environnement de connexion ouvert pourrait également présenter des avantages pour les auteurs d'attaques. Ces derniers n'auraient pas besoin de passer beaucoup de temps à étudier des protocoles de télécommunication complexes et pourraient donc parvenir plus facilement à trouver un point d'intrusion dans un réseau. Par conséquent, pour ce qui est des réseaux IMT-2020, il n'est plus raisonnable de supposer que les communications internes sont fiables. De fait, les changements qui distinguent la 4G des IMT-2020 nuisent à la relation de confiance qu'il existe entre les opérateurs de réseau.

En outre, les réseaux IMT-2020 sont conçus pour être plus flexibles et ainsi répondre aux différentes exigences de service. Il convient tout particulièrement de noter que le découpage de réseau a été introduit dans les réseaux IMT-2020. Les réseaux IMT-2020 peuvent également permettre d'exposer certaines capacités aux services. Grâce à cette exposition des capacités, un service IMT-2020 pourra contrôler certaines fonctions de réseau. Ces nouvelles fonctions rendront les limites de sécurité entre les réseaux et les services IMT-2020 plus ambiguës.

La présente Recommandation vise à identifier les parties prenantes présentes dans un écosystème des IMT-2020, à analyser les relations de confiance entre elles, à recenser les menaces et à préciser les responsabilités qui incombent à chaque partie prenante en matière de sécurité, à définir les limites de sécurité entre les parties prenantes et à établir un cadre de sécurité fondé sur ces relations de confiance.

Recommandation UIT-T X.1812

Cadre de sécurité fondé sur des relations de confiance pour l'écosystème des IMT-2020

1 Domaine d'application

La présente Recommandation définit un cadre de sécurité fondé sur des relations de confiance pour un écosystème des télécommunications mobiles internationales 2020 (IMT-2020). Elle décrit une approche générale pour:

– identifier les scénarios de fourniture des services IMT-2020;
– identifier les parties prenantes présentes dans un écosystème des IMT-2020;
– analyser les relations de confiance entre les parties prenantes;
– recenser les menaces qui pèsent sur chaque partie prenante;
– clarifier les responsabilités qui incombent à chaque partie prenante en matière de sécurité;
– spécifier les limites de sécurité entre les parties prenantes;
– spécifier les exigences de sécurité fondées sur un modèle de confiance; et
– établir un cadre de sécurité fondé sur des relations de confiance entre les parties prenantes.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut de Recommandation.

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 unité opérationnelle [b-ISO/TS 21089]: service ou sous-service distinct et compétent au sein d'un organisme.

NOTE – Une unité opérationnelle peut être un département, un service ou une unité spécialisée au sein d'un organisme de soins de santé.

3.1.2 déploiement [b-ISO/CEI/IEEE 24765]: phase d'un projet au cours de laquelle un système est mis en service et les problèmes de mise en service sont résolus.

3.1.3 développeur [b-NIST SP 800-53]: entité incluant: i) les développeurs ou les fabricants de systèmes d'information, de composants système ou de services de système d'information; ii) les intégrateurs de systèmes; iii) les distributeurs; et iv) les revendeurs des produits.

3.1.4 domaine [b-ISO/CEI 14888-1]: ensemble d'entités qui fonctionnent selon une unique politique de sécurité.

EXEMPLE – Des certificats de clés publiques créés par une seule autorité ou par plusieurs autorités appliquant la même politique de sécurité.

3.1.5 système informatique [b-ISO/CEI 27000]: ensemble d'applications, de services, d'actifs informatiques ou d'autres composants du traitement de l'information.

3.1.6 cycle de vie [b-ISO/CEI/IEEE 15288]: évolution d'un système, d'un produit, d'un service, d'un projet ou d'une autre entité d'origine humaine, de sa conception à son retrait.

3.1.7 fonction de réseau [b-UIT-T Y.3100]: dans le contexte des IMT-2020, fonction de traitement au sein d'un réseau.

NOTE 1 – Les fonctions de réseau incluent, sans s'y limiter, les fonctionnalités des nœuds de réseau, par exemple la gestion des sessions, la gestion de la mobilité et les fonctions de transport, dont on définit le comportement fonctionnel et les interfaces.

NOTE 2 – Les fonctions de réseau peuvent être mises en œuvre dans un équipement matériel dédié ou dans un logiciel, de manière virtuelle.

NOTE 3 – Les fonctions de réseau ne sont pas considérées comme des ressources, mais toute fonction de réseau peut être instanciée en utilisant les ressources.

3.1.8 partie prenante [b-ISO/PAS 19450]: personne physique, organisation ou groupe de personnes ayant un intérêt, ou pouvant être affectées, lorsqu'un système est envisagé, conçu ou déployé.

3.1.9 fournisseur [b-ISO 10393]: organisation ou personne fournissant un produit ou un service.

3.1.10 développement de système [b-ISO/CEI 2382]: processus comprenant généralement l'analyse des besoins, la conception de système, la mise en œuvre, la documentation et l'assurance de qualité.

3.1.11 confiance [b-ISO/CEI 25010]: mesure dans laquelle un utilisateur ou une autre partie prenante est convaincu(e) qu'un produit ou un système se comportera comme prévu.

3.1.12 niveau de confiance [b-ISO 28598-1]: estimation par le client de "la valeur" des preuves empiriques, complémentaires et indirectes attestant de l'aptitude du fournisseur à satisfaire aux exigences de qualité spécifiées.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 fournisseur de services externe: ensemble d'entités incluant: a) les entités qui font partie de l'organisation mais qui sont en dehors des limites établies pour les autorisations de sécurité des systèmes d'information organisationnels; b) les entités extérieures à l'organisation, issues soit du secteur public (par exemple les organismes fédéraux) soit du secteur privé (par exemple les fournisseurs de services commerciaux); ou c) une combinaison d'acteurs des secteurs public et privé.

NOTE – Adaptée de [b-NIST SP 800-53].

3.2.2 chaîne d'approvisionnement: réseau d'organisations qui interviennent, en aval ou en amont, dans les processus et activités qui produisent de la valeur sous la forme de produits et de services destinés au consommateur final.

3.2.3 cycle de développement d'un système: approche structurée pour la planification, la création, le test, le déploiement et la maintenance d'un système d'information.

3.2.4 modèle de confiance: modèle comportant des éléments qui décrivent les relations et les chaînes de confiance entre les parties prenantes.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

2G	deuxième génération
3G	troisième génération
4G	quatrième génération
5G	cinquième génération
5GC	réseau central de cinquième génération (*fifth generation core*)
BS	station de base (*base station*)
CAB	organisme d'évaluation de la conformité (*conformity assessment body*)
E2E	bout en bout (*end to end*)
HO	opérateur du réseau de rattachement (*home operator*)
ICP	fournisseur de contenus Internet (*Internet content provider*)
TIC	technologies de l'information et de la communication
IMT-2020	télécommunications mobiles internationales 2020 (*international mobile telecommunications-2020*)
IoT	Internet des objets (*Internet of Things*)
IoV	Internet des véhicules (*Internet of Vehicles*)
IPX	échange de paquets interréseaux (*internetwork packet exchange*)
ISP	fournisseur de services Internet (*internet service provider*)
IT	technologie de l'information (*information technology*)
NE	élément de réseau (*network element*)
NESAS	mécanisme d'assurance de la sécurité des équipements de réseau (*network equipment security assurance scheme*)
NF	fonction de réseau (*network function*)
NFV	virtualisation des fonctions de réseau (*network function virtualization*)
NPN	réseau non public (*non-public network*)
PII	informations d'identification personnelle (*personally identifiable information*)
PLMN	réseau mobile terrestre public (*public land mobile network*)
SCAS	spécification des garanties de sécurité (*security assurance specification*)
SDL	cycle de développement sécurisé (*security development lifecycle*)
UICC	carte à circuit intégré universelle (*universal integrated circuit card*)
VNF	fonction de réseau virtualisée (*virtualized network function*)
VO	opérateur du réseau visité (*visited operator*)

5 Conventions

Dans la présente Recommandation:

L'expression "**il est recommandé**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

L'expression "**peut, à titre d'option**" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour

le distributeur de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services de l'activer ou non, mais comme la possibilité pour le distributeur de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité avec la présente Recommandation.

6 Aperçu général

Avant l'ère de la 5G, les systèmes de télécommunication étaient principalement utilisés pour fournir des services de téléphonie et d'accès à l'Internet ainsi que des services connexes. En raison des contraintes de ces systèmes en termes de capacité et de débit, les cas d'utilisation étaient généralement simples. En particulier, seuls un petit nombre d'acteurs intervenaient dans un système de communication. Concernant le service d'appel, les acteurs qui interviennent sont l'appelant, l'appelé et le réseau mobile. Concernant le service de données, les acteurs sont le terminal, le réseau mobile et les fournisseurs de services ou d'applications. En outre, des distributeurs interviennent pour appuyer la création des réseaux et des systèmes d'applications. Les fabricants de terminaux et les fournisseurs de cartes à circuits intégrés universelles (UICC) interviennent au niveau du terminal. Il s'agit des principaux acteurs intervenant dans les systèmes de télécommunication 2G, 3G et 4G.

Toutefois, il en va autrement pour l'écosystème des IMT-2020. L'écosystème implique davantage de parties prenantes, pas uniquement celles qui interviennent dans un système de télécommunication au niveau du terminal, du réseau et du service. Au niveau du terminal, les abonnés ne sont plus uniquement des utilisateurs finals, comme c'était le cas précédemment, étant donné qu'il existe, à part le téléphone, de nombreux types d'appareils mobiles pouvant être partagés entre de multiples parties. Au niveau du réseau, les IMT-2020 introduisent toute une gamme de nouvelles fonctionnalités. Par exemple, la virtualisation des fonctions des réseaux IMT-2020 permet de s'affranchir des limites des connexions fixes entre les entités de réseau et de piloter les réseaux par logiciel, ce qui permet de dépasser les limites du déploiement de réseau en termes de sécurité. De plus en plus de techniques informatiques appliquées aux réseaux IMT-2020 peuvent également être exploitées par les auteurs d'attaques. Le service d'exposition des capacités de réseau permet d'ouvrir l'interface via le plan de commande, alors que l'auteur d'une attaque l'ouvre via le plan d'utilisateur. Concernant les services, des acteurs des secteurs verticaux interviennent, notamment des entreprises industrielles et commerciales. Il existe donc plusieurs catégories de fournisseurs de services, à savoir notamment les opérateurs des plates-formes en nuage, les sociétés d'analyse de données, les fournisseurs d'applications, etc., comme indiqué dans la Figure 1.

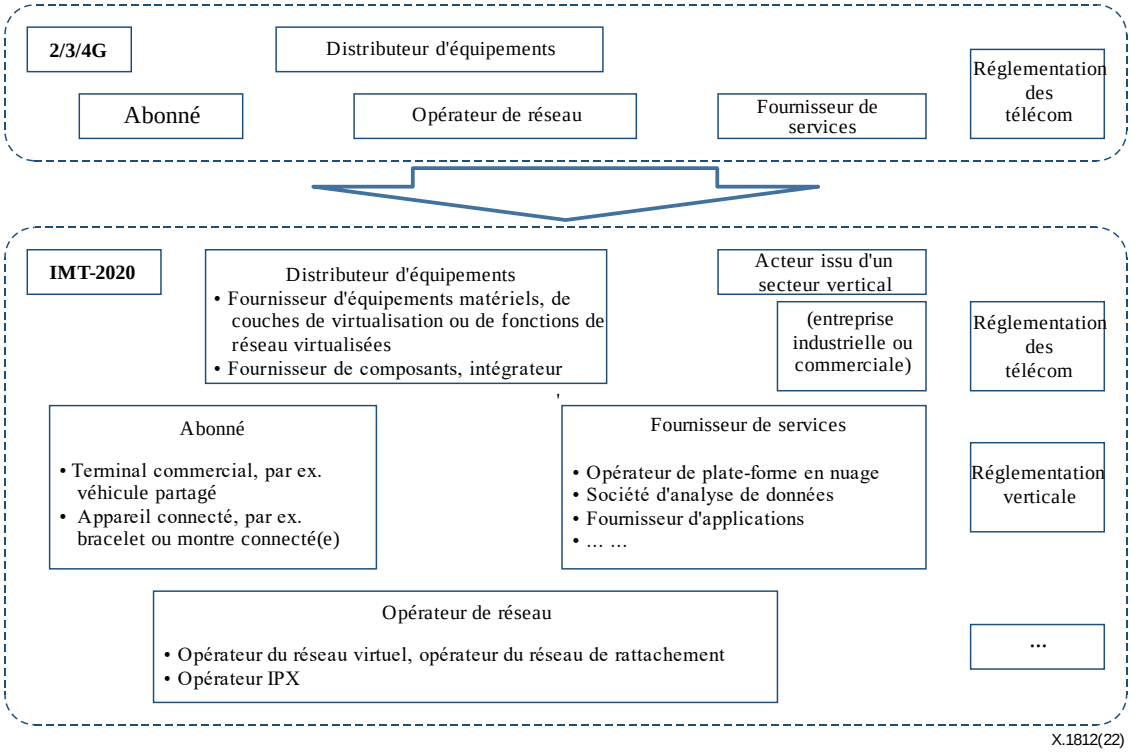


Figure 1 – Évolution de l'écosystème 2G, 3G et 4G vers celui des IMT-2020

Dans ce cas, la relation de confiance au sein du système IMT-2020 est différente. Les utilisateurs ou les abonnés et les systèmes de réseaux ou de services sont bien plus rapprochés qu'avant. Complexe et caractérisée par une longue traîne, la chaîne d'approvisionnement pousse les opérateurs à s'intéresser davantage à l'évaluation des fournisseurs. Les services et les réseaux étant étroitement liés, les secteurs verticaux dépendent fortement des réseaux et ont besoin de niveaux de confiance et de sécurité plus rigoureux. La fourniture d'un nouveau modèle de confiance pour l'écosystème des IMT-2020 doit être examinée, afin de formuler clairement des exigences de sécurité et des limites de sécurité entre les parties prenantes. De cette façon, il est possible d'accroître l'efficacité des communications autant que possible avec la garantie de la sécurité des données.

Cinq facteurs ont des incidences sur la fiabilité d'un système IMT-2020, à savoir la résilience, la sécurité des communications, la gestion d'identité, la protection des informations d'identification personnelle (PII) et la garantie de la sécurité.

- Résilience: la résilience est la capacité d'une organisation à éviter d'être affectée par les perturbations. L'intégration de diverses fonctionnalités complémentaires se chevauchant partiellement dans les IMT-2020 peut contribuer à rendre un système IMT-2020 plus résistant aux cyberattaques et aux incidents d'origine non malveillante.
- Sécurité des communications: la sécurité des communications est appliquée à la communication de données sur les réseaux IMT-2020. Dans un système IMT-2020, il est primordial de garantir la sécurité des communications, aussi bien pour les appareils que pour l'infrastructure du système lui-même.
- Gestion d'identité: un système de gestion d'identité englobe les politiques et les processus relatifs à la gestion du cycle de vie, de la valeur, du type et des métadonnées facultatives des attributs qui composent les identités des entités intervenant dans un système IMT-2020. Il est recommandé de fournir des solutions sûres de gestion d'identité pour identifier et authentifier les abonnés, qu'ils se trouvent ou non en itinérance, et pour faire en sorte que seuls les abonnés réels puissent accéder aux services de réseau. Les systèmes de ce type sont basés sur des primitives cryptographiques et sur des caractéristiques de sécurité fortes.

- Protection des informations d'identification personnelle (PII): dans la norme [b-ISO/TS 21719-2], la confidentialité des données est définie comme les droits et obligations des personnes physiques et des organisations concernant le recueil, l'utilisation, la conservation, la divulgation et la suppression des informations personnelles. La protection des informations d'identification personnelle comprend la protection des informations d'identification personnelle pouvant être utilisées par des parties non autorisées pour identifier les abonnés.
- Garantie de la sécurité: la garantie de la sécurité fournit des motifs justifiant la confiance dans le fait qu'une affirmation selon laquelle les objectifs de sécurité ont été atteints s'est avérée ou s'avèrera. La garantie de la sécurité est un moyen de garantir que les équipements de réseau répondent aux exigences de sécurité et que des processus sûrs de développement et de cycle de vie des produits ont été adoptés pour leur conception.

7 Cadre de sécurité étayé par le modèle de confiance

La présente Recommandation vise à analyser et à déterminer le rôle des parties prenantes de l'écosystème des IMT-2020 et les relations de confiance entre les divers rôles grâce à l'analyse de plusieurs scénarios types. Il est également question de déterminer le niveau de confiance et les facteurs essentiels à prendre en compte. On y trouvera donc des recommandations sur les moyens de déterminer les exigences de sécurité compte tenu du niveau de confiance et de former un cadre de sécurité fondé sur une relation de confiance, comme indiqué dans la Figure 2.

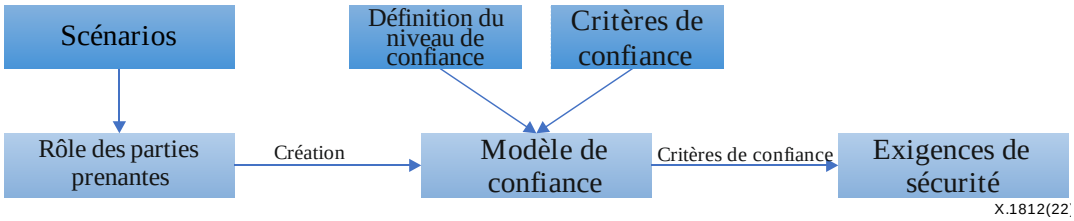


Figure 2 – Voie à suivre pour bâtir un cadre de sécurité fondé sur des relations de confiance pour l'écosystème des IMT-2020

Compte tenu du rôle et des relations de toutes les parties prenantes, de leur modèle de confiance et de leurs exigences de sécurité, on trouvera dans la Figure 3 un cadre de sécurité étayé par le modèle de confiance défini dans la présente Recommandation. Toutes les composantes de ce cadre sont décrites aux paragraphes 8 (rôle des parties prenantes), 9 (modèle de confiance) et 10 (exigences de sécurité).

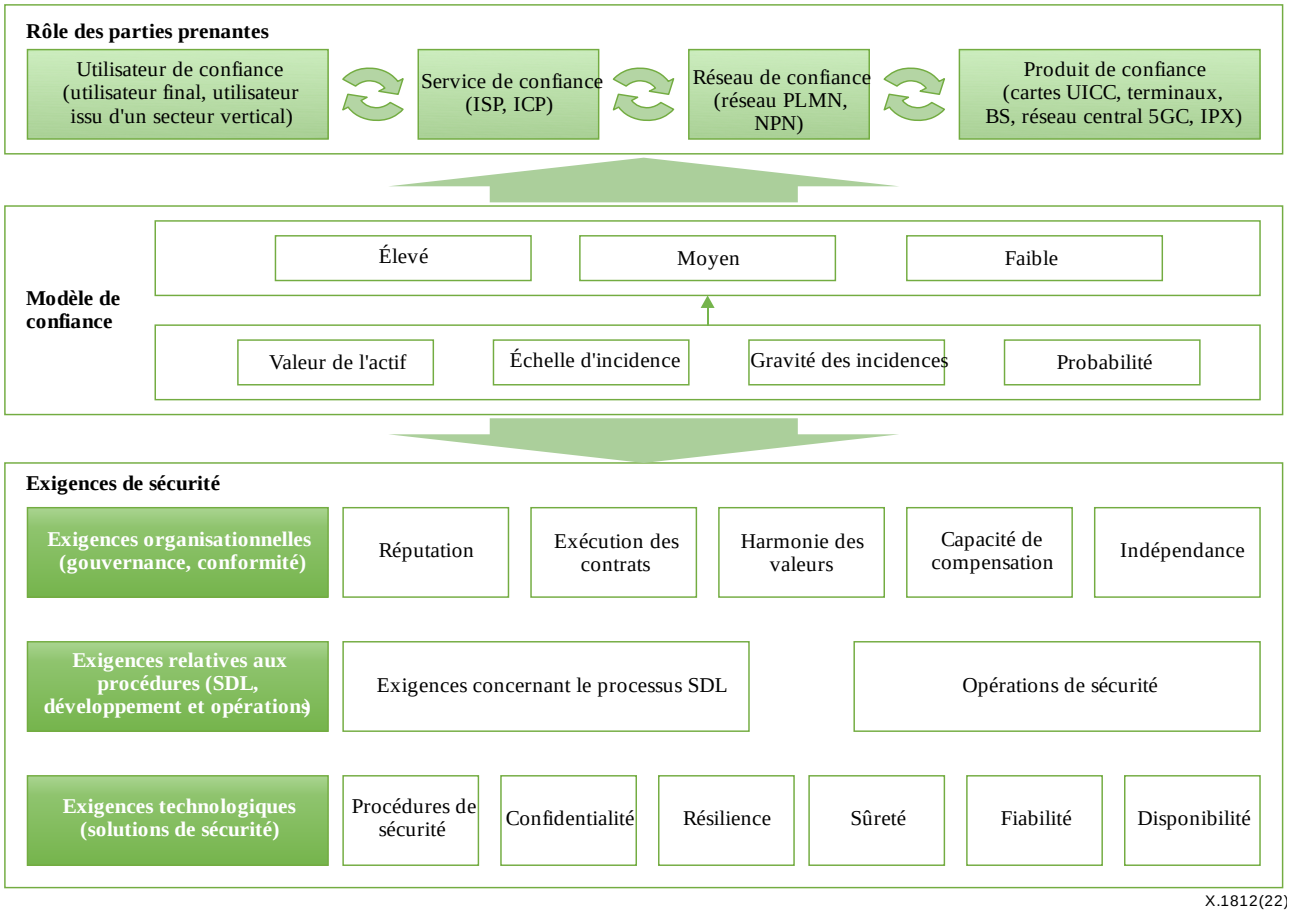


Figure 3 – Cadre de sécurité étayé par le modèle de confiance fondé sur des relations de confiance entre les parties prenantes

5GC: réseau central de cinquième génération; BS: station de base; ICP: fournisseur de contenus Internet; ISP: fournisseur de services Internet; NPN: réseau non public; SDL: cycle de développement sécurisé

8 Rôle des parties prenantes dans les scénarios de l'écosystème des IMT-2020

8.1 Généralités

Le système de télécommunication actuel peut être divisé en trois sous-systèmes: terminal, réseau et service. Il est nécessaire d'examiner les relations possibles à la fois entre les sous-systèmes et au sein de ceux-ci. Étant donné que la relation terminal-réseau a déjà été étudiée par d'autres organisations de normalisation telles que le Projet de partenariat de troisième génération (3GPP), elle ne sera pas davantage examinée dans la présente partie.

L'ensemble des cinq scénarios abordés dans les paragraphes ci-après englobent toutes les relations possibles entre les systèmes, à l'exception de la relation terminal-réseau.

8.2 Scénario 1: déploiement de la virtualisation de réseau dans le domaine d'un opérateur de réseau

8.2.1 Considérations générales

Ce scénario concerne essentiellement les relations au sein des réseaux.

Pour ce qui est réseaux de télécommunication actuels, les éléments de réseau (NE) qui sont déployés dans un réseau sont généralement mis en œuvre en tant que dispositifs physiques spécialisés. Chaque élément de réseau est mis en œuvre sous la forme d'un ou de plusieurs serveurs physiques, selon sa capacité. Des câbles – dont des câbles à fibre optique –, des commutateurs ainsi que des routeurs sont

utilisés pour connecter ces dispositifs de réseau aux interfaces physiques. Les principales parties prenantes intervenant dans ce scénario sont: les utilisateurs ou abonnés, les fabricants de terminaux mobiles, les fournisseurs de cartes UICC, les distributeurs de dispositifs de réseau et les opérateurs. Ces parties prenantes sont présentées dans la Figure 4.

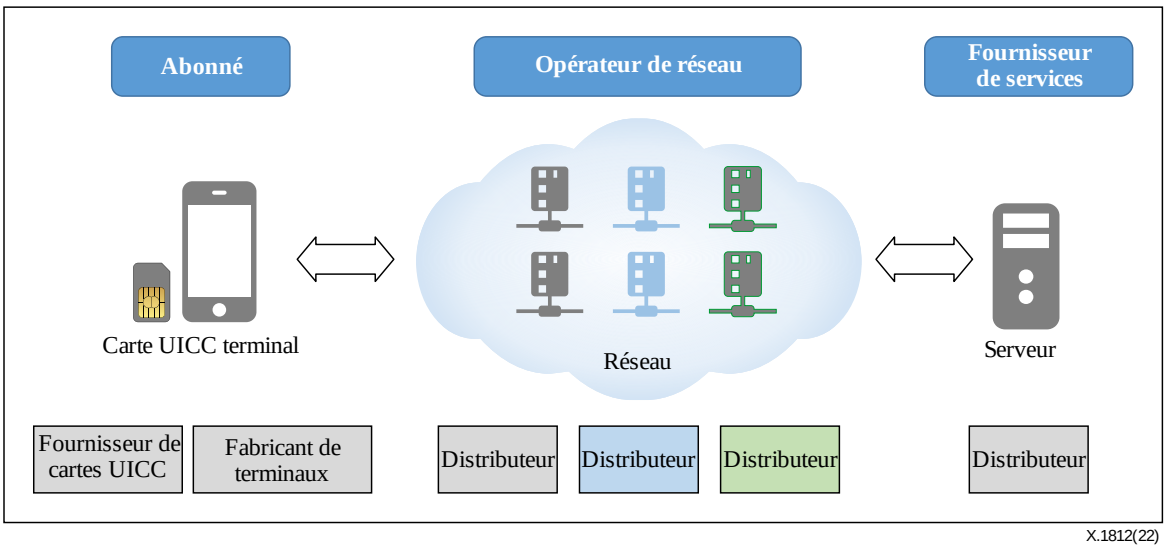


Figure 4 – Principales parties prenantes intervenant dans le domaine d'un opérateur de réseau

Pour ce qui est des IMT-2020, les technologies de réseaux pilotés par logiciel/virtualisation des fonctions de réseau ont été largement perfectionnées et ont progressivement commencé à être déployées dans le réseau. Les technologies de l'information sont également de plus en plus utilisées pour le développement des réseaux de télécommunications. Lorsque l'architecture réseau des IMT-2020 a été conçue, une architecture novatrice fondée sur les services a été adoptée afin de mieux exploiter les technologies de l'information pour le déploiement et la maintenance. L'élément de réseau (NE) est remplacé par la fonction de réseau (NF), qui permet une exploitation et une maintenance plus souples. La fonction de réseau peut être mise en œuvre sous la forme d'une fonction de réseau virtualisée (VNF), voire même d'applications logicielles exécutées dans une machine virtuelle. Cela semble indiquer que la virtualisation de réseau sera largement utilisée dans le déploiement des réseaux IMT-2020. De ce fait, la mise en œuvre ne concerne plus les dispositifs matériels et logiciels intégrés originaux, mais elle se fait désormais par le biais d'une combinaison de trois couches, à savoir les équipements matériels, la couche virtuelle et la fonction de réseau virtualisée. Par conséquent, les principales parties prenantes intervenant dans ce scénario sont: les utilisateurs ou abonnés, les fabricants de terminaux mobiles, les fournisseurs de cartes à circuits intégrés universelles (UICC), les distributeurs d'éléments de réseau (fournisseurs d'équipements matériels, fournisseurs de couches de virtualisation, fournisseurs de fonctions de réseau virtualisées) et les opérateurs de réseau. Ces parties prenantes sont présentées dans la Figure 5.

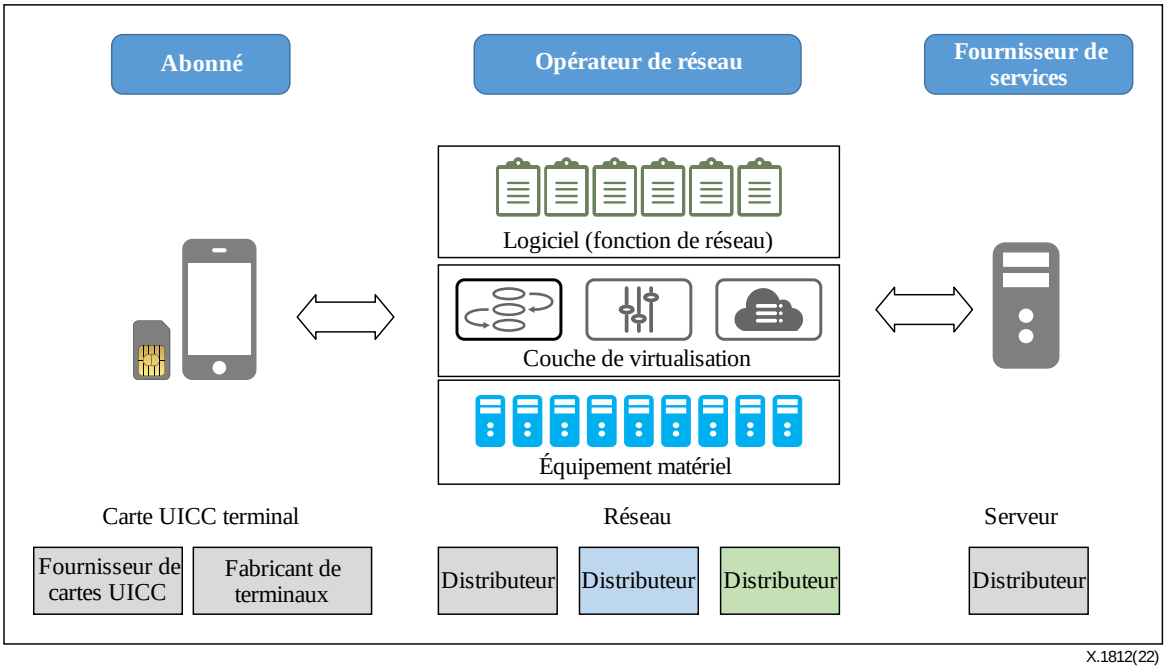


Figure 5 – Principales parties prenantes intervenant dans le déploiement de la virtualisation de réseau au sein du domaine d'un opérateur de réseau

8.2.2 Rôles joués par les parties prenantes dans ce scénario

Les parties prenantes susmentionnées jouent les rôles ci-après dans ce scénario:

- Utilisateurs ou abonnés: il s'agit des utilisateurs finals, par exemple les clients de services de télécommunication. Les équipements d'abonnés comprennent le terminal mobile fourni par un fabricant et la carte UICC par un distributeur de cartes.
- Fabricant de terminaux mobiles: cette entité fournit des terminaux pouvant être utilisés par les utilisateurs ou abonnés pour communiquer avec un réseau.
- Fournisseur de cartes UICC: cette entité fournit des cartes UICC pouvant être utilisées pour représenter l'identité des abonnés.
- Distributeur d'éléments de réseau: cette entité fournit des appareils ou des composants d'appareils pouvant être assemblés pour créer un système de télécommunication ou un système/une plate-forme de service.

  NOTE – S'il fournit des composants, il peut également appartenir à la catégorie des fournisseurs d'équipements matériels, des fournisseurs de couches de virtualisation ou des fournisseurs de fonctions de réseau virtualisées.
- Opérateur de réseau: cette entité possède ou contrôle tous les éléments nécessaires pour vendre et fournir des services de télécommunication aux abonnés et aux fournisseurs de services.

8.3 Scénario 2: interconnexion et itinérance

8.3.1 Considérations générales

Ce scénario concerne essentiellement les relations au sein des réseaux.

Un réseau de télécommunication mobile peut permettre d'offrir des services aux utilisateurs du monde entier sur la base de l'interconnexion et de la coordination entre les opérateurs à l'échelle mondiale. Cette interconnexion et cette coordination entre les opérateurs impliquent une coordination et une coopération au niveau des couches de service et de transport.

Jusqu'à présent, le principe de conception adopté pour garantir l'interconnexion entre les opérateurs de réseaux mobiles terrestres publics (PLMN) était que les opérateurs (au niveau des services) pouvaient se faire entièrement confiance et que la transmission des données de signalisation et d'utilisateur était également fiable. Afin que les messages de signalisation soient correctement transmis à un opérateur donné, le fournisseur IPX a été introduit. Toutefois, du fait de la croissance des réseaux et de l'utilisation de l'Internet, les connexions IPX sont de plus en plus complexes et peuvent également être attaquées via l'Internet. Par conséquent, les opérateurs peuvent uniquement garantir la sécurité des connexions IPX qui les concernent directement, et non celle des liaisons entre les opérateurs et de toutes les autres liaisons des opérateurs. Ce qui précède est illustré dans la Figure 6.

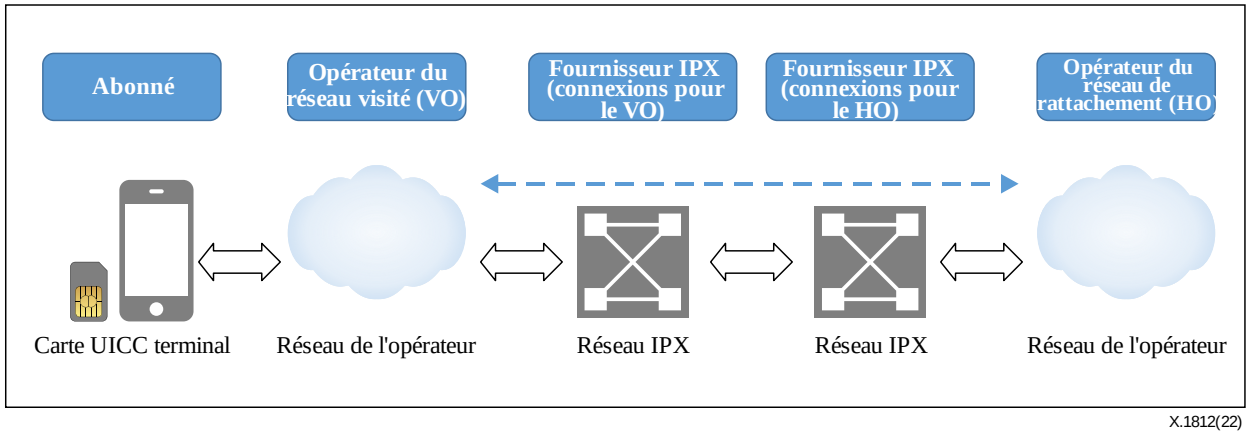


Figure 6 – Principales parties prenantes intervenant dans le scénario d'interconnexion et d'itinérance

En outre, de nombreuses vulnérabilités identifiées chez les opérateurs ont été exploitées, ce qui a permis aux auteurs d'attaques de cibler d'autres opérateurs en utilisant des dispositifs compromis en tant que portes d'entrée. Par conséquent, les opérateurs se méfient désormais également des messages transmis au sein de la couche service [b-3GPP TS 33.501].

Les principaux acteurs intervenant dans un tel scénario sont les utilisateurs ou abonnés, les opérateurs des réseaux visités, les opérateurs des réseaux de rattachement et les opérateurs IPX (fournisseur de connexions IPX pour l'opérateur du réseau visité ou fournisseur de connexions IPX pour l'opérateur du réseau de rattachement).

8.3.2 Rôles joués par les parties prenantes dans ce scénario

Les parties prenantes susmentionnées jouent les rôles ci-après dans ce scénario:

- Utilisateurs ou abonnés: il s'agit des utilisateurs finals, c'est-à-dire les clients de services de télécommunication.
- Opérateurs du réseau visité: ces opérateurs offrent des services d'accès à l'abonné lorsque ce dernier se trouve en dehors de la zone de couverture de l'opérateur du réseau de rattachement.
- Opérateur du réseau de rattachement: il s'agit de l'opérateur auprès duquel les utilisateurs ont souscrit un abonnement et qui leur fournit des services.
- Opérateur IPX (fournisseur de connexions IPX pour l'opérateur du réseau visité ou fournisseur de connexions IPX pour l'opérateur du réseau de rattachement): cette entité fournit un service d'échange de paquets interréseaux entre les opérateurs.

8.4 Scénario 3: location de voiture avec contrôle à distance

8.4.1 Considérations générales

Ce scénario concerne essentiellement les relations au sein des terminaux et les relations terminal-service.

De plus en plus de véhicules communiquent avec une plate-forme distante par le biais d'un module de communication intégré dans le véhicule ou installé ultérieurement. Dans ces véhicules, il est possible de transférer des données spécifiques sur l'état vers une plate-forme distante ou d'obtenir des instructions auprès de cette plate-forme. Dans ce contexte, le véhicule comprend deux éléments: l'un concerne les télécommunications et est fourni par le fabricant de terminaux et l'autre est le véhicule lui-même, fabriqué dans l'usine automobile.

Le réseau traditionnel de communication mobile permet principalement de fournir à l'abonné des services de téléphonie, de messages courts et d'accès au réseau de données. L'abonné est l'utilisateur final du terminal. Pour ce qui est des services de location de voitures, les conducteurs qui utilisent des véhicules équipés de terminaux de communication ne sont pas des abonnés. Par ailleurs, le locataire de la voiture doit généralement utiliser une application sur son terminal mobile pour interagir avec la plate-forme via un réseau de communication afin d'obtenir des données sur le véhicule à distance ou de contrôler un véhicule loué à distance, notamment pour localiser le véhicule, déverrouiller ou verrouiller la portière sans la clé ou allumer ou éteindre la climatisation.

Les principales parties prenantes intervenant dans ce type de cas sont donc, comme le montre la Figure 7: le locataire du véhicule, le véhicule lui-même (qui constitue un terminal mobile), les fabricants de terminaux mobiles, les fournisseurs de cartes UICC, les constructeurs automobiles, les distributeurs d'éléments de réseau, les opérateurs de réseau et les fournisseurs d'applications.

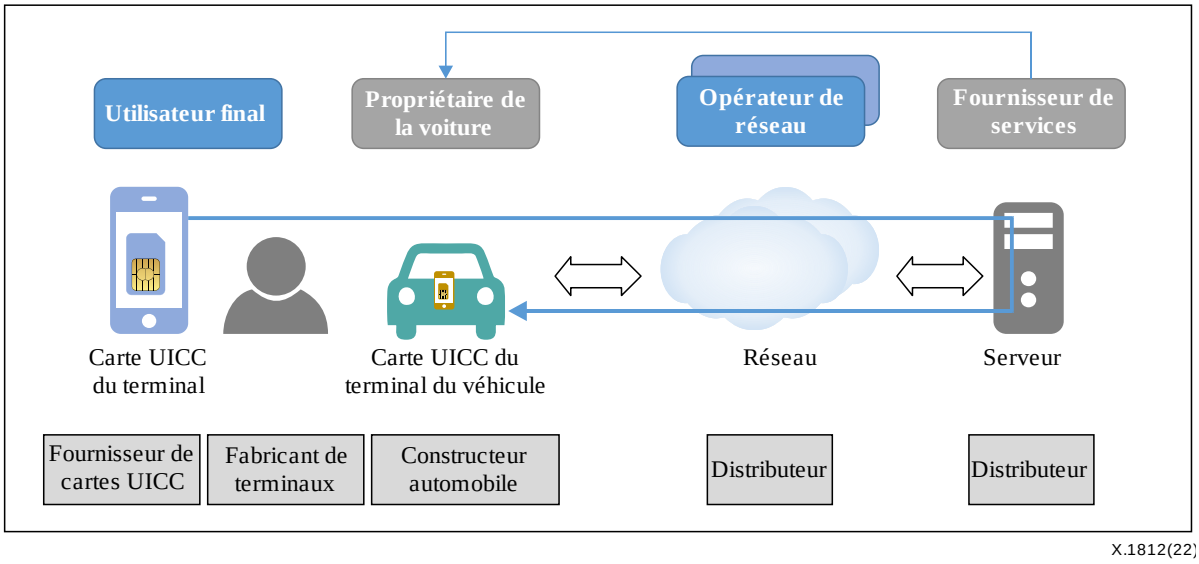


Figure 7 – Principales parties prenantes intervenant dans le scénario d'une location de voiture avec contrôle à distance

8.4.2 Rôles joués par les parties prenantes dans ce scénario

Les parties prenantes susmentionnées jouent les rôles ci-après dans ce scénario:

- Locataire du véhicule: un utilisateur donné loue une voiture auprès d'une agence de location de voitures. Cette personne est également abonnée à un réseau mobile et possède un terminal mobile.
- Véhicule: le véhicule appartient à une agence de location de voitures et embarque un terminal mobile spécifique intégré pouvant être considéré comme abonné à un réseau mobile.

- Fabricant de terminaux mobiles: cette entité fournit des terminaux pouvant être utilisés par les abonnés pour communiquer avec le réseau.
- Fournisseur de cartes UICC: cette entité fournit des cartes UICC pouvant être utilisées pour représenter l'identité de l'abonné.
- Constructeur automobile: cette entité produit des véhicules embarquant ou non un terminal mobile.
- Distributeur d'éléments de réseau: cette entité fournit des appareils ou des composants d'appareils pouvant être assemblés pour créer un système de télécommunication ou un système ou une plate-forme de service.
- Opérateur de réseau: cette entité possède ou contrôle tous les éléments nécessaires pour vendre et fournir des services de télécommunication aux abonnés et aux fournisseurs de services.
- Fournisseur d'applications: cette entité fournit des applications permettant d'offrir des services de location de voitures aux utilisateurs.

8.5 Scénario 4: exposition des capacités de réseau pour le secteur privé

8.5.1 Considérations générales

Ce scénario concerne essentiellement les relations réseau-service et les relations au sein des services.

Les IMT-2020 prévoient de nouvelles fonctionnalités telles que le large bande mobile évolué, les connexions de l'Internet des objets (IoT) massif et les communications ultra-fiables présentant un faible temps de latence. Grâce à ces fonctionnalités, un réseau IMT-2020 peut offrir un meilleur support de connexion aux secteurs verticaux, notamment le secteur privé.

Par rapport aux communications personnelles, les communications au sein d'un secteur vertical supposent des besoins différents comme la diversité des services, la distinction fonctionnelle et l'hétérogénéité des technologies. En général, les communications verticales dans la couche d'application s'accompagnent d'exigences strictes en matière de sécurité telles que l'isolation des communications vis-à-vis des autres utilisateurs issus du secteur privé et le renforcement des capacités de gestion ou de la collaboration avec les opérateurs de réseau par le biais de fonctionnalités spécifiques telles que l'exposition des capacités.

Par rapport aux services traditionnels, les services des secteurs verticaux permettent une coopération avec les opérateurs de réseau. Les fournisseurs d'applications interviennent donc, tout comme les fournisseurs liés aux serveurs d'applications ou aux plates-formes en nuages.

Au niveau du terminal, à l'instar du scénario 3, le dispositif terminal peut également comprendre deux éléments: l'un concerne les communications et est fourni par le fabricant de terminaux et l'autre concerne les applications verticales spécifiques, qui sont fournies par d'autres fabricants de terminaux industriels.

Dans ce cas, comme indiqué dans la Figure 8, les principales parties prenantes intervenant sont: les utilisateurs issus des secteurs verticaux, les fabricants de terminaux de communication, les fournisseurs de cartes UICC, les fabricants de terminaux industriels, les distributeurs d'éléments de réseau, les fournisseurs de serveurs d'applications ou les fournisseurs de services relatifs aux plates-formes en nuage, les fournisseurs d'applications et les opérateurs de réseau.

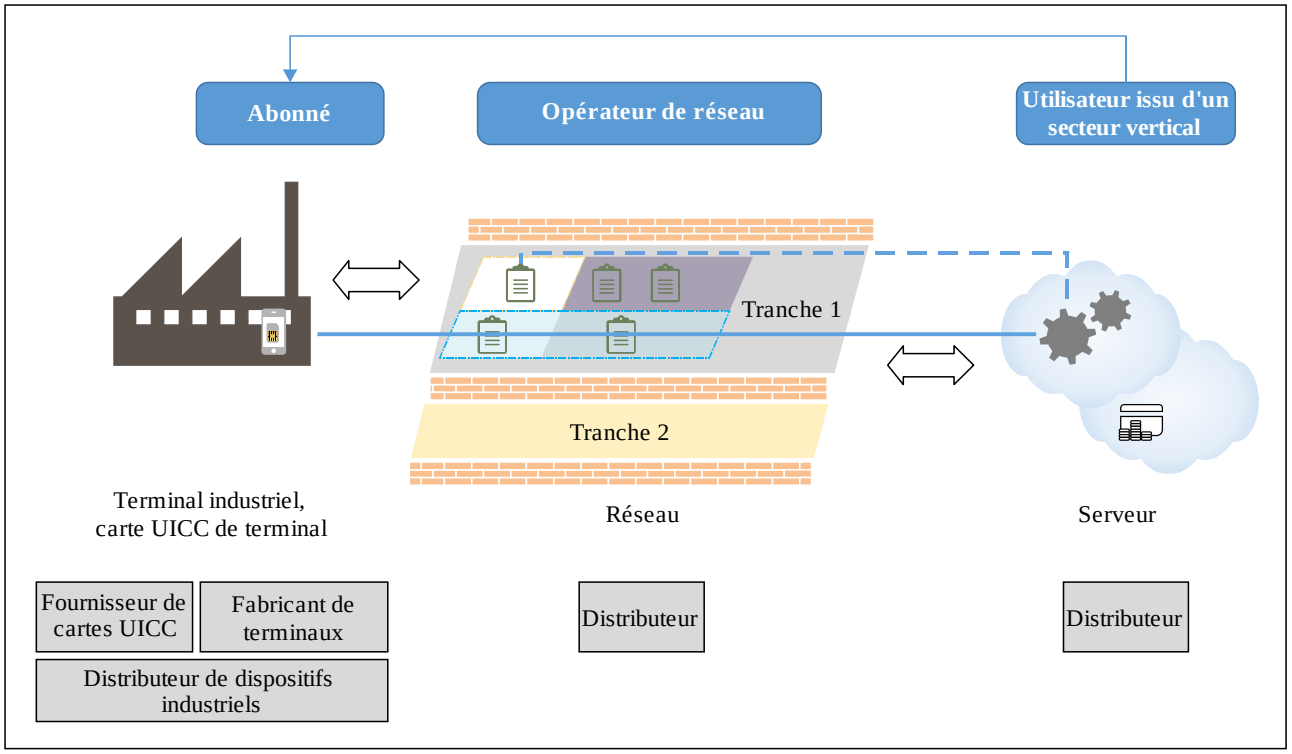


Figure 8 – Principales parties prenantes intervenant dans le scénario d'exposition des capacités de réseau

8.5.2 Rôles joués par les parties prenantes dans ce scénario

Les parties prenantes susmentionnées jouent les rôles ci-après dans ce scénario:

- Utilisateur issu d'un secteur vertical: l'utilisateur issu d'un secteur vertical contrôle un terminal industriel à distance via le réseau de télécommunication en utilisant des applications spécialisées exécutées sur des serveurs d'applications ou des plates-formes en nuage publiques ou privées.
- Fabricant de terminaux de communication: cette entité fournit des terminaux pouvant être utilisés par les abonnés pour communiquer avec le réseau.
- Fournisseur de cartes UICC: cette entité fournit des cartes UICC pouvant être utilisées pour représenter l'identité des abonnés.
- Fabricant de terminaux industriels: cette entité fournit des machines, des réseaux ou des systèmes industriels aux usines ou aux entreprises.
- Distributeur d'éléments de réseau: cette entité fournit des appareils ou des composants d'appareils pouvant être assemblés pour créer un système de télécommunication ou un système ou une plate-forme de services.
- Fournisseur de serveurs d'applications ou fournisseur de services relatifs aux plates-formes en nuage: ces entités possèdent les infrastructures et les plates-formes permettant d'offrir des services de stockage et des ressources de calcul pour les applications de la couche supérieure.
- Fournisseur d'applications: l'usine ou l'entreprise recueille des informations ou fournit des solutions de signalisation des commandes pour les terminaux industriels.
- Opérateur de réseau: cette entité possède ou contrôle tous les éléments nécessaires pour vendre et fournir des services de télécommunication aux abonnés et aux fournisseurs de services.

8.6 Scénario 5: chaînes d'approvisionnement

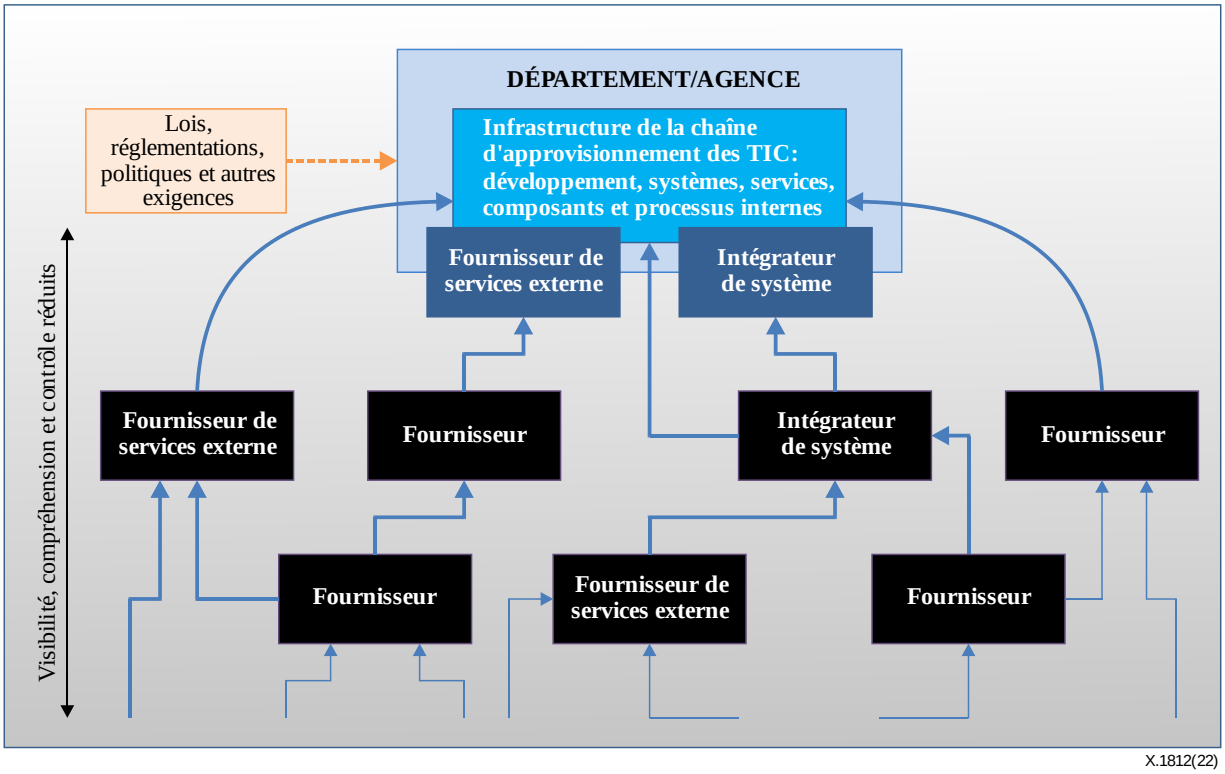
8.6.1 Considérations générales

L'écosystème des IMT-2020 désigne une communauté comprenant nombre d'organisations qui, de par les nombreuses technologies et les vastes connaissances spécialisées qu'elles apportent, contribuent à faire fonctionner les services et les applications des IMT-2020.

Une chaîne d'approvisionnement est un système constitué d'organisations, de personnes physiques, d'activités, d'informations et de ressources qui jouent un rôle dans le transfert d'un produit ou d'un service depuis le fournisseur vers le client. La gestion des risques liés à la chaîne d'approvisionnement correspond aux mesures coordonnées d'une organisation pour identifier, surveiller, détecter et limiter les menaces à la continuité et à la rentabilité de la chaîne d'approvisionnement. La gestion des risques liés à la chaîne d'approvisionnement dans l'écosystème des IMT-2020 comprend les quatre aspects de sécurité fondamentaux suivants:

- L'aspect sécurité: il concerne la confidentialité, l'intégrité et la disponibilité des informations a) qui décrivent la chaîne d'approvisionnement (par exemple les informations relatives aux trajectoires transversales des produits et services des IMT-2020, aussi bien sur le plan logique que physique); ou b) qui circulent dans la chaîne d'approvisionnement (par exemple, propriété intellectuelle pour les éléments contenus dans des produits et services IMT-2020), ainsi que les informations relatives aux parties prenantes intervenant dans la chaîne d'approvisionnement (toute entité qui est au contact d'un produit ou service des IMT-2020 au cours de son cycle de vie).
- L'aspect intégrité: il consiste à veiller à ce que les produits ou les services des IMT-2020 concernés par la chaîne d'approvisionnement soient authentiques ou qu'ils n'aient pas été altérés, qu'ils fonctionnent selon les spécifications définies par l'acquéreur et qu'ils n'aient aucune fonctionnalité additionnelle non sollicitée.
- L'aspect résilience: il consiste à veiller à ce que la chaîne d'approvisionnement fournisse les produits et les services demandés en cas de tension ou d'interruption.
- L'aspect qualité: il consiste à réduire les vulnérabilités qui pourraient limiter la fonction prévue d'un composant, le rendre défaillant ou créer des opportunités d'exploitation.

Ce scénario concerne essentiellement les chaînes d'approvisionnement et les relations à l'intérieur de celles-ci. La Figure 9 montre les principaux acteurs intervenant dans les scénarios des chaînes d'approvisionnement.



TIC: technologies de l'information et de la communication.

Figure 9 – Principales parties prenantes intervenant dans les scénarios des chaînes d'approvisionnement

8.6.2 Rôles joués par les parties prenantes dans ce scénario

De nombreuses parties prenantes interviennent dans une chaîne d'approvisionnement: le développeur ou le fabricant, l'intégrateur de système, le distributeur, les revendeurs et le fournisseur du produit, et le fournisseur de services externe.

Le développeur ou le fabricant fait référence: i) aux développeurs ou aux fabricants de systèmes d'information, de composants de systèmes ou de services de système d'information; ii) aux intégrateurs de systèmes; iii) aux distributeurs; ou iv) aux revendeurs du produit.

Un intégrateur de système est une personne physique ou une entreprise chargée de réunir les sous-systèmes de composants pour former un tout et de veiller à ce que ces sous-systèmes fonctionnent ensemble. Cette pratique s'appelle l'intégration des systèmes.

Un distributeur est toute entité qui fournit des biens ou des services à une entreprise ou à des personnes physiques. Dans de nombreux cas, le distributeur fabrique les produits puis les vend à un client. Une entreprise est une entité juridique séparée de la société contractante qui fournit des services tels que le conseil ou le développement de logiciels.

Un revendeur de produit est une entreprise ou une personne physique qui acquiert des biens ou des services dans l'intention de les vendre plutôt que de les consommer ou de les utiliser.

Un fournisseur est une entité qui fournit des biens et des services à une autre entité.

Le fournisseur de services externe inclut: i) les entités qui font partie de l'organisation mais qui sont en dehors des limites établies pour les autorisations de sécurité des systèmes d'information organisationnels; ii) les entités extérieures à l'organisation, issues soit du secteur public (par exemple les organismes fédéraux) soit du secteur privé (par exemple les fournisseurs de services commerciaux); ou iii) une combinaison d'acteurs des secteurs public et privé.

8.7 Parties prenantes de l'écosystème des IMT-2020

Sur la base des cas d'utilisation décrits dans les paragraphes 8.2 à 8.6, l'écosystème des IMT-2020 peut être divisé en quatre types de parties prenantes, qui sont représentées dans la Figure 10: le fabricant, l'opérateur de réseau, le fournisseur de services et l'utilisateur final.

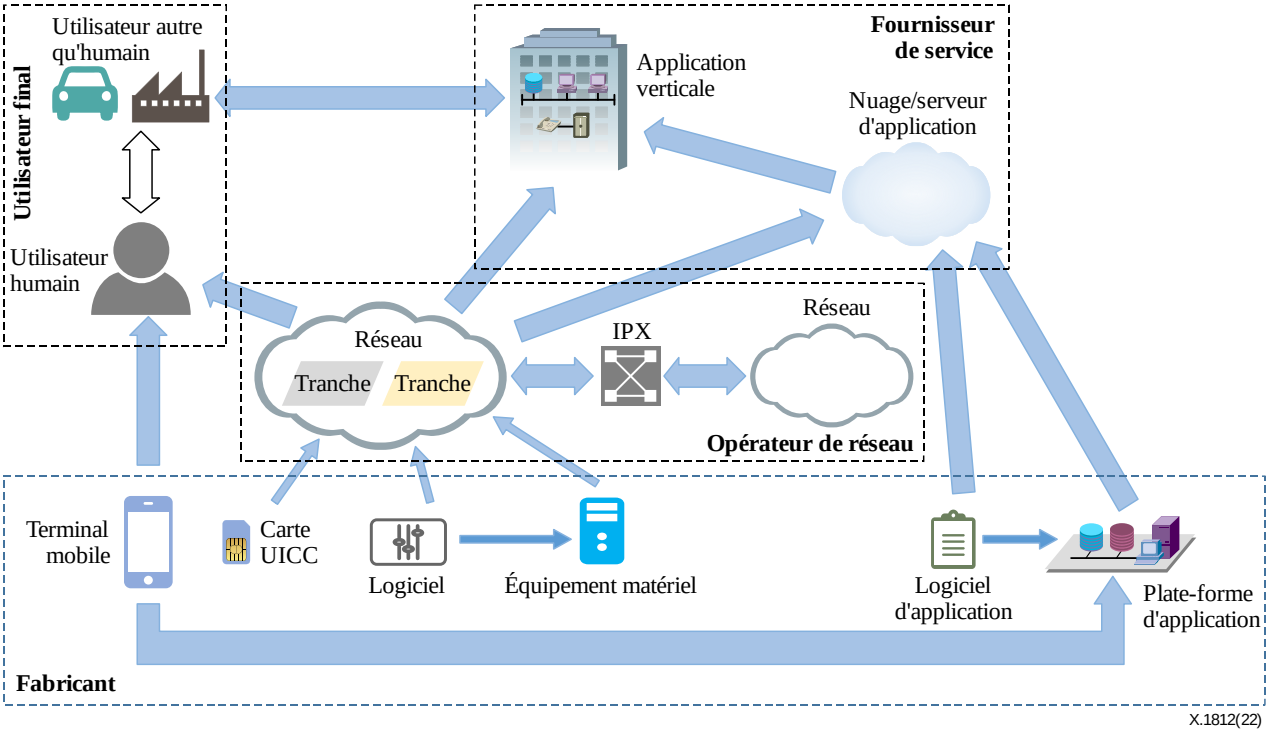


Figure 10 – Parties prenantes de l'écosystème des IMT-2020

Une partie prenante peut avoir un lien direct avec une autre partie prenante et un lien indirect avec d'autres entités par l'intermédiaire d'une partie prenante, par exemple en jouant un rôle dans la chaîne d'approvisionnement.

Dans l'écosystème des IMT-2020, les fabricants peuvent être considérés comme un groupe de développeurs ou de fabricants, d'intégrateurs de systèmes et de distributeurs. Les opérateurs de réseau peuvent être considérés comme des revendeurs de produits et des fournisseurs de services de réseau. Les fournisseurs de services peuvent être considérés comme des parties prenantes externes.

Les fabricants de composants fournissent les éléments techniques essentiels aux fabricants de dispositifs hertziens et aux fabricants d'équipements de réseau, mais ils peuvent également les fournir directement aux opérateurs de réseau. Les fabricants de dispositifs hertziens fournissent des équipements aux utilisateurs finals ou des composants qui seront intégrés aux machines industrielles, tandis que les fabricants d'équipements de réseau produisent les équipements destinés à appuyer l'infrastructure de réseau (cela inclut les technologies hertziennes et filaires). Les opérateurs de réseau associent ces dispositifs avec les composants de réseau, les équipements de réseau et les réseaux d'autres opérateurs, grâce à l'échange IPX, pour créer un réseau opérationnel à l'échelle mondiale qui puisse bénéficier aux utilisateurs finals. Les utilisateurs finals passent des appels téléphoniques, envoient des messages texte et exécutent des applications sur le réseau. Les opérateurs de réseau fournissent également des services de communication et des services connexes aux fournisseurs de services externes grâce à leur service d'exposition des capacités du réseau et à d'autres services spécifiques.

9 Niveau, critères et modèle de confiance

9.1 Considérations générales

Comme défini dans le paragraphe 3.1.11, la confiance est la mesure dans laquelle un utilisateur ou une autre partie prenante est convaincu(e) qu'un produit ou un système se comportera comme prévu. En outre, la confiance joue un rôle important dans l'écosystème des IMT-2020. La présente Recommandation définit un modèle de confiance pour l'écosystème des IMT-2020, afin de permettre aux parties prenantes de prendre des décisions motivées en matière de confiance et de sécurité.

Le modèle de confiance de l'écosystème des IMT-2020 est divisé en trois niveaux.

- Le premier niveau consiste à répondre aux exigences définies par les pouvoirs publics et les organismes de réglementation en matière de confiance. Les facteurs clés de la confiance comprennent l'adoption des normes internationales et l'établissement d'une certification publique et transparente.
- Le deuxième niveau de confiance consiste à répondre aux exigences des organismes industriels en matière de confiance. En ce qui concerne ces acteurs, les facteurs clés de la confiance comprennent l'identification des parties prenantes, des acteurs offrant des solutions de bout en bout (E2E), de l'utilisateur final dans le marché, du modèle économique, des niveaux de confiance et des relations de confiance.
- Le troisième niveau de confiance consiste à susciter la confiance en offrant des solutions techniques basées sur les facteurs clés des deux premiers niveaux.

La présente Recommandation concerne essentiellement le deuxième et le troisième niveau, autrement dit les organismes industriels et les solutions techniques.

L'opérateur d'un réseau IMT-2020 doit pouvoir compter sur des dispositifs ou des équipements fournis par des fabricants pour établir son système de réseau. Ainsi, il doit pouvoir avoir confiance dans le fait que les fabricants fourniront des dispositifs qui répondront à ses exigences.

Le fournisseur de services a besoin du réseau pour transmettre des informations et il doit donc pouvoir avoir confiance dans le fait que l'opérateur de réseau fera en sorte que les données soient transférées de manière fiable et rapide. Le fournisseur de service doit également pouvoir compter sur les dispositifs fournis par les fabricants afin d'établir ses services et il doit donc pouvoir avoir confiance dans le fait que les fabricants fourniront des dispositifs qui répondront à ses exigences.

Les utilisateurs finals doivent pouvoir compter sur le réseau pour transmettre des données et sur les applications de service. Ils doivent donc pouvoir avoir confiance dans le fait que l'accès au réseau fourni par l'opérateur de réseau est légal et efficace. Leurs exigences vis-à-vis du fournisseur de service en termes de confiance sont similaires.

9.2 Niveaux de confiance

De par la nature même de la confiance, il est difficile de la quantifier de manière rationnelle. Dans le modèle de confiance défini dans la présente Recommandation, une approche qualitative du niveau de confiance est introduite afin d'amener une réflexion sur les incidences des différents degrés de confiance.

Les services basés sur les IMT-2020 fonctionnent dans des contextes variés et ils impliquent donc des exigences diverses en termes de confiance. Par exemple, les différents secteurs verticaux offrent différents services, qui fonctionnent dans des scénarios divers, et leur positionnement en matière de confiance est donc différent. En outre, certains secteurs comme celui des réseaux intelligents rentrent dans la catégorie des infrastructures essentielles nationales, tandis que d'autres, comme le secteur de la location de voitures, concernent uniquement des scénarios moins critiques du quotidien.

Si un secteur vertical donné est considéré comme faisant partie de l'infrastructure essentielle, alors il est évident que les acteurs de ce secteur auront davantage besoin d'avoir confiance dans le fait que le

système des IMT-2020 se comportera comme prévu. Autrement dit, un niveau plus élevé de confiance doit être atteint pour ce secteur, étant donné que tout dommage porterait atteinte à la stabilité nationale. En revanche, un niveau de confiance moins élevé serait nécessaire dans le cas des secteurs dont les défaillances auraient des incidences relativement faibles.

Par exemple, les services IoT à bande étroite liés notamment à l'Internet des véhicules (IoV), à l'Internet industriel, aux réseaux intelligents et à l'arrosage des fleurs impliquent tous des niveaux de confiance différents, étant donné que les défaillances qui pourraient subvenir dans ces secteurs auraient des incidences différentes sur la société ou sur les utilisateurs.

Le niveau de confiance nécessaire dans un cas de figure donné dépend du niveau d'incidence qu'une défaillance d'un secteur vertical donné pourrait avoir sur la société et sur le pays. L'acteur qui est le mieux placé pour déterminer ce niveau de confiance est probablement l'organisation verticale elle-même, étant donné que les représentants de nombreux domaines participent à ses travaux et qu'elle dispose des compétences spécialisées nécessaires pour réaliser l'analyse requise. Par ailleurs, la définition du niveau de confiance relève de ses obligations de diligence due. Par conséquent, dans les cas de figure où le niveau de confiance doit être plus élevé, les responsabilités incombant aux parties prenantes concernées doivent être accrues. En d'autres termes, il est également nécessaire de garantir un niveau de confiance plus élevé pour ces parties prenantes.

Aux fins du modèle de confiance défini dans la présente Recommandation, on partira du postulat que le niveau de confiance des différentes parties peut être décrit selon trois niveaux qualitatifs: élevé, moyen ou faible. Ce postulat tient à deux raisons principales:

- Premièrement, l'assignation de valeurs quantitatives à des niveaux de confiance est susceptible de poser de nombreux problèmes, étant donné qu'il n'existe aucune unité de mesure évidente pour la confiance (contrairement, par exemple, à l'analyse des risques, où la mesure peut se baser sur une combinaison entre la probabilité d'occurrence et une évaluation du coût d'impact annualisé).
- Deuxièmement, cette échelle à trois niveaux est suffisamment complète pour s'appliquer à de nombreux cas d'utilisation existants, mais elle est également adoptée dans d'autres contextes, par exemple dans le cadre du mécanisme d'assurance de la sécurité des équipements de réseau (NESAS) (voir [b-GSMA FS.13], [b-GSMA FS.14], [b-GSMA FS.15] et [b-GSMA FS.16]), pour évaluer les exigences relatives à la confiance.

La difficulté consiste à déterminer la signification de ces trois niveaux de confiance afin que le modèle décrit dans la présente Recommandation puisse être utilisé de manière cohérente. Les critères de confiance, établis pour permettre de définir les niveaux de confiance, sont énoncés au paragraphe 9.3.

En raison de la diversité des équipements et du large éventail de scénarios de déploiement dans des secteurs verticaux donnés, en pratique le niveau de confiance général devrait être affiné selon le contexte. Par exemple, il est évident que le niveau de confiance nécessaire pour la conduite autonome varie en fonction de la technologie de l'Internet des véhicules, du réseau de campus ou du macroréseau qui sont utilisés.

L'exemple ci-après montre également que la définition du niveau de confiance doit être complexe et adaptée au contexte. Supposons qu'un opérateur sélectionne des fabricants d'équipements de réseau en fonction du niveau de confiance défini. Si un seul niveau de confiance est défini, tous les fabricants d'équipements de réseau doivent être sélectionnés sur la base d'un niveau de confiance unique. Toutefois, le réseau central est plus sensible et a plus de valeur et d'influence que les antennes, par exemple. Par conséquent, dans un scénario type, le niveau de confiance du fabricant des équipements du réseau central devra être plus élevé que celui du fabricant de l'antenne.

Afin d'affiner davantage le niveau de confiance, celui-ci est défini séparément pour l'unité d'activité et le scénario d'activité. Dans le cas d'un secteur vertical, cela signifie que le niveau de confiance de l'ensemble du secteur vertical et celui du scénario spécifique au sein du secteur vertical devront faire

l'objet de définitions distinctes. Le Tableau 1 montre les combinaisons possibles de niveaux de confiance dans les deux cas de figure.

Tableau 1 –Niveau de confiance de l'unité d'activité et des scénarios d'activité, et relation entre les deux

Niveau de confiance de l'unité d'activité	Niveau de confiance des scénarios d'activité
Élevé	Élevé
	Moyen
	Faible
Moyen	Moyen
	Faible
Faible	Faible

Pour faire en sorte que la définition du niveau de confiance soit plus pratique et plus universelle, il est recommandé de définir la composante du niveau de confiance de manière souple. Par exemple, la composante du niveau de confiance pourrait être définie en fonction de la valeur de l'actif ou de la zone de déploiement.

Prenons un exemple concret: le niveau de confiance associé à l'ensemble du réseau électrique est élevé mais, au sein de ce réseau, les câbles et les poteaux électriques n'ont pas autant de valeur que les capteurs et les infrastructures de transmission de signaux du réseau IMT-2020. Même s'il comprend des capteurs et des infrastructures de transmission de signaux, un réseau intelligent déployé dans une petite ville n'est pas aussi sensible qu'un réseau intelligent déployé dans une métropole.

Le Tableau 2 montre les niveaux de confiance possibles dans la relation existant entre un secteur vertical et une partie prenante.

Tableau 2 – Niveaux de confiance possibles entre un secteur vertical et une partie prenante

Niveau de confiance du système	Niveau de confiance de la composante	Niveau de confiance de la partie prenante
Élevé	Élevé	Élevé
	Moyen	Moyen
	Faible	Faible
Moyen	Moyen	Moyen
	Faible	Faible
Faible	Faible	Faible

9.3 Critères de confiance

Pour déterminer si le niveau de confiance est élevé, moyen ou faible, il est nécessaire d'évaluer les relations de confiance entre les parties prenantes. La relation de confiance entre deux parties prenantes données est influencée par de nombreux facteurs, et le degré de confiance entre plusieurs parties prenantes de deux catégories différentes sera également variable. Il est donc nécessaire de définir les critères d'évaluation individuellement.

Étant donné que le niveau de confiance est choisi pour limiter les préjudices causés par les éventuelles menaces, ainsi que les risques qu'elles entraînent, les critères peuvent inclure la valeur de l'actif, l'échelle d'incidence, la gravité des incidences et la probabilité d'occurrence du risque et se baser sur les normes relatives à la gestion des risques, notamment les normes [b-NIST SP800-30], [b-ISO 31000] et [b-ISO/CEI 27005].

- Actifs: L'importance de ce facteur est claire. Plus un actif est important, plus il est nécessaire qu'il soit entièrement sous le contrôle de la partie prenante, et plus le niveau de confiance doit être élevé.
- Échelle d'incidence: Pour une partie prenante de grande envergure, plus le champ d'influence est large, plus les incidences d'une éventuelle défaillance seront importantes. Par conséquent, un niveau de confiance élevé est nécessaire si le champ d'influence est large. Par exemple, un opérateur aura besoin d'un niveau de confiance plus faible vis-à-vis d'un distributeur de petites cellules couvrant des zones limitées que vis-à-vis d'un distributeur d'éléments du réseau central couvrant une zone importante.
- Gravité des incidences: Pour une partie prenante œuvrant au sein d'une infrastructure essentielle, les défaillances ont des conséquences plus graves, et elle doit donc déployer davantage d'efforts pour prévenir ces défaillances. Par conséquent, elle a d'autant plus besoin de procéder à des évaluations prudentes lorsqu'elle interagit avec d'autres parties. Ainsi, plus une défaillance a des incidences importantes sur une relation, plus le niveau de confiance doit être élevé.
- Probabilité d'occurrence du risque: Si la probabilité d'occurrence est élevée, le risque est davantage susceptible de se produire.

L'écosystème des IMT-2020 est très complexe. Chaque catégorie de parties prenantes, par exemple les utilisateurs finals, les fabricants d'équipements, les opérateurs de réseau et les fournisseurs de services englobe tout un éventail de cas spécifiques. Étant donné que la confiance est un concept subjectif, il est difficile de la mesurer et d'établir des normes dans ce domaine. Le niveau de confiance entre deux instances est également distinct. Toutefois, il est nécessaire de définir un ensemble de niveaux de confiance généraux pouvant être utilisé dans la plupart des situations, afin de fournir des indications à toutes les entités de l'écosystème des IMT-2020. Les niveaux de confiance sont les suivants: faible, moyen et élevé.

Le Tableau 3 donne un exemple de la manière dont un niveau de confiance général peut être défini sur la base des différents critères de confiance.

Tableau 3 – Critères utilisés pour définir le niveau de confiance

Niveau de confiance général	Critères utilisés pour définir le niveau de confiance			
	Valeur de l'actif	Échelle d'incidence	Gravité des incidences	Probabilité d'occurrence du risque
Élevé	Élevé	Élevé	Élevé	Élevé
Moyen	Moyen	Moyen	Moyen	Moyen
Faible	Faible	Faible	Faible	Faible

Lorsque les différents facteurs sont mis en correspondance, comme illustré dans le Tableau 3, il est important que les critères de confiance utilisés pour définir le niveau de confiance tiennent compte des mesures d'atténuation des risques qui ont déjà été adoptées ou qu'il est prévu de mettre en œuvre. Par exemple, lorsque l'Internet existant est utilisé pour le commerce électronique haut de gamme, la valeur de l'actif, l'échelle d'incidence et la gravité des incidences peuvent tous être décrits comme étant très élevés. En outre, il semblerait au premier abord que la probabilité d'une attaque soit également très haute, étant donné que les protocoles de communication Internet n'intègrent pas de fonctionnalités de sécurité robustes. En utilisant le Tableau 3, nous pourrions en déduire que le niveau de confiance dans l'Internet doit être élevé afin de répondre aux besoins du commerce électronique. Toutefois, malgré le fait que le niveau de confiance dans l'Internet est, en réalité, faible étant donné que l'Internet n'offre aucune garantie en termes de confidentialité, d'intégrité ou de disponibilité des

canaux de communication, le commerce électronique est très largement et efficacement utilisé pour les immenses volumes de transactions.

De fait, si ce scénario fonctionne, c'est parce que les risques liés à la confidentialité et à l'intégrité des transferts de données sont écartés grâce à l'utilisation courante de la sécurité dans la couche transport (norme [b-IETF RFC 5246]) pour protéger les communications entre les points d'extrémité de communication, qui pourraient être intégrés aux exigences de sécurité définies au paragraphe 10.2.

En conclusion, le calcul du niveau de confiance nécessaire doit tenir compte du niveau de menace réel après que des mesures d'atténuation des risques spécifiques aux applications aient été adoptées. Sinon, des demandes non réalistes risquent d'être formulées concernant le niveau de confiance nécessaire dans les fournisseurs d'équipements et de services, ce qui pourrait entraîner une augmentation considérable des coûts.

9.4 Modèle de confiance basé sur la cartographie des relations de confiance

Afin d'établir des limites de sécurité et des mesures de sécurité interopérables et normalisées pour les IMT-2020, il est nécessaire de concevoir et d'utiliser le modèle de confiance de manière appropriée. Pour faire en sorte que le modèle de confiance soit efficace, les relations de confiance doivent être analysées.

En outre, compte tenu des facteurs mentionnés au paragraphe 9.2, la relation de confiance générale entre deux parties est unidirectionnelle et non bidirectionnelle. Le Tableau 4 montre un exemple d'analyse des relations de confiance entre différentes catégories de parties prenantes.

Tableau 4 – Relations de confiance entre les parties prenantes

Sujet	**Objet**			
	Utilisateur final	**Fabricant**	**Opérateur de réseau**	**Fournisseur de services**
Utilisateur final		Moyen/faible	Élevé/moyen/ faible	Élevé/moyen/ faible
Fabricant	–		Élevé	Élevé
Opérateur de réseau	Faible	Élevé/moyen/ faible		Élevé/moyen/ faible
Fournisseur de services	Élevé/moyen/ faible	Élevé/moyen/ faible	Élevé/moyen/faible	

Les relations de confiance entre les différents partenaires de l'écosystème des IMT-2020 sont généralement très complexes. Il est donc nécessaire d'établir un modèle de confiance qui tienne compte de cette complexité. Autrement dit, la relation de confiance générale peut être précisée afin de lui attribuer des valeurs de confiance au niveau d'un sous-système. Le Tableau 5 montre un exemple d'analyse des relations de confiance au niveau d'un sous-système.

Tableau 5 – Relations de confiance au niveau d'un sous-système de fabricants

Sujet	Objet			
	Puce/modem	**Module**	**Fournisseur de dispositifs**	**Fournisseur de logiciels**
Puce/modem				
Module	Élevé/moyen			
Fournisseur de dispositifs	Élevé/moyen	Élevé/moyen		
Fournisseur de logiciels	Élevé/moyen	Élevé/moyen	Élevé/moyen	

Sur la base du modèle décrit dans le Tableau 6, un scénario de bout en bout de location de voiture est fourni à titre d'exemple.

Tableau 6 – Modèle de confiance basé sur les relations de confiance dans un scénario de location de voiture

Sujet		Objet						
		Fournisseur de services (véhicule)	**Locataire du véhicule**	**Fabricant**			**Opérateur de réseau**	**Fournisseur de services**
				Terminaux/ cartes UICC	**Automobiles (à l'exclusion des terminaux et des cartes UICC)**	**Équipements de réseau**		
Véhicule			Moyen/ faible	Moyen	Élevé/moyen	–	Élevé/ moyen/ faible	Élevé
Locataire du véhicule		Élevé/ moyen		Moyen/ faible	Moyen/faible	–	Élevé/ moyen/ faible	Élevé/ moyen/ faible
Fabricant	**Terminaux/ cartes UICC**	–	–		–	–	Élevé	Élevé
	Automobiles	–	–	–		–	–	Élevé
	Équipements de réseau	–	–	–	–		Élevé	–
Opérateur de réseau		Faible	Faible	Élevé/ moyen/ faible	–	Élevé/ moyen/ faible		Élevé/ moyen/ faible
Fournisseur de services		Élevé	Moyen/ faible	Élevé/ moyen/ faible	Élevé/moyen	–	Élevé/ moyen/ faible	

10 Exigences de sécurité étayées par un modèle de confiance basé sur les relations de confiance

10.1 Considérations générales

Dans un scénario donné, un système est établi par diverses parties prenantes, qui fournissent des fonctions et des services différents pour faire en sorte que le système se comporte et fonctionne comme prévu, afin d'en tirer profit. Ensemble, ces parties prenantes constituent l'écosystème.

Lorsque l'écosystème est en marche, des menaces et des dangers potentiels peuvent apparaître et entraver les activités commerciales. Pour éviter que les menaces ne se transforment en préjudice, toutes les parties prenantes doivent contribuer à faire en sorte que l'écosystème fonctionne en continu, qu'il respecte la législation et que ses acteurs fournissent des produits, des solutions et des services sûrs en adoptant des processus de conception sécurisés.

Le modèle de confiance défini au paragraphe 9 peut être utilisé pour définir des exigences de sécurité basées sur la confiance, à l'intention des parties prenantes.

10.2 Exigences de sécurité basées sur le niveau de confiance

10.2.1 Aperçu général

Le niveau de confiance vis-à-vis d'une partie prenante peut être utilisé pour déterminer si la partie prenante en question est en mesure de fournir une capacité adéquate de défense contre les dommages. Des exigences de sécurité peuvent être définies pour atténuer ces dommages. Dans ce contexte, les exigences de sécurité peuvent être basées sur les capacités de l'organisation, à savoir notamment le niveau professionnel du personnel, l'utilisation de processus de développement sécurisés tels que le cycle de développement sécurisé ou des capacités de sécurité des procédures opérationnelles ainsi que la capacité technologique liée à la solution permettant d'assurer la fiabilité. Pour plus de détails, se référer aux normes et aux pratiques telles que la norme [b-NIST FICIC] et la norme [b-BSIMM] (voir le Tableau 7).

Tableau 7 – Niveau de confiance et catégories d'exigences de sécurité

Niveau de confiance	**Catégories d'exigences de sécurité**		
Sujet	**Objet**		
	Capacité de l'organisation (crédit satisfaisant)	Sécurité pendant le développement et le cycle de vie d'un produit, ou capacité d'application de la sécurité (procédure satisfaisante)	Capacité technologique liée à la solution permettant d'assurer la fiabilité (solution satisfaisante)
Élevé	√	√	√
Moyen	√	√	–
Faible	√	–	–

10.2.2 Exigences institutionnelles

10.2.2.1 Introduction

Les capacités de sécurité liées à la confiance d'une organisation recouvrent plusieurs aspects: la réputation de l'organisation, sa capacité à exécuter les contrats, l'harmonie des valeurs, les compensations possibles en cas de ruptures de contrat et son indépendance.

10.2.2.2 Réputation

La réputation correspond au degré selon lequel, historiquement, une entité a respecté les objectifs spécifiés pour un produit ou un système. La réputation est une appréciation qui pourrait être fondée sur une connaissance directe ou indirecte des interactions antérieures des parties prenantes. Elle est utilisée pour évaluer le niveau de confiance vis-à-vis d'une partie prenante. En tant que représentation de l'assurance, la confiance s'appuie généralement sur des données historiques pour déterminer s'il est probable que la partie prenante concernée soit digne de confiance à l'avenir. Par conséquent, lorsqu'une partie prenante donnée a, par le passé, bien respecté les termes d'un accord, sa réputation dans le secteur sera également meilleure, lui permettant ainsi de susciter une confiance plus élevée chez l'autre partie. Les données destinées à la gestion de la réputation peuvent être obtenues grâce à différentes ressources fiables et largement reconnues, sur la base d'éléments concrets tels que des certificats ou des rapports annuels et financiers officiels. En revanche, il est possible qu'une partie prenante donnée ait des réputations différentes dans des secteurs distincts. Par exemple, la relation entre un fabricant de dispositifs et un opérateur de réseau ou un fournisseur de services est celle d'un distributeur et d'un client, tandis que la relation entre différents fabricants peut être basée sur la concurrence. Un fabricant de dispositifs peut donc avoir une bonne réputation aux yeux d'un opérateur de réseau ou d'un fournisseur de services, mais une mauvaise réputation aux yeux d'un concurrent. Par conséquent, au moment d'examiner les informations fournies par des entités extérieures concernant la réputation du fabricant, les opérateurs de réseau ou les fournisseurs de services ne peuvent pas utiliser les informations sur la réputation obtenues auprès d'un fabricant concurrent comme source primaire

10.2.2.3 Exécution des contrats

Dans le cas où un contrat est exécuté dans le cadre d'une coopération continue ou composée de plusieurs phases intermittentes, la qualité de l'exécution du contrat aura des incidences sur la confiance que les deux parties s'accorderont, ainsi que sur leur relation de confiance. Lorsque le contrat est dûment exécuté, une confiance mutuelle naît et une relation de confiance étroite est instaurée. Au contraire, lorsque le contrat est mal exécuté, la confiance mutuelle s'amenuise et la relation de confiance en pâtit. Dans le cas où plusieurs phases intermittentes de coopération se succèdent, par exemple, lorsqu'un utilisateur sollicite un fournisseur de services à plusieurs reprises, ses expériences précédentes influeront directement sur sa confiance dans le système de services. Dans ce cas, il est recommandé d'associer les données d'expérience de l'utilisateur à l'exécution du contrat d'utilisateur et non à la réputation du fournisseur.

10.2.2.4 Harmonie des valeurs

Lorsque des parties prenantes partagent les mêmes valeurs, elles entretiennent une relation plus étroite et leurs attentes sur le long terme sont plus en phase. De ce fait, une confiance mutuelle plus profonde est instaurée entre ces parties prenantes et leur relation de confiance est améliorée.

10.2.2.5 Compensation

La capacité de compensation a trait à la compensation qui est attendue si un engagement n'est pas respecté. La compensation attendue peut être considérée comme une garantie supplémentaire qu'une partie prenante s'efforcera d'exécuter le contrat, même dans des conditions anormales. En règle générale, plus la compensation est généreuse, plus les pertes subies par l'autre partie sont minimes. Cette capacité permettra de renforcer la confiance dans l'autre partie. Par exemple, les lois régionales régissant le cyberenvironnement peuvent édicter le niveau et la sévérité de la sanction ou compensation imposée aux différentes parties prenantes, pour faire en sorte qu'elles soient fiables.

10.2.2.6 Indépendance

L'indépendance d'une partie prenante fait référence à son autonomie dans l'exécution du contrat. L'indépendance inclut la capacité d'une société mère à contrôler une filiale, ainsi que l'influence des

autorités sur l'entité commerciale. Plus une entité collabore avec un nombre important de parties prenantes, plus elle sera influencée par celles-ci, et plus leur relation de confiance sera affectée.

10.2.2.7 Résumé

Le Tableau 8 montre un exemple des liens qui peuvent exister entre les niveaux de confiance et les capacités d'une organisation. Dans la pratique, le choix exact des aspects qui seront nécessaires pour atteindre les niveaux de confiance moyen et faible dépend du domaine d'application. Par exemple, dans certains cas, on peut exiger d'un fournisseur qu'il ait une réputation correcte afin de lui accorder un niveau faible de confiance, tandis que dans d'autres cas, cet aspect peut ne pas être important, même lorsqu'un niveau moyen de confiance est nécessaire.

Tableau 8 – Niveau de confiance et exigences de sécurité concernant les capacités d'une organisation

Niveau de confiance	Exigences de sécurité concernant les capacités d'une organisation				
	Réputation	**Exécution des contrats**	**Harmonie des valeurs**	**Capacité de compensation**	**Indépendance**
Élevé	√	√	√	√	√
Moyen	(√)	√		√	(√)
Faible		√		(√)	

10.2.3 Exigences relatives aux procédures

10.2.3.1 Introduction

La capacité d'application de la sécurité peut être atteinte grâce aux capacités suivantes: sécurité pendant le développement et le cycle de vie d'un produit et capacité d'application de la sécurité.

10.2.3.2 Sécurité pendant le développement et le cycle de vie d'un produit

Dans le cadre du mécanisme NESAS, le développement et le cycle de vie d'un produit concernent tous les aspects pouvant avoir des incidences sur la durée de vie d'un produit réseau, notamment sa planification, sa conception, sa mise en œuvre, sa fourniture, son actualisation et, à terme, le ralentissement de sa production. À l'heure actuelle, pour ce qui est des réseaux IMT-2020, le mécanisme NESAS, conçu conjointement par la Global System for Mobile Communications Association (GSMA) et le Projet 3GPP, prévoit des exigences concernant la sécurité du développement et du cycle de vie des équipements de ces réseaux qui portent sur les étapes par lesquelles passent les produits réseau tout au long de leur développement (notamment la planification, la conception, la mise en œuvre, les tests, le lancement, la production et la livraison) et de leur cycle de vie (c'est-à-dire les étapes par lesquelles passent les produits réseau développés jusqu'à leur fin de vie, notamment leur maintenance et leur mise à jour). Il est recommandé de se référer à ce mécanisme pour évaluer les processus des distributeurs en matière de développement et de gestion du cycle de vie des produits.

10.2.3.3 Capacités en termes d'opérations de sécurité

Par capacités en termes d'opérations de sécurité, il faut comprendre que le produit ou le réseau doit être géré de manière adéquate lorsqu'il est utilisé à des fins commerciales, notamment en déployant des mesures de sécurité et en les durcissant et en limitant les accès.

10.2.3.4 Résumé

Pour ce qui est des capacités en termes d'opérations de sécurité, il est donc recommandé d'adopter les exigences de sécurité qui figurent dans le Tableau 9.

Tableau 9 – Niveau de confiance et exigences de sécurité concernant les capacités en termes d'opérations de sécurité

Niveau de confiance	Exigences de sécurité concernant les capacités en termes d'opérations de sécurité	
	Développement du système et sécurité tout au long du cycle de vie d'un produit	**Opérations de sécurité**
Élevé	√	√
Moyen	(√)	√
Faible	=	√

10.2.4 Exigences technologiques

La capacité à être digne de confiance peut être atteinte en respectant des niveaux appropriés sur les plans suivants: procédures de sécurité, confidentialité, résilience, sûreté, fiabilité et disponibilité. Il est donc recommandé que les produits et les solutions de sécurité fournis par une partie prenante présentent ces caractéristiques essentielles pour être dignes de confiance, comme indiqué dans plusieurs documents tels que les normes [b-BSI 10754-1] et [b-NIST SP800-160v1].

Le Tableau 10 montre un exemple des liens qui peuvent exister entre les niveaux de confiance et la fiabilité d'une organisation. Comme indiqué plus haut, dans la pratique, le choix exact des aspects qui sont nécessaires pour atteindre les niveaux de confiance moyen et faible dépend du domaine d'application. Par exemple, dans certains cas, on peut exiger un niveau adéquat de protection de la confidentialité des données pour accorder un niveau faible de confiance, tandis que dans d'autres cas, cet aspect peut ne pas être important, même lorsqu'un niveau moyen de confiance est nécessaire.

Tableau 10 – Niveau de confiance et exigences de sécurité concernant la capacité à être digne de confiance

Niveau de confiance	Exigences de sécurité concernant la capacité à être digne de confiance					
	Procédures de sécurité	**Confidentialité**	**Résilience**	**Sûreté**	**Fiabilité**	**Disponibilité**
Élevé	√	√	√	√	√	√
Moyen	√	(√)	(√)	(√)	(√)	√
Faible	√	–	–	(√)	(√)	–

Dans le contexte d'une mise en œuvre réelle, les exigences précises dépendent des scénarios de fourniture de service, et une certaine souplesse doit être permise. Comme indiqué précédemment, si le niveau de confiance est faible, une exigence spécifique plus stricte, telle que la confidentialité, peut être nécessaire, même si les exigences de sécurité sont relativement faibles.

10.3 Interpréter le niveau de confiance pour préciser les exigences de garantie

Une fois que le niveau de confiance nécessaire a été défini pour un cas d'utilisation précis, il faut interpréter ce niveau de confiance pour pouvoir prendre des décisions de mise en œuvre et d'exploitation.

Pour ce faire, on pourra mettre en correspondance le niveau de confiance nécessaire avec les exigences spécifiques mentionnées au paragraphe 10.2, auxquelles il sera possible de satisfaire grâce à la garantie des produits et des systèmes. Il existe plusieurs techniques normalisées bien établies pour garantir la fiabilité des produits et des systèmes grâce à des tests et des évaluations, qui peuvent être réalisés par des tierces parties spécialisées, par exemple. Les résultats de ces tests et de ces évaluations peuvent servir de base pour mettre en correspondance le niveau de confiance nécessaire, qui est

obtenu suite à une analyse décrite au paragraphe 9.4, avec les exigences précises de garantie concernant l'acquisition et l'utilisation des équipements et des services.

Le but de l'exemple donné dans le Tableau 11 est de permettre la mise en correspondance des niveaux de confiance nécessaires avec les décisions commerciales et opérationnelles basées sur la confiance et sur les évaluations des produits et des systèmes.

Tableau 11 – Exemple de mise en correspondance du niveau de confiance nécessaire avec les exigences de garantie

Niveau de confiance nécessaire	Type d'entité chargée de la garantie	Exemples de mécanismes de garantie de la sécurité
Élevé	Évaluation réalisée par un organisme public reconnu	Critères communs [b-ISO/CEI 15408 (toutes les parties)] Organismes nationaux de régulation [b-ISO/CEI 27001] Mécanisme NESAS Spécification de garantie de sécurité (SCAS) [b-3GPP TS33.511] [b-3GPP TS33.512] [b-3GPP TS33.513] [b-3GPP TS33.514] [b-3GPP TS33.515] [b-3GPP TS33.516] [b-3GPP TS33.517] [b-3GPP TS33.518] [b-3GPP TS33.519]
Moyen	Évaluation réalisée par un organisme d'évaluation de la conformité (CAB) accrédité	Critères communs [b-ISA/CEI 62443 (toutes les parties)] [b-ISO/CEI 27001] Mécanisme NESAS et spécification SCAS
Faible	Évaluation réalisée par un organisme d'évaluation de la conformité ou auto-évaluation	Critères communs Mécanisme NESAS et spécification SCAS

Même au sein d'un mécanisme de garantie spécifique, différents degrés ou types de garantie peuvent être appropriés pour différents niveaux de confiance.

- Certaines techniques, notamment celles décrites dans la norme [b-ISO/CEI 15408 (toutes les parties)], permettent de définir plusieurs niveaux de garantie, si bien que des niveaux de confiance différents peuvent, à titre d'option, exiger des niveaux d'évaluation selon la norme [b-ISO/CEI 15408 (toutes les parties)] eux-aussi différents. Toutefois, d'autres mécanismes, comme celui défini dans la norme [b-ISO/CEI 27001] n'autorisent qu'un seul niveau d'évaluation.
- Le degré d'assurance pouvant être atteint à partir d'une évaluation peut, à titre d'option, varier en fonction de l'organisme qui réalise l'évaluation (comme indiqué dans la colonne du milieu du Tableau 11). Par exemple, une auto-évaluation conforme aux exigences de la norme [b-ISO/CEI 27001] pourrait être adéquate pour un niveau de confiance faible.

En outre, l'importance accordée à une évaluation peut être accrue par d'autres facteurs, par exemple:

- le fait que l'équipement ou le service soit essentiel à l'exécution de la tâche, ou qu'il soit uniquement l'un des nombreux vecteurs par lesquels une fonction particulière peut être fournie (par exemple grâce à la redondance);
- le fait qu'il existe de nombreuses évaluations de l'assurance relatives à différents aspects d'un produit, d'un système ou d'un service.

Bibliographie

[b-UIT-T Y.3100] Recommandation UIT-T Y.3100 (2017), *Réseaux IMT-2020: termes et définitions*.

[b-ISO 10393] ISO 10393:2013, *Rappel de produits de consommation – Lignes directrices pour les fournisseurs*.

[b-ISO 28598-1] ISO 28598-1:2017, *Règles d'échantillonnage pour acceptation fondées sur le principe d'attribution de priorités (APP) – Partie 1: Lignes directrices relatives à l'approche APP*.

[b-ISO 31000] ISO 31000:2018, *Management du risque – Lignes directrices*. Disponible [consulté le 18-07-2022] à l'adresse suivante: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:fr.

[b-ISO/CEI 2382] ISO/CEI 2382:2015, *Technologies de l'information – Vocabulaire*.

[b-ISO/CEI 14888-1] ISO/CEI 14888-1:2008, *Technologies de l'information – Techniques de sécurité – Signatures digitales avec appendice – Partie 1: Généralités*.

[b-ISO/CEI/IEEE 15288] ISO/CEI/IEEE 15288:2015, *Ingénierie des systèmes et du logiciel – Processus du cycle de vie du système*.

[b-ISO/CEI 15408 (toutes les parties)] ISO/CEI 15408, *Technologies de l'information – Techniques de sécurité – Critères d'évaluation pour la sécurité TI*.

[b-ISO/CEI/IEEE 24765] ISO/CEI/IEEE 24765:2017, *Ingénierie des systèmes et du logiciel – Vocabulaire*.

[b-ISO/CEI 25010] ISO/CEI 25010:2011, *Ingénierie des systèmes et du logiciel – Exigences de qualité et évaluation des systèmes et du logiciel (SQuaRE) – Modèles de qualité du système et du logiciel*.

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

[b-ISO/CEI 27001] ISO/CEI 27001:2013, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences*.

[b-ISO/CEI 27005] ISO/CEI 27005:2018, *Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information*.

[b-ISO/PAS 19450] Spécification publiée sans restriction ISO/PAS 19450:2015, *Systèmes d'automatisation et intégration – Object-Process Methodology*.

[b-ISO/TS 21089] Spécification technique ISO/TS 21089:2018, *Informatique de santé – Flux d'information "trusted end-to-end"*.

[b-ISO/TS 21719-2] Spécification technique ISO/TS 21719-2:2018, *Perception de télépéage – Personnalisation des équipements embarqués – Partie 2: Utilisation des communications dédiées à courte portée*.

[b-ISO/TS 22318] Spécification technique ISO/TS 22318:2021, *Sécurité et résilience – Systèmes de management de la continuité d'activité – Lignes directrices pour le management de la continuité de la chaîne d'approvisionnement*.

[b-ISA/CEI 62443] ISA/CEI 62443 (toutes les parties) [série de normes sur la cybersécurité des systèmes d'automatisation et de commande].

[b-GSMA FS.13] GSM Association (2022). *Network equipment security assurance scheme – Overview*, Document official FS.13, version 2.1. Londres: GSM Association. 29 p. Disponible [consulté le 17-07-2022] à l'adresse suivante: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.13-v2.1.pdf.

[b-GSMA FS.14] GSM Association (2022). *Network equipment security assurance scheme – Security test laboratory accreditation*, Document officiel FS.14, version 2.1. Londres: GSM Association. 15 p. Disponible [consulté le 17-07-2022] à l'adresse suivante: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.14-v2.1.pdf.

[b-GSMA FS.15] GSM Association (2022). *Network equipment security assurance scheme – Development and lifecycle assessment methodology*, Document officiel FS.15, version 2.1. Londres: GSM Association. 33 p. Disponible [consulté le 17-07-2022] à l'adresse suivante: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.15-v2.1.pdf.

[b-GSMA FS.16] GSM Association (2022). *Network equipment security assurance scheme – Development and lifecycle security requirements*, Document officiel FS.16, version 2.1. Londres: GSM Association. 22 p. Disponible [consulté le 17-07-2022] à l'adresse suivante: https://www.gsma.com/security/wp-content/uploads/2022/02/FS.16-v2.1.pdf.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The transport layer security (TLS) protocol – Version 1.2*.

[b-IETF RFC 6733] IETF RFC 6733 (2012), *Diameter base protocol*.

[b-3GPP TS 33.501] Spécification technique 3GPP TS 33.501 V17.6.0 (2022), *Security architecture and procedures for 5G system*.

[b-3GPP TS 33.511] Spécification technique 3GPP TS 33.511 V17.1.0 (2022), *Security assurance specification (SCAS) for the next generation node B (gNodeB) network product class*.

[b-3GPP TS 33.512] Spécification technique 3GPP TS 33.512 V17.3.0 (2022), *5G security assurance specification (SCAS); Access and mobility management function (AMF)*.

[b-3GPP TS 33.513] Spécification technique 3GPP TS 33.513 V17.0.0 (2022), *5G security assurance specification (SCAS); User plane function (UPF)*.

[b-3GPP TS 33.514] Spécification technique 3GPP TS 33.514 V17.0.0 (2022), *5G security assurance specification (SCAS) for the unified data management (UDM) network product class*.

[b-3GPP TS 33.515] Spécification technique 3GPP TS33.515 V17.0.0 (2022), *5G security assurance specification (SCAS) for the session management function (SMF) network product class*.

[b-3GPP TS 33.516] Spécification technique 3PGP TS33.516 V17.0.0 (2022), *5G security assurance specification (SCAS) for the authentication server function (AUSF) network product class*.

[b-3GPP TS 33.517] Spécification technique 3GPP TS33.517 V17.0.0 (2022), *5G security assurance specification (SCAS) for the security edge protection proxy (SEPP) network product class*.

[b-3GPP TS 33.518] Spécification technique 3GPP TS33.518 V17.0.0 (2022), *5G security assurance specification (SCAS) for the network repository function (NRF) network product class*.

[b-3GPP TS 33.519] Spécification technique 3GPP TS33.519 V17.0.0 (2022), *5G security assurance specification (SCAS) for the network exposure function (NEF) network product class*.

[b-BSI 10754-1] BS 10754-1:2018, *Information technology. Systems trustworthiness – Governance and management specification*.

[b-BSIMM] British Standards Institution (2021). *Building security in maturity model*, BSIMM 12. Londres: British Standards Institution.

[b-NIST FICIC] NIST (2018). *Cadre pour l'amélioration de la cybersécurité des infrastructures critiques*, Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology. 48 p. Disponible [consulté le 18-07-2022] à l'adresse suivante: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018fr.pdf.

[b-NIST SP800-30] Joint Task Force Transformation Initiative (2012). *Guide for conducting risk assessments*, NIST Special Publication, NIST SP800-30 Rev.1. Gaithersburg, MD: National Institute of Standards and Technology. 95 p. Disponible [consulté le 18-07-2022] à l'adresse suivante: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[b-NIST SP800-53] NIST SP 800-53 Rev 5 2020, *Security and privacy controls for information systems and organizations.*

[b-NIST SP800-160v1] Ross, R., McEvilley, M., Carrier Oren, J. (2018). *Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems – Volume 1*, NIST Special Publication, NIST SP800-160v1. Gaithersburg, MD: National Institute of Standards and Technology. 243 p. Disponible [consulté le 18-07-2022] à l'adresse suivante: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf

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

Imprimé en Suisse
Genève, 2022