ITUPublications
Recommandations

Union Internationale des Télécommunications
Secteur de la Normalisation

Recommandation

UIT-T X.1816 (03/2023)

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

Sécurité des IMT-2020

Lignes directrices et exigences relatives à la classification des capacités de sécurité des tranches de réseau IMT-2020

RECOMMANDATIONS UIT-T DE LA SÉRIE X

Réseaux de données, communication entre systèmes ouverts et sécurité

RÉSEAUX PUBLICS DE DONNÉES	X.1-X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200-X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300-X.399
SYSTÈMES DE MESSAGERIE	X.400-X.499
ANNUAIRE	X.500-X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600-X.699
GESTION OSI	X.700-X.799
SÉCURITÉ	X.800-X.849
APPLICATIONS OSI	X.850-X.899
TRAITEMENT RÉPARTI OUVERT	X.900-X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	X.1000-X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	X.1100-X.1199
SÉCURITÉ DU CYBERESPACE	X.1200-X.1299
APPLICATIONS ET SERVICES SÉCURISÉS (2)	X.1300-X.1499
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	X.1500-X.1599
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	X.1600-X.1699
COMMUNICATIONS QUANTIQUES	X.1700-X.1729
SÉCURITÉ DES DONNÉES	X.1750-X.1799
SÉCURITÉ DES IMT-2020	**X.1800-X.1819**

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

Recommandation UIT-T X.1816

Lignes directrices et exigences relatives à la classification des capacités de sécurité des tranches de réseau IMT-2020

Résumé

La définition des fonctions et processus de base liés aux technologies de découpage de réseau a établi des bases solides en vue de la première étape du déploiement des IMT-2020 et de l'utilisation commerciale des services de découpage de réseau. En tant que réseau logique de bout en bout qui est personnalisé à la demande, le découpage peut fournir des capacités de sécurité différenciées: premièrement, le découpage des réseaux IMT-2020 permet de prendre les mesures de sécurité nécessaires à la mise en œuvre de réseaux différenciés. Deuxièmement, les réseaux IMT-2020 permettent de prendre certaines mesures de sécurité facultatives au niveau des tranches. Certaines mesures de sécurité peuvent aussi offrir plusieurs options de sécurité et les opérateurs peuvent disposer de différentes ressources de sécurité. Celles-ci peuvent assurer différents niveaux de garantie de la sécurité ou de qualité de fonctionnement en ce qui concerne des aspects autres que la sécurité. Les clients de tranches ont également des exigences de sécurité particulières et peuvent demander des tranches de réseau personnalisées avec des niveaux de protection de la sécurité différents aux opérateurs de tranches. Les clients de tranches et les opérateurs de tranches doivent faire face à un certain nombre de difficultés lorsqu'ils choisissent les capacités de sécurité de leurs tranches, notamment en ce qui concerne les coûts de gestion et le manque d'homogénéité des définitions. L'objectif de la Recommandation UIT-T X.1816 est de décrire des capacités de sécurité des tranches de réseau IMT-2020 différenciées et de donner des lignes directrices concernant la classification de ces capacités de sécurité pour aider l'écosystème des IMT-2020 à mieux comprendre et choisir les capacités de sécurité des tranches de réseau.

Historique*

Édition	Recommandation	Approbation	Commission d'études	ID unique
1.0	UIT-T X.1816	03-03-2023	17	11.1002/1000/15114

Mots clés

Classification, IMT-2020, tranche de réseau, capacités de sécurité.

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

AVANT-PROPOS

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

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

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

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

NOTE

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

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et 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 développeurs 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

Page

1 Champ d'application 1

2 Références 1

3 Définitions 1

3.1 Termes définis ailleurs 1

3.2 Termes définis dans la présente Recommandation 2

4 Abréviations et acronymes 2

5 Conventions 3

6 Présentation de la classification des capacités de sécurité des tranches de réseau IMT-2020 3

7 Capacités de sécurité des tranches de réseau IMT-2020 4

7.1 Modèle pour les descriptions des capacités de sécurité des tranches de réseau 4

7.2 Capacités de sécurité des tranches de réseau IMT-2020 différenciées 5

7.3 Classification des capacités de sécurité des tranches de réseau IMT-2020 8

8 Classification des dimensions de sécurité sur la base des capacités de sécurité des tranches 9

8.1 Méthode et principe de classification des dimensions de sécurité sur la base des capacités de sécurité des tranches 9

8.2 Dimensions de sécurité dont les niveaux sont basés sur les capacités de sécurité des tranches de réseau IMT-2020 9

9 Lignes directrices et exigences relatives aux types de sécurité des tranches 13

10 Lignes directrices et exigences à l'intention des parties prenantes concernant la classification des capacités de sécurité des tranches de réseau 13

Appendice I – Qualité de fonctionnement pour les options des capacités de sécurité des tranches de réseau IMT-2020 15

Appendice II – Exemple de types de sécurité des tranches de réseau IMT-2020 de base 17

Bibliographie 18

Recommandation UIT-T X.1816

Lignes directrices et exigences relatives à la classification des capacités de sécurité des tranches de réseau IMT-2020

1 Champ d'application

La présente Recommandation vise à fournir des lignes directrices et des exigences pour la classification des capacités de sécurité des tranches de réseau IMT-2020. Elle indique:

– la définition des capacités de sécurité des tranches de réseau IMT-2020 différenciées;

– les principes et les méthodes permettant de déterminer la classification des capacités de sécurité des tranches de réseau IMT-2020.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute Recommandation ou autre référence étant sujette à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. 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 d'une Recommandation.

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

[UIT-T X.1047] Recommandation UIT-T X.1047 (2021), *Exigences et architecture de sécurité pour la gestion et l'orchestration des tranches de réseau*.

[3GPP TS 33.501] Spécification technique 3GPP TS 33.501 V17.1.0 (2021), *3rd Generation Partnership Project; Groupe de spécification technique – Aspects "services" et "système"*; *Security architecture and procedures for 5G system (Release 17).*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 tranche de réseau [b-UIT-T Y.3100]: réseau logique qui offre des capacités de réseau et des caractéristiques de réseau spécifiques.

NOTE 1 – Les tranches de réseau permettent de créer des réseaux personnalisés qui offrent des solutions souples pour différents scénarios de marché présentant des exigences diverses en ce qui concerne les fonctionnalités, la qualité de fonctionnement et l'attribution des ressources.

NOTE 2 – Une tranche de réseau peut être en mesure d'exposer ses capacités.

NOTE 3 – Le comportement d'une tranche de réseau est réalisé via une ou plusieurs instances de tranche de réseau.

3.1.2 instance de tranche de réseau [b-UIT-T Y.3100]: instance de tranche de réseau créée sur la base d'un modèle de tranche de réseau.

3.1.3 sous-réseau des tranches de réseau [b-ETSI TS 128 530]: représentation des aspects gestion d'un ensemble de fonctions gérées et des ressources requises (par exemple ressources de calcul, de stockage et de réseau).

3.2 Termes définis dans la présente Recommandation

Aucune.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AAA authentification, autorisation et comptabilité (*authentification, authorization and accounting*)

ACL liste de contrôle d'accès (*access control list*)

AMF fonction de gestion d'accès et de mobilité (*access and mobility management function*)

CN réseau central (*core network*)

CU unité centrale (*central unit*)

DDoS déni de service réparti (*distributed denial of service*)

DU unité répartie (*distributed unit*)

EAP protocole d'authentification extensible (*extensible authentication protocol*)

ENSI information de tranche de réseau externe (*external network slice information*)

gNB nœud B NR

IMT-2020 Télécommunications mobiles internationales-2020 (*International Mobile Telecommunications-2020*)

NAT traduction d'adresse réseau (*network address translation*)

NFV virtualisation des fonctions de réseau (*network function virtualization*)

ng-eNB nœud B évolué de prochaine génération (*next generation evolved node-B*)

NSSAI information d'aide à la sélection de tranche de réseau (*network slice selection assistance information*)

S-NSSAI information d'aide à la sélection de tranche de réseau unique (*single network slice selection assistance information*)

PDU unité de données protocolaire (*protocol data unit*)

PNF fonction de réseau physique (*physical network function*)

RAN réseau d'accès radioélectrique (*radio access network*)

RB support radioélectrique (*radio bearer*)

TLS sécurité dans la couche transport (*transport layer security*)

UE équipement d'utilisateur (*user equipment*)

URL localisateur uniforme de ressources (*uniform resource location*)

VNF fonction de réseau virtuelle (*virtual network function*)

WAF application web de pare-feu (*web application firewall*)

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. Ces mots n'impliquent pas que la mise en œuvre du vendeur doit incorporer l'option et que la caractéristique peut éventuellement être activée par l'opérateur du réseau/le fournisseur de service. Ils signifient plutôt que le fabricant peut incorporer la caractéristique à titre facultatif et revendiquer néanmoins la conformité avec la spécification.

6 Présentation de la classification des capacités de sécurité des tranches de réseau IMT-2020

La sécurité des tranches de réseau est la condition préalable à la mise en place d'un découpage de réseau. Les clients de tranches qui utilisent des services de communication de tranche ont besoin d'une garantie de sécurité correspondante adaptée à la mise en œuvre de leurs tranches et peuvent aussi avoir des exigences de sécurité particulières, en fonction de ceux de leurs services qui utilisent des tranches. Ils peuvent donc demander aux exploitants des tranches de réseau personnalisées avec une protection de la sécurité différente. Pour les opérateurs de tranches qui conçoivent, construisent et exploitent des réseaux et fournissent des tranches de réseau, le découpage fait intervenir de nombreux domaines (communications sans fil, transmission, réseaux centraux et gestion par exemple) et peut fournir des capacités de sécurité différenciées: premièrement, le découpage de réseaux IMT-2020 fournit des mesures de sécurité permettant de mettre en œuvre des réseaux différenciés. Deuxièmement, les réseaux IMT-2020 prennent en charge certaines mesures de sécurité facultatives au niveau des tranches. Certaines mesures de sécurité peuvent aussi comporter plusieurs options de sécurité et les opérateurs peuvent disposer de différentes ressources de sécurité. Cela peut se traduire par différents niveaux de garantie de la sécurité ou de qualité de fonctionnement en ce qui concerne des aspects autres que la sécurité. Les capacités de sécurité d'une tranche doivent donc être déterminées en fonction des exigences des clients et des capacités de sécurité que le réseau peut fournir. Les clients de tranches ou les opérateurs de tranches qui choisissent les capacités de sécurité de leurs tranches doivent faire face à un certain nombre de difficultés:

- Les exigences de sécurité des clients peuvent être vagues et peu nombreuses ou ne pas être suffisantes pour pouvoir être mises en correspondance avec les capacités de sécurité.
- Les clients peuvent avoir des exigences de sécurité qui dépassent les capacités du réseau.
- Le coût en termes de connaissances pour les parties prenantes en ce qui concerne les capacités de sécurité et leurs différences peut varier et il se peut que la combinaison de capacités choisie ne soit pas acceptable. Par exemple, la protection assurée par les capacités retenues peut ne pas être suffisante pour plusieurs domaines ou parties prenantes.
- Le nombre de combinaisons de capacités de sécurité des tranches peut être considérable et les coûts de gestion et d'orchestration des opérateurs peuvent être relativement élevés.

Des capacités de sécurité des tranches de réseau IMT-2020 différenciées ainsi qu'une méthode de classification et de combinaison de ces capacités seront recommandées pour les raisons suivantes:

- Aider le secteur privé à parvenir à une compréhension unifiée des capacités de sécurité des tranches et des différences entre les capacités de sécurité des tranches (par exemple sur le plan de la qualité de fonctionnement).
- Fournir une classification générale de base des capacités de sécurité des tranches de réseau IMT-2020, afin que le secteur privé comprenne clairement les possibilités offertes par le découpage en matière de sécurité et les fasse mieux cadrer avec la plupart des applications industrielles.

- Faciliter l'itinérance entre différentes tranches ainsi que la réutilisation des tranches.
- Fournir aux utilisateurs professionnels une référence leur permettant de choisir des tranches appropriées à même de répondre à leurs exigences.
- Sert de référence aux superviseurs du secteur privé pour élaborer les plans et stratégies de développement des tranches.
- Fournir une référence aux fournisseurs de services pour déployer leurs services dans les tranches appropriées.
- Fournir une référence aux opérateurs pour élaborer les plans de développement des tranches et évaluer la valeur et le prix des tranches.
- Fournir une référence permettant aux équipementiers de planifier les feuilles de route des technologies et des produits pour les tranches.

La méthodologie comprend les éléments suivants:

- Liste des capacités de sécurité différenciées générales relatives au découpage, sous une forme structurée, comprenant le nom, la description, la dimension de sécurité et les options. Cette liste est donnée au paragraphe 7.
- Pour chaque dimension de sécurité, plusieurs niveaux peuvent être constitués en combinant les capacités de sécurité relatives au découpage correspondantes avec différentes options sur la base de certains principes. Ces niveaux sont décrits au paragraphe 8.
- En outre, les types de sécurité de base des tranches qui constituent les dimensions de sécurité peuvent être constitués en choisissant un niveau pour chaque mesure de sécurité en fonction de certains principes. Ces types de sécurité sont indiqués au paragraphe 9.
- Les parties prenantes peuvent utiliser le principe, les méthodes et les résultats de la classification pour décider des capacités de sécurité d'une tranche. Ces éléments font l'objet du paragraphe 10.

7 Capacités de sécurité des tranches de réseau IMT-2020

7.1 Modèle pour les descriptions des capacités de sécurité des tranches de réseau

Le paragraphe 7 donne la liste des capacités de sécurité générales des réseaux IMT-2020 qui peuvent varier d'une tranche de réseau à l'autre. Les descriptions des capacités de sécurité devraient être claires, concises et sans équivoque. Chaque description devrait comprendre les éléments suivants:

- Description de la capacité: description détaillée de la capacité de sécurité des tranches de réseau IMT-2020 permettant une mise en œuvre différenciée.
- Nom de la capacité: nom unique et acronyme attribués à la capacité de sécurité.
- Dimension de sécurité de la capacité: aspect particulier de la sécurité dont la capacité de sécurité doit tenir compte de par sa conception. Il existe huit (8) dimensions de sécurité: contrôle d'accès, authentification, non-répudiation, confidentialité des données, sécurité de la communication, intégrité des données, disponibilité et confidentialité [UIT-T X.805].
- Options de la capacité: choix multiples pour chaque capacité de sécurité, qui peuvent varier d'une tranche à l'autre. Dans la présente Recommandation, chaque option est désignée par un numéro associé à l'acronyme de la capacité en question. Note: Les options sont générales et ne sont pas liées à telle ou telle mise en œuvre de réseau. Elles peuvent être encore subdivisées afin de correspondre à une mise en œuvre particulière.

7.2 Capacités de sécurité des tranches de réseau IMT-2020 différenciées

7.2.1 Capacité d'authentification et d'autorisation propre aux tranches de réseau

- Description de la capacité: le système IMT-2020 fournit des fonctions optionnelles d'authentification et d'autorisation propres aux tranches de réseau [3GPP TS 33.501] entre un équipement d'utilisateur (UE) et un serveur d'authentification, d'autorisation et de comptabilité (AAA-S) pouvant appartenir à une entreprise tierce externe. L'authentification et l'autorisation propres à la tranche de réseau peuvent être déclenchées sur la base de l'information d'aide à la sélection de tranche de réseau unique (S-NSSAI) après l'authentification primaire. Le serveur AAA peut également être à l'origine de la révocation d'une autorisation, d'une nouvelle authentification ou d'une nouvelle autorisation propre aux tranches.
- Nom de la capacité: authentification et autorisation propres aux tranches de réseau (NSSAA, *network slice-specific authentication and authorization*).
- Dimension de sécurité de la capacité: authentification, contrôle d'accès.
- Option de la capacité:
  - NSSAA.0: inactive
  - NSSAA.1: active

7.2.2 Capacité d'isolation des tranches de réseau pour les ressources de réseau

- Description de la capacité: les tranches de réseau IMT-2020 utilisent les ressources de l'infrastructure unifiée des opérateurs. Il existe diverses solutions d'isolation permettant d'empêcher que les éléments des tranches de réseau accèdent aux éléments se trouvant dans des tranches différentes ou les influencent au moyen des ressources de l'infrastructure partagée. Du point de vue des domaines du sous-réseau des tranches:
  - Concernant le réseau d'accès (AN, *access network*): pour l'interface radioélectrique, le partage dynamique des ressources du support radioélectrique (RB) et la réservation statique des ressources du support radioélectrique sont possibles pour l'attribution des ressources. La première option offre un effet de couverture et une utilisation des ressources améliorés et plus souples, tandis que la seconde présente une fiabilité accrue mais un coût plus élevé. Pour le niveau de base, l'unité centrale (CU) et l'unité répartie (DU) de différentes tranches peuvent être les mêmes. Pour des niveaux d'isolation plus élevés, il est possible de les isoler sur le plan physique en allouant du matériel spécifique à chacune d'elles ou de les isoler sur le plan logique en utilisant la virtualisation des fonctions de réseau (NFV) (par exemple une machine virtuelle/un conteneur) pour partager le matériel.
  - Concernant le réseau de transport (TN, *transport network*): l'isolation sur les réseaux de transport peut être inexistante, physique (par exemple isolation physique des fonctions de réseau, isolation physique des liaisons réseau, etc.) ou logique (par exemple isolation logique des fonctions de réseau, isolation logique/virtuelle des liaisons du réseau, etc.) [UIT-T X.1047].
  - Concernant le réseau central (CN, *core network*): l'isolation physique des ressources du réseau central peut comprendre l'isolation des fonctions de réseau physiques (PNF) spéciales, l'isolation des liaisons réseau physiques spéciales, l'isolation de l'emplacement géographique, l'isolation des ressources de calcul, l'isolation de la mémoire, l'isolation du stockage, l'isolation de la fonction PNF fondée sur la sécurité, etc. L'isolation logique des ressources du réseau central peut comprendre l'isolation des fonctions de réseau virtuelles (VNF), l'isolation des liaisons virtuelles, l'isolation des technologies de virtualisation, l'isolation des ressources virtuelles de calcul, l'isolation de la mémoire virtuelle, l'isolation du stockage virtuel, l'isolation de l'emplacement géographique du

matériel virtualisé afin de fournir des ressources virtuelles, l'isolation de la fonction VNF fondée sur la sécurité, etc. [UIT-T X.1047].

Du point de vue des types de ressources et des techniques d'isolation:

- Concernant les ressources de l'interface radioélectrique: partage du support radioélectrique ou réservation du support radioélectrique.
- Concernant les ressources des fonctions de réseau des réseaux AN/TN/CN: isolation physique, isolation logique ou aucune isolation.

- Nom de la capacité: isolation des tranches pour les ressources de réseau (SIR).
- Mesure de sécurité de la capacité: contrôle d'accès, disponibilité, confidentialité.
- Options de la capacité et fonctionnalités correspondantes:
  - SIR.0: aucune isolation.
  - SIR.1: isolation logique + partage du support radioélectrique.
  - SIR.2: isolation logique et physique + partage du support radioélectrique.
  - SIR.3: isolation physique + partage du support radioélectrique.
  - SIR.4: isolation logique + réservation du support radioélectrique.
  - SIR.5: isolation logique et physique + réservation du support radioélectrique.
  - SIR.6: isolation physique + réservation du support radioélectrique.

7.2.3 Capacité de protection des données dans le plan utilisateur

- Description de la capacité: le système IMT-2020 peut fournir des capacités de protection des données dans le plan utilisateur différenciées au niveau de la tranche. Le nœud B évolué de prochaine génération (ng-eNB)/nœud B NR (gNB) peut décider d'activer ou non la protection de la confidentialité ou de l'intégrité du plan utilisateur pour chaque session PDU, conformément à la politique de sécurité du plan utilisateur reçue. La politique de sécurité du plan utilisateur peut être configurée de manière à indiquer si cette protection est "requise" ou "non nécessaire". Des algorithmes de chiffrement facultatifs sont disponibles [3GPP TS 33.501].
- Nom de la capacité: protection des données dans le plan utilisateur (UPDP).
- Mesure de sécurité de la capacité: confidentialité des données, intégrité des données.
- Option de la capacité:
  - UPDP.0: ne pas activer la protection de la confidentialité ou de l'intégrité du plan utilisateur.
  - UPDP.1: activer la protection de la confidentialité ou de l'intégrité du plan utilisateur au moyen des algorithmes de chiffrement facultatifs.

7.2.4 Capacité de protection aux limites

- Description de la capacité: il est important de protéger une tranche de réseau contre les attaques de réseau en déployant des fonctions/fonctionnalités de contrôle de la sécurité aux limites, en particulier aux limites du réseau central (par exemple une configuration de protection du point N6 à l'interface N6) [b-3GPP TS 28.541]. Suivant les utilisateurs des tranches de réseau, les fonctions/fonctionnalités de contrôle de la sécurité peuvent être différentes et pourraient être modifiées de manière dynamique en fonction des besoins. Les fonctions de contrôle de la sécurité comprennent notamment les pare-feu, la traduction d'adresse réseau (NAT), les anti-logiciels malveillants,, le contrôle parental, les fonctions de protection contre le déni de service réparti (DDoS), etc. [b-3GPP TS 28.541]. Les fonctionnalités comprennent les règles de renvoi, les règles de filtrage, la configuration des paramètres, etc. Les exigences pourraient être le contrôle d'accès au réseau de données et le mécanisme de tunnelisation.

- Nom de la capacité: protection aux limites (BP).
- Mesure de sécurité de la capacité: contrôle d'accès, disponibilité, sécurité de la communication.
- Option de la capacité:
  - BP.0: aucune fonction de contrôle de la sécurité.
  - BP.1: fonctions/fonctionnalités de contrôle de la sécurité déployées.

7.2.5 Capacités de protection des services d'application

- Description de la capacité: les opérateurs peuvent déployer des dispositifs de sécurité ou des modules de sécurité du côté du réseau pour assurer une protection de sécurité différente pour les services d'application utilisant des tranches et pour les utilisateurs utilisant les services d'application. Par exemple, le réseau de l'opérateur peut assurer la détection d'un terminal anormal, le nettoyage du trafic réseau, la détection d'un localisateur uniforme de ressources (URL) malveillant et fournir une application web de pare-feu (WAF), un dispositif anti-DDoS, etc.
- Nom de la capacité: protection des services d'application (ASP, *application service protection*).
- Mesure de sécurité de la capacité: sécurité de la communication, contrôle d'accès, disponibilité.
- Option de la capacité:
  - ASP.0: aucune protection des services d'application.
  - ASP.1: protection des services d'application déployée.

7.2.6 Capacité de protection de la confidentialité de l'identificateur EAP pendant la l'authentification et l'autorisation NSSAA

- Description de la capacité: plusieurs méthodes de protocole d'authentification extensible (EAP) [b-IETF RFC 3748] sont possibles pour l'authentification propre à une tranche. Une méthode EAP permettant d'assurer la protection de la confidentialité (par exemple une méthode EAP de sécurité dans la couche transport (TLS) [b-IETF RFC 5216] ou une méthode EAP-TTLS [b-IETF RFC 5281]) peut être choisie pour protéger la confidentialité de l'identificateur EAP utilisé pour l'authentification et l'autorisation NSSAA fondées sur le protocole EAP [3GPP TS 33.501].
- Nom de la capacité: protection de la confidentialité de l'identificateur EAP pendant l'authentification et l'autorisation NSSAA (PPEAP, *privacy protection of the EAP ID during NSSAA*).
- Mesure de sécurité de la capacité: confidentialité.
- Option de la capacité:
  - PPEAP.0: aucune méthode EAP permettant d'assurer la protection de la confidentialité n'est utilisée.
  - PPEAP.1: utilisation de méthodes EAP permettant d'assurer la protection de la confidentialité.

7.2.7 Capacité de protection de la confidentialité de l'information (S-)NSSAI

- Description de la capacité: l'information NSSAI est utilisée pour identifier la tranche de réseau/le type de service. Certaines informations concernant le réseau et les clients de l'opérateur pourraient être déduites de l'information NSSAI et de son utilisation. Un réseau IMT-2020 offre des capacités de protection de la confidentialité de l'information (S-)NSSAI, en permettant de ne pas utiliser l'information NSSAI ou d'utiliser d'autres informations à l'extérieur du domaine de l'opérateur. Au cours de la procédure d'enregistrement, la fonction

de gestion d'accès et de mobilité (AMF) peut fournir à l'UE, dans le message d'acceptation d'enregistrement, un paramètre de mode d'inclusion de l'information NSSAI pour l'établissement de la connexion à la strate d'accès, indiquant si l'UE doit inclure l'information NSSAI lors de l'établissement de la connexion à la strate d'accès et quand il doit le faire, en fonction des différents modes. Par défaut, l'UE ne doit pas fournir l'information NSSAI à la strate d'accès pour l'accès 3GPP, sauf s'il reçoit une indication selon laquelle il doit fonctionner selon un autre mode [b-3GPP TS 23.502]. Au cours de l'authentification et de l'autorisation NSSAA, si le serveur AAA utilisé appartient à une tierce partie, l'information S-NSSAI, qui fait partie du réseau central IMT-2020, peut éventuellement être mise en correspondance dans le réseau de l'opérateur avec une information de tranche de réseau externe (ENSI), qui est transmise et utilisée en dehors du domaine de l'opérateur [3GPP TS 33.501].

- Nom de la capacité: protection de la confidentialité de l'information (S-)NSSAI (PPSI, *privacy protection of the (S-)NSSAI*).
- Mesure de sécurité de la capacité: confidentialité.
- Option de la capacité:
  - PPSI.0: information NSSAI utilisée à l'extérieur du domaine de l'opérateur.
  - PPSI.1: information NSSAI non utilisée à l'extérieur du domaine de l'opérateur ou utilisation d'une autre information.

7.3 Classification des capacités de sécurité des tranches de réseau IMT-2020

Les capacités de sécurité des tranches de réseau IMT-2020 peuvent être classées en fonction de la dimension de sécurité qui leur est associée, comme indiqué dans le Tableau 7-1.

Tableau 7-1 – Classification des capacités de sécurité des tranches de réseau IMT-2020 en fonction de la dimension de sécurité

Dimension de sécurité **Capacité de sécurité des tranches**	**Authentification et autorisation propres aux tranches de réseau (NSSAA)**	**Isolation de tranches des ressources de réseau (SIR)**	**Protection des données du plan d'utilisateur (UPDP)**	**Protection aux limites (BP)**	**Protection des services d'appli-cation (ASP)**	**Protection de la confidentialité des données de l'identificateur EAP pendant la procédure NSSAA (PPEAP)**	**Protection de la confidentialité des informations associées à la procédure (S-)NSSAI (PPSI)**
Contrôle d'accès	√	√		√	√		
Authentification	√						
Non-répudiation							
Confidentialité des données			√				
Sécurité de la communication				√	√		
Intégrité des données			√				
Disponibilité		√		√	√		
Respect de la vie privée		√				√	√

8 Classification des dimensions de sécurité sur la base des capacités de sécurité des tranches

8.1 Méthode et principe de classification des dimensions de sécurité sur la base des capacités de sécurité des tranches

La méthode classification de chaque dimension de sécurité est la suivante:

1) Il est recommandé de dresser une liste des capacités de sécurité et des options correspondant à la dimension de sécurité. S'il existe une faible probabilité qu'une capacité de sécurité ait une incidence sur une dimension de sécurité donnée, cette capacité de sécurité pourra éventuellement être exclue de la liste des dimensions de sécurité et figurer uniquement dans la liste des autres dimensions de sécurité principalement touchées.

2) Il est recommandé de dresser une liste des combinaisons des différentes options des capacités et de déterminer les différents niveaux des dimensions de sécurité. Si une dimension de sécurité est assurée par plusieurs capacités de sécurité, chaque niveau d'effet de protection devrait rester compatible pour plusieurs domaines ou parties prenantes lorsque les options des capacités de sécurité sont combinées. La notation xx.nn (par exemple, AC.1, ..., DI.0) désigne le nom du niveau de la dimension de sécurité xx.

On trouvera au § 8.2 la liste générique des huit dimensions de sécurité , dont les niveaux sont basés sur les capacités de sécurité et les options énumérées au paragraphe 7.

8.2 Dimensions de sécurité dont les niveaux sont basés sur les capacités de sécurité des tranches de réseau IMT-2020

8.2.1 Contrôle d'accès basé sur les capacités de sécurité des tranches de réseau IMT-2020

Le contrôle d'accès peut être assuré au moyen de capacités dont les options comprennent, entre autres, l'authentification et l'autorisation propres aux tranches de réseau, l'isolation de tranches de ressources de réseau, la protection aux limites et la protection des services d'application. Il existe diverses combinaisons de capacités avec différentes options pour assurer différents niveaux de contrôle d'accès. Ces combinaisons, fondées sur le paragraphe 7, sont les suivantes:

Tableau 8-1 – Niveaux de contrôle d'accès

<table>
<tr><th colspan="12">Dimension de sécurité – Contrôle d'accès (AC)</th></tr>
<tr><th>Capacité</th><th colspan="2">Authentification et autorisation propres aux tranches de réseau (NSSAA)</th><th colspan="2">Protection des services d'application (ASP)</th><th colspan="7">Isolation de tranches de ressources de réseau (SIR)</th><th colspan="2">Protection aux limites (BP)</th><th>Nom du niveau</th></tr>
<tr><th>Options</th><th>NSSAA.0</th><th>NSSAA.1</th><th>ASP.0</th><th>ASP.1</th><th>SIR.0</th><th>SIR.1</th><th>SIR.2</th><th>SIR.3</th><th>SIR.4</th><th>SIR.5</th><th>SIR.6</th><th>BP.0</th><th>BP.1</th><th></th></tr>
<tr><td rowspan="5">Combinaison</td><td colspan="2" rowspan="5">NSSAA.0</td><td colspan="2" rowspan="5">ASP.0</td><td colspan="7">SIR.0</td><td colspan="2">BP.0</td><td>AC.0000</td></tr>
<tr><td colspan="7">SIR.0</td><td colspan="2">BP.1</td><td>AC.0001</td></tr>
<tr><td colspan="7">SIR.1
SIR.4</td><td colspan="2">BP.0</td><td>AC.0010
AC.0040</td></tr>
<tr><td colspan="7">SIR.1
SIR.4</td><td colspan="2">BP.1</td><td>AC.0011
AC.0041</td></tr>
<tr><td colspan="7">SIR.2
SIR.5</td><td colspan="2">BP.0</td><td>AC.0020
AC.0050</td></tr>
</table>

Tableau 8-1 – Niveaux de contrôle d'accès

Dimension de sécurité – Contrôle d'accès (AC)															
Capacité	**Authentification et autorisation propres aux tranches de réseau (NSSAA)**		**Protection des services d'application (ASP)**		**Isolation de tranches de ressources de réseau (SIR)**							**Protection aux limites (BP)**		**Nom du niveau**
Options	**NSSAA.0**	**NSSAA.1**	**ASP.0**	**ASP.1**	**SIR.0**	**SIR.1**	**SIR.2**	**SIR.3**	**SIR.4**	**SIR.5**	**SIR.6**	**BP.0**	**BP.1**	
					SIR.2 SIR.5								BP.1	AC.0021 AC.0051
					SIR.3 SIR.6								BP.1	AC.0031 AC.0061
				ASP.1	SIR.0							BP.0		AC.0100
					SIR.0								BP.1	AC.0101
					SIR.1 SIR.4							BP.0		AC.0110 AC.0140
					SIR.1 SIR.4								BP.1	AC.0111 AC.0141
					SIR.2 SIR.5							BP.0		AC.0120 AC.0150
					SIR.2 SIR.5								BP.1	AC.0121 AC.0151
					SIR.3 SIR.6								BP.1	AC.0131 AC.0161
	NSSAA.1		ASP.0		SIR.0							BP.0		AC.1000
					SIR.0								BP.1	AC.1001
					SIR.1 SIR.4							BP.0		AC.1010 AC.1040
					SIR.1 SIR.4								BP.1	AC.1011 AC.1041
					SIR.2 SIR.5							BP.0		AC.1020 AC.1050
					SIR.2 SIR.5								BP.1	AC.1021 AC.1051
					SIR.3 SIR.6								BP.1	AC.1031 AC.1061
				ASP.1	SIR.0							BP.0		AC.1100
					SIR.0								BP.1	AC.1101
					SIR.1 SIR.4							BP.0		AC.1110 AC.1140
					SIR.1 SIR.4								BP.1	AC.1111 AC.1141
					SIR.2 SIR.5							BP.0		AC.1120 AC.1150
					SIR.2 SIR.5								BP.1	AC.1121 AC.1151
					SIR.3 SIR.6								BP.1	AC.1131 AC.1161

8.2.2 Authentification basée sur les capacités de sécurité des tranches de réseau IMT-2020

L'authentification peut être assurée par des capacités comme l'authentification et l'autorisation propres aux tranches de réseau. Il existe deux niveaux d'authentification , comme indiqué dans le tableau suivant:

Tableau 8-2 – Niveaux d'authentification

Dimension de sécurité: Authentification (Au)			
Capacité	**Authentification et autorisation propres aux tranches de réseau (NSSAA)**		**Nom du niveau**
Options	**NSSAA.0**	**NSSAA.1**	
Combinaison	NSSAA.0		Au.0
	NSSAA.1		Au.1

8.2.3 Non-répudiation basée sur les capacités de sécurité des tranches de réseau IMT-2020

Aucune capacité décrite au paragraphe 7 n'assure la non-répudiation.

8.2.4 Confidentialité des données basée sur les capacités de sécurité des tranches de réseau IMT-2020

La confidentialité des données peut être assurée par des capacités comme la protection des données du plan d'utilisateur. Il existe deux niveaux d'authentification, comme indiqué dans le tableau suivant:

Tableau 8-3 – Niveaux de confidentialité des données

Dimension sécurité – Confidentialité des données (DC)			
Capacité	**Protection des données du plan d'utilisateur (UPDP)**		**Nom du niveau**
Options	**UPDP.0**	**UPDP.1**	
Combinaison	UPDP.0		DC.0
	UPDP.1		DC.1

8.2.5 Sécurité de la communication basée sur les capacités de sécurité des tranches de réseau IMT-2020

La sécurité de la communication peut être assurée par des capacités comme la protection aux limites et la protection des services d'application. Il existe diverses combinaisons de capacités avec différentes options permettant d'obtenir différents niveaux de sécurité de la communication, comme indiqué dans le tableau suivant:

Tableau 8-4 – Niveaux de sécurité des communications

Dimension de sécurité – Sécurité de la communication (CS)					
Capacités	**Protection aux limites (BP)**		**Protection des services d'application (ASP)**		**Nom du niveau**
Options	**BP.0**	**BP.1**	**ASP.0**	**ASP.1**	
Combinaisons	BP.0		ASP.0		CS.00
	BP.0		ASP.1		CS.01
	BP.1		ASP.0		CS.10
	BP.1		ASP.1		CS.11

8.2.6 Intégrité des données fondée sur les capacités de sécurité des tranches de réseau IMT-2020

L'intégrité des données peut être assurée par des capacités comme la protection des données du plan d'utilisateur. Il existe deux niveaux d'intégrité des données, comme indiqué dans le tableau suivant:

Tableau 8-5 – Niveaux d'intégrité des données

Dimension de sécurité: Intégrité des données (DI)			
Capacité	**Protection des données du plan d'utilisateur (UPDP)**		**Nom du niveau**
Options	**UPDP.0**	**UPDP.1**	
Combinaison	UPDP.0		DI.0
	UPDP.1		DI.1

8.2.7 Disponibilité basée sur les capacités de sécurité des tranches de réseau IMT-2020

La disponibilité des données peut être assurée par des capacités comme l'isolation de tranches de ressources de réseau, la protection aux limites et la protection des services d'application. Il existe diverses combinaisons de capacités avec différentes options permettant d'obtenir différents niveaux de disponibilité, comme indiqué dans le tableau suivant:

Tableau 8-6 – Niveaux de disponibilité

Dimension de sécurité: disponibilité (Av)							
Capacité	**Protection des services d'application (ASP)**		**Isolation de tranches de ressources de réseau (SIR)**		**Protection aux limites (BP)**		**Nom du niveau**
Options Combinaison	**ASP.0**	**ASP.1**	**SIR.1/SIR.2/SIR.3**	**SIR.4/SIR.5/SIR.6**	**BP.0**	**BP.1**	
	ASP.0		SIR.1/SIR.2/SIR.3		BP.0		Av.000
					BP.1		Av.001
			SIR.4/SIR.5/SIR.6		BP.0		Av.010
					BP.1		Av.011
	ASP.1		SIR.1/SIR.2/SIR.3		BP.0		Av.100
					BP.1		Av.101
			SIR.4/SIR.5/SIR.6		BP.0		Av.110
					BP.1		Av.111

8.2.8 Confidentialité des données basée sur les capacités de sécurité des tranches de réseau IMT-2020

La confidentialité des données peut être assurée par des capacités comme la protection de la confidentialité des données de l'identificateur EAP au cours de la procédure NSSAA et de la protection de la confidentialité des informations associées à la procédure (S-)NSSAI. Il existe diverses combinaisons de capacités avec différentes options permettant d'obtenir différents niveaux de confidentialité des données, comme indiqué dans le tableau suivant:

Tableau 8-7 – Niveaux de respect de la confidentialité

<table>
<tr><th colspan="5">Dimension de sécurité – Respect de la vie privée (Pr)</th></tr>
<tr><th rowspan="2">Capacités</th><th colspan="2">Protection de la confidentialité des données de l'identificateur EAP pendant la procédure NSSAA (PPEAP)</th><th colspan="2">Protection de la confidentialité des informations associées à la procédure (S-)NSSAI (PPSI)</th><th rowspan="2">Nom du niveau</th></tr>
<tr><th>Options</th><th>PPEAP.0</th><th>PPEAP.1</th><th>PPSI.0</th><th>PPSI.1</th></tr>
<tr><td rowspan="4">Combinaisons</td><td colspan="2">PPEAP.0</td><td colspan="2">PPSI.0</td><td>Pr.00</td></tr>
<tr><td colspan="2">PPEAP.0</td><td colspan="2">PPSI.1</td><td>Pr.01</td></tr>
<tr><td colspan="2">PPEAP.1</td><td colspan="2">PPSI.0</td><td>Pr.10</td></tr>
<tr><td colspan="2">PPEAP.1</td><td colspan="2">PPSI.1</td><td>Pr.11</td></tr>
</table>

9 Lignes directrices et exigences relatives aux types de sécurité des tranches

Un ensemble de dimensions de sécurité peut caractériser un type de sécurité des tranches de réseau et se distinguer par une catégorie de service. On pourra définir de nombreux types de sécurité des tranches en combinant les dimensions de sécurité et les différents niveaux. Néanmoins, toutes les combinaisons ne sont pas acceptables.

La méthode et le principe permettant de créer des types de sécurité des tranches sont les suivants:

1) Il est recommandé de déterminer en premier lieu les niveaux des dimensions de sécurité les plus prioritaires en fonction des exigences de service et de la qualité de fonctionnement des niveaux.
2) Il est recommandé de déterminer les niveaux des autres dimensions de sécurité en fonction des exigences de service et de la qualité de fonctionnement des niveaux.
3) Il est recommandé de vérifier s'il existe une incompatibilité entre chaque dimension de sécurité aux fins de coordination. Dans une tranche, pour différentes dimensions de sécurité ayant la même capacité de sécurité, les options de la capacité de sécurité devraient être compatibles.
4) Lorsque les options de certaines capacités ou le niveau de certaines dimensions de sécurité sont mis à jour pour un type de sécurité des tranches, il est recommandé de modifier les capacités et les dimensions de sécurité associées dans un souci de cohérence.

10 Lignes directrices et exigences à l'intention des parties prenantes concernant la classification des capacités de sécurité des tranches de réseau

Il est recommandé aux opérateurs de tranches d'établir leur propre liste des capacités de sécurité des tranches à partir de la liste générique des capacités de sécurité des tranches figurant dans le paragraphe 7 et de leurs capacités de sécurité privées.

Il est recommandé aux opérateurs de tranches d'établir leur propre liste de dimensions de sécurité avec des niveaux fondés sur la liste générique des dimensions de sécurité et sur leurs capacités de sécurité privées ou sur d'autres dimensions , conformément à la méthode décrite au paragraphe 8.

Il est recommandé aux opérateurs de tranches d'établir leur propre liste des types de sécurité des tranches, conformément à la méthode décrite au paragraphe 9.

Il est recommandé aux opérateurs de tranches de décider des capacités et des options de sécurité pour une instance de tranche (par exemple, au cours de l'approvisionnement [b-ETSI TS 128 531]) en fonction de leur liste de capacités de sécurité des tranches, de leur liste de dimensions de sécurité par niveau ou de leur liste de types de sécurité des tranches, en établissant une correspondance avec les niveaux des dimensions de sécurité ou les types de sécurité des tranches.

Il est recommandé aux clients de tranches de choisir des combinaisons de capacités et d'options de sécurité dans la liste générique des capacités de sécurité des tranches ou dans la liste de capacités de sécurité des tranches de l'opérateur, s'ils connaissent précisément leurs exigences en matière de sécurité et les capacités de sécurité correspondantes.

Il est recommandé aux clients de tranches de choisir les niveaux des dimensions de sécurité connexes en fonction de la qualité de fonctionnement des niveaux indiquée dans la liste générique des dimensions de sécurité par niveau ou dans la liste des dimensions de sécurité par niveau établie par l'opérateur, s'ils connaissent l'effet de certaines des dimensions de sécurité qu'ils veulent obtenir.

Il est recommandé aux clients de tranches de choisir un type dans la liste des types de sécurité des tranches de l'opérateur, s'ils ne connaissent pas en détail le contenu des dimensions de sécurité.

Appendice I

Qualité de fonctionnement pour les options des capacités de sécurité des tranches de réseau IMT-2020

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

NOTE – La qualité de fonctionnement dépend de certains aspects précis de la mise en œuvre et peut varier en fonction de l'évolution des technologies.

- Qualité de fonctionnement pour les options NSSAA:
  - NSSAA.0: niveau de base.
  - NSSAA.1: davantage d'autonomie (pour les secteurs verticaux).
- Qualité de fonctionnement pour les options SIR:
  - SIR.0: aucune isolation: niveau de base
  - SIR.1: isolation logique + partage du RB: l'option SIR.1 offre plus de flexibilité et peut entraîner moins de coûts que les options SIR.2 et SIR.3.
  - SIR.2: isolation logique + physique + partage du RB: l'option SIR.2 offre plus de flexibilité et peut entraîner moins de coûts que l'option SIR.3. L'option SIR.2 est plus fiable que l'option SIR.1.
  - SIR.3: isolation physique + partage du RB: l'option SIR.3 est plus fiable et nécessite plus de ressources que les options SIR.1 et SIR.2.
  - SIR.4: isolation logique+ partage du RB: l'option SIR.4 offre plus de flexibilité et peut entraîner moins de coûts que les options SIR.5 et SIR.6.
  - SIR.5: isolation logique + physique + réservation du RB: l'option SIR.5 offre plus de flexibilité et peut entraîner moins de coûts que l'option SIR.6. L'option SIR.2 est plus fiable que l'option SIR.4.
  - SIR.6: isolation physique + réservation du RB: l'option SIR.6 présente un temps de latence plus faible et une fiabilité et des coûts plus élevés que les autres options.

Les options avec isolation logique peuvent nécessiter moins de ressources de serveur que les options avec isolation physique, mais la première peut entraîner plus de coûts en termes de contre-mesures de sécurité que la seconde, pour un effet de protection similaire.

Les options avec isolation physique peuvent assurer un niveau de contrôle d'accès plus élevé que les options avec isolation logique.

Les options comprenant le partage du RB offrent un effet de couverture accru et plus flexible et une meilleure utilisation des ressources plus que les options comprenant la réservation du RB.

- Qualité de fonctionnement pour les options UPDP:
  - UPDP.0: aucune protection des données au niveau de l'interface radioélectrique et latence inférieure à celle de l'option UPDP.1.
  - UPDP.1: protection des données au niveau de l'interface radioélectrique, avec des effets de protection différents selon les algorithmes de chiffrement facultatifs.
- Qualité de fonctionnement pour les options BP:
  - BP.0: niveau de base.
  - BP.1: protection aux limites avec des effets de protection différents selon les fonctions/fonctionnalités facultatives de contrôle de la sécurité déployées.

- Qualité de fonctionnement pour les options ASP:
  - ASP.0: niveau de base.
  - ASP.1: protection des services d'application avec des effets de protection différents selon les fonctionnalités facultatives de protection des services d'application employées.
- Qualité de fonctionnement pour les options PPEAP:
  - PPEAP.0: l'identité de l'équipement d'utilisateur est révélée.
  - PPEAP.1: l'identité de l'équipement d'utilisateur est anonyme.
- Qualité de fonctionnement pour les options PPSI:
  - PPSI.0: la procédure (S-)NSSAI est révélée.
  - PPSI.0: la procédure (S-)NSSAI n'est pas révélée.

Appendice II

Exemple de types de sécurité des tranches de réseau IMT-2020 de base

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

Le tableau suivant, qui indique les types de sécurité des tranches de base, est établi à partir de la méthode décrite au paragraphe 9 et pourra être utilisé directement ou adapté par les parties prenantes, afin de créer leurs propres types de sécurité des tranches.

Tableau II.1 – Exemples de types de sécurité des tranches de base

Type de sécurité des tranches	Contrôle d'accès	Authen-tification	Dispo-nibilité	Sécurité de la commu-nication	Confiden-tialité des données	Intégrité des données	Non-répudia-tion	Respect de la vie privée	Évalu-ation	Services appropriés
0	AC.0	Au.0	Av.0	CS.0	DC.0	DI.0	–	Pr.0	Sécurité de base	Réseau public
1	AC.1161	Au.1	Av.111	CS.11	DC.1	DI.1	–	Pr.11	Niveau de sécurité élevé, coût très élevé	Types de sécurité élevée (par ex. lignes privées pour les pouvoirs publics, le secteur des finances, titres et clients des réseaux de distribution d'électricité)
2	AC.0000	Autor.0	Av.0	CS.0	–	–	–	–	Faible coût	Type à faible coût, accès Internet et vidéo OTT
3	AC.xx61	–	Av.x11	–	–	–	–	Pr.xx4 Pr.xx6	Niveau élevé d'isola-tion, coût élevé	Type d'isolation forte
4	–	–	Av.x1x	–	DC.0	DI.0	–	–	Faible latence	Faible latence (par ex., pour les jeux en nuage)

NOTE – l'indication x dans le numéro de série du nom du niveau désigne une valeur quelconque.

Bibliographie

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

[b-3GPP TS 23.502] 3GPP TS 23.502, *Procedures for the 5G System (5GS)*. <https://www.3gpp.org/ftp/Specs/archive/23_series/23.502>

[b-3GPP TS 28.541] 3GPP TS 28.541, *Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3*. <https://www.3gpp.org/ftp/Specs/archive/28_series/28.541>

[b-IETF RFC 3748] IETF RFC 3748, *Extensible Authentication Protocol (EAP)*. <https://tools.ietf.org/html/rfc3748>

[b-IETF RFC 5216] IETF RFC 5216, *The EAP-TLS Authentication Protocol*. <https://www.rfc-editor.org/rfc/rfc5216.html>

[b-IETF RFC 5281] IETF RFC 5281, *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)*. <https://datatracker.ietf.org/doc/html/rfc5281>

[b-ETSI TS 128 530] Spécification technique, ETSI TS 128 530 V17.1.0 (2022), *5G; Management and orchestration; Concepts, use cases and requirements* (Spécification technique 3GPP 28.530 v17.2.0 Version 17). <https://www.etsi.org/deliver/etsi_ts/128500_128599/128530/17.02.00_60/ts_128530v170200p.pdf>

[b-ETSI TS 128 531] Spécification technique, ETSI TS 128 531 V16.9.0 (2021), *5G; Management and orchestration; Achats;* (Spécification technique 3GPP TS 28.531 v16.6.0 Version 16). <https://www.etsi.org/deliver/etsi_ts/128500_128599/128531/16.06.00_60/ts_128531v160600p.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	Equipements 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, 2023