UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T Q.1531

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(06/2000)

SÉRIE Q: COMMUTATION ET SIGNALISATION

Réseau intelligent

Prescriptions de sécurité dans les TPU pour l'ensemble de services 1

Recommandation UIT-T Q.1531

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE Q

COMMUTATION ET SIGNALISATION

SIGNALISATION DANS LE SERVICE MANUEL INTERNATIONAL	Q.1–Q.3
EXPLOITATION INTERNATIONALE AUTOMATIQUE ET SEMI-AUTOMATIQUE	Q.4–Q.59
FONCTIONS ET FLUX D'INFORMATION DES SERVICES DU RNIS	Q.60–Q.99
CLAUSES APPLICABLES AUX SYSTÈMES NORMALISÉS DE L'UIT-T	Q.100–Q.119
SPÉCIFICATIONS DES SYSTÈMES DE SIGNALISATION N° 4 ET N° 5	Q.120–Q.249
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION N° 6	Q.250–Q.309
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION R1	Q.310–Q.399
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION R2	Q.400–Q.499
COMMUTATEURS NUMÉRIQUES	Q.500–Q.599
INTERFONCTIONNEMENT DES SYSTÈMES DE SIGNALISATION	Q.600–Q.699
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION N° 7	Q.700–Q.799
INTERFACE Q3	Q.800–Q.849
SYSTÈME DE SIGNALISATION D'ABONNÉ NUMÉRIQUE N° 1	Q.850–Q.999
RÉSEAUX MOBILES TERRESTRES PUBLICS	Q.1000–Q.1099
INTERFONCTIONNEMENT AVEC LES SYSTÈMES MOBILES À SATELLITES	Q.1100–Q.1199
RÉSEAU INTELLIGENT	**Q.1200–Q.1699**
PRESCRIPTIONS ET PROTOCOLES DE SIGNALISATION POUR LES IMT-2000	Q.1700–Q.1799
RNIS À LARGE BANDE	Q.2000–Q.2999

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

Recommandation UIT-T Q.1531

Prescriptions de sécurité dans les TPU pour l'ensemble de services 1

Résumé

La présente Recommandation spécifie les prescriptions de sécurité pour les télécommunications TPU concernant les communications entre l'utilisateur et le réseau ainsi qu'entre réseaux, qui s'appliquent à l'ensemble de services 1 des télécommunications TPU, tel qu'il est défini dans la Recommandation F.851 [1]. La présente Recommandation traite de toutes les caractéristiques de sécurité pour les télécommunications TPU utilisant des accès avec une signalisation multifréquence DTMF et les accès utilisateur basés sur la signalisation DSS1 hors bande.

Source

La Recommandation Q.1531 de l'UIT-T, élaborée par la Commission d'études 11 (1997-2000) de l'UIT-T, a été approuvée le 15 juin 2000 selon la procédure définie dans la Résolution 1 de la CMNT.

Mots clés

Sécurité, télécommunications TPU.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) 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.

La Conférence mondiale de normalisation des télécommunications (CMNT), 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 la CMNT.

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.

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 à acquérir 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 la base de données des brevets du TSB.

TABLE DES MATIÈRES

Recommandation UIT-T Q.1531

Prescriptions de sécurité dans les TPU pour l'ensemble de services 1

1 Domaine d'application

La présente Recommandation UIT spécifie les prescriptions de sécurité pour les télécommunications TPU concernant les communications entre l'utilisateur et le réseau ainsi qu'entre réseaux, qui s'appliquent à l'ensemble de services 1 des télécommunications TPU, tel qu'il est défini dans la Recommandation F.851 [1]. L'utilisateur dispose en général de deux méthodes d'accès aux télécommunications TPU, à savoir l'accès utilisateur dans la bande basé sur la signalisation multifréquence DTMF et l'accès utilisateur hors bande, tel que la signalisation DSS1. Les prescriptions sont fonction de la méthode utilisée. La présente Recommandation traite toutes les caractéristiques de sécurité pour les télécommunications TPU utilisant des accès avec signalisation multifréquence DTMF et des accès utilisateur hors bande basés sur la signalisation DSS1.

2 Références normatives

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.

[1] Recommandation UIT-T F.851 (1995), *Télécommunications personnelles universelles – Description du service (ensemble de services 1)*.

3 Définitions des termes

3.1 Termes définis dans la Recommandation F.851 [1]

Les termes suivants sont définis dans la Recommandation F.851 [1]:

– authentification;
– identification;
– mobilité personnelle;
– TPU (télécommunications personnelles universelles);
– profil de service TPU;
– gestion de profil de service TPU;
– fournisseur de services TPU;
– abonné TPU;
– utilisateur TPU.

3.2 Termes non définis dans la Recommandation F.851 [1]

La présente Recommandation définit les termes suivants:

3.2.1 autorisation: propriété permettant d'établir et de faire appliquer des droits d'accès.

3.2.2 confidentialité: propriété permettant d'interdire la mise à disposition ou la divulgation, à des individus, des entités ou des processus non autorisés, des informations concernant une entité ou un abonné.

3.2.3 intégrité: propriété permettant d'interdire la modification non autorisée des informations contenues dans un objet.

3.2.4 respect de la vie privée: fourniture de fonctionnalités évitant que les utilisateurs ne subissent de restriction de leur liberté d'action.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

CS-1 ensemble de capacités 1 (*capability set 1*)

CS-2 ensemble de capacités 2 (*capability set 2*)

DSS1 système de signalisation d'abonné numérique n° 1 (*digital subscriber signalling system No. 1*)

DTMF multifréquence à deux tonalités (*dual tone multiple frequency*)

IC-card carte à puce (*integrated circuit-card*)

MAC code d'authentification de message (*message authentication code*)

OCPIN numéro PIN pour les appels de départ (*outgoing call PIN*)

OSI interconnexion des systèmes ouverts (*open systems interconnection*)

PIN numéro d'identification personnel (*personal identification number*)

PINX commutateur de réseau privé à intégration de services (*private integrated network exchange*)

PUI identité d'utilisateur personnelle (*personal user identity*)

RGT réseau de gestion des télécommunications

RI réseau intelligent

RMTP réseau mobile terrestre public

RNIS réseau numérique à intégration de services (*integrated services digital network*)

SAPIN numéro PIN de réponse sécurisée (*secure answering PIN*)

SCP point de commande du service (*service control point*)

SDP point de données du service (*service data point*)

SS n° 7 système de signalisation n° 7 (*signalling system No. 7*)

TPU télécommunications personnelles universelles

5 Introduction

La latitude dont disposent les utilisateurs TPU pour se déplacer librement d'un terminal à un autre implique également que des tentatives d'utilisation frauduleuse de leur abonnement peuvent être faites à partir de tout terminal. Il en résulte que les abonnés TPU sont plus exposés à des tentatives d'utilisation frauduleuse de leur abonnement que des abonnés ordinaires. Il est nécessaire que le service TPU fournisse des mécanismes de sécurité suffisants pour garantir que les risques encourus par des abonnés TPU ne paraissent pas exagérés en comparaison avec des abonnés ordinaires.

Les mécanismes de sécurité fournis par le service TPU ne doivent toutefois pas, quel que soit le niveau de protection fourni, être perçus par l'utilisateur TPU comme une gêne supplémentaire mais faire partie des procédures TPU générales.

La sécurité d'un contexte TPU concerne les problèmes suivants:

a) fraudes;

b) confidentialité;

c) disponibilité du service;

d) schéma de protection.

5.1 Fraudes

Les fraudes correspondent à une utilisation abusive d'équipements TPU par des utilisateurs non autorisés, en particulier pour un service TPU donnant lieu à une taxation qui sera imputée sur le compte d'un utilisateur TPU légitime. Les besoins suivants en découlent:

a) authentification des utilisateurs et des abonnés;

b) détails des appels;

c) audits.

5.2 Confidentialité

La confidentialité consiste à ne pas révéler des informations concernant l'utilisateur TPU et l'abonné TPU à toute personne qui ne possède pas une autorisation légale pour leur examen. Ces informations englobent les suivantes:

a) contenu d'une communication;

b) détails comptables;

c) détails d'appel;

d) détails d'enregistrement.

5.3 Disponibilité du service

La possibilité, pour les utilisateurs TPU, de bénéficier à tout instant des services TPU souhaités peut être limitée par les contraintes suivantes:

a) fiabilité du service;

b) refus de service.

5.4 Schéma de protection

Les spécifications des télécommunications TPU doivent définir des mécanismes permettant de protéger les entités suivantes contre toute menace de la sécurité:

a) utilisateurs TPU;

b) exploitants de réseaux avec capacités TPU et fournisseurs de services;

c) service TPU,

compte tenu des conditions prévues pour la fourniture des télécommunications TPU. Ces dernières constitueront un système ouvert avec un accès universel, ce qui nécessite de limiter au maximum les possibilités de fraude.

6 Description générale

6.1 Objectifs généraux de sécurité

Les objectifs généraux suivants s'appliquent pour la sécurité des télécommunications TPU:

a) l'utilisateur TPU peut employer le service TPU avec un risque minimal de mise en danger de la vie privée ou de taxation erronée liée à une utilisation frauduleuse;

b) la sécurité dont bénéficie un utilisateur TPU ou un exploitant de réseau lorsqu'il fait appel aux services TPU doit être comparable à celle qui est fournie par les réseaux fixes ou mobiles actuels pour l'utilisation des mêmes services;

c) la sécurité dont bénéficie un fournisseur de services TPU ou un exploitant de réseau doit être au moins comparable à celle qui est fournie par les réseaux fixes ou mobiles actuels et doit protéger leurs intérêts commerciaux;

d) les caractéristiques légales, réglementaires et commerciales de la sécurité fournie par les télécommunications TPU doivent tenir compte d'une disponibilité universelle;

e) la sécurité fournie par les télécommunications TPU doit être normalisée de manière adéquate afin de permettre un interfonctionnement et un nomadisme internationaux sécurisés.

6.2 Prescriptions générales concernant la sécurité

L'introduction des télécommunications TPU et des puissantes fonctionnalités de communication qu'elles fournissent nécessitent que divers mécanismes de sécurité soient mis à la disposition des utilisateurs concernés. Les niveaux de sécurité permis par ces mécanismes dépendent des facteurs suivants:

a) choix d'un mécanisme de sécurité particulier;

b) choix des terminaux TPU et des équipements TPU;

c) utilisation effective des procédures TPU;

d) choix des procédures d'accès et d'authentification.

Il convient de noter que certains de ces mécanismes de sécurité sont perçus comme faisant partie intégrante de certaines procédures TPU. Il est souhaitable, d'une manière générale, que tous les mécanismes de sécurité pris en charge par le service TPU soient d'une utilisation simple et soient perçus comme faisant partie des procédures TPU générales.

Il est souhaitable que les fournisseurs de services TPU prennent en charge un certain nombre de niveaux de sécurité qui sont proposés au choix des utilisateurs TPU au moment de la souscription de l'abonnement.

Le niveau de sécurité proposé à l'utilisateur TPU dépend largement du choix du niveau d'authentification.

7 Menaces visant la sécurité des télécommunications TPU

La souplesse du service TPU implique que les abonnés TPU sont très exposés à une utilisation frauduleuse de leur abonnement. Les utilisateurs TPU peuvent employer en principe tout terminal mondial pour émettre ou recevoir des appels qui feront l'objet d'une taxation de leur compte. Une personne malveillante peut, de même, utiliser de manière frauduleuse le compte de l'abonné TPU à partir de tout terminal mondial. La prudence recommande que le service TPU assure, vis-à-vis d'une attaque frauduleuse ou malveillante effectuée par tout participant, une protection spécifique pour les points suivants:

a) comptes des abonnés;

b) responsabilité des utilisateurs vis-à-vis de leurs abonnés;

c) détails personnels des utilisateurs;

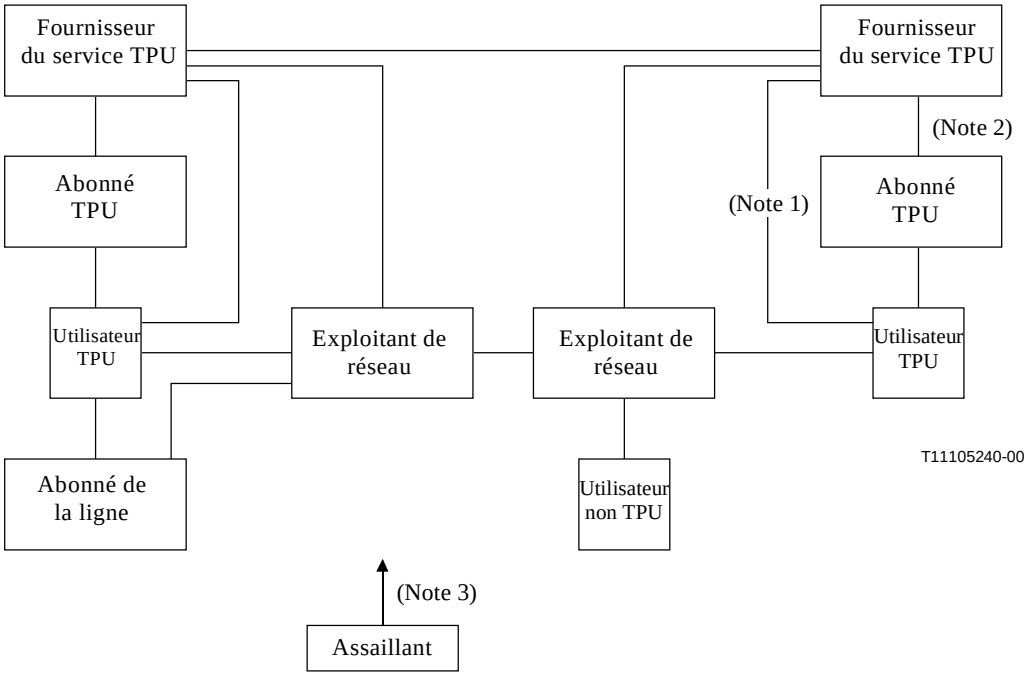
d) intégrité du réseau;

e) flux financiers des exploitants de réseau;

f) réputation des exploitants de réseau.

Les divers participants TPU sont engagés dans une grande variété de relations. Toutes les relations doivent être surveillées par des accords adéquats tenant également compte des diverses contraintes légales dans les pays concernés.

La Figure 1 représente le diagramme de relations entre les participants impliqués dans les télécommunications TPU. L'assaillant n'est pas représenté à un emplacement déterminé dans le diagramme étant donné que la relation dépend uniquement du type d'attaque qu'il effectue.



NOTE 1 – Par exemple, accès et gestion du profil de service.
NOTE 2 – Par exemple, taxation et gestion du profil de service.
NOTE 3 – Un assaillant peut effectuer une attaque sur tout participant et sur toute liaison entre participants.

Figure 1/Q.1531 – Modèle de participants TPU et de leurs relations

7.1 Menaces liées aux fonctionnalités TPU

La liste qui suit indique les principales menaces visant les services TPU.

Usurpation de l'identité d'un utilisateur TPU

Un assaillant peut intercepter des données d'authentification et les utiliser afin d'émettre des appels de départ en utilisant un numéro TPU, de sorte que l'abonné TPU de ce numéro TPU devra payer les taxes afférentes aux appels effectués par l'assaillant.

Un assaillant peut utiliser des données interceptées pour s'immatriculer pour des appels arrivée destinés au numéro TPU d'une autre personne. L'utilisateur TPU perdra de ce fait ses appels arrivée qui peuvent être renvoyés par l'assaillant; l'abonné TPU correspondant devra éventuellement payer les taxes afférentes à ces appels (par exemple en cas de partage des taxes).

Usurpation de l'identité d'un fournisseur de services TPU

Un grand nombre de menaces majeures peuvent concerner la sécurité de l'utilisateur TPU si un tiers réussit à se faire passer pour un fournisseur de services TPU.

Lecture ou modification non autorisée de données d'abonnement faite par l'utilisateur ou l'abonné

Un utilisateur ou un abonné peut lire ou modifier des données d'abonnement dans le profil de service sans l'autorisation du fournisseur du service, en accord avec son abonné (et peut-être avec le fournisseur du service) en raison d'une protection défectueuse du profil de service.

Données de facturation incorrectes

Des données de facturation incorrectes peuvent constituer une menace pour la comptabilité, concernant aussi bien l'abonné que le fournisseur du service et l'exploitant de réseau qui se facturent mutuellement pour l'utilisation du service et du réseau.

Interception de l'identité de l'utilisateur, des informations d'authentification et des données d'immatriculation

Les données d'immatriculation, l'identité de l'utilisateur et les données d'authentification peuvent être interceptées lors de l'enregistrement, par exemple au moyen d'un faux terminal, de l'interception des informations de radiation électromagnétique ou par écoute sur la ligne, etc. Toutes les autres menaces peuvent en découler.

Immatriculation non autorisée

Une immatriculation peut être faite avec un numéro personnel arbitraire sur un accès terminal sélectionné, sans que l'abonné de la ligne en ait connaissance. Ce dernier peut alors recevoir des appels arrivée gênants ou indésirables. Il peut être obligé de payer pour l'appel en cas de partage des taxes.

Utilisation non autorisée de l'équipement d'accès TPU

Un équipement contenant des informations d'autorisation peut être volé et utilisé par un imposteur. L'accès temporaire à l'équipement peut également permettre l'extraction des informations d'authentification.

La liste qui suit indique les principales menaces visant les fonctionnalités TPU optionnelles et les mécanismes de protection des tiers.

Menaces liées à l'immatriculation pour les appels de départ (y compris l'immatriculation pour tous les appels et l'immatriculation avec lien, faites à distance ou non)

Il est possible qu'une personne souscrive à un abonnement, l'utilise de manière intensive et ne paye pas sa facture. L'impact éventuel est accru par la possibilité d'effectuer simultanément des immatriculations multiples pour les appels de départ.

L'usurpation de l'identité d'un utilisateur TPU lors de l'immatriculation pour les appels de départ, l'immatriculation pour tous les appels et l'immatriculation avec lien donnera lieu à un risque économique important dans le cas où un assaillant se procure des données d'authentification valides.

Il est possible qu'un utilisateur immatriculé ne soit pas en mesure de superviser le ou les terminaux immatriculés, de sorte qu'un assaillant peut effectuer des appels sans payer de facture (se référer également au paragraphe "Usurpation de l'identité d'un utilisateur TPU").

Une immatriculation sur un téléphone RNIS implique l'enregistrement de tous les autres terminaux connectés sur le même bus RNIS. L'utilisateur TPU court le danger d'ignorer qu'il a effectué une immatriculation pour plusieurs terminaux (situés éventuellement dans d'autres pièces).

Menaces liées à la réponse sécurisée aux appels arrivée – Spécifiée par l'appelé

Si un tiers réussit à se faire passer pour un fournisseur de services TPU, il peut alors demander l'exécution d'une authentification en émettant simplement un appel pour l'utilisateur TPU. Le code d'authentification qui est fourni dans ce cas peut être enregistré et réutilisé ultérieurement pour effectuer de manière illégale une immatriculation ou un appel de départ, etc., si une procédure d'authentification simple est utilisée.

Menaces liées à la prise d'appel

Un utilisateur non valide peut procéder à la prise d'un appel en l'absence d'une authentification de l'utilisateur.

Menaces liées à l'immatriculation d'adresse terminale multiple

Dans le cas d'une immatriculation d'adresse terminale multiple, la menace liée à un détournement de l'abonnement (avec l'intention de ne pas payer de facture) et la menace d'usurpation d'identité entraîneront un niveau de risques et d'évaluation plus important.

Menaces liées à la réinitialisation d'immatriculations

Ce service a pour objet de protéger des tiers contre des immatriculations TPU indésirables. Il peut toutefois provoquer également un refus de service pour les utilisateurs TPU. Ceci peut être particulièrement fâcheux si l'immatriculation est annulée sans la connaissance de l'utilisateur TPU.

7.2 Menaces liées aux communications entre réseaux

Un certain nombre de procédures ont été définies pour les communications entre réseaux propres aux télécommunications TPU, afin de permettre l'échange de données d'exploitation, de maintenance et de taxation entre des fournisseurs de services TPU et des exploitants de réseau avec capacités TPU.

La liste qui suit indique les principales menaces visant la communication entre réseaux pour le service TPU.

Usurpation de l'identité d'entités TPU

Un assaillant peut se faire passer pour une entité TPU (par exemple un point SCP ou SDP) pour un acheminement ou une réception illégale d'appels à travers un réseau avec capacités TPU.

Modification, suppression ou reproduction de données de signalisation TPU

Un assaillant peut modifier des informations de signalisation pour perturber le service ou manipuler des informations de taxation.

Interception de données de signalisation TPU

Un assaillant peut intercepter des données de signalisation en vue d'obtenir des informations concernant, par exemple, l'emplacement des utilisateurs ou des informations internes aux fournisseurs de services TPU qui communiquent.

Usurpation de l'identité de l'origine, répudiation, modification, suppression et reproduction de fichiers et de messages

Un assaillant peut effectuer à son profit l'une de ces actions, en particulier pour manipuler des données de taxation.

Interception de fichiers et de messages

Un assaillant peut intercepter des fichiers et des messages, par exemple en vue d'obtenir des informations concernant l'emplacement des utilisateurs ou découvrir des informations confidentielles stockées dans les bases de données des fournisseurs de services TPU.

Confidentialité des données dans un environnent concurrentiel

Les communications entre réseaux peuvent également poser des problèmes de sécurité relatifs à la nature concurrentielle des données de l'abonné du service.

7.3 Situations involontaires

La liste qui suit indique les menaces liées à des situations non prévues.

Connexion réseau vers une base de données incorrecte

Une situation non prévue peut se présenter lorsque le point SCP n'est pas connecté au point SDP correct. Des informations portant sur des personnes non concernées peuvent être divulguées dans ce cas. Un utilisateur TPU peut, par exemple, avoir été authentifié par "son" point SDP, mais une nouvelle tentative d'extraction peut s'effectuer à partir d'un autre point SDP à la suite d'une erreur de connexion.

8 Prescriptions système concernant la sécurité

Le présent paragraphe décrit les prescriptions de sécurité système s'appliquant à un ou plusieurs abonnés impliqués dans le service TPU.

Les prescriptions système concernant la sécurité TPU sont regroupées selon les catégories suivantes:

a) prescriptions liées au service;

b) prescriptions liées à l'accès;

c) prescriptions de fonctionnement du réseau;

d) prescriptions de gestion de la sécurité.

8.1 Prescriptions liées au service

Les prescriptions de sécurité suivantes liées au service s'appliquent pour les télécommunications TPU:

a) les fonctionnalités de sécurité fournies pour la protection des utilisateurs TPU doivent être conviviales et faciles à utiliser. Elles doivent autant que possible être transparentes pour les utilisateurs et nécessiter une interaction aussi faible que possible entre l'utilisateur et le réseau;

b) les fonctionnalités de sécurité fournies pour la protection des utilisateurs TPU ne doivent pas accroître de manière significative le temps d'établissement des appels;

c) les fonctionnalités de sécurité ne doivent pas réduire le niveau de sécurité fourni en cas de nomadisme;

d) les fonctionnalités de sécurité fournies par les télécommunications TPU doivent fonctionner avec les divers environnements TPU et ne pas être limitées par toute couche Physique ou méthode d'accès;

e) le respect de la vie publique des utilisateurs non TPU ne doit pas être affecté par l'utilisation des équipements ou des services TPU.

8.2 Prescriptions liées à l'accès

Les prescriptions de sécurité suivantes liées à l'accès s'appliquent pour les télécommunications TPU:

a) il doit être très difficile pour des assaillants de se faire passer pour un utilisateur ou un abonné TPU;

b) il doit être très difficile pour des intrus de se faire passer pour un fournisseur de services ou un exploitant de réseau TPU qui communique avec un utilisateur TPU ou avec un autre fournisseur de services TPU;

c) il doit être très difficile pour des intrus d'accéder en lecture ou en modification à des informations stockées ou transmises pour un utilisateur TPU;

d) le fournisseur de services TPU doit disposer de mécanismes permettant de démontrer la correction et l'authenticité de transactions effectuées avec des utilisateurs TPU;

e) il doit être très difficile pour des intrus d'accéder à la structure de signalisation d'un réseau avec capacités TPU et aux fonctions de commandes connexes ou déplacer des fausses commandes.

8.3 Prescriptions de fonctionnement du réseau

Les prescriptions de sécurité suivantes liées au fonctionnement du réseau s'appliquent aux télécommunications TPU:

a) la sécurité devant être fournie par les télécommunications TPU doit être normalisée de manière adéquate afin de fournir un interfonctionnement et un nomadisme internationaux sécurisés. Il est toutefois nécessaire de permettre, dans le cadre des mécanismes de sécurité des télécommunications TPU, une indépendance maximale entre les participants impliqués dans leur fonctionnement, ainsi qu'une souplesse maximale pour tous les participants en ce qui concerne leurs politiques et mécanismes de sécurité propres;

b) les mécanismes de sécurité des télécommunications TPU doivent utiliser aussi peu que possible des connexions de signalisation à distance en temps réel (par exemple, pour éviter la mise en œuvre de connexions de signalisation internationale lors de chaque mise à jour pour un emplacement ou un appel en cas de nomadisme).

8.4 Prescriptions de gestion de la sécurité

Les prescriptions de sécurité suivantes liées à la gestion de la sécurité s'appliquent pour les télécommunications TPU:

a) la mise à jour et la gestion des clés et des équipements de sécurité distribués aux utilisateurs doivent être faciles et sécurisées;

b) la gestion des clés de sécurité au sein d'un fournisseur de services et entre fournisseurs de services TPU doit être sécurisée;

c) le fournisseur de services TPU doit disposer de mécanismes sécurisés pour le stockage des événements liés aux utilisateurs ou aux abonnés TPU;

d) il doit être très difficile pour des intrus de se faire passer pour un fournisseur de services TPU lors de la communication avec des exploitants de réseau avec capacités TPU et réciproquement;

e) les mécanismes de sécurité fournis par les télécommunications TPU doivent disposer de moyens de gestion de version et permettre une mise à jour facile pendant la durée de vie des télécommunications TPU.

9 Fonctionnalités de sécurité pour les télécommunications TPU

Comme c'est le cas pour tous les systèmes mis à la disposition du public, des fonctionnalités de sécurité des télécommunications TPU nombreuses et diverses doivent être fournies et faire l'objet d'une coopération afin d'obtenir le niveau global de sécurité nécessaire.

Les services de sécurité sont caractérisés par les propriétés suivantes:

prévention: a pour objet d'interdire la menace;

compte rendu: fournit à la gestion-systèmes ou à l'utilisateur des informations concernant la sécurité;

limitation: introduction de limitations dans le système dans le but de réduire les conséquences de violations éventuelles de la sécurité;

restauration: retour rapide, sécurisé et ordonné à un fonctionnement normal après l'apparition d'un problème de sécurité;

dissuasion: a pour objet de décourager les fraudeurs potentiels du fait qu'ils ont connaissance de cette fonctionnalité de sécurité.

Toutes ces propriétés sont nécessaires et utiles dans l'architecture globale de sécurité des télécommunications TPU.

Il est possible d'identifier les fonctionnalités de sécurité suivantes pour les télécommunications TPU:

a) confidentialité;

b) authentification;

c) intégrité;

d) autorisation et contrôle d'accès;

e) respect de la vie privée et anonymat;

f) disponibilité du service;

g) limitation des événements;

h) compte rendu d'événement.

9.1 Fonctionnalités du service TPU fournissant la sécurité

Ces fonctionnalités ne suffisent pas de manière intrinsèque à faire échec à une menace donnée, mais contribuent néanmoins à atteindre (en conjonction avec d'autre mesures de sécurité) le niveau de sécurité requis.

Limitation de la facture

La limitation de la facture ou du crédit est le seul moyen efficace de limiter les conséquences d'une consommation importante et éventuellement non autorisée, effectuée par l'utilisateur ou par un assaillant se faisant passer pour lui. La valeur limite des taxes cumulées doit être fixée par le fournisseur du service en coopération avec l'abonné. Pour être efficace, ce contrôle doit se faire en conjonction avec l'authentification de tout appel de départ (ce principe peut même être étendu au contrôle des appels arrivée, compte tenu de la manière dont ces appels sont taxés par l'exploitant du service et de sa politique de sécurité). Le fournisseur du service n'autorisera pas de nouvel appel qui accroît le montant des taxes une fois que la limite est atteinte. Cette situation doit être portée à la connaissance de l'utilisateur immédiatement avant que la limite soit atteinte et lors de chaque tentative d'appel une fois cette limite atteinte.

Le fournisseur du service peut assurer une protection supplémentaire interdisant les fonctionnalités de suivi d'appel de départ, d'immatriculation pour les appels de départ ou d'immatriculation distante pour les appels de départ.

Facturation détaillée

La facturation détaillée joue un rôle important dans le cas de certaines menaces qu'il n'est pas possible de détecter ou d'interdire par d'autres moyens. Son inconvénient est évidemment que la détection des problèmes est retardée jusqu'au moment de la réception de la facture et dépend de

l'examen détaillé de cette dernière. La connaissance de l'existence d'une facturation détaillée a un effet dissuasif qui peut limiter une utilisation abusive du service par certaines personnes.

Des précautions spéciales sont nécessaires pour le respect de la vie privée.

Supervision des activités

Cette mesure de sécurité consiste à superviser en temps réel les activités et les événements liés au compte d'un utilisateur ou au service TPU proprement dit, incluant tout ou partie des tentatives d'authentification, des activités d'appel et des indications de taxation. Le profil d'activité d'un utilisateur peut indiquer un emploi abusif de son compte. La supervision des activités est la seule protection dont dispose le fournisseur du service TPU (et de manière indirecte, ses abonnés et ses utilisateurs) pour réagir rapidement dans le cas d'une utilisation frauduleuse. Ceci est particulièrement nécessaire lorsqu'une authentification faible est utilisée.

Annonces

La fourniture d'annonces joue un rôle important dans la sécurité du service. Elle doit être conçue avec soin afin d'informer les utilisateurs et les tiers au sujet des divers états de leur connexion ou de leur relation avec l'exploitant ou le fournisseur du service.

Des précautions spéciales sont nécessaires pour le respect de la vie privée.

Blocage des immatriculations

Le blocage des immatriculations peut permettre à des tiers d'interdire de manière permanente des immatriculations TPU. Il est possible de fournir une protection importante contre des tiers si le blocage des télécommunications TPU constitue par défaut l'état initial pour toutes les lignes d'abonné et si les immatriculations TPU sont autorisées uniquement après un déblocage actif de la part de l'abonné. Ceci peut être le processus normal pour les immatriculations à distance. Le déblocage peut se faire de diverses manières, par exemple sur autorisation écrite de l'abonné, permettant, soit des immatriculations de numéros TPU désignés, soit des immatriculations pour tout numéro TPU. Il est également possible d'utiliser des procédures en ligne. Le consentement peut être soumis à diverses conditions en fonction de l'offre faite à cet effet par le fournisseur du service TPU. Le tiers doit être en mesure d'annuler des accords antérieurs.

Les immatriculations locales ne doivent pas être soumises à cette prescription lorsqu'elles sont faites pour une ligne donnée à partir du même terminal.

Réinitialisation des immatriculations

La réinitialisation des immatriculations est une fonctionnalité essentielle du service TPU. Elle ne fournit toutefois pas de protection complète pour les problèmes d'immatriculation indésirable du fait que des tiers ne sont pas en général familiarisés avec les procédures de réinitialisation.

Engagements contractuels

Les conditions d'abonnement doivent définir des engagements contractuels portant sur les problèmes de sécurité. La liste qui suit indique certaines des conditions pouvant faire l'objet d'un engagement dûment signé par l'abonné:

a) conformité aux règles (énoncées par le fournisseur du service TPU et jointes au contrat d'abonnement) concernant le traitement sécurisé de l'identité PUI et du numéro PIN dans le cas d'une authentification faible, ainsi que les règles correspondantes d'utilisation de l'équipement TPU;

b) compte rendu immédiat au fournisseur du service après la perte d'un numéro PIN ou d'un équipement, ainsi que dans le cas d'autres situations pouvant conduire à des fraudes ou à une utilisation non conforme;

c) respect des restrictions d'utilisation du service qui peuvent être imposées en raison de la protection des tiers;

d) acceptation des conditions du service concernant les accords de limitation du niveau de crédit ou du montant de la facture;

e) acceptation des limitations du service que le fournisseur peut être conduit à introduire ultérieurement en vue de protéger le service TPU en tant que tel contre des utilisations non conformes ou des fraudes;

f) acceptation de la responsabilité dans l'éventualité de fraudes ou d'utilisation non conforme du compte de l'abonné, lorsque ce dernier a commis des fautes graves portant sur le respect des règles;

g) imposer les directives et restrictions correspondantes à ses utilisateurs (autres que l'abonné).

9.2 Fonctionnalités de sécurité pour l'accès utilisateur

De nombreuses menaces seront traitées par des fonctionnalités qui sont déjà présentes dans le concept de service TPU. Leur description est donnée par la Recommandation UIT-T F.851 [1] dans le cadre de l'offre générale de service TPU. La liste qui suit indique les services spécifiques de sécurité requis pour la partie principale des menaces.

Authentification de l'utilisateur ou de l'abonné TPU

Les menaces résultant de l'usurpation d'identité vis-à-vis du fournisseur du service TPU sont les plus sérieuses qui ont été identifiées et l'authentification de l'utilisateur TPU (et de l'abonné TPU) constitue la fonctionnalité de sécurité la plus importante des télécommunications TPU. L'authentification forte utilisant un équipement TPU intelligent (par exemple un équipement avec une signalisation de type DTMF ou un équipement avec carte à puce) est recommandée pour cette raison. L'authentification faible ne fournit pas de manière intrinsèque une solution satisfaisante; elle est acceptable uniquement si elle est complétée par plusieurs autres fonctionnalités de sécurité et par des limitations du service.

Contrôle de l'accès à l'équipement d'accès TPU

Les deux fonctionnalités suivantes sont nécessaires pour le contrôle de l'accès à des informations sensibles stockées dans l'équipement d'accès TPU:

a) authentification de l'utilisateur ou du propriétaire vis-à-vis de l'équipement;

b) protection physique forte, par exemple au moyen d'une carte à puce.

Contrôle d'accès système aux informations de profil de service

Les utilisateurs, les abonnés et le personnel du fournisseur de services auront accès à diverses parties du profil de service. Un contrôle de l'accès système est nécessaire pour la gestion de l'accès aux bases de données de profil de service. Une partie de ce contrôle d'accès se fera évidemment par l'authentification de l'utilisateur ou de l'abonné TPU. Une solution matérielle et logicielle dédiée sera utilisée pour l'authentification personnelle et le contrôle d'accès au sein de l'environnement local du fournisseur de services.

Gestion sécurisée du processus d'abonnement

Il s'agit avant tout de disposer de procédures saines et rigoureuses pour l'administration des abonnements, de toutes les informations secrètes et des équipements, ainsi que de systèmes de contrôle d'accès adéquats pour les abonnements.

Les abonnements peuvent être traités (en partie) en utilisant des moyens de télécommunications si des mesures de sécurité adéquates sont prises (authentification et contrôle d'accès). Il est plus probable qu'un processus manuel sera utilisé pour l'abonnement (avec présence personnelle ou par courrier), les mesures de sécurité adéquates étant prises dans cet environnement.

La conception du service doit prendre en compte des menaces telles que les suivantes:

a) modification non autorisée des données d'abonnement par l'utilisateur ou l'abonné;

b) retrait d'abonnement non autorisé;

c) refus de service à la suite d'une défaillance d'équipement;

d) livraison incorrecte d'équipements TPU.

Les fonctionnalités de sécurité permettant d'atteindre le niveau de gestion de sécurité nécessaire peuvent varier considérablement en fonction des différents environnements des fournisseurs de services et sont en dehors du domaine d'application de la présente Recommandation.

9.3 Fonctionnalités de sécurité pour les communications entre réseaux

Les prescriptions suivantes doivent être prises en compte pour les communications entre réseaux:

a) dialogues sécurisés;

b) transferts de fichier sécurisés.

Les prescriptions de sécurité décrites peuvent s'appliquer non seulement pour les télécommunications TPU, mais également pour la protection d'autres communications entre des réseaux RI. Les fonctions de sécurité seront utilisées, dans la mesure du possible, de manière commune par tous les services RI pour des raisons d'efficacité.

Il s'ensuit que l'allocation de fonctionnalités de sécurité doit être prise en considération dans le cadre de la structure OSI. Les besoins de sécurité suivants ont été identifiés:

a) les fonctions de sécurité doivent, dans la mesure du possible, être indépendantes des réseaux sous-jacents;

b) les protocoles de sécurité doivent, dans la mesure du possible, être indépendants des protocoles de la couche Application.

Les fonctionnalités de sécurité définies dans le présent sous-paragraphe sont mises entre deux entités du RI. Les liaisons réseau sont fournies par le système SS7.

Les fonctionnalités de sécurité mentionnées ci-dessous sont données à titre d'exemple. Les fonctionnalités et mécanismes de sécurité nécessaires doivent être pris en considération dans le cadre de l'élaboration d'une architecture générale de sécurité du RI.

9.3.1 Dialogue sécurisé

Les dialogues sécurisés doivent se constituer d'une procédure d'authentification mutuelle, d'un service de confidentialité et d'un service d'intégrité de données sur la liaison de communication. Les mécanismes de sécurité suivants peuvent être fournis:

a) authentification mutuelle;

b) chiffrement sur la liaison;

c) intégrité des données sur la liaison;

d) gestion de clés pour la prise en charge des fonctionnalités précédentes.

9.3.2 Transfert de fichier sécurisé

Les fichiers doivent être protégés par les fonctionnalités de sécurité suivantes: intégrité des données de fichier et confidentialité du fichier. Les mécanismes de sécurité suivants peuvent être fournis:

a) signature numérique ou code MAC pour l'intégrité des données de fichier;

b) chiffrement de fichier;

c) gestion de clés pour la prise en charge des fonctionnalités précédentes.

La protection et la vérification de l'intégrité ainsi que le chiffrement et le déchiffrement sont des fonctions locales des entités de communication respectives.

9.4 Limites de la sécurité

Le présent sous-paragraphe identifie les menaces qui peuvent ne pas être prises en compte par des fonctionnalités de sécurité pertinentes. Certaines de ces menaces peuvent être considérées comme moins importantes, soit en raison de leur faible probabilité, soit à cause de leurs conséquences limitées, et souvent pour les deux raisons à la fois. D'autres menaces ont été identifiées contre lesquelles il n'existe pas de protection réalisable (justifiable sur le plan économique).

9.4.1 Accès utilisateur basé sur la signalisation multifréquence DTMF

Les menaces non prises en compte incluent toutes celles qui sont liées à une interception ou à une manipulation active des lignes utilisées pour les immatriculations TPU. Les menaces d'interception touchent un point faible important, en particulier si des données d'authentification (par exemple une identité PUI ou un numéro PIN) sont enregistrées. Les risques sont en outre considérablement accrus dans le cas d'utilisation d'une authentification faible à la place de l'identification forte recommandée. Ceci est particulièrement vrai lorsque l'immatriculation est transmise par voie hertzienne, par exemple pour un accès RMTP, ou si elle traverse un équipement qui possède une fonctionnalité intrinsèque d'enregistrement, par exemple un centre PINX. Ceci est l'une des raisons qui contribuent à limiter le service TPU lorsqu'une authentification faible est utilisée.

La protection contre des immatriculations malveillantes sur des terminaux de tiers non informés ou non consentants n'a pas reçu de solution définitive dans le cas d'un accès utilisateur basé sur la signalisation DTMF, parce que la réinitialisation des immatriculations n'est pas disponible d'une manière générale. Les indications, tonalités de numérotation, etc., recommandées ne suffisent pas. Les conditions de blocage par défaut et l'agrément actif utilisant un enregistrement préalable ou un accord en ligne sont possibles mais ne sont pas nécessairement suffisants.

9.4.2 Accès utilisateur basé sur la signalisation DSS1 hors bande

Seules les menaces liées à la manipulation active de la ligne et l'interception de données personnelles ne sont pas traitées, compte tenu du fait qu'une authentification bidirectionnelle est disponible sur les accès DSS1.

La manipulation active de la ligne en relation avec une immatriculation malveillante peut en partie être traitée par des fonctionnalités de gestion, telles que la réinitialisation des immatriculations, la limitation de la facture et la limitation du service.

L'interception de codes d'authentification n'a aucun impact lorsqu'une authentification forte est utilisée.

10 Mécanismes de sécurité pour les télécommunications TPU

10.1 Mécanismes de contrôle d'accès

Des mécanismes de contrôle d'accès seront utilisés pour les domaines suivants:

a) accès au service basé sur l'identité de l'utilisateur ou de l'abonné;

b) accès au profil de service et à d'autres données de gestion, effectué par des utilisateurs, des abonnés, le personnel autorisé appartenant aux fournisseurs de services et par des demandes en provenance d'entités du réseau de rattachement ou du réseau visité;

c) accès aux données stockées au sein de l'équipement d'accès TPU.

10.1.1 Contrôle de l'accès aux services

On peut considérer le contrôle de l'accès au service TPU ou à certaines fonctions de service comme un processus combiné avec l'identification et l'authentification des participants impliqués.

Les mécanismes de contrôle d'accès aux services utiliseront les listes d'authentification suivantes:

listes blanches

Les listes blanches sont des listes de contrôle d'accès ou des listes de fonctionnalités qui spécifient les services que des utilisateurs et des abonnés TPU individuels ont l'autorisation d'utiliser. Elles peuvent être implémentées comme faisant partie des données de profil du service correspondant;

listes noires

Les listes noires spécifient les identités pour lesquelles une demande d'accès au service TPU sera rejetée, par exemple parce que l'utilisateur TPU a dépassé sa limite de crédit. Les listes noires seront mises à jour à chaque fois que c'est nécessaire. Elles seront implémentées dans l'entité d'authentification (par exemple le point SCP ou SDP);

listes grises

Le fournisseur TPU peut également définir des listes grises contenant des identités pour lesquelles des mesures supplémentaires doivent être prises, par exemple l'activation d'une supervision détaillée des activités.

Dans le cas de l'authentification faible, une identité PUI est bloquée si l'accès est refusé de manière temporaire à la suite d'un trop grand nombre de tentatives d'authentification erronées. Le blocage sera effectué dans une entité d'authentification. Il est nécessaire de disposer d'une procédure de déblocage, compte tenu de la possibilité d'un blocage malveillant d'une identité PUI. L'utilisateur dont l'identité PUI est bloquée subira néanmoins une gêne importante.

Dans le cas de l'authentification forte, une identité ne sera pas bloquée parce qu'on considère que l'authentification apporte une sécurité suffisante. La clé de l'utilisateur doit être modifiée si sa clé et son algorithme ont été divulgués.

10.1.2 Contrôle d'accès aux données de profil de service

L'accès aux données de profil de service sera limité pour les sujets suivants possédant des droits différents:

a) utilisateur TPU;

b) abonné TPU;

c) fournisseur de services TPU.

On peut classer, du point de vue de l'utilisateur TPU, les informations stockées dans les données de profil de service en informations fixes et en informations variables. Les informations fixes sont définies en général au moment de la souscription de l'abonnement et peuvent uniquement être modifiées par le fournisseur du service TPU, éventuellement à la demande de l'abonné TPU. Les informations variables peuvent être modifiées par l'utilisateur TPU ou par son abonné TPU, de manière explicite en utilisant les fonctions de gestion du profil de service TPU ou de manière implicite par les fonctions TPU de mobilité personnelle.

Le fournisseur du service TPU doit garantir que seul le personnel autorisé peut accéder aux données. La spécification des mécanismes est de la responsabilité du fournisseur du service TPU et se trouve en dehors du domaine d'application de la présente Recommandation. L'accès de signalisation (par exemple, pour le système SS7) sera protégé par l'authentification des entités réseau et par des listes d'autorisation contenant les fournisseurs de services qui ont des contrats de mobilité, conformément aux accords passés entre fournisseurs de services.

10.1.3 Contrôle d'accès aux données contenues dans les équipements TPU

Le mécanisme de contrôle d'accès utilisera une protection physique forte contre la lecture.

Le mécanisme de contrôle d'accès utilisé pour les équipements TPU peut être pris en charge par une vérification du détenteur de l'équipement.

10.2 Mécanismes d'authentification de l'utilisateur

10.2.1 Degrés d'authentification

Le degré d'authentification (fort ou faible) dépend de la méthode d'authentification utilisée. Le degré d'authentification utilisé doit être suffisant pour réduire les risques de sécurité prévisibles.

L'authentification doit en général être suffisamment forte pour garantir un niveau de sécurité convenable lors de l'accès à des services TPU à travers des réseaux prenant en charge les télécommunications TPU, visités par des utilisateurs TPU. La procédure d'authentification adoptée peut faire l'objet d'une négociation entre le fournisseur du service TPU et les réseaux visités. Les utilisateurs TPU et les fournisseurs de services TPU ont la latitude de prendre en charge divers mécanismes d'authentification pour obtenir le degré d'authentification nécessaire.

On peut classer l'authentification TPU selon un certain nombre de types, dont les suivants:

authentification unidirectionnelle avec un numéro PIN fixe

La procédure d'authentification est réalisée dans ce cas par l'émission du numéro PIN correct par l'utilisateur TPU;

authentification unidirectionnelle avec codes d'authentification variables

La procédure d'authentification utilise également dans ce cas une seule étape de transmission, mais avec un code d'authentification variable;

authentification bidirectionnelle avec codes d'authentification variables

La procédure d'authentification utilise dans ce cas deux étapes de transmission avec un mode avec mise à l'épreuve et réponse;

10.2.2 Types d'équipements TPU

Si l'authentification de l'identité de l'utilisateur TPU est faite au moyen d'un équipement TPU, le niveau de protection dépend alors de la réalisation de cet équipement. Les équipements TPU peuvent se présenter sous diverses formes en fonction des terminaux réseau et des services utilisés, qui peuvent imposer diverses limitations aux mécanismes de sécurité pouvant être fournis d'une manière simple et conviviale. Il peut, de ce fait, être nécessaire de disposer de procédures d'authentification différentes pour les diverses réalisations des équipements TPU. Les réalisations possibles incluent les suivantes:

absence d'équipement TPU

Il peut être nécessaire, dans ce cas, de saisir manuellement l'identité PUI à des fins d'identification et de limiter la procédure d'authentification à la saisie d'un numéro PIN;

équipement TPU avec carte à piste magnétique

Ce type d'équipement TPU nécessite un terminal équipé d'un lecteur de carte à piste magnétique et d'une interface de signalisation permettant de communiquer avec le réseau;

équipement TPU unidirectionnel avec tonalités (par exemple DTMF)

Cet équipement peut, soit simuler simplement la succession de tonalités émise par l'utilisateur TPU pour entrer un numéro PIN pour l'authentification, soit contenir une intelligence permettant de

fournir des procédures d'authentification comparables à celles qui sont possibles avec une carte à puce utilisant une authentification unidirectionnelle (l'équipement TPU fonctionne uniquement en émission de données). L'équipement intelligent doit être en mesure de stocker et de générer des informations de synchronisation. Il doit également, dans le cas d'utilisation d'une clé d'authentification, être en mesure de stocker la clé d'authentification et de générer le code d'authentification;

équipement TPU de type modem

Les fonctionnalités fournies dans ce cas sont identiques à celles du cas précédent, mais utilisent une signalisation acoustique dans la bande conforme à une norme de modem. Dans le cas idéal, les procédures d'authentification doivent être identiques à celles fournies par une carte à puce utilisant une authentification unidirectionnelle ou bidirectionnelle (c'est-à-dire que l'équipement TPU fonctionne en émission et en réception de données). L'équipement intelligent doit être en mesure de stocker et de générer des informations de synchronisation. Il doit également, dans le cas d'utilisation d'une clé d'authentification, être en mesure de stocker la clé d'authentification et de générer le code d'authentification;

équipement TPU avec carte à puce

Il est possible d'utiliser une procédure d'authentification unidirectionnelle ou bidirectionnelle. L'authentification du fournisseur de services TPU peut être combinée avec l'authentification de l'identité de l'abonné (authentifications mutuelles). Une carte à puce doit être en mesure de stocker la clé d'authentification et de générer le code d'authentification.

10.2.3 Signalisation de l'utilisateur

10.2.3.1 Signalisation multifréquence DTMF basée sur l'accès utilisateur (conforme à l'ensemble CS-1 du RI)

Limitations

Les télécommunications TPU seront fournies sur des réseaux existants pour l'ensemble de services TPU 1. L'authentification peut uniquement être effectuée de certaines manières, compte tenu des limitations de ces réseaux et des terminaux qui leur sont connectés.

Les mécanismes d'authentification fournissent des options limitées; l'échange d'informations s'effectuera de manière unidirectionnelle et la signalisation se limitera aux tonalités DTMF.

La signalisation unidirectionnelle permet aux utilisateurs TPU de s'authentifier vis-à-vis du réseau. Elle ne leur permet pas d'authentifier le réseau. Elle impose également des limites aux mécanismes d'authentification.

Choix du type d'authentification

Deux types d'authentification avec signalisation DTMF basée sur l'accès utilisateur sont possibles: l'authentification unidirectionnelle avec un numéro PIN fixe ou l'authentification unidirectionnelle avec un code d'authentification variable. La deuxième méthode est préférable si l'utilisateur TPU a besoin d'une authentification plus forte.

Clé d'authentification

Une clé d'authentification est une identité fournie à un utilisateur et servant dans un processus d'authentification. Elle se présente en général sous la forme d'un nombre spécifié de chiffres ou de bits.

Une clé d'authentification est en général une information longue stockée dans le matériel et utilisée en entrée pour une fonction cryptographique.

Fonctionnalités d'authentification unidirectionnelle avec un numéro PIN

a) il s'agit d'une authentification faible;

b) le numéro TPU ne doit pas être modifié, même si le fournisseur peut établir que son numéro PIN a été divulgué à des utilisateurs non autorisés. L'utilisation de l'identité PUI peut fournir une solution;

c) l'équipement doit contenir une identité PUI secrète afin de permettre une utilisation conviviale;

d) un utilisateur TPU émet son numéro PIN à destination du fournisseur du service;

e) l'identité PUI et le numéro PIN sont comparés avec les valeurs correspondantes stockées par le fournisseur du service;

f) l'accès échoue s'il n'y a pas concordance;

g) un compteur du nombre de tentatives d'authentification infructueuses est nécessaire pour protéger le numéro PIN contre une utilisation frauduleuse;

h) l'identité PUI est bloquée lorsque le compteur atteint une valeur maximale;

i) un numéro PIN spécial est nécessaire pour le déblocage en raison de la possibilité d'un blocage malveillant d'une identité PUI. L'utilisateur dont l'identité PUI est bloquée subira néanmoins une gêne importante.

Fonctionnalités d'authentification unidirectionnelle avec codes d'authentification variables

a) il s'agit d'une authentification forte;

b) l'identité PUI secrète n'est absolument pas nécessaire, car il est très difficile de découvrir la clé d'authentification et l'algorithme d'une personne. L'utilisation de l'identité PUI peut être optionnelle;

c) l'équipement émet vers le réseau un code d'authentification variable et des informations de synchronisation (par exemple, une indication de temps ou un numéro de série).

NOTE – Il est également possible d'utiliser plusieurs codes d'authentification variables.

d) l'équipement et le fournisseur du service disposent d'une clé d'utilisateur et d'un algorithme;

e) le fournisseur du service calcule le code d'authentification variable au moyen d'une clé d'utilisateur, d'un algorithme et des informations de synchronisation fournies par l'utilisateur;

f) l'authentification peut être valable pour une certaine période de temps;

g) le code d'authentification variable calculé est comparé à celui qui a été émis par l'utilisateur;

h) l'authentification échoue s'il n'y a pas concordance;

i) il est possible de ne pas utiliser de compteur du nombre de tentatives d'authentification infructueuses et de valeur maximale correspondante. Dans ce cas, il n'y a pas de limite pour le nombre de telles tentatives;

j) le numéro TPU ne doit pas être bloqué, même si la clé et l'algorithme ont été divulgués;

k) la clé de l'utilisateur doit être modifiée lorsque la clé et l'algorithme ont été divulgués;

l) l'équipement exige que l'utilisateur TPU s'identifie vis-à-vis de l'équipement pour interdire un emploi frauduleux par des utilisateurs non autorisés. Ceci peut se faire, par exemple, au moyen d'un numéro PIN local. L'authentification de l'utilisateur vis-à-vis de l'équipement est un problème local d'implémentation. Le numéro PIN est disponible uniquement pour l'interface entre l'utilisateur et l'équipement TPU. L'entrée du numéro PIN sur l'équipement peut être une fonction optionnelle pour des raisons de facilité d'utilisation;

m) l'équipement utilise un protocole de communication normalisé pour transmettre des données d'authentification et de commande à destination du fournisseur du service TPU local (par exemple, sur un canal vocal).

Authentification supplémentaire faible pour des appels de départ effectués après une immatriculation pour les appels de départ

a) cette authentification optionnelle peut être utilisée pour chaque appel de départ lorsqu'une immatriculation pour les appels de départ est activée, en plus de l'authentification normale faite au moment de l'immatriculation;

b) chaque utilisateur se voit attribuer un numéro OCPIN spécial dont la valeur sera différente de celle du numéro PIN si l'utilisateur est autorisé à employer une authentification faible;

c) l'utilisateur émet son numéro OCPIN chaque fois qu'il souhaite établir un appel à partir du terminal sur lequel il est immatriculé. Le numéro OCPIN peut être stocké dans l'équipement pour en faciliter l'utilisation;

d) la valeur du numéro OCPIN est vérifiée par le réseau et l'utilisateur sera autorisé à continuer si cette valeur est correcte.

Authentification supplémentaire faible pour la réponse sécurisée à des appels TPU arrivée – Spécifiée par l'appelé

a) cette authentification est faite pour une réponse sécurisée à des appels arrivée – spécifiée par l'appelé, dans le cas d'un accès DTMF lorsque l'utilisateur ne peut pas employer son équipement TPU. Il s'agit d'une option du fournisseur du service permettant de donner à l'utilisateur le choix d'employer, soit uniquement l'authentification forte, soit l'authentification forte complétée par cette fonctionnalité;

b) chaque utilisateur peut recevoir l'attribution d'un numéro SAPIN au moment de la souscription de l'abonnement. La valeur du numéro SAPIN doit être différente de celle du numéro PIN si l'utilisateur est autorisé à employer l'authentification faible;

c) l'utilisateur doit s'authentifier lors de la réception de chaque appel au moyen du terminal sur lequel il s'est enregistré;

d) l'utilisateur émet son numéro SAPIN. Ce numéro peut être stocké dans l'équipement pour en faciliter l'utilisation;

e) le réseau vérifie la valeur du numéro SAPIN et fait aboutir l'appel si cette valeur est correcte.

10.2.3.2 Accès utilisateur basé sur la signalisation DSS1 hors bande

Limitations

La fonctionnalité d'accès utilisateur hors bande, basée par exemple sur la signalisation DSS1, sera disponible pour les télécommunications TPU basées sur l'ensemble CS-2 du RI ou sur un ensemble ultérieur. Ceci permettra de réduire les limitations imposées aux réseaux et aux terminaux. L'utilisation de cet accès permet d'employer divers types d'authentification, par exemple l'authentification unidirectionnelle, l'authentification bidirectionnelle avec un mode avec mise à l'épreuve et réponse, l'authentification mutuelle, etc. Il sera également possible d'utiliser divers types d'équipement TPU décrits au 10.2.2. Il convient d'appliquer dans ce cas une authentification forte utilisant un équipement intelligent.

Choix du type d'authentification

Le RNIS offre une fonctionnalité de signalisation bidirectionnelle qui permet une mise en œuvre facile de mécanismes d'authentification bidirectionnelle. Il permet également une authentification mutuelle, c'est-à-dire la possibilité d'authentification des utilisateurs vis-à-vis du fournisseur du service TPU et de l'authentification de ce dernier vis-à-vis des utilisateurs.

Clé d'authentification

Une clé d'authentification est une identité fournie à un utilisateur et employée dans un processus d'authentification. Il s'agit en général d'un nombre spécifié de bits ou de chiffres.

Une clé d'authentification est en général une information longue qui est utilisée en entrée pour une fonction cryptographique.

Fonctionnalités d'authentification avec mise à l'épreuve et réponse

a) il s'agit d'une authentification forte;

b) le fournisseur du service envoie un numéro aléatoire à l'équipement;

c) l'équipement utilise une clé d'authentification et le nombre aléatoire pour calculer le code d'authentification variable qui est ensuite émis à destination du fournisseur du service;

d) l'équipement et le fournisseur du service disposent d'une clé d'utilisateur et d'un algorithme;

e) le fournisseur du service calcule le code d'authentification variable au moyen de la clé de l'utilisateur et de l'algorithme;

f) le code d'authentification variable calculé est comparé à celui qui a été émis par l'utilisateur;

g) l'authentification échoue s'il n'y a pas concordance;

h) il est possible de ne pas utiliser de compteur du nombre de tentatives d'authentification infructueuses et de valeur maximale correspondante;

i) le numéro TPU ne doit pas être bloqué, même si la clé a été divulguée. Une autre clé et un autre algorithme sont fournis à l'utilisateur;

j) le type d'authentification avec mise à l'épreuve et réponse nécessite l'emploi d'un équipement intelligent;

k) l'équipement exige que l'utilisateur TPU s'identifie vis-à-vis de l'équipement pour interdire un emploi frauduleux par des utilisateurs non autorisés. Ceci peut se faire, par exemple, au moyen d'un numéro PIN local. L'authentification de l'utilisateur vis-à-vis de l'équipement est un problème local d'implémentation. Le numéro PIN est disponible uniquement pour l'interface entre l'utilisateur et l'équipement TPU. L'entrée du numéro PIN sur l'équipement peut être une fonction optionnelle pour des raisons de facilité d'utilisation;

l) l'équipement utilise un protocole normalisé avec mise à l'épreuve et réponse sur le canal D du RNIS.

10.3 Mécanismes de gestion de la sécurité

Il est nécessaire de détecter le plus tôt possible des menaces visant tout participant impliqué dans les télécommunications TPU et de prendre des mesures adéquates. Les mécanismes de sécurité mentionnés précédemment seront pris en charge à cet effet par un processus de suivi d'audit de sécurité et de traitement d'événement. Le contrôle de la taxation est une mesure permettant de limiter les dommages potentiels à un montant acceptable. La gestion des informations fournit à l'utilisateur la possibilité de prendre connaissance des événements pertinents pour la sécurité.

10.3.1 Suivi d'audit de sécurité

Le suivi d'audit de sécurité a pour fonction de détecter les menaces intrinsèques contre la sécurité, par exemple les accès non autorisés à des données système ou utilisateur et des modifications non autorisées de droits d'accès.

Le système peut contenir des composants d'audit qui enregistrent les données suivantes dans un journal d'événements:

a) utilisation du mécanisme d'identification et d'authentification (date, heure, identité de l'utilisateur, identité de la ligne appelante ou numéro de code de la zone d'origine, chiffres numérotés, réussite ou échec de la tentative, nombre de mises à jour de synchronisation);

b) tentatives d'accès au profil de service (date, heure, identité de l'utilisateur, nom de l'objet, type de tentative d'accès, réussite ou échec de la tentative);

c) actions effectuées par les fournisseurs de services TPU et les exploitants de réseau (date, heure, identité de l'utilisateur, type d'action, nom de l'objet lié à l'action; on peut citer les exemples suivants: introduction, suppression ou suspension d'utilisateur, montage ou démontage de média de stockage, démarrage ou arrêt du système).

Les mécanismes permettant de générer, de gérer et d'analyser un suivi d'audit sont en dehors du domaine d'application de la présente Recommandation. Ils sont propres au système et peuvent être pris en charge par les mécanismes de sécurité du RGT.

10.3.2 Actions de traitement d'événements

Des actions adéquates seront effectuées, en fonction de l'analyse (en ligne ou en temps différé) des données d'audit, en vue d'imposer la politique de sécurité. Les actions suivantes sont possibles:

a) alarme fournie à l'administrateur de sécurité;

b) blocage de l'accès de l'utilisateur au système;

c) interruption d'un appel (par exemple, dans le cas d'appels internationaux particulièrement longs).

Les mécanismes permettant le traitement des événements sont en dehors du domaine d'application de la présente Recommandation. Ils sont propres au système et peuvent être pris en charge par les mécanismes de sécurité du RGT.

10.3.3 Contrôle de la taxation

La gestion de la taxation doit prendre de grandes précautions pour le traitement de la sécurité. Les données personnelles et de taxation doivent être stockées, traitées et transmises d'une manière garantissant le respect de la vie privée de l'utilisateur et l'intégrité des données.

L'analyse des menaces a mis en évidence un grand nombre de problèmes et de menaces relatifs à la taxation et à la facturation. Il est possible de prévenir ces menaces, ou au moins de réduire la possibilité de leur apparition, par l'utilisation de l'authentification complétée par des mécanismes de contrôle d'accès et des procédures de gestion. Toutefois, compte tenu avant tout de problèmes d'acceptation, il peut être nécessaire de protéger les utilisateurs vis-à-vis d'un montant de facturation inattendu. La limitation du montant des factures est recommandée, en particulier dans le cas d'utilisation d'une authentification faible.

10.3.4 Gestion des informations

Il est nécessaire de disposer d'une fonctionnalité permettant d'informer les utilisateurs TPU, les abonnés TPU et d'autres participants au sujet d'actions qui affectent le respect de leur vie privée, la sécurité et la taxation. Ces informations doivent être fournies dans la mesure du possible en ligne par des annonces (parlées ou par affichage) ou par des tonalités spéciales de numérotation. La spécification des informations fournies aux participants impliqués est de la responsabilité du fournisseur du service. Le contenu de ces informations est en dehors du domaine d'application de la présente Recommandation.

Les fournisseurs de services TPU éviteront avec soin de fournir trop d'informations. Des assaillants potentiels ne doivent pas pouvoir faire un mauvais usage de telles informations pour leurs attaques. Le contenu des informations et des annonces sera en outre choisi avec soin pour ne pas affecter le respect de la vie privée des utilisateurs TPU et d'autres participants.

Un utilisateur TPU sera informé des risques présentés par les fonctionnalités et les services complémentaires TPU et des moyens permettant de les minimiser.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
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	Transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, de télégraphie, de télécopie, circuits téléphoniques et circuits loués internationaux
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
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 et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information et protocole Internet
Série Z	Langages et aspects informatiques généraux des systèmes de télécommunication

Genève, 2001