UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T E.113

(05/97)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE E: EXPLOITATION GÉNÉRALE DU RÉSEAU, SERVICE TÉLÉPHONIQUE, EXPLOITATION DES SERVICES ET FACTEURS HUMAINS

Exploitation, numérotage, acheminement et service mobile – Exploitation des relations internationales – Dispositions de caractère général concernant les Administrations

---

Procédures de validation pour le service des cartes internationales de facturation des télécommunications

Recommandation UIT-T E.113

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE E

EXPLOITATION GÉNÉRALE DU RÉSEAU, SERVICE TÉLÉPHONIQUE, EXPLOITATION DES SERVICES ET FACTEURS HUMAINS

EXPLOITATION, NUMÉROTAGE, ACHEMINEMENT ET SERVICE MOBILE	
EXPLOITATION DES RELATIONS INTERNATIONALES	E.100–E.229
Définitions	E.100–E.103
Dispositions de caractère général concernant les Administrations	**E.104–E.119**
Dispositions de caractère général concernant les usagers	E.120–E.139
Exploitation des relations téléphoniques internationales	E.140–E.159
Plan de numérotage du service téléphonique international	E.160–E.169
Plan d'acheminement international	E.170–E.179
Tonalités utilisées dans les systèmes nationaux de signalisation	E.180–E.199
Service mobile maritime et service mobile terrestre public	E.200–E.229
DISPOSITIONS OPÉRATIONNELLES RELATIVES À LA TAXATION ET À LA COMPTABILITÉ DANS LE SERVICE TÉLÉPHONIQUE INTERNATIONAL	E.230–E.299
Taxation dans les relations téléphoniques internationales	E.230–E.249
Procédures de rémunération des moyens mis à disposition entre Administrations	E.250–E.259
Mesure et enregistrement des durées de conversation aux fins de la comptabilité	E.260–E.269
Etablissement et échange des comptes internationaux	E.270–E.299
UTILISATION DU RÉSEAU TÉLÉPHONIQUE INTERNATIONAL POUR LES APPLICATIONS NON TÉLÉPHONIQUES	E.300–E.329
Généralités	E.300–E.319
Phototélégraphie	E.320–E.329
DISPOSITIONS DU RNIS CONCERNANT LES USAGERS	E.330–E.399
QUALITÉ DE SERVICE, GESTION DE RÉSEAU ET INGÉNIERIE DU TRAFIC	
GESTION DE RÉSEAU	E.400–E.489
INGÉNIERIE DU TRAFIC	E.490–E.799
QUALITÉ DE SERVICE: CONCEPTS, MODÈLES, OBJECTIFS, PLANIFICATION DE LA SÛRETÉ DE FONCTIONNEMENT	E.800–E.899

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

RECOMMANDATION UIT-T E.113

PROCÉDURES DE VALIDATION POUR LE SERVICE DES CARTES INTERNATIONALES DE FACTURATION DES TÉLÉCOMMUNICATIONS

Résumé

L'utilisation croissante et l'augmentation du nombre des cartes de facturation ont amené les entités émettrices de cartes (ou leurs agents agréés) à prendre des dispositions en vue d'empêcher toute utilisation frauduleuse.

Pour offrir un tel service, il est donc essentiel d'uniformiser les procédures de validation et d'autorisation d'utilisation de ces cartes. L'objet de la présente Recommandation est de définir les procédures de validation entre Administrations. Il ne s'agit pas de spécifier des équipements, les fonctionnalités, ou des techniques de transmission de données associés à ces procédures.

Source

La Recommandation UIT-T E.113, révisée par la Commission d'études 1 de l'UIT-T (1997-2000), a été approuvée le 26 mai 1997 selon la procédure définie dans la Résolution n° 1 de la CMNT.

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'études 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 n° 1 de la CMNT.

Dans certains secteurs de la technologie 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 avait/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

Introduction

La mise en place du service des cartes internationales de facturation des télécommunications défini dans la Recommandation E.116 se poursuit.

L'utilisation croissante et l'augmentation du nombre des cartes de facturation ont amené les entités émettrices de cartes (ou leurs agents agréés) à prendre des dispositions en vue d'empêcher toute utilisation frauduleuse.

Pour offrir un tel service, il est donc essentiel d'uniformiser les procédures de validation et d'autorisation d'utilisation de ces cartes. L'objet de la présente Recommandation est de définir les procédures de validation entre Administrations. Il ne s'agit pas de spécifier des équipements, les installations, ou des techniques de transmission de données associés à ces procédures.

Il faut tenir compte du fait que les procédures de validation des cartes de facturation des télécommunications entre les Administrations varieront en fonction de facteurs tels que les possibilités des systèmes à cartes, les accords bilatéraux et la manière dont la carte est présentée. Il convient d'assurer la souplesse de ce processus pour obtenir une participation maximale des Administrations dans les cas où des interfaces automatisées n'existeraient pas ou ne seraient pas uniformément disponibles. Lorsque de telles interfaces automatisées existent, une implémentation uniforme bien définie est souhaitable.

Recommandation E.113[1]

PROCÉDURES DE VALIDATION POUR LE SERVICE DES CARTES INTERNATIONALES DE FACTURATION DES TÉLÉCOMMUNICATIONS

(Melbourne, 1988; révisée en 1993 et 1997)

1 Méthodes de validation

Pour contrôler la validité d'une carte de facturation, il existe plusieurs méthodes qui se répartissent en deux grandes catégories: la validation complète et la validation limitée.

La validation complète consiste à contrôler le numéro de la carte par comparaison avec les informations se trouvant dans la base de données de l'entité émettrice, et à établir une communication en temps réel entre l'entité acceptante de la carte et l'entité émettrice. La validation complète, plus exhaustive que les autres méthodes, est faisable avec les systèmes de cartes de facturation automatisés ou semi-automatisés.

La validation limitée fait intervenir une ou plusieurs techniques, telles qu'un caractère spécial, un code ou un contrôle par rapport aux informations d'une base de données partielle, ces techniques étant déterminées par l'entité émettrice et spécifiées dans un accord d'exploitation. Les méthodes de validation limitée minimisent les communications entre les Administrations.

2 Procédures de validation complète

2.1 Flux d'informations de validation

Les informations fournies par la carte ou l'utilisateur sont introduites dans un terminal ayant accès au système de cartes de facturation des télécommunications d'une Administration donnée. Ce système doit ensuite communiquer avec l'entité émettrice pour valider la carte et en autoriser l'utilisation.

Le flux d'informations de validation comporte trois messages:

– demande d'autorisation;

– réponse à la demande d'autorisation;

– description de communication.

La demande d'autorisation est un message de l'entité acceptante vers l'entité émettrice de la carte, fournissant les détails d'une tentative d'utilisation d'une carte de facturation des télécommunications. L'entité émettrice interroge alors ses propres systèmes internes pour trouver la réponse. Elle communique ensuite avec l'entité acceptante pour fournir la réponse positive ou négative à la demande d'autorisation (en précisant dans ce cas le motif du refus). Ce message est défini ici comme la réponse à la demande d'autorisation. L'utilisateur de la carte doit ensuite être informé en retour de la réponse à la tentative d'utilisation, dans la mesure permise par les possibilités du système téléphonique de l'Administration. Sous réserve de l'existence d'accords entre les Administrations et les entités émettrices de cartes, un troisième message dénommé description de communication, sera adressé par l'entité acceptante à l'entité émettrice de la carte, dès l'achèvement d'une communication ou d'une tentative d'appel. Ce message contiendra les informations nécessaires à une évolution plus complète des communications établies par l'usager.

Les sous-paragraphes 2.2 à 2.4 décrivent respectivement les composantes fonctionnelles des messages de *demande d'autorisation*, de *réponse à la demande d'autorisation* et de *description de communication*.

Le Tableau 1 donne un résumé des composantes fonctionnelles en précisant leur caractère obligatoire ou facultatif. L'Annexe A contient des orientations sur la sécurité en cas de validation via le réseau X.25.

---

[1] La présente Recommandation remplace la Recommandation E.113 du *Livre bleu*, Fascicule II.2.

Tableau 1/E.113 – Résumé des composantes d'informations pour la validation (Note 1)

Composantes	Messages		
	Demande d'autorisation	**Réponse à la demande d'autorisation**	**Description de communication (Note 3)**
identificateur de type de message	O	O	O
identificateur de référence de message	O	O	O
numéro de compte primaire	O	F	O
identificateur de l'entité acceptante	O	–	–
date d'expiration	F	–	–
PIN	O (Note 2)	–	–
identificateur de service	F	–	–
numéro de téléphone demandeur	F	–	–
numéro de téléphone demandé	O	–	–
cachet de date et heure	F	–	–
code de réponse	–	O	–
sous-numéro de compte d'usager	–	F	–
indicateur de restriction	–	F	–
numéros spécifiés	–	F	–
code de description de communication	–	–	O
heure de début de la communication	–	–	O
heure de fin de communication	–	–	O
taxation estimée	–	–	F
durée de communication	–	–	F
indication de message de description de communication	–	–	F

O Obligatoire

F Facultatif

NOTE 1 – Les composantes facultatives sont subordonnées à l'existence d'accords entre Administrations.

NOTE 2 – Obligatoire si appliqué par l'émetteur de la carte.

NOTE 3 – L'ensemble de ce message est facultatif et est subordonné à l'existence d'accords entre Administrations (voir 2.4).

2.2 Demande d'autorisation

Les composantes de base d'une demande adressée par l'entité acceptante à l'entité émettrice de la carte pour valider une carte de facturation et en autoriser l'utilisation sont les suivantes.

2.2.1 Identificateur de type de message (obligatoire)

Un identificateur de type de message doit être inclus dans ce message. Il est fourni à l'entité émettrice de la carte par l'entité acceptante pour indiquer qu'il s'agit d'une demande d'autorisation.

2.2.2 Identificateur de référence de message (obligatoire)

Un identificateur de référence de message doit être inclus dans le message. Son but est de lier sans ambiguïté ce message à une transaction de validation particulière.

2.2.3 Numéro de compte primaire (obligatoire)

Le numéro de compte primaire de la carte (19 caractères visibles au maximum) défini dans la Recommandation E.118 doit être inclus dans le message, tel qu'il est fourni par la carte ou par l'usager. Faisant partie du numéro de compte primaire, le numéro d'identification de l'entité émettrice de la carte peut être utilisé par l'entité acceptante pour identifier la carte et diriger la demande d'autorisation vers la base de données concernée.

2.2.4 Identificateur d'émetteur de carte de l'entité acceptante (obligatoire)

L'identificateur de l'entité acceptante doit être inclus dans ce message; il peut être utilisé par l'entité émettrice de la carte pour identifier l'Administration qui accepte la carte de télécommunication. L'identificateur de l'entité acceptante doit contenir le numéro d'identification d'émetteur de carte de l'entité acceptante.

2.2.5 Date d'expiration (facultatif)

La date d'expiration de la carte, si elle est spécifiée, peut être incluse dans ce message. L'inclusion de cette information ne dispense pas l'Administration d'origine de s'assurer, dans les limites des possibilités de son système local de cartes de facturation, que la validité de la carte n'est pas expirée.

2.2.6 Numéro d'identification personnel (obligatoire)

L'utilisation d'un numéro d'identification personnel (PIN, *personal identification number*) est laissée à la discrétion de l'entité émettrice de la carte. Cette dernière peut utiliser cette information pour authentifier l'utilisateur et, le cas échéant, autoriser l'utilisation de la carte. S'il existe, le numéro d'identification personnel doit être inclus dans ce message et, de préférence, sous forme codée. Pour les émetteurs de cartes de télécommunication, il est recommandé de limiter la longueur du PIN à 6 chiffres; pour les cartes d'autres domaines d'activités, les PIN pourront être plus longs.

2.2.7 Identificateur du service (facultatif)

Une indication du service pour lequel l'utilisateur va être débité sur sa carte de facturation doit figurer dans le message; elle permettra à l'entité émettrice de tenir compte de toute restriction de service apportée à l'utilisation de la carte. Cet identificateur doit préciser le service support et les éventuels services complémentaires demandés.

2.2.8 Numéro de téléphone demandeur (facultatif)

Le numéro de téléphone international demandeur complet devrait, dans les cas où il est connu, être inclus dans ce message. Eventuellement, l'indicatif de pays de l'UIT peut être fourni dans les cas où le numéro de téléphone demandeur n'est pas connu. L'utilisation de cette information est subordonnée à l'existence d'accords entre les Administrations. Cette information est nécessaire à certaines Administrations pour contrôler les restrictions d'utilisation de certaines cartes ainsi qu'aux entités émettrices de cartes pour s'assurer qu'il existe des accords de facturation, de prélèvement des taxes et de solde de compte pour la communication demandée. Elle est également utilisée dans la détection des fraudes.

2.2.9 Numéro de téléphone demandé (obligatoire)

Le numéro de téléphone international demandé complet devrait être inclus dans ce message. L'utilisation de cette information est subordonnée à l'existence d'accords entre les Administrations. Cette information est nécessaire à certaines Administrations pour contrôler les restrictions d'utilisation de certaines cartes ainsi qu'aux entités émettrices de cartes pour s'assurer qu'il existe des accords de facturation, de prélèvement des taxes et de solde de compte pour la communication demandée. Elle est également utilisée dans la détection des fraudes.

2.2.10 Cachet de date et heure (facultatif)

Un cachet de date et heure devrait être inclus dans ce message. L'information indiquera le mois, le jour, l'heure, la minute et la seconde en temps universel coordonné (UTC, *coordinated universal time*) où la *demande d'autorisation* a été introduite dans le système.

2.3 Réponse à la demande d'autorisation

Les composantes de base de la réponse de l'entité émettrice de la carte à *une demande d'autorisation* sont les suivantes.

2.3.1 Identificateur de type de message (obligatoire)

Un identificateur de type de message doit être inclus dans ce message. Il est fourni par l'entité émettrice de la carte pour indiquer à l'entité acceptante qu'il s'agit d'une réponse à une demande d'autorisation.

2.3.2 Identificateur de référence de message (obligatoire)

Un identificateur de référence de message doit être inclus dans ce message. Son but est de lier sans ambiguïté ce message à une transaction de validation particulière.

2.3.3 Numéro de compte primaire (facultatif)

Le numéro de compte primaire, décrit en 2.2.3, devrait être inclus dans ce message. Il est fourni pour s'assurer du lien entre *la demande d'autorisation* et *la réponse à la demande d'autorisation*.

2.3.4 Code de réponse (obligatoire)

Le code de réponse doit être inclus dans ce message pour indiquer la suite donnée à *la demande d'autorisation*. Les définitions spécifiques et les codes correspondants nécessitent un complément d'étude. Les réponses possibles pourraient inclure:

– service approuvé;

– service limité approuvé: voir 2.3.6 et 2.3.7;

– service refusé: pour dépassement du seuil de crédit ou pour non-paiement;

– service refusé: non validité du numéro de compte ou de la combinaison numéro de compte/PIN;

– service refusé: PIN incorrect (des tentatives ultérieures de nouvelle présentation peuvent être autorisées);

– service refusé: dépassement du nombre admissible de tentatives de présentation du PIN (chaque entité émettrice de cartes peut fixer une limite, par exemple, 3 tentatives);

– service refusé: carte périmée;

– service refusé: restrictions de service pour le numéro de compte ou la combinaison numéro de compte/PIN;

– service refusé: service non autorisé pour le numéro de compte considéré;

– service refusé: communication non autorisée à partir du poste considéré (c'est-à-dire pas d'accord entre l'entité émettrice de la carte et l'entité acceptante);

– service refusé: indisponibilité de la base de données de validation de l'entité émettrice de la carte;

– service refusé: tentative de validation effectuée auprès d'une entité autre que l'entité émettrice de la carte;

– erreur dans le format de message (message mutilé);

– traitement impossible du message en raison de l'absence ou de l'insuffisance des informations.

L'utilisation des codes de réponse particuliers et la suite qui y est donnée sont subordonnées aux accords conclus entre les Administrations concernées. Pour certaines des réponses ci-dessus, il convient de fixer des seuils distincts pour le nombre de renouvellement des tentatives.

L'information fournie en retour à l'utilisateur de la carte ne doit pas permettre à un utilisateur frauduleux d'effectuer des tentatives ultérieures d'utilisation non autorisée de la carte de facturation.

2.3.5 Sous-numéro de compte de l'usager (facultatif)

Le sous-numéro de compte de l'usager est utilisé pour permettre au titulaire de la carte de contrôler les dépenses de télécommunication lorsque plusieurs numéros PIN sont associés à un même numéro de compte primaire. L'utilisation de cette composante est subordonnée à l'existence d'accords entre les Administrations, et cette information est normalement enregistrée pour être incluse ultérieurement dans le relevé de facturation afin que l'usager facturé puisse ventiler correctement ces dépenses.

2.3.6 Indicateur de restriction (facultatif)

L'indicateur de restriction informe l'entité acceptante que la carte présentée est soumise à restriction, et indique la nature de la restriction. L'utilisation de cette composante est subordonnée à l'existence d'accords entre Administrations et peut compléter le code de réponse décrit ci-dessus pour le contrôle des cartes à restriction.

2.3.7 Numéros spécifiés (facultatif)

Certains titulaires de carte peuvent être soumis à la restriction de ne pouvoir appeler qu'un ou plusieurs numéros déterminés. Si le numéro appelé n'est pas associé au numéro de compte de la carte, cette composante permettra de transmettre ces numéros à l'entité acceptante. L'utilisation de cette composante est subordonnée à l'existence d'accords entre Administrations et peut compléter le code de réponse décrit ci-dessus pour le contrôle des cartes à restriction.

2.4 Description de communication (facultatif)

Les sous-paragraphes suivants décrivent les principales composantes d'un message de l'entité acceptante à l'entité émettrice de la carte destiné à contrôler l'utilisation de la carte au regard de la limite de crédit de l'usager et de rassembler d'autres statistiques utiles aux besoins de l'exploitation.

Ce message supplémentaire a pour but premier de mieux contrôler en temps voulu l'utilisation frauduleuse possible de la carte de facturation. Il n'est pas censé remplacer les mécanismes de facturation et de règlement qui pourraient être établis par d'autres Recommandations.

2.4.1 Identificateur de type de message (obligatoire)

Un identificateur de type de message doit être inclus dans ce message. Il est fourni par l'entité acceptante pour indiquer à l'entité émettrice de la carte qu'il s'agit d'un message de description de communication.

2.4.2 Identificateur de référence de message (obligatoire)

Un identificateur de référence de message doit être inclus dans ce message. Son but est de lier sans ambiguïté ce message à une transaction de validation particulière.

2.4.3 Numéro de compte primaire (obligatoire)

Le numéro de compte primaire décrit en 2.2.3 doit être inclus dans ce message. Il est fourni pour s'assurer du lien entre *la demande d'autorisation* et *la description de la communication*.

2.4.4 Code de description de communication (obligatoire)

Le code de description de la communication doit être inclus dans le message POUR INDIQUER SI la communication A ou N'A PAS abouti ET COMMENT.

– appel automatique à destination de l'Administration émettrice de la carte;

– appel de poste par opératrice, à destination de l'Administration émettrice de la carte;

– communication avec préavis par opératrice à destination de l'Administration émettrice de la carte;

– appel automatique à destination d'un pays tiers;

– appel de poste par opératrice à destination d'un pays tiers;

– communication avec préavis par opératrice à destination d'un pays tiers;

– appel automatique à l'intérieur du pays de l'entité acceptante;

– appel de poste par opératrice à l'intérieur du pays de l'entité acceptante;

– communication avec préavis par opératrice à l'intérieur du pays de l'entité acceptante;

– non taxable;

– libre appel;

– taxes fixes, par exemple taxes afférentes au service de renseignements;

– ad hoc (acheminement par des fonctionnalités autres que celles de l'émetteur de la carte).

2.4.5 Heure de début de communication (obligatoire)

La date et l'heure de début de la communication doivent être incluses dans ce message. Si le code de description indique que l'appel n'a pas abouti, cet élément d'information doit indiquer la date et l'heure de l'échec en précisant le mois, le jour, l'heure et la minute, en temps universel coordonné (UTC).

2.4.6 Heure de fin de communication (obligatoire)

La date et l'heure de fin de communication doivent être incluses dans le message. Cet élément d'information doit préciser le mois, le jour, l'heure et la minute en UTC. Ce paramètre peut être omis si le 2.4.7 figure dans le message.

2.4.7 Durée de communication (facultatif)

La durée de la communication, en minutes, doit être incluse dans ce message. Ce paramètre peut être omis si le 2.4.6 y figure.

2.4.8 Taxation estimée (facultatif)

La taxation estimée doit être incluse dans ce message. La taxe doit être calculée en DTS (droits de tirage spéciaux).

2.4.9 Indicateur de message de description de communication (facultatif)

Ce champ indique si le message de description est envoyé en fin de communication ou périodiquement au cours de celle-ci.

3 Procédures de validation limitée

Les informations contenues dans la carte sont communiquées par son titulaire à une opératrice. Les informations additionnelles définies par l'entité émettrice sont également communiquées pour valider, de manière limitée, le numéro de carte. Par une série d'opérations définie par l'entité émettrice, l'opératrice procède à la validation. Dans la mesure du possible, les Administrations sont invitées à automatiser les opérations au niveau de la table d'opératrice ou en utilisant un dispositif additionnel. Les procédures à suivre doivent rester suffisamment simples pour éviter qu'il soit absolument nécessaire de les automatiser si on veut les appliquer.

3.1 Types de procédures de validation limitée

On distingue plusieurs types de procédures de validation limitée qui peuvent être employés indépendamment ou conjointement. Si la validation positive n'est pas utilisée, il est fortement recommandé de procéder à une vérification par rapport à un fichier de cartes interdites ou une liste noire. En cas d'impossibilité, il faut utiliser au minimum une des procédures de validation suivantes:

a) vérification de la correspondance entre les chiffres "X" et "Y" du numéro de carte;

b) vérification de la correspondance entre les chiffres "X" du numéro de carte et les chiffres "Y" du numéro d'identification personnel (PIN) ou autre information d'identification personnelle ("code d'autorisation" par exemple) qui fait intervenir un moyen de contrôle et de validation;

c) vérification du chiffre de contrôle de parité au moyen de la formule de Luhn ou d'un autre algorithme. Il faut préciser que la vérification du chiffre de contrôle de parité n'est pas l'unique moyen d'effectuer une validation limitée; l'algorithme est suffisamment compliqué pour nécessiter un calcul automatique du chiffre;

3.2 Localisation des informations d'identification personnelle

Il n'est pas nécessaire que les informations d'identification personnelle se trouvent sur la carte. Lorsque ces informations se trouvent sur la carte, elles doivent clairement être identifiées par l'utilisateur par un terme comme "code d'autorisation". Elles peuvent comporter un ou plusieurs caractères (lettres ou chiffres). L'utilisateur devra fournir les informations d'identification personnelle lorsque l'opératrice les lui demandera.

Annexe A

Sécurité au cours de la validation via le réseau X.25

A.1 Certaines entités émettrices de cartes font la validation via le réseau X.25. La présente annexe contient un examen des risques associés à cette méthode ainsi que des mesures de protection.

En général, la validation est effectuée par l'envoi de la demande à une ou plusieurs bases de données de validation. Cette demande comportera généralement au minimum le numéro de compte primaire (PAN, *primary account number*), le numéro d'identification personnel (PIN) et le numéro de destination. La ou les bases de données contrôlent le numéro PAN et son format ainsi que le numéro PIN. Elles vérifient généralement le numéro de destination par rapport à une liste de numéros permis (tant pour le client que pour le service). Si tous les contrôles sont positifs, la base de données de validation renvoie une réponse positive. Dans le cas contraire, elle renvoie généralement un code d'erreur indiquant la nature du défaut.

Le réseau de validation est exposé aux risques résultant:

- d'une modification – une réponse de validation peut être modifiée dans le but de produire une réponse positive qui permettrait qu'une communication interdite ne soit établie;
- d'un défaut de confidentialité – les demandes de validation pourraient être surveillées dans le but de déterminer les numéros PAN et PIN; ces numéros valables pourraient être utilisés pour établir les communications non autorisées;
- d'un refus d'accès – l'accès à la base de données de validation pourrait être refusé, faisant échouer les demandes. Cela permettrait de faire des appels non autorisés au cas où le service fonctionnerait moyennant une validation limitée. Il serait également possible de dépasser un seuil préétabli sans déclencher d'alarme (cela dépendrait du mode de fonctionnement du service).

Pour être protégé contre ces risques, le processus de validation doit satisfaire aux conditions suivantes:

- il doit être impossible de lire une demande de validation sans y être autorisé;
- il doit être impossible de modifier une demande de validation, ou sa réponse, sans que cela ne soit détecté;
- il doit être impossible d'envahir le réseau avec des messages à partir d'une adresse d'utilisateur du réseau (NUA, *network user address*) qui est extérieure au groupe de bases de données de validation.

Certaines mesures peuvent être prises pour répondre aux conditions ci-dessus.

- *Groupe fermé d'utilisateurs (CUG, closed user group*)

  Le CUG permet à un nombre d'éléments prédéterminé de communiquer sur un réseau sans donner accès à d'autres parties. Le CUG est un moyen relativement simple et suffisamment efficace de limiter l'accès et peut minimiser les possibilités d'envahissement du réseau depuis l'extérieur du groupe. Le CUG ne protège aucunement les données contre les indiscrétions ou les modifications.

- *Chiffrement*

  Le chiffrement contribue à la protection contre les indiscrétions et dans une certaine mesure contre les modifications. Il serait très difficile de modifier des données chiffrées sans que cela ne soit détecté au déchiffrement.

- *Authentification*

  L'authentification permettrait de détecter les modifications dans les demandes et les réponses de validation et effectuerait une vérification de l'identité de l'expéditeur.

A.2 Recommandations

Comme la vulnérabilité la plus grande se situe au niveau des indiscrétions, il est recommandé de chiffrer les demandes de validation. Le chiffrement des réponses est également utile au niveau de la protection contre les modifications. La réponse de validation doit être enchaînée à quelques données aléatoires. Si la réponse de validation est très courte et que sa variabilité est très limitée (c'est-à-dire "1 ou 0"), le résultat chiffré sera plus facile à prévoir. Le protocole X.25 contribue à détecter les modifications par les totaux de contrôle habituels.

Il n'est pas recommandé d'utiliser l'authentification étant donné qu'elle ne garantit pas réellement une sécurité plus grande.

Si possible, il convient d'établir un groupe fermé d'utilisateurs étant donné que cela contribue à la protection contre les accès extérieurs non autorisés pouvant entraîner la désorganisation du réseau et éventuellement le refus d'accès au service.

Le chiffrement s'applique le mieux au niveau des paquets, c'est-à-dire à la couche Réseau ou à la couche Application. Le chiffrement au niveau des couches du réseau nécessitera des unités de chiffrement X.25 spécialisées. Le chiffrement de la couche Application peut être réalisé soit au niveau du matériel, soit au niveau du logiciel.

Le choix recommandé est le chiffrement au niveau application car il permet:

- de modifier rapidement l'algorithme de chiffrement en cas de soupçons à son sujet;
- de modifier aisément le chiffrement compte tenu des règlements du pays de destination. A titre d'exemple, le chiffrement n'est généralement pas permis en France et aux Etats-Unis, les autorités peuvent exiger que l'algorithme soit simplifié.

Deux types fondamentaux d'algorithmes de chiffrement existent pour les applications de ce type:

- l'algorithme asymétrique (tel que le RSA) où l'on utilise une touche pour chiffrer les données et une touche différente (connue seulement du destinataire réel) pour les déchiffrer;
- l'algorithme symétrique (tel que le DES) nécessitant l'emploi de la même touche pour le chiffrement et le déchiffrement des données. Cette touche ne doit être connue que de l'expéditeur et du destinataire réel.

Si le nombre de parties concernées est faible, l'algorithme symétrique semble le plus approprié. Toutefois, dans l'utilisation internationale des cartes de facturation, beaucoup de parties peuvent entrer en ligne de compte. Un algorithme asymétrique est recommandé, ne serait-ce que pour communiquer les touches à utiliser.

Un organe séparé devrait conserver un répertoire des touches agréées qui serait utilisé en cas de litige et qui permettrait de disposer d'une référence fiable.

A.3 Procédures de sécurité pour la validation

Il est recommandé d'adopter les règles suivantes:

1) utiliser des groupes fermés d'utilisateurs pour limiter l'accès au réseau X.25;
2) faire appel au chiffrement au niveau application;
3) utiliser un algorithme de chiffrement asymétrique pour communiquer les touches à utiliser;
4) limiter éventuellement le chiffrement aux données confidentielles. Les éléments qu'il faut en tout cas chiffrer sont:
   - le numéro PAN;
   - le numéro PIN;
   - le numéro de destination;
   - la réponse "oui" ou "non" du système de validation.

   Pour protéger davantage le caractère confidentiel, il conviendra de chiffrer également le numéro de départ.
5) Si l'on utilise pour le chiffrement des données un algorithme symétrique:
   - les touches doivent être changées toutes les 100 validations;
   - des données pseudo-aléatoires (telles que l'heure en centièmes de seconde) doivent être enchaînées à la réponse de validation.
6) Le chiffrement ne doit pas augmenter de plus de 50 ms chaque demande/réponse de validation.
7) Un organe indépendant unique doit être désigné comme dépositaire du répertoire public des touches. L'organisation ainsi désignée sera le médiateur en cas de différend concernant les touches agréées.

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 pour données et communication entre systèmes ouverts
Série Z	Langages de programmation