UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

T.36

Amendement 1
(04/99)

SÉRIE T: TERMINAUX DES SERVICES TÉLÉMATIQUES

Capacités de sécurité à utiliser avec les télécopieurs du Groupe 3

Amendement 1

Recommandation UIT-T T.36 – Amendement 1

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE T

TERMINAUX DES SERVICES TÉLÉMATIQUES

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

RECOMMANDATION UIT-T T.36

CAPACITÉS DE SÉCURITÉ À UTILISER AVEC LES TÉLÉCOPIEURS DU GROUPE 3

AMENDEMENT 1

Résumé

L'Amendement 1 à la Recommandation T.36 définit le mode d'outrepassement associé au système de chiffrement HKM/HFX.

Source

L'Amendement 1 à la Recommandation UIT-T T.36, élaboré par la Commission d'études 8 (1997-2000) de l'UIT-T, a été approuvé le 1er avril 1999 selon la procédure définie dans la Résolution nº 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 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, le terme *exploitation reconnue (ER)* désigne tout particulier, toute entreprise, toute société ou tout organisme public qui exploite un service de correspondance publique. Les termes *Administration, ER* et *correspondance publique* sont définis dans la *Constitution de l'UIT (Genève, 1992).*

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

CAPACITÉS DE SÉCURITÉ À UTILISER AVEC LES TÉLÉCOPIEURS DU GROUPE 3

AMENDEMENT 1

(Genève, 1999)

1) Sous-paragraphe A.2.2

Modifier comme suit le sous-paragraphe A.2.2:

A.2.2 Fonctions

La gestion de clés est assurée par le système HKM défini à l'Annexe C/T.36. Trois procédures sont spécifiées:

1) le mode d'enregistrement (voir C.4);
2) le mode sécurisé (voir C.5);
3) le mode outrepassement (voir C.7).

L'enregistrement définit des secrets mutuels et garantit la sécurité de toutes les transmissions ultérieures, au cours desquelles le système HKM assure une authentification mutuelle, fournit une clé de session secrète qui garantit la confidentialité et l'intégrité des documents et assure une confirmation de réception ainsi qu'une confirmation ou une réfutation de l'intégrité des documents.

La confidentialité des documents est assurée grâce à un système de chiffrement défini à l'Annexe D/T.36. Ce système utilise une clé de 12 chiffres décimaux équivalant à environ 40 bits.

L'intégrité des documents est assurée au moyen du système spécifié à l'Annexe E/T.36, qui définit l'algorithme de hachage utilisé ainsi que les calculs associés et les échanges d'informations.

2) Nouveau sous-paragraphe C.7

Ajouter le nouveau sous-paragraphe C.7 suivant:

C.7 Mode outrepassement

Le mode outrepassement permet aux opérateurs de télécopieurs de communiquer de manière indépendante et en secret en utilisant deux télécopieurs sécurisés conformes à la Recommandation T.36 sans engager une procédure d'enregistrement entre les deux télécopieurs. Cela est possible si l'on évite de recourir aux procédures de gestion automatiques des clés du mode sécurisé (voir C.5). Aucune primitive mutuelle n'est créée, aucun nombre crypté enregistré n'est extrait et aucune clé de session secrète n'est établie. Au lieu de cela, une clé de session secrète prédéfinie de 12 chiffres, adoptée d'un commun accord, est introduite par l'utilisateur du télécopieur de départ qui, avec un système de chiffrement, assure la confidentialité du document. L'utilisateur du télécopieur de destination introduit la même clé adoptée d'un commun accord qui sert, avec le système de chiffrement, à déchiffrer le document reçu.

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 Y	Infrastructure mondiale de l'information
Série Z	Langages et aspects informatiques généraux des systèmes de télécommunication