Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

M.3016.1

Corrigendum 1

(11/2005)

SÉRIE M: GESTION DES TÉLÉCOMMUNICATIONS Y COMPRIS LE RGT ET MAINTENANCE DES RÉSEAUX

Réseau de gestion des télécommunications

Sécurité pour le plan de gestion: prescriptions de sécurité

Corrigendum 1

Recommandation UIT-T M.3016.1 (2005) – Corrigendum 1

RECOMMANDATIONS UIT-T DE LA SÉRIE M

GESTION DES TÉLÉCOMMUNICATIONS Y COMPRIS LE RGT ET MAINTENANCE DES RÉSEAUX

Introduction et principes généraux de maintenance et organisation de la maintenance	M.10–M.299
Systèmes de transmission internationaux	M.300–M.559
Circuits téléphoniques internationaux	M.560–M.759
Systèmes de signalisation à canal sémaphore	M.760–M.799
Systèmes internationaux de télégraphie et de phototélégraphie	M.800–M.899
Liaisons internationales louées par groupes primaires et secondaires	M.900–M.999
Circuits internationaux loués	M.1000–M.1099
Systèmes et services de télécommunication mobile	M.1100–M.1199
Réseau téléphonique public international	M.1200–M.1299
Systèmes internationaux de transmission de données	M.1300–M.1399
Appellations et échange d'informations	M.1400–M.1999
Réseau de transport international	M.2000–M.2999
Réseau de gestion des télécommunications	**M.3000–M.3599**
Réseaux numériques à intégration de services	M.3600–M.3999
Systèmes de signalisation par canal sémaphore	M.4000–M.4999

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

Recommandation UIT-T M.3016.1

Sécurité pour le plan de gestion: prescriptions de sécurité

Corrigendum 1

Résumé

Le présent corrigendum vise à corriger un certain nombre d'erreurs relevées dans la Rec. UIT-T M.3016.1.

Source

Le Corrigendum 1 de la Recommandation UIT-T M.3016.1 (2005) a été approuvé le 13 novembre 2005 par la Commission d'études 4 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

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.

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

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

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

NOTE

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

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets 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 M.3016.1

Sécurité pour le plan de gestion: prescriptions de sécurité

Corrigendum 1

1) Correction des erreurs

1.1) Paragraphe I.2.2: Sécurité SNMP

Dans la 1ère phrase, remplacer:

... permet:

par:

... permet (entre autres):

Dans le 2e alinéa, remplacer la 5e phrase:

Les versions 1 et 2 du protocole SNMP créent des risques importants en matière de sécurité dans plusieurs réseaux et ne devraient donc être utilisées qu'en dernier recours.

par ce qui suit:

Les versions 1 et 2 du protocole SNMP créent des risques importants en matière de sécurité. De plus, en décembre 2002, l'IETF a conféré aux protocoles SNMPv1 et SNMPv2c le statut HISTORIC ("historique") et les a remplacés par la version 3 du protocole SNMP, qui est une norme Internet (à part entière) (STD 62). Les versions 1 et 2 du protocole SNMP ne devraient donc pas être utilisées.

Dans le 2e alinéa, supprimer la dernière phrase et ses deux tirets (la révision de la Rec. UIT-T Q.812 ayant été publiée en 2004):

La Commission d'études 4 de l'UIT-T envisage l'établissement de deux nouvelles piles de protocoles:

– SNMPv3 ou V2C avec TLS au-dessus du protocole de commande de transmission (sans commande d'accès);
– SNMPv3 avec modèle de sécurité d'utilisateur au-dessus du protocole de datagramme d'utilisateur (pile novatrice).

Dans le 3e alinéa, remplacer les phrases suivantes:

Lorsque le protocole SNMP est mis en œuvre, il est préférable de choisir la version 3. Celle-ci est plus sûre et devrait être utilisée dans tous les nouveaux systèmes car elle assure la protection contre la modification des données, l'usurpation d'identité, le reséquencement des messages et la perte de confidentialité.

par:

La version 3 du protocole SNMP est plus sûre et doit être utilisée dans tous les nouveaux systèmes, car elle assure la protection contre la modification des données, l'usurpation d'identité, le reséquencement des messages et la perte de confidentialité.

Supprimer le 3e tiret sous le 3e alinéa (puisqu'il n'y a PAS de chaîne communautaire pour le protocole SNMPv3, il n'y a pas lieu de mentionner ce point dans la liste des mesures destinées au protocole SNMPv3):

– il convient de ne pas utiliser la chaîne communautaire par défaut;

Remplacer le 5e tiret du 3e alinéa (puisque l'algorithme DES est obsolète et peut à présent facilement être déchiffré; il n'utilise qu'une clé à 56 bits, qui est considérée comme insuffisante à l'heure actuelle):

– par défaut, le protocole SNMPv3 utilise l'algorithme (DES, *data encryption standard*), mais des algorithmes davantage sécurisés peuvent être utilisés;

par:

– par défaut, le protocole SNMPv3 utilise la norme de chiffrement des données (DES, *data encryption standard*), mais des algorithmes plus sûrs DEVRAIENT être utilisés (par exemple la norme de chiffrement évoluée (AES, *advanced encryption standard*) spécifiée dans la norme RFC 3826);

Remplacer le 6e tiret du 3e alinéa:

– le protocole SNMPv3 devrait être utilisé au minimum avec AuthNoPriv, qui assure l'authentification mais pas la confidentialité des transactions, mais de préférence avec AuthPriv;

par:

– le protocole SNMPv3 admet trois niveaux de sécurité: noAuthNoPriv, authNoPriv et authPriv. Il convient d'utiliser le niveau de sécurité approprié, en fonction des objets de la base d'informations de gestion (MIB, *management information base*) auxquels on accède. Les parties relatives aux considérations de sécurité dans les documents MIB devraient être étudiées avec soin avant d'établir des configurations appropriées de commande d'accès dans le modèle de commande d'accès fondé sur la vue (VACM, *view-based access control model*);

Remplacer le 8e tiret du 3e alinéa:

– tout service ou toute capacité qui n'est pas explicitement requis devrait être désactivé, y compris le protocole SNMP s'il est activé.

par:

– tout service ou toute capacité qui n'est pas explicitement requis devrait être désactivé. En d'autres termes, s'il n'est pas requis/nécessaire, le service SNMP devrait être désactivé.

1.2) Bibliographie

Remplacer les références suivantes:

– IETF RFC 1157 (1990), *A Simple Network Management Protocol (SNMP),* (disponible à l'adresse http://www.ietf.org/rfc/rfc1157.txt?number=1157).

– IETF RFC 2271 (1998), *An Architecture for Describing Simple Network Management Frameworks,* (disponible à l'adresse http://www.ietf.org/rfc/rfc2271.txt?number=2271).

– IETF RFC 2272 (1998), *Message Processing and Dispatching for the Simple Network Management Protocol*, (disponible à l'adresse http://www.ietf.org/rfc/rfc2272.txt?number=2272)

– IETF RFC 2273 (1998), *SNMPv3 Applications*, (disponible à l'adresse http://www.ietf.org/rfc/rfc2273.txt?number=2273).

– IETF RFC 2275 (1998), *View-based Access Control Model for the Simple Network Management Protocol*, (disponible à l'adresse http://www.ietf.org/rfc/rfc2275.txt?number=2275).

– IETF RFC 1905 (1996), *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*, (disponible à l'adresse http://www.ietf.org/rfc/rfc1905.txt?number=1905).

par les références suivantes:

– IETF RFC 1157 (1990), *Simple Network Management Protocol (SNMP)*, (Also STD0015) (Status: HISTORIC) (disponible à l'adresse http://www.ietf.org/rfc/rfc1157).

– IETF RFC 3410 (2002), *Introduction and Applicability Statements for Internet Standard Management Framework*, (Status: INFORMATIONAL) (disponible à l'adresse http://www.ietf.org/rfc/rfc3410.txt).

– IETF RFC 3411 (2002), *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*, STD 62 (disponible à l'adresse http://www.ietf.org/rfc/rfc3411.txt).

– IETF RFC 3412 (2002), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*, STD 62 (disponible à l'adresse http://www.ietf.org/rfc/rfc3412.txt).

– IETF RFC 3413 (2002), *Simple Network Management Protocol (SNMP) Applications*, STD 62 (disponible à l'adresse http://www.ietf.org/rfc/rfc3413.txt).

– IETF RFC 3414 (2002), *User-Based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, STD 62 (disponible à l'adresse http://www.ietf.org/rfc/rfc3414.txt).

– IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*, STD 62 (disponible à l'adresse http://www.ietf.org/rfc/rfc3415.txt).

– IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*, STD 62 (disponible à l'adresse http://www.ietf.org/rfc/rfc3416.txt).

Ajouter à la bibliographie les nouvelles références suivantes:

– IETF RFC 1901 (1996), *Introduction to Community-based SNMPv2*, (Status: HISTORIC) (disponible à l'adresse http://www.ietf.org/rfc/rfc1901.txt).

– IETF RFC 3826 (2004), *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*, (Status: PROPOSED STANDARD) (disponible à l'adresse http://www.ietf.org/rfc/rfc3826.txt).

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
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	Réseaux câblés et 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	**Gestion des télécommunications y compris le RGT et maintenance des réseaux**
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2006