Union internationale des télécommunications

UIT-T M.3016.1

(04/2005)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

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

Recommandation UIT-T M.3016.1

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

Résumé

La présente Recommandation établit les prescriptions de sécurité pour le plan de gestion du réseau de gestion des télécommunications. Elle porte en particulier sur la question de la sécurité du plan de gestion pour les éléments de réseau (NE, *network element*) et les systèmes de gestion (MS, *management system*), qui font partie de l'infrastructure des télécommunications.

Source

La Recommandation UIT-T M.3016.1 a été approuvée le 13 avril 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

Introduction

L'infrastructure des télécommunications est essentielle pour les communications et l'économie mondiales. Il est donc indispensable que les fonctions de gestion de cette infrastructure soient correctement sécurisées. Malgré les nombreuses normes de sécurité applicables à la gestion des réseaux de télécommunication, les divers équipements et logiciels de télécommunications installés sont peu conformes à ces normes et ne sont pas toujours compatibles entre eux. La présente Recommandation établit les prescriptions de sécurité qui permettront aux fournisseurs d'équipements ou de logiciels, aux exploitants et aux fournisseurs de services de mettre en place une infrastructure de gestion des télécommunications sécurisée. Cet ensemble de prescriptions correspond à la situation actuelle, mais les technologies vont évoluer et les conditions vont changer. Pour être utile, la présente Recommandation devra évoluer à mesure que les conditions le justifieront. La présente Recommandation est destinée à servir de base. Pour répondre à leurs besoins particuliers, les fournisseurs de services pourront définir des prescriptions additionnelles, qui viendront compléter celles qui sont définies dans la présente Recommandation.

La présente Recommandation fait partie de la série M.3016.x de Recommandations de l'UIT-T visant à fournir des indications et des recommandations pour la sécurisation du plan de gestion des réseaux en évolution:

– Rec. UIT-T M.3016.0 – Sécurité pour le plan de gestion: aperçu général.
– Rec. UIT-T M.3016.1 – Sécurité pour le plan de gestion: prescriptions de sécurité.
– Rec. UIT-T M.3016.2 – Sécurité pour le plan de gestion: services de sécurité.
– Rec. UIT-T M.3016.3 – Sécurité pour le plan de gestion: mécanismes de sécurité.
– Rec. UIT-T M.3016.4 – Sécurité pour le plan de gestion: formulaire de sécurité.

Recommandation UIT-T M.3016.1

Sécurité pour le plan de gestion: prescriptions de sécurité

1 Domaine d'application

Les Recommandations UIT-T M.3016.1 à M.3016.3 établissent un ensemble de prescriptions, de services et de mécanismes afin de sécuriser correctement les fonctions de gestion nécessaires à la prise en charge de l'infrastructure des télécommunications. Les niveaux requis de prise en charge de la sécurité pouvant varier d'une administration à l'autre ou d'une organisation à l'autre, les Recommandations UIT-T M.3016.1 à M.3016.3 ne précisent pas si une prescription, un service ou un mécanisme est obligatoire ou facultatif.

La présente Recommandation établit les prescriptions de sécurité pour le plan de gestion du réseau de gestion des télécommunications. Elle porte en particulier sur la question de la sécurité du plan de gestion pour les éléments de réseau (NE, *network element*) et les systèmes de gestion (MS, *management system*), qui font partie de l'infrastructure des télécommunications.

La présente Recommandation est de nature générique et ne porte donc pas sur les prescriptions applicables à une interface particulière du réseau de gestion des télécommunications (RGT).

Le formulaire défini dans la Rec. UIT-T M.3016.4 vise à aider les organisations, administrations et autres organismes nationaux ou internationaux à déterminer si la prise en charge des différentes prescriptions est obligatoire ou facultative et à spécifier les intervalles de valeurs, les valeurs, etc., et ce, afin de faciliter l'implémentation de leurs politiques de sécurité.

1.1 Objet

La Rec. UIT-T M.3016.0 recense un certain nombre d'objectifs de sécurisation du réseau de gestion et de menaces qui font que ces objectifs risquent de ne pas être remplis. La présente Recommandation établit des prescriptions sur la base de ces objectifs et menaces et détermine les services de sécurité à mettre en place. La définition des services repose sur des mécanismes utilisant des algorithmes. Les autres Recommandations de la série s'appuient sur la structure établie dans la Rec. UIT-T M.3016.0 (Aperçu général) et donnent des détails sur les diverses autres étapes qu'il faut suivre pour sécuriser le plan de gestion.

1.2 Relation avec l'architecture de sécurité X.805

La Rec. UIT-T X.805 définit l'architecture de sécurité permettant d'assurer la sécurité de réseau de bout en bout. Dans l'architecture de sécurité X.805, un ensemble complexe de fonctionnalités de sécurité de réseau de bout en bout est subdivisé logiquement en trois composants architecturaux distincts: dimensions de sécurité, couches de sécurité et plans de sécurité (voir la Figure 2/X.805). Une dimension de sécurité est un ensemble de mesures de sécurité conçues pour traiter un aspect particulier de la sécurité de réseau. La Rec. UIT-T X.805 définit trois couches de sécurité: relatives à l'infrastructure, aux services et aux applications qui, ensemble, permettent d'offrir des solutions fondées sur le réseau. Un plan de sécurité correspond à un certain type d'activité de réseau protégée par les dimensions de sécurité. La Rec. UIT-T X.805 définit trois plans de sécurité: plan de gestion, plan de commande et plan d'utilisateur final. Pour offrir une solution complète, il convient d'appliquer les mesures de sécurité (par exemple contrôle d'accès, authentification) à chaque type d'activité de réseau (activité du plan de gestion, activité du plan de commande ou activité du plan d'utilisateur final) concernant l'infrastructure, les services et les applications de réseau. La présente Recommandation porte en particulier sur la question de la sécurité du plan de gestion pour les éléments de réseau (NE) et les systèmes de gestion (MS), qui font partie de l'infrastructure de réseau.

1.3 Relation avec les prescriptions de sécurité des réseaux de télécommunication de la Recommandation E.408

La Rec. UIT-T E.408 donne un aperçu général des prescriptions de sécurité et définit un cadre qui identifie les menaces qui pèsent sur la sécurité des réseaux de télécommunication en général (fixes ou mobiles, voix ou données) et indique comment planifier des contre-mesures afin de limiter les risques découlant de ces menaces. Elle est de nature générique et ne porte pas sur les prescriptions applicables à des réseaux particuliers. La série M.3016.x établit les prescriptions, services et mécanismes de sécurité pour les réseaux de télécommunication, autrement dit pour le plan de gestion du réseau de gestion des télécommunications d'une manière générale.

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. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

- Recommandation UIT-T E.408 (2004), *Prescriptions de sécurité des réseaux de télécommunication*.
- Recommandation UIT-T G.8080/Y.1304 (2001), *Architecture du réseau optique à commutation automatique (ASON)*, plus Amendement 2 (2005).
- Recommandation UIT-T M.3010 (2000), *Principes du réseau de gestion des télécommunications*.
- Recommandation UIT-T M.3013 (2000), *Considérations relatives aux réseaux de gestion des télécommunications*.
- Recommandation UIT-T M.3016.0 (2005), *Sécurité pour le plan de gestion: aperçu général*.
- Recommandation UIT-T M.3016.2 (2005), *Sécurité pour le plan de gestion: services de sécurité*.
- Recommandation UIT-T M.3016.3 (2005), *Sécurité pour le plan de gestion: mécanismes de sécurité.*
- Recommandation UIT-T M.3016.4 (2005), *Sécurité pour le plan de gestion: formulaire de sécurité*.
- Recommandation UIT-T X.509 (2000), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*, plus Corr. technique 1 (2001), Corr. technique 2 (2002) et Corr. technique 3 (2003).
- Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*, plus Amendement 1 (1996), *service et mécanismes de sécurité de couche 2 pour réseaux locaux*.
- Recommandation UIT-T X.805 (2003), *Architecture de sécurité pour les systèmes assurant des communications de bout en bout*.
- IETF RFC 1750 (1994), *Randomness Recommendations for Security*.

3 Termes et définitions

La présente Recommandation utilise les termes suivants tirés de la Rec. UIT-T G.8080/Y.1304:

– plan de commande;

– plan de gestion;

– plan de transport.

La présente Recommandation utilise les termes suivants tirés de la Rec. UIT-T M.3010:

– système de gestion;

– élément de réseau.

La présente Recommandation utilise les termes suivants tirés de la Rec. UIT-T M.3013:

– système de gestion d'élément.

La présente Recommandation utilise les termes suivants tirés de la Rec. UIT-T X.509:

– authentification forte.

La présente Recommandation utilise les termes suivants tirés de la Rec. UIT-T X.800:

– contrôle d'accès;

– authentification.

La présente Recommandation définit les termes suivants:

3.1 actions d'administration de sécurité essentielles, qui sont notamment les suivantes:

a) définir et assigner des privilèges d'utilisateur;

b) ajouter et supprimer des identités d'utilisateur;

c) désactiver l'utilisation d'identités d'utilisateur particulières comme identités de connexion;

d) initialiser et réinitialiser des mots de passe de connexion;

e) initialiser et modifier des clés de chiffrement;

f) fixer, pour le système, la durée de validité des mots de passe de connexion;

g) fixer, pour le système, le nombre maximal d'échecs de connexion pour chaque identité de connexion;

h) supprimer un verrouillage ou modifier la valeur de temporisation de verrouillage du système;

i) fixer la valeur de temporisation d'inactivité du système;

j) configurer la journalisation de sécurité et les alarmes de sécurité du système;

k) gérer les processus de journalisation de sécurité;

l) mettre à jour les logiciels de sécurité;

m) terminer les sessions d'utilisateur ou de système.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations suivantes:

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

ACS serveur de contrôle d'accès (*access control server*)

ALE estimation des pertes annuelles (*annualized loss expectancy*)

ANSI Institut national américain de normalisation (*American National Standards Institute*)

CC	centre de commutation (*central office*)
CORBA	architecture de courtier commun de requête sur des objets (*common object request broker architecture*)
CSI	interopérabilité sécurisée commune (*common secure interoperability*)
DoS	déni de service (*denial of service*)
EMS	système de gestion d'élément (*element management system*)
FTP	protocole de transfert de fichiers (*file transfer protocol*)
HAZMAT	matières dangereuses (*hazardous materials*)
HTTP	protocole de transfert hypertexte (*hypertext transfer protocol*)
IETF	groupe de travail d'ingénierie Internet (*Internet Engineering Task Force*)
IP	protocole Internet (*Internet protocol*)
IPsec	sécurité du protocole Internet (*Internet protocol security*)
ISO/CEI	Organisation Internationale de Normalisation (*international organization for standardization*)/Commission électrotechnique internationale
LAES	surveillance électronique légalement autorisée (*lawfully authorized electronic surveillance*)
MS	système de gestion (*management system*); (tout système EMS, NMS ou OSS)[1]
NE	élément de réseau (*network element*)
NE/MS	NE ou MS
NMS	système de gestion de réseau (*network management system*)
NTP	protocole relatif au temps dans le réseau (*network time protocol*)
OAM&P	exploitation, administration, maintenance et fourniture (*operations, administration, maintenance and provisioning*)
OASIS	Organization for the Advancement of Structured Information Standards
OEM	fabricant d'équipements d'origine (*original equipment manufacturer*)
ORB	courtier de requêtes sur des objets (*object request broker*)
OS	système d'exploitation (*operating system*)
OSS	système support d'exploitation (*operations support system*)
RFC	demande de commentaires (*request for comments*)
RGT	réseau de gestion des télécommunications
SAML	langage de balisage d'assertions de sécurité (*security assertion markup language*)
SNMP	protocole simple de gestion de réseau (*simple network management protocol*)
SOAP	protocole simplifié d'accès aux objets (*simple object access protocol*)
SSH	coquille sécurisée (*secure shell*)
SSL	couche de connecteurs sécurisée (*secure socket layer*)

[1] Les systèmes OSS peuvent généralement être utilisés dans le même contexte que les systèmes MS dans les différentes couches de la hiérarchie du réseau de gestion des télécommunications.

TCP protocole de commande de transmission (*transmission control protocol*)

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

UIT-T Union internationale des télécommunications – Secteur de la normalisation des télécommunications

XML langage de balisage extensible (*extensible markup language*)

5 Conventions

Dans les Recommandations UIT-T M.3016.1 à M.3016.3, on utilise des descripteurs pour identifier les prescriptions, les services et les mécanismes. Chaque descripteur est constitué de l'une des étiquettes suivantes à trois lettres, suivie par un nombre:

– REQ pour une prescription (*requirement*);

– SER pour un service;

– MEC pour un mécanisme.

6 Prescriptions de sécurité

Le présent paragraphe contient les prescriptions de sécurité concernant l'exploitation, l'administration, la maintenance et la fourniture (OAM&P, *operations, administration, maintenance and provisioning*) ainsi que le système support d'exploitation (OSS, *operations support system*) du **plan de gestion**.

La Figure 1/M.3016.0 décrit les relations entre les objectifs de sécurité, les menaces, les risques, les prescriptions de sécurité et les services de sécurité. Elle décrit le processus consistant à partir des "menaces" et des "objectifs de sécurité" pour déterminer les "prescriptions de sécurité", lesquelles sont ensuite concrétisées par un ensemble de "services de sécurité". Ces derniers, qui visent à contrecarrer les menaces, utilisent des "mécanismes de sécurité", lesquels reposent sur des "algorithmes de sécurité". Le Tableau 1 (qui est le Tableau 4/M.3016.0) donne la correspondance entre prescriptions et services de sécurité. Conformément au Tableau 1, les prescriptions de sécurité décrites dans le présent paragraphe sont classées comme suit:

– vérification d'identité;

– contrôle d'accès et autorisation;

– protection de la confidentialité;

– protection de l'intégrité des données;

– imputabilité;

– journalisation et audit de sécurité;

– envoi d'alarme de sécurité.

NOTE – Le rétablissement après une transgression de sécurité nécessite un complément d'étude.

Tableau 1/M.3016.1 – Correspondance entre prescriptions et services de sécurité (Tableau 4/M.3016.0)

Prescription fonctionnelle	Service de sécurité
Vérification d'identité	Authentification d'utilisateur Authentification d'entité homologue Authentification de l'origine des données
Contrôle d'accès et autorisation	Contrôle d'accès
Protection de la confidentialité – données stockées	Contrôle d'accès Confidentialité
Protection de la confidentialité – données transférées	Confidentialité
Protection de l'intégrité des données – données stockées	Contrôle d'accès
Protection de l'intégrité des données – données transférées	Intégrité
Imputabilité	Non-répudiation
Journalisation d'activités	Trace d'audit
Envoi d'alarme de sécurité	Alarme de sécurité
Audit de sécurité	Trace d'audit

6.1 Vérification d'identité

L'**authentification** a un double objectif en matière de sécurisation du **plan de gestion**:

1) vérifier l'identité des parties en communication et ce, afin de pouvoir établir des communications privées avec une entière intégrité des données et une entière confidentialité entre deux systèmes;
2) offrir un mécanisme de base pour la journalisation dans un système de gestion et/ou l'audit des activités de gestion de n'importe quel système.

6.1.1 Authentification d'utilisateur, mots de passe et identités d'utilisateur

Par **authentification d'utilisateur**, on entend l'**authentification** des clients participant à la gestion du réseau. Dans ce cas, l'**authentification** permet de prouver l'identité de l'utilisateur légitime et d'éviter les attaques de type usurpation d'identité lancées par des utilisateurs illégitimes. Avec une **authentification** correcte, il est possible de suivre les activités et de restreindre les activités ou rôles des utilisateurs conformément aux autorisations définies préalablement (voir le § 6.3).

L'**authentification** repose, au minimum, sur l'utilisation d'une identité d'utilisateur et d'un **mot de passe complexe** statique. D'autres mécanismes peuvent être utilisés si les administrateurs des éléments NE/MS sont sûrs que le niveau de sécurité est au moins aussi élevé que le niveau de sécurité offert par une identité d'utilisateur et un **mot de passe complexe** statique. Les autres mécanismes envisageables sont notamment les suivants:

– identité d'utilisateur et **authentification à double facteur** avec générateur de mots de passe à utilisation unique,[2]
– **authentification à double facteur** avec carte à puce sur laquelle sont stockés les pouvoirs de manière protégée.

REQ 1: pour la connexion, la journalisation et l'audit concernant les éléments NE/MS, une authentification forte devrait être prise en charge.

[2] Le présent paragraphe ne porte pas sur les mots de passe dynamiques car ceux-ci sont considérés comme étant en dehors du domaine d'application de la présente Recommandation.

REQ 1 constitue la prescription de sécurité. La description du mécanisme d'authentification général figure dans la Rec. UIT-T M.3016.3. Les techniques d'**authentification** et les techniques d'identification unique vont probablement continuer à être améliorées.

Concernant l'identification unique sécurisée, le protocole continue à demander les pouvoirs à l'entité ou aux entités; toutefois, un utilisateur n'est pas obligé de saisir les pouvoirs s'ils sont mis de façon sécurisée en mémoire cache (Kerberos, par exemple).

Les prescriptions suivantes facilitent le maintien de la complexité des mots de passe et sont utiles pour l'audit et la journalisation.

REQ 2: chaque élément NE/MS devrait mettre en application l'**authentification** conformément à la politique de l'organisation.

REQ 3: chaque élément NE/MS devrait prendre en charge les règles de complexité minimales relatives à l'**authentification** conformément à la politique de l'organisation.

REQ 4: les éléments NE/MS devraient faire en sorte que le mot de passe de connexion d'un utilisateur ne puisse pas être modifié par un autre utilisateur sans que le premier utilisateur n'en ait connaissance.

REQ 5: chaque élément NE/MS devrait vérifier automatiquement que chaque nouveau mot de passe de connexion est différent du précédent. Le degré de différence devrait être configurable conformément à la politique de l'organisation.

Comme les mots de passe sont généralement enregistrés par le biais d'un chiffrement irréversible, la saisie de l'ancien mot de passe est également nécessaire pour permettre à l'élément NE/MS de déterminer le degré de différence entre l'ancien mot de passe et le nouveau.

REQ 6: chaque élément NE/MS devrait faire en sorte que les mots de passe ne puissent pas être réutilisés. Les paramètres à utiliser à cette fin devraient être configurables conformément à la politique de l'organisation.

REQ 7: chaque identité d'utilisateur devrait être associée à un mot de passe de connexion réglable qui lui est propre.

REQ 8: les mots de passe devraient pouvoir être modifiés à la discrétion de leur utilisateur, un intervalle de temps minimal devant être respecté entre deux modifications. Cet intervalle de temps minimal devrait être configurable conformément à la politique de l'organisation et fixé par l'**administrateur de sécurité de système**.

REQ 9: chaque élément NE/MS devrait prendre en charge un contrôle des mots de passe à plusieurs niveaux, certaines identités d'utilisateur pouvant être verrouillées (par exemple, suite à une expiration de la validité du mot de passe ou à un échec de connexion), d'autres non.

6.1.2 Valeurs par défaut pour l'authentification

L'utilisation correcte des mots de passe par défaut a largement été examinée dans la littérature relative à la sécurité. Historiquement, cela va du mot de passe par défaut intégré dans le programme au mot de passe par défaut associé à chaque version ou mise à jour du logiciel. Les prescriptions relatives aux valeurs par défaut pour l'**authentification** sont les suivantes.

REQ 10: l'une des prescriptions suivantes devrait s'appliquer:

- le logiciel de configuration devrait créer un mot de passe d'initialisation unique pour chaque application figurant dans la nouvelle version ou mise à jour[3] du logiciel;

[3] Ceci est analogue à la pratique selon laquelle chaque disque compact acheté dans le commerce comporte un mot de passe d'activation unique.

- si un mot de passe par défaut est utilisé, le système devrait exiger qu'il soit remplacé par un mot de passe unique avant que le dispositif soit mis en service;
- si un dispositif est fourni sans mot de passe ou avec un mot de passe néant, un mot de passe unique devrait être assigné pendant le processus d'installation avant que le dispositif soit mis en service.

REQ 11: la durée de validité des mots de passe de connexion du système devrait être configurable si la fonctionnalité est également intégrée dans l'application. A l'expiration de la durée de validité, le mot de passe de connexion associé à une application affectée devrait retourner à l'état par défaut d'origine défini dans la prescription REQ 10. Tous les privilèges de modification de mot de passe devraient être révoqués pour tous les utilisateurs sauf pour le rôle d'utilisateur qui possède le niveau le plus élevé d'autorité de sécurité pour le système ou pour l'application considérée.

REQ 12: la valeur de temporisation d'inactivité du système devrait être configurable si la fonctionnalité est également intégrée dans l'application. Lorsque la temporisation d'inactivité du système est déclenchée, l'accès au système pour une identité d'utilisateur donnée devrait être interdit et le processus de connexion pour cet utilisateur devrait être désactivé.

REQ 13: le nombre maximal d'échecs de connexion successifs pour une certaine identité d'utilisateur défini dans le système devrait être configurable si la fonctionnalité est également intégrée dans l'application. Lorsque ce nombre est atteint, la temporisation d'inactivité du système définie dans la prescription REQ 12 devra être invoquée.

6.2 Contrôle d'accès et autorisation

Chaque élément NE/MS doit obligatoirement prendre en charge le principe du "moindre privilège" (autrement dit, une personne aura un rôle et ne sera autorisée à visualiser des données, à modifier des données ou à lancer des **actions de gestion** que pour les fonctions autorisées par ce rôle). Le présent paragraphe définit les prescriptions de base applicables à l'implémentation du "moindre privilège" par le biais d'une bonne administration de sécurité de système.

6.2.1 Administration de la sécurité

Chaque élément NE/MS doit faire en sorte que seuls les utilisateurs autorisés puissent gérer les ressources de sécurité de système. Toutes les actions administratives sont reliées à des rôles d'utilisateur, lesquels sont assignés à des individus spécifiques. Seuls quelques types de rôles d'utilisateur sont examinés, mais de nombreux autres types de rôles d'utilisateur avec des degrés de privilèges variables peuvent exister, notamment en ce qui concerne les **actions de gestion** de sécurité essentielles. L'objectif est de faire en sorte que seuls les utilisateurs autorisés et privilégiés puissent gérer les ressources de sécurité essentielles.

REQ 14: chaque élément NE/MS devrait permettre de définir plusieurs types de rôles d'utilisateur et d'assigner à chacun d'eux des **actions de gestion**.

On pourrait créer une hiérarchie des rôles d'utilisateur, dans laquelle un rôle d'utilisateur a une autorité moins grande qu'un rôle d'utilisateur davantage privilégié par le fait que des tâches différentes ou moins nombreuses lui sont assignées. Citons par exemple le cas d'une hiérarchie dans laquelle un rôle d'utilisateur peut effectuer toutes les **actions de gestion** ("superutilisateur" informatique par exemple) et un autre rôle d'utilisateur dispose uniquement d'un accès en lecture seule pour surveiller les dispositifs (opérateur par exemple).

REQ 15: chaque élément NE/MS devrait prendre en charge un type d'utilisateur par défaut, avec un ensemble minimal ou restrictif d'**actions de gestion**.

REQ 16: chaque élément NE/MS devrait prendre en charge les **actions d'administration de sécurité essentielles** suivantes, la liste n'étant pas exhaustive:

- définir et assigner des privilèges d'utilisateur et de groupe;
- conserver un enregistrement de toutes les demandes d'identités de connexion au système;
- ajouter et supprimer des identités d'utilisateur;
- désactiver et activer l'utilisation d'identités d'utilisateur spécifiques comme identités de connexion;
- initialiser et réinitialiser les mots de passe de connexion;
- initialiser et modifier les clés de chiffrement;
- fixer, pour le système, la durée de validité des mots de passe de connexion;
- fixer, pour le système, le nombre maximal d'échecs de connexion pour chaque identité de connexion;
- supprimer un verrouillage ou modifier la valeur de temporisation de verrouillage du système;
- fixer la valeur de temporisation d'inactivité du système;
- configurer la journalisation de sécurité et les alarmes de sécurité du système;
- surveiller tous les journaux de sécurité du système;
- gérer les processus de journalisation de sécurité du système;
- mettre à jour les logiciels de sécurité;
- terminer les sessions d'utilisateur ou de système;
- déléguer des autorisations de sécurité à des personnes spécifiques assurant d'autres rôles;
- établir les règles de complexité des mots de passe.

REQ 17: chaque élément NE/MS devrait prendre en charge les **actions de gestion** de sécurité d'application suivantes, la liste n'étant pas exhaustive:

- définir et assigner de nouveaux privilèges d'utilisateur ou de groupe au niveau de l'application;
- conserver un enregistrement de toutes les demandes d'identités de connexion à l'application;
- ajouter et supprimer des utilisateurs au niveau de l'application;
- surveiller tous les journaux de sécurité de l'application;
- configurer la journalisation de sécurité et les alarmes de sécurité de l'application;
- gérer les processus de journalisation de sécurité de l'application;
- terminer les sessions d'application d'utilisateur.

6.2.2 Utilisation et fonctionnement des éléments NE/MS

Les prescriptions du présent paragraphe s'appliquent à la fois à l'accès distant et à l'accès par console à un élément NE/MS. Ces prescriptions obligatoires constituent un ensemble de base pour les éléments NE/MS qui stockent effectivement les identités d'utilisateur et les mots de passe. De nombreux éléments NE/MS font appel à un serveur ACS centralisé pour stocker les identités d'utilisateur et les mots de passe. Les prescriptions obligatoires formulées tout au long de la présente Recommandation s'appliquent aux éléments NE/MS qui conservent les identités d'utilisateur et les mots de passe ou qui font appel à un serveur ACS pour le stockage des identités d'utilisateur et des mots de passe.

REQ 18: les éléments NE/MS devraient procéder à une synchronisation temporelle de manière authentifiée (par exemple NTP version 3).

REQ 19: pour un élément NE/MS, chaque **action de gestion** devrait être associée à une seule SESSION autorisée.

REQ 20: chaque SESSION devrait être établie par le biais d'une **authentification** appropriée, comme détaillé dans la prescription REQ 1.

REQ 21: les communications entre un élément NE/MS et un serveur ACS aux fins d'acheminement des pouvoirs d'**authentification** devraient se faire sur une **connexion sécurisée**.

REQ 22: les éléments NE/MS devraient utiliser le **contrôle d'accès** et des partitions pour autoriser, refuser ou contrôler d'une manière ou d'une autre l'accès d'un utilisateur, d'un groupe d'utilisateurs ou d'un système distant aux éléments NE/MS et devraient assurer une fonctionnalité telle que les données, transactions et équipements utilisables par les utilisateurs soient restreints à ce qui leur est nécessaire pour remplir leur rôle. Les permissions d'accès devraient notamment être les suivantes: lecture seule et écriture seule, cette liste n'étant pas exhaustive.

6.2.3 Processus de connexion

REQ 23: les éléments NE/MS devraient pouvoir assigner à chaque individu une identité d'utilisateur unique pour la connexion à une application ou à un serveur informatique.

REQ 24: les éléments NE/MS devraient pouvoir, lorsque c'est nécessaire, obliger automatiquement l'utilisateur à modifier son mot de passe lors de son premier accès après l'établissement de son compte et lors de son premier accès après la réinitialisation de son mot de passe.

NOTE – En ce qui concerne la prescription qui suit (REQ 25), une distinction doit être faite selon qu'elle se rapporte à la gestion d'un élément de réseau (NE) ou à celle d'un système de gestion (MS). Dans le cas des éléments de réseau, un dispositif doit être surveillé par le biais de plusieurs mécanismes, éventuellement simultanément, pendant les modifications de configuration. Dans le cas des systèmes de gestion, ce n'est pas nécessaire.

L'objet de cette prescription est de gérer la capacité pour les utilisateurs de consommer toutes les ressources disponibles d'un élément NE/MS. Le personnel d'exploitation devrait ajuster les valeurs par défaut applicables aux éléments de réseau en fonction des besoins pour une situation particulière et devrait surveiller et examiner les tentatives de dépassement des limites fixées, car celles-ci peuvent indiquer une faiblesse sur le plan opérationnel ou une tentative d'activités malveillantes.

REQ 25: les éléments NE/MS devraient empêcher, contrôler ou limiter l'utilisation active simultanée de la même identité d'utilisateur, selon le cas. Le nombre de sessions actives simultanément devrait être configurable sur la base de l'identité d'utilisateur.

REQ 26: une application d'élément NE/MS ne devrait pas nécessiter de privilèges d'accès de **superutilisateur** pour fonctionner correctement.

REQ 27: les éléments NE/MS devraient pouvoir afficher à l'utilisateur, au cours du processus de connexion, les date et heure de sa dernière **authentification** réussie.

REQ 28: une déclaration d'exclusivité personnalisable et un avertissement de propriété privée devraient être affichés sur l'écran de saisie initial avant que tout accès logique ne soit autorisé. Les équipements devraient prendre en charge une longueur minimale de 1600 caractères. Un message par défaut devrait être fourni.

On donne ci-après un exemple d'avertissement.

```
AVERTISSEMENT! Ce système informatique et ce réseau sont
PRIVÉS et PROPRIÉTAIRES et ne sont accessibles qu'aux
utilisateurs autorisés. L'utilisation de ce système
```

informatique ou de ce réseau de façon non autorisée est strictement interdite et pourra entraîner des poursuites pénales, des mesures disciplinaires à l'encontre des employés pouvant aller jusqu'au licenciement, ou la rupture de contrats avec des fournisseurs d'équipements ou de services. Le propriétaire, ou ses agents, peut surveiller toute activité ou communication sur le système informatique ou sur le réseau. Le propriétaire, ou ses agents, peut extraire toute information stockée dans le système informatique ou dans le réseau. L'accès à ce système informatique ou à ce réseau et son utilisation valent consentement à toute surveillance ou extraction d'informations aux fins d'application de la loi et à d'autres fins. Les utilisateurs ne peuvent prétendre ni à une confidentialité des communications acheminées sur le système informatique ou sur le réseau ni à une confidentialité des informations qui y sont stockées, y compris les informations stockées localement ou à distance sur un disque dur ou sur un autre support utilisé avec ce système informatique ou ce réseau.

Il est recommandé que chaque entité élabore un avertissement approprié.

REQ 29: pour tout échec d'une tentative de connexion, l'utilisateur devrait uniquement être avisé du fait que le processus de connexion a échoué ou qu'il n'est pas valide. Des informations telles que "identité d'utilisateur non valide" ou "mot de passe non valide" ne devraient pas être communiquées.

REQ 30: les éléments NE/MS devraient **verrouiller** la connexion à partir d'un compte d'utilisateur après qu'un nombre maximal configurable d'échecs de connexion a été atteint. Le **verrouillage** devrait inclure l'interface de la console. Le **verrouillage** ne devrait PAS inclure le compte par défaut d'origine qui prend en charge toutes les actions de gestion.

REQ 31: les éléments NE/MS ne devraient PAS avoir de mécanisme permettant de contourner l'**authentification** de connexion et les processus de connexion.

REQ 32: les éléments NE/MS ne devraient jamais afficher un pouvoir en clair (mot de passe par exemple) sur quelque support que ce soit (écrans de terminal, copies papier par exemple) ni le stocker dans des journaux.

REQ 33: les éléments NE/MS devraient appliquer une durée de validité configurable pour les mots de passe.

Une implémentation générale et acceptable de la prescription REQ 33 consiste pour le système à imposer que l'utilisateur saisisse un nouveau mot de passe immédiatement après avoir authentifié cet utilisateur avec l'ancien mot de passe. Autre solution: le système peut imposer à un administrateur de changer correctement le mot de passe. Si un compte n'est pas utilisé pendant un certain temps, il sera considéré comme inactif.

REQ 34: si la durée de validité d'un mot de passe de connexion a expiré pour le système considéré, l'élément NE/MS devrait **verrouiller** la connexion pour l'identité d'utilisateur correspondante jusqu'à ce que le mot de passe soit correctement changé.

REQ 35: si un compte reste inactif pendant une durée minimale configurable, l'élément NE/MS devrait envoyer une alerte.

REQ 36: si un compte reste inactif pendant une durée minimale configurable, l'élément NE/MS devrait désactiver le compte après avoir envoyé une alerte de désactivation. Le

processus de DESACTIVATION ne devrait PAS inclure les comptes d'**administrateur de système**, d'**administrateur de sécurité de système** ni de **superutilisateur**.

REQ 37: la réactivation d'une identité de connexion **désactivée** ne peut être opérée que par un administrateur correctement connecté auquel est assignée l'action d'administration de sécurité essentielle permettant d'initialiser et de réinitialiser les mots de passe de connexion.

Les options relatives à la réactivation des identités de connexion peuvent être configurées sous la forme d'un paramètre de système au niveau des rôles.

REQ 38: la réinitialisation d'une identité de connexion VERROUILLEE et la suppression de la situation de **verrouillage** ne peuvent être opérées que par un administrateur correctement connecté auquel est assignée l'action d'administration de sécurité essentielle permettant de supprimer un verrouillage ou de modifier la valeur de temporisation de verrouillage du système.

Les options relatives à la suppression d'un **verrouillage** d'identités de connexion peuvent être configurées sous la forme d'un paramètre de système au niveau des rôles.

6.2.4 Processus de déconnexion

REQ 39: chaque **session** établie correctement devrait être déconnectée par l'utilisateur ou par le système après une certaine période d'inactivité.

REQ 40: un élément NE/MS devrait déconnecter une **session** établie correctement lorsque la durée écoulée depuis la dernière activité pour cette **session** a atteint la valeur de temporisation d'inactivité configurable du système.

6.2.5 Applications

REQ 41: un type de rôle d'utilisateur devrait rester inchangé pendant toute la durée d'exécution d'une application d'élément NE/MS, jusqu'à ce qu'il soit mis fin à cette application.

L'utilisateur ne devrait pas pouvoir utiliser de mécanisme de séquence de commandes (l'échappement vers un mode de **superutilisateur**, par exemple). Par ailleurs, en cas de défaillance de l'application, celle-ci ne doit jamais laisser l'utilisateur dans un rôle différent avec davantage de privilèges. L'utilisateur doit toujours procéder à une nouvelle authentification (nouvelle connexion) pour pouvoir remplir un rôle différent.

6.3 Protection de la confidentialité

Le présent paragraphe établit des prescriptions relatives aux algorithmes cryptographiques et à la gestion des clés de chiffrement pour permettre de garantir plus facilement la sécurité des systèmes et des réseaux. Les algorithmes symétriques sont normalement utilisés pour les services de confidentialité et d'intégrité. Les clés utilisées dans ces algorithmes sont normalement échangées par le biais d'un processus étroitement lié à l'authentification. Il est également possible d'utiliser des algorithmes asymétriques pour les services d'authentification et d'échange de clés. Les méthodes utilisées pour générer, stocker, distribuer, détruire et révoquer ces clés sont extrêmement importantes. De plus, des facteurs tels que la longueur de clé, le choix de la clé et le choix de l'algorithme ont une incidence directe sur le niveau de sécurité offert par un système cryptographique donné.

L'**authentification protégée** et la confidentialité des données sont fondées sur des méthodes de chiffrement, lesquelles utilisent des algorithmes spéciaux qui sont normalisés et ouverts à tous, ce qui permet de bien les examiner et de les mettre en œuvre facilement. La "force" du chiffrement dépend de l'algorithme de chiffrement et de la longueur de clé qui sont utilisés (la force correspond à la durée nécessaire pour extorquer la ou les valeurs de clé utilisées avec un algorithme donné).

Les protocoles de sécurité (par exemple IPsec, SSL, SSH) assurent généralement l'**authentification**, l'intégrité et la confidentialité. Les extensions de sécurité relatives à d'autres protocoles tels que SNMPv3 (*simple network management protocol version 3*)[4], CORBA (*common object request broker architecture*), BGP (*border gateway protocol*) et OSPF (*open shortest path first*) sont conçues pour assurer l'**authentification** et l'intégrité. L'**authentification protégée** et l'intégrité sont essentielles entre éléments NE/MS et, dans certains cas, la confidentialité est également requise.

6.3.1 Algorithmes de chiffrement symétriques

Un système de chiffrement symétrique ou à clé secrète est un système de chiffrement dans lequel les clés de chiffrement et de déchiffrement sont identiques. Dans un tel système, il faut prévoir des arrangements relatifs au partage entre les individus d'une clé secrète unique (par exemple la clé de chiffrement). La clé doit être distribuée aux individus par des moyens sécurisés ou générée en interne (par exemple sur la base d'une clé racine secrète partagée) car la connaissance de la clé de chiffrement implique la connaissance de la clé de déchiffrement et inversement.

REQ 42: pour toutes les applications de chiffrement symétriques, la force des algorithmes devrait être conforme à la politique du pays, de l'entreprise ou de l'organisation.

6.3.2 Algorithmes de chiffrement asymétriques

Dans un système de chiffrement asymétrique, la clé de chiffrement est liée à la clé de déchiffrement mais les deux clés sont différentes. L'une est rendue publique, tandis que l'autre est gardée secrète. La clé publique est différente de la clé privée, et il n'existe pas de méthode connue permettant d'obtenir la clé privée à partir de la clé publique. Les clés publiques font l'objet d'une large distribution tandis que la clé privée est toujours gardée secrète. L'emploi du chiffrement asymétrique est généralement limité au chiffrement de clés symétriques pour l'échange de ces clés et à la signature de condensés de message pour les signatures numériques. Pour l'échange de clés, c'est la clé publique du destinataire qui est utilisée et pour la signature de condensés de message, c'est la clé privée du signataire qui est utilisée.

REQ 43: pour toutes les applications de chiffrement asymétriques, la force des algorithmes devrait être conforme à la politique du pays, de l'entreprise ou de l'organisation.

REQ 44: pour toutes les applications d'échange de clés, la force des algorithmes devrait être conforme à la politique du pays, de l'entreprise ou de l'organisation.

6.3.3 Gestion des clés de chiffrement

La gestion des clés de chiffrement est difficile et souvent complexe car en plus de la génération des clés entrent en jeu l'expiration, l'échange sécurisé et la publication sécurisée. Pour de plus amples informations, on se reportera au Document RFC 1750 de l'IETF (*Randomness Recommendations for Security*).

6.3.4 Communications

La sécurisation du **plan de gestion** dans un réseau moderne repose avant tout sur la sécurisation des communications de gestion. L'Annexe A porte sur les architectures et les protocoles à utiliser pour sécuriser les **communications de gestion**. Les prescriptions obligatoires définies dans le présent paragraphe s'appliquent à toutes les interfaces d'un RGT, décrites dans la Rec. UIT-T M.3010, *Principes du réseau de gestion des télécommunications*.

REQ 45: pour chaque interface physique ou logique d'élément NE/MS qui achemine du **trafic de gestion**, l'élément NE/MS devrait pouvoir être configurée de manière à sécuriser le **trafic de gestion** au moyen d'une **authentification forte** et d'une protection cryptographique afin d'assurer la confidentialité, l'intégrité et la protection "antirejeu".

---

[4] Le protocole SNMPv3 peut aussi assurer la confidentialité.

REQ 46: tout mot de passe en clair ne devrait être transmis que par le biais d'une **connexion sécurisée**, sauf en cas de recours à un mécanisme avec mots de passe à utilisation unique, auquel cas les mots de passe à utilisation unique peuvent être envoyés en clair à condition qu'il n'y ait pas de serveur intermédiaire.

6.4 Protection de l'intégrité des données

6.4.1 Algorithmes de protection de l'intégrité des données

Des algorithmes de condensé de message avec clé combinés à des fonctions de hachage peuvent être utilisés pour assurer l'intégrité des données pour des messages de longueur arbitraire.

REQ 47: pour toutes les applications de protection de l'intégrité des données par une méthode symétrique, la force des algorithmes devrait être conforme à la politique du pays, de l'entreprise ou de l'organisation.

REQ 48: pour toutes les applications de protection de l'intégrité des données par une méthode asymétrique, la force des algorithmes devrait être conforme à la politique du pays, de l'entreprise ou de l'organisation.

6.4.2 Elaboration et fourniture des éléments NE/MS

La sécurité d'un élément NE/MS dépend de l'ensemble de son cycle de vie. La sécurité est une question à prendre en considération aussi bien pendant la conception des grandes lignes que pendant la conception détaillée, l'élaboration, la mise en place et le retrait d'un produit. Des contrôles et des tests appropriés tout au long du cycle de vie sont cruciaux pour offrir des niveaux de sécurité acceptables. Les paragraphes I.5.2 et I.5.3 contiennent d'autres considérations relatives au cycle de vie.

REQ 49: tous les logiciels fournis à un fournisseur de services ou à un autre client devraient inclure, en fonction des besoins, des mécanismes d'**authentification** par chiffrement et de protection de l'intégrité (signatures numériques ou **authentification** de message par une méthode symétrique par exemple) tels que spécifiés dans la Rec. UIT-T M.3016.3.

REQ 50: tous les éléments NE/MS recevant des logiciels devraient pouvoir interpréter les mécanismes d'**authentification** par chiffrement et de protection de l'intégrité et pouvoir vérifier la source et l'intégrité des logiciels, en fonction des besoins.

REQ 51: toutes les mises à jour de logiciels, y compris les programmes de correction, devraient être transmises par le biais d'une **connexion sécurisée** aux éléments NE/MS destinés à les recevoir.

Les éléments NE/MS devraient pouvoir déterminer électroniquement le niveau courant de révision de leurs logiciels et matériels et valider les configurations appropriées de logiciels et de micrologiciels.

6.5 Imputabilité

L'objectif de l'imputabilité est de garantir que toutes les actions exécutées par une entité lui sont imputables.

REQ 52: tous les éléments NE/MS devraient pouvoir empêcher à toute entité de nier être responsable des actions qu'elle a effectuées et de leurs effets.

Voir également les prescriptions REQ 49 et REQ 50 concernant l'imputabilité liée à l'élaboration et à la fourniture des éléments NE/MS.

6.6 Journalisation et audit de sécurité

Il est important que chaque élément NE/MS dispose de capacités adéquates pour mener des activités d'investigation, d'audit, de détection en temps réel, d'analyse et de protection, pour que des mesures

correctives correctes puissent être prises. Le présent paragraphe porte sur les journaux d'audit de sécurité, mais les détails propres au contenu et au format de ces journaux sortent du cadre de la présente Recommandation.

Il est à noter que les activités d'investigation et d'analyse judiciaire peuvent porter aussi bien sur les messages OAM&P non liés à la sécurité que sur les informations stockées dans les journaux d'audit de sécurité décrits dans le présent paragraphe. La journalisation des messages OAM&P non liés à la sécurité, parfois appelés messages de "modification récente", est nécessaire pour toutes les actions susceptibles de faire l'objet d'un audit.

REQ 53: les éléments NE/MS devraient pouvoir journaliser toute action qui modifie les attributs et les services de sécurité, les contrôles d'accès et les paramètres de configuration des dispositifs.

REQ 54: les éléments NE/MS devraient pouvoir configurer les **actions d'administration de sécurité essentielles** qui doivent être incluses dans le journal de sécurité.

REQ 55: les éléments NE/MS devraient pouvoir journaliser chaque tentative de connexion et son résultat, chaque déconnexion ou terminaison de session (à distance ou depuis la console) ainsi que chaque tentative de connexion ayant entraîné l'invocation de la temporisation d'inactivité du système définie dans la prescription REQ 12 et son résultat.

Il est recommandé que les entrées de journal d'audit soient envoyées à un serveur d'audit inaltérable après que l'élément NE/MS leur a attribué une étiquette de séquence et les a authentifiées par chiffrement (signées).

REQ 56: les éléments NE/MS devraient pouvoir procéder à une journalisation à distance par le biais d'une **connexion sécurisée**.

REQ 57: chaque entrée de journal devrait contenir les informations suivantes:

- une description de l'action ou l'action proprement dite qui fait l'objet de la journalisation;
- l'identité et le niveau de sécurité de l'utilisateur ou du processus qui a lancé l'action;
- les date et heure auxquelles l'action s'est produite;
- des informations d'origine et de destination de réseau, si c'est applicable (par exemple au moment de la connexion);
- une indication du succès ou de l'échec de l'activité.

6.7 Envoi d'alarme de sécurité

Certains événements doivent être signalés sous la forme d'alarmes de sécurité (voir, par exemple, la prescription REQ 35). Toutefois, le recensement des événements qui doivent être signalés sort du cadre de la présente Recommandation.

REQ 58: tous les éléments NE/MS devraient pouvoir envoyer des alarmes pour certains événements sélectionnés.

REQ 59: tous les éléments NE/MS devraient pouvoir permettre à l'utilisateur de définir les critères de sélection des événements qui entraînent l'envoi d'alarmes.

6.8 Protection du RCD

Pour protéger l'infrastructure de gestion, et le RCD en général, il est utile que l'opérateur de réseau inspecte le trafic en provenance ou à destination de réseaux extérieurs au RCD (par exemple, en provenance de réseaux homologues ou de clients) et prenne les mesures qui s'imposent. A titre d'exemple, les paquets provenant de réseaux extérieurs et ayant une adresse IP source appartenant à l'espace d'adresses du RCD ne devraient pas être autorisés à entrer dans le RCD.

REQ 60: tous les éléments NE/MS avec connectivité fondée sur les paquets devraient interdire le trafic qui ne satisfait pas à la politique de sécurité du RCD.

Annexe A

Mappage entre les prescriptions, les services et les mécanismes de sécurité

La présente annexe indique, pour chaque prescription de sécurité, les services de sécurité (définis dans la Rec. UIT-T M.3016.2) et les mécanismes de sécurité (définis dans la Rec. UIT-T M.3016.3) correspondants.

Prescriptions de sécurité M.3016.1		Services de sécurité M.3016.2	Mécanismes de sécurité M.3016.3
REQ 1:	pour la connexion, la journalisation et l'audit concernant les éléments NE/MS, une authentification forte devrait être prise en charge.	**SER 1, SER 2, SER 3, SER 8**	**MEC 1-MEC 13**
REQ 2:	chaque élément NE/MS devrait mettre en application l'**authentification** conformément à la politique de l'organisation.	**SER 1, SER 2, SER 3**	**MEC 1-MEC 6**
REQ 3:	chaque élément NE/MS devrait prendre en charge les règles de complexité minimales relatives à l'**authentification** conformément à la politique de l'organisation.	**SER 1, SER 2, SER 3**	**MEC 1-MEC 6**
REQ 4:	les éléments NE/MS devraient faire en sorte que le mot de passe de connexion d'un utilisateur ne puisse pas être modifié par un autre utilisateur sans que le premier utilisateur n'en ait connaissance.	**SER 8**	**MEC 7-MEC 11**
REQ 5:	chaque élément NE/MS devrait vérifier automatiquement que chaque nouveau mot de passe de connexion est différent du précédent. Le degré de différence devrait être configurable conformément à la politique de l'organisation.	**SER 1**	**MEC 7-MEC 11**
REQ 6:	chaque élément NE/MS devrait faire en sorte que les mots de passe ne puissent pas être réutilisés. Les paramètres à utiliser à cette fin devraient être configurables conformément à la politique de l'organisation.	**SER 1**	**MEC 7-MEC 11**
REQ 7:	chaque identité d'utilisateur devrait être associée à un mot de passe de connexion réglable qui lui est propre.	**SER 1**	**MEC 7-MEC 11**
REQ 8:	les mots de passe devraient pouvoir être modifiés à la discrétion de leur utilisateur, un intervalle de temps minimal devant être respecté entre deux modifications. Cet intervalle de temps minimal devrait être configurable conformément à la politique de l'organisation et fixé par l'**administrateur de sécurité de système**.	**SER 1**	**MEC 7-MEC 11**

Prescriptions de sécurité M.3016.1		Services de sécurité M.3016.2	Mécanismes de sécurité M.3016.3
REQ 9:	chaque élément NE/MS devrait prendre en charge un contrôle des mots de passe à plusieurs niveaux, certaines identités d'utilisateur pouvant être verrouillées (par exemple, suite à une expiration de la validité du mot de passe ou à un échec de connexion), d'autres non.	**SER 1, SER 2, SER 3, SER 4**	**MEC 20-MEC 23**
REQ 10:	l'une des prescriptions suivantes devrait s'appliquer: • le logiciel de configuration devrait créer un mot de passe d'initialisation unique pour chaque application figurant dans la nouvelle version ou mise à jour du logiciel; • si un mot de passe par défaut est utilisé, le système devrait exiger qu'il soit remplacé par un mot de passe unique avant que le dispositif soit mis en service; • si un dispositif est fourni sans mot de passe ou avec un mot de passe néant, un mot de passe unique devrait être assigné pendant le processus d'installation avant que le dispositif soit mis en service.	**SER 1, SER 2, SER 3**	**MEC 7-MEC 11**
REQ 11:	la durée de validité des mots de passe de connexion du système devrait être configurable si la fonctionnalité est également intégrée dans l'application. A l'expiration de la durée de validité, le mot de passe de connexion associé à une application affectée devrait retourner à l'état par défaut d'origine défini dans la prescription REQ 10. Tous les privilèges de modification de mot de passe devraient être révoqués pour tous les utilisateurs sauf pour le rôle d'utilisateur qui possède le niveau le plus élevé d'autorité de sécurité pour le système ou pour l'application considérée.	**SER 4**	**MEC 7-MEC 11**
REQ 12:	la valeur de temporisation d'inactivité du système devrait être configurable si la fonctionnalité est également intégrée dans l'application. Lorsque la temporisation d'inactivité du système est déclenchée, l'accès au système pour une identité d'utilisateur donnée devrait être interdit et le processus de connexion pour cet utilisateur devrait être désactivé.	**SER 4**	**MEC 7-MEC 11**
REQ 13:	le nombre maximal d'échecs de connexion successifs pour une certaine identité d'utilisateur défini dans le système devrait être configurable si la fonctionnalité est également intégrée dans l'application. Lorsque ce nombre est atteint, la temporisation d'inactivité du système définie dans la prescription REQ 12 devra être invoquée.	**SER 4**	**MEC 7-MEC 11**
REQ 14:	chaque élément NE/MS devrait permettre de définir plusieurs types de rôles d'utilisateur et d'assigner à chacun d'eux des **actions de gestion**.	**SER 4**	**MEC 20-MEC 23**

Prescriptions de sécurité M.3016.1	Services de sécurité M.3016.2	Mécanismes de sécurité M.3016.3
REQ 15: chaque élément NE/MS devrait prendre en charge un type d'utilisateur par défaut, avec un ensemble minimal ou restrictif d'**actions de gestion**.	**SER 4**	**MEC 20-MEC 23**
REQ 16: chaque élément NE/MS devrait prendre en charge les **actions d'administration de sécurité essentielles** suivantes, la liste n'étant pas exhaustive: • définir et assigner des privilèges d'utilisateur et de groupe; • conserver un enregistrement de toutes les demandes d'identités de connexion au système; • ajouter et supprimer des identités d'utilisateur; • désactiver et activer l'utilisation d'identités d'utilisateur spécifiques comme identités de connexion; • initialiser et réinitialiser les mots de passe de connexion; • initialiser et modifier les clés de chiffrement; • fixer, pour le système, la durée de validité des mots de passe de connexion; • fixer, pour le système, le nombre maximal d'échecs de connexion pour chaque identité de connexion; • supprimer un verrouillage ou modifier la valeur de temporisation de verrouillage du système; • fixer la valeur de temporisation d'inactivité du système; • configurer la journalisation de sécurité et les alarmes de sécurité du système; • surveiller tous les journaux de sécurité du système; • gérer les processus de journalisation de sécurité du système; • mettre à jour les logiciels de sécurité; • terminer les sessions d'utilisateur ou de système; • déléguer des autorisations de sécurité à des personnes spécifiques assurant d'autres rôles; • établir les règles de complexité des mots de passe.	**SER 4, SER 8**	**MEC 20-MEC 23**

Prescriptions de sécurité M.3016.1	Services de sécurité M.3016.2	Mécanismes de sécurité M.3016.3
REQ 17: chaque élément NE/MS devrait prendre en charge les **actions de gestion** de sécurité d'application suivantes, la liste n'étant pas exhaustive: • définir et assigner de nouveaux privilèges d'utilisateur ou de groupe au niveau de l'application; • conserver un enregistrement de toutes les demandes d'identités de connexion à l'application; • ajouter et supprimer des utilisateurs au niveau de l'application; • surveiller tous les journaux de sécurité de l'application; • configurer la journalisation de sécurité et les alarmes de sécurité de l'application; • gérer les processus de journalisation de sécurité de l'application; • terminer les sessions d'application d'utilisateur.	**SER 4, SER 8**	**MEC 20-MEC 23**
REQ 18: les éléments NE/MS devraient procéder à une synchronisation temporelle de manière authentifiée (par exemple, NTP version 3).	**SER 8**	**N/A**
REQ 19: pour un élément NE/MS, chaque **action de gestion** devrait être associée à une seule SESSION autorisée.	**SER 4**	**MEC 20-MEC 23**
REQ 20: chaque SESSION devrait être établie par le biais d'une **authentification** appropriée, comme détaillé dans la prescription REQ 1.	**SER 1, SER 2, SER 3**	**MEC 1-MEC 12**
REQ 21: les communications entre un élément NE/MS et un serveur ACS aux fins d'acheminement des pouvoirs d'**authentification** devraient se faire sur une **connexion sécurisée**.	**SER 5, SER 6**	**MEC 19**
REQ 22: les éléments NE/MS devraient utiliser le **contrôle d'accès** et des partitions pour autoriser, refuser ou contrôler d'une manière ou d'une autre l'accès d'un utilisateur, d'un groupe d'utilisateurs ou d'un système distant aux éléments NE/MS et devraient assurer une fonctionnalité telle que les données, transactions et équipements utilisables par les utilisateurs soient restreints à ce qui leur est nécessaire pour remplir leur rôle. Les permissions d'accès devraient notamment être les suivantes: lecture seule et écriture seule, cette liste n'étant pas exhaustive.	**SER 4**	**MEC 20-MEC 23**
REQ 23: les éléments NE/MS devraient pouvoir assigner à chaque individu une identité d'utilisateur unique pour la connexion à une application ou à un serveur informatique.	**SER 1, SER 2, SER 3**	**MEC 7-MEC 11**

Prescriptions de sécurité M.3016.1	Services de sécurité M.3016.2	Mécanismes de sécurité M.3016.3
REQ 24: les éléments NE/MS devraient pouvoir, lorsque c'est nécessaire, obliger automatiquement l'utilisateur à modifier son mot de passe lors de son premier accès après l'établissement de son compte et lors de son premier accès après la réinitialisation de son mot de passe.	**SER 4**	**MEC 7-MEC 11**
REQ 25: les éléments NE/MS devraient empêcher, contrôler ou limiter l'utilisation active simultanée de la même identité d'utilisateur, selon le cas. Le nombre de sessions actives simultanément devrait être configurable sur la base de l'identité d'utilisateur.	**SER 1, SER 2, SER 3, SER 4**	**MEC 7-MEC 11**
REQ 26: une application d'élément NE/MS ne devrait pas nécessiter de privilèges d'accès de **superutilisateur** pour fonctionner correctement.	**SER 4**	**MEC 20-MEC 23**
REQ 27: les éléments NE/MS devraient pouvoir afficher à l'utilisateur, au cours du processus de connexion, les date et heure de sa dernière **authentification** réussie.	**SER 4, SER 8**	**MEC 7-MEC 11**
REQ 28: une déclaration d'exclusivité personnalisable et un avertissement de propriété privée devraient être affichés sur l'écran de saisie initial avant que tout accès logique ne soit autorisé. Les équipements devraient prendre en charge une longueur minimale de 1600 caractères. Un message par défaut devrait être fourni.	**SER 4**	**N/A**
REQ 29: pour tout échec d'une tentative de connexion, l'utilisateur devrait uniquement être avisé du fait que le processus de connexion a échoué ou qu'il n'est pas valide. Des informations telles que "identité d'utilisateur non valide" ou "mot de passe non valide" ne devraient pas être communiquées.	**SER 8**	**MEC 7-MEC 11**
REQ 30: les éléments NE/MS devraient **verrouiller** la connexion à partir d'un compte d'utilisateur après qu'un nombre maximal configurable d'échecs de connexion a été atteint. Le **verrouillage** devrait inclure l'interface de la console. Le **verrouillage** ne devrait PAS inclure le compte par défaut d'origine qui prend en charge toutes les actions de gestion.	**SER 4**	**MEC 7-MEC 11**
REQ 31: les éléments NE/MS ne devraient PAS avoir de mécanisme permettant de contourner l'**authentification** de connexion et les processus de connexion.	**SER 1, SER 2, SER 3**	**MEC 7-MEC 11**
REQ 32: les éléments NE/MS ne devraient jamais afficher un pouvoir en clair (mot de passe par exemple) sur quelque support que ce soit (écrans de terminal, copies papier par exemple) ni le stocker dans des journaux.	**SER 8**	**MEC 7-MEC 11**
REQ 33: les éléments NE/MS devraient appliquer une durée de validité configurable pour les mots de passe.	**SER 4**	**MEC 7-MEC 11**

Prescriptions de sécurité M.3016.1	Services de sécurité M.3016.2	Mécanismes de sécurité M.3016.3
REQ 34: si la durée de validité d'un mot de passe de connexion a expiré pour le système considéré, l'élément NE/MS devrait **verrouiller** la connexion pour l'identité d'utilisateur correspondante jusqu'à ce que le mot de passe soit correctement changé.	**SER 4**	**MEC 7-MEC 11**
REQ 35: si un compte reste inactif pendant une durée minimale configurable, l'élément NE/MS devrait envoyer une alerte.	**SER 4, SER 8, SER 9**	**MEC 7-MEC 11** **MEC 33-MEC 37**
REQ 36: si un compte reste inactif pendant une durée minimale configurable, l'élément NE/MS devrait désactiver le compte après avoir envoyé une alerte de désactivation. Le processus de DESACTIVATION ne devrait PAS inclure les comptes d'**administrateur de système**, d'**administrateur de sécurité de système** ni de **superutilisateur**.	**SER 4, SER 8**	**MEC 7-MEC 11** **MEC 20-MEC 23**
REQ 37: la réactivation d'une identité de connexion désactivée ne peut être opérée que par un administrateur correctement connecté auquel est assignée l'action d'administration de sécurité essentielle permettant d'initialiser et de réinitialiser les mots de passe de connexion.	**SER 4**	**MEC 7-MEC 11** **MEC 20-MEC 23**
REQ 38: la réinitialisation d'une identité de connexion VERROUILLEE et de la suppression de situation de verrouillage ne peuvent être opérées que par un administrateur correctement connecté auquel est assignée l'action d'administration de sécurité essentielle permettant de supprimer un verrouillage ou de modifier la valeur de temporisation de verrouillage du système.	**SER 4**	**MEC 7-MEC 11** **MEC 20-MEC 23**
REQ 39: chaque **session** établie correctement devrait être déconnectée par l'utilisateur ou par le système après une certaine période d'inactivité.	**SER 4**	**MEC 33-MEC 37**
REQ 40: un élément NE/MS devrait déconnecter une **session** établie correctement lorsque la durée écoulée depuis la dernière activité pour cette **session** a atteint la valeur de temporisation d'inactivité configurable du système.	**SER 4**	**MEC 7-MEC 11**
REQ 41: un type de rôle d'utilisateur devrait rester inchangé pendant toute la durée d'exécution d'une application d'élément NE/MS, jusqu'à ce qu'il soit mis fin à cette application.	**SER 4**	**MEC 20-MEC 23**
REQ 42: pour toutes les applications de chiffrement symétriques, la force des algorithmes devrait être conforme à la politique du pays, de l'entreprise ou de l'organisation.	**SER 5, SER 6**	**MEC 24-MEC 26**
REQ 43: pour toutes les applications de chiffrement asymétriques, la force des algorithmes devrait être conforme à la politique du pays, de l'entreprise ou de l'organisation.	**SER 5, SER 6**	**MEC 27-MEC 28**
REQ 44: pour toutes les applications d'échange de clés, la force des algorithmes devrait être conforme à la politique du pays, de l'entreprise ou de l'organisation.	**SER 5, SER 6**	**MEC 38-MEC 40**

Prescriptions de sécurité M.3016.1	Services de sécurité M.3016.2	Mécanismes de sécurité M.3016.3
REQ 45: pour chaque interface physique ou logique d'élément NE/MS qui achemine du **trafic de gestion**, l'élément NE/MS devrait pouvoir être configurée de manière à sécuriser le **trafic de gestion** au moyen d'une **authentification forte** et d'une protection cryptographique afin d'assurer la confidentialité, l'intégrité et la protection "antirejeu".	**SER 2, SER 3, SER 5, SER 6**	**MEC 24-MEC 32**
REQ 46: tout mot de passe en clair ne devrait être transmis que par le biais d'une **connexion sécurisée**, sauf en cas de recours à un mécanisme avec mots de passe à utilisation unique, auquel cas les mots de passe à utilisation unique peuvent être envoyés en clair à condition qu'il n'y ait pas de serveur intermédiaire.	**SER 1, SER 2, SER 3, SER 5, SER 6**	**MEC 19**
REQ 47: pour toutes les applications de protection de l'intégrité des données par une méthode symétrique, la force des algorithmes devrait être conforme à la politique du pays, de l'entreprise ou de l'organisation.	**SER 5**	**MEC 29-MEC 30**
REQ 48: pour toutes les applications de protection de l'intégrité des données par une méthode asymétrique, la force des algorithmes devrait être conforme à la politique du pays, de l'entreprise ou de l'organisation.	**SER 5**	**MEC 31-MEC 32**
REQ 49: tous les logiciels fournis à un fournisseur de services ou à un autre client devraient inclure, en fonction des besoins, des mécanismes d'**authentification** par chiffrement et de protection de l'intégrité (signatures numériques ou **authentification** de message par une méthode symétrique par exemple) tels que spécifiés dans la Rec. UIT-T M.3016.3.	**SER 7**	**MEC 29-MEC 32**
REQ 50: tous les éléments NE/MS recevant des logiciels devraient pouvoir interpréter les mécanismes d'**authentification** par chiffrement et de protection de l'intégrité et pouvoir vérifier la source et l'intégrité des logiciels, en fonction des besoins.	**SER 7**	**MEC 29-MEC 32**
REQ 51: toutes les mises à jour de logiciels, y compris les programmes de correction, devraient être transmises par le biais d'une **connexion sécurisée** aux éléments NE/MS destinés à les recevoir.	**SER 5, SER 6**	**MEC 19**
REQ 52: tous les éléments NE/MS devraient pouvoir empêcher à toute entité de nier être responsable des actions qu'elle a effectuées et de leurs effets.	**SER 7**	**MEC 29-MEC 32**
REQ 53: les éléments NE/MS devraient pouvoir journaliser toute action qui modifie les attributs et les services de sécurité, les contrôles d'accès et les paramètres de configuration des dispositifs ainsi que chaque tentative de connexion ayant entraîné l'invocation de la temporisation d'inactivité du système définie dans la prescription REQ 12 et son résultat.	**SER 8**	**MEC 33-MEC 37**

Prescriptions de sécurité M.3016.1	Services de sécurité M.3016.2	Mécanismes de sécurité M.3016.3
REQ 54: les éléments NE/MS devraient pouvoir configurer les **actions d'administration de sécurité essentielles** qui doivent être incluses dans le journal de sécurité.	**SER 4**	**MEC 33-MEC 37**
REQ 55: les éléments NE/MS devraient pouvoir journaliser chaque tentative de connexion et son résultat, chaque déconnexion ou terminaison de session (à distance ou depuis la console).	**SER 8**	**MEC 33-MEC 37**
REQ 56: les éléments NE/MS devraient pouvoir procéder à une journalisation à distance par le biais d'une **connexion sécurisée**.	**SER 5, SER 6, SER 8**	**MEC 33-MEC 37** **MEC 19**
REQ 57: chaque entrée de journal devrait contenir les informations suivantes: • une description de l'action ou l'action proprement dite qui fait l'objet de la journalisation; • l'identité et le niveau de sécurité de l'utilisateur ou du processus qui a lancé l'action; • les date et heure auxquelles l'action s'est produite; • des informations d'origine et de destination de réseau, si c'est applicable (par exemple au moment de la connexion); • une indication du succès ou de l'échec de l'activité.	**SER 8**	**MEC 33-MEC 37**
REQ 58: tous les éléments NE/MS devraient pouvoir envoyer des alarmes pour certains événements sélectionnés.	**SER 9**	**MEC 41**
REQ 59: tous les éléments NE/MS devraient pouvoir permettre à l'utilisateur de définir les critères de sélection des événements qui entraînent l'envoi d'alarmes.	**SER 9**	**MEC 41**
REQ 60: tous les éléments NE/MS avec connectivité fondée sur les paquets devraient interdire le trafic qui ne satisfait pas à la politique de sécurité du RCD.	**SER 10**	**MEC 42**

Appendice I

Autres considérations relatives à la sécurité

Les procédures de sécurité détaillées dans les paragraphes qui suivent sont de nature didactique. Elles sortent du cadre des prescriptions détaillées définies dans la présente Recommandation, mais devraient être prises en considération lorsqu'il s'agit de sécuriser un système. Certaines dispositions apparaissent comme étant à caractère obligatoire, mais elles ne sont fournies qu'à titre d'information et d'exemple. Les protocoles et recommandations figurant dans le présent appendice feront l'objet d'examens et de contributions dans l'avenir. Ils ne visent aucunement à inclure ou à exclure un contenu particulier dans les normes existantes ou à venir.

I.1 Applicabilité à l'exploitation, à l'administration, à la maintenance et à la fourniture dans les entreprises

Les réseaux d'entreprise isolés traditionnels appartiennent au passé. Les entreprises actuelles sont réparties en plusieurs sites, pouvant couvrir de grandes zones géographiques et nécessitant des connexions de réseau extranet avec leurs clients et leurs partenaires. Les entreprises doivent offrir à leurs partenaires et à leurs clients un accès à leurs données internes et prendre des décisions opérationnelles sur la base de ces données.

Les réseaux d'entreprise sont développés et administrés par l'entreprise proprement dite ou sont achetés sous forme de réseau géré auprès d'un fournisseur de réseau, qui offre à l'entreprise des services lui permettant de gérer sa partie de l'environnement de réseau.

Dans certains cas, le fournisseur de réseau doit pouvoir accéder aux données de dérangement et de performance et doit pouvoir configurer divers composants du réseau, d'où la nécessité de mettre en place des mécanismes de sécurité appropriés. Ces mécanismes doivent offrir un contrôle approprié afin de protéger non seulement le réseau géré de l'entreprise mais aussi le réseau interne propre du fournisseur. Le réseau interne peut être interconnecté à ce type de réseau d'entreprise et peut faire partie de l'infrastructure de télécommunications. Pour résumer, les prescriptions de sécurité applicables au trafic d'exploitation, d'administration, de maintenance et de fourniture formulées dans la présente Recommandation s'appliquent entièrement aux réseaux des entreprises et des fournisseurs de services/exploitants.

I.2 Architecture de courtier commun de requête sur des objets, protocole simple de gestion de réseau, langage de balisage extensible et protocole simplifié d'accès aux objets

Il convient de tenir compte des considérations de sécurité suivantes en ce qui concerne l'architecture de courtier commun de requête sur des objets (CORBA, *common object request broker architecture*), le protocole simple de gestion de réseau (SNMP, *simple network management protocol*), le langage de balisage extensible (XML, *extensible markup language*) et le protocole simple d'accès aux objets (SOAP, *simple object access protocol*). Par ailleurs, d'autres protocoles peuvent tout aussi bien s'appliquer (protocole d'échange extensible par blocs (BEEP, *blocks extensible exchange protocol*) par exemple). Bien qu'aucune modification de ces protocoles en évolution ne soit proposée, on peut tenir compte des considérations suivantes pour améliorer la sécurité.

I.2.1 CORBA

Le service de sécurité CORBA comprend les fonctionnalités d'authentification des parties (utilisateurs humains et objets), d'autorisation d'accès aux objets par les parties, d'audit de sécurité, de sécurité des communications, de non-répudiation et d'administration. L'ensemble de ces fonctionnalités peut être exagéré pour de nombreuses applications. En effet, certaines applications

pourront avoir besoin uniquement des fonctionnalités de sécurisation des communications et d'authentification au niveau du système fondées sur la technologie (TLS, *transport layer security*) – et sur la technologie d'origine (SSL, *secure socket layer*) – pour des raisons de disponibilité et de simplicité. D'autres applications pourront n'avoir besoin d'aucune sécurité. Les prescriptions facultatives ci-dessous correspondent à trois choix possibles:

– absence de sécurité;

– les courtiers de requête sur des objets (ORB, *object request brokers*) utilisent TLS (ou SSL) pour assurer la sécurité des communications et l'authentification au niveau du système, ce qui correspond à une sécurité de "session";

– les courtiers ORB utilisent le service de sécurité CORBA pour assurer la sécurité des communications, l'authentification et la non-répudiation et pour fournir des listes de contrôle d'accès pour les groupes ou individus accédant à des opérations ou des objets individuels.

Pour plus d'informations sur la sécurité dans le cadre de l'architecture CORBA, on pourra se reporter aux Recommandations UIT-T Q.816, *Services RGT à architecture CORBA* et Q.816.1, *Services RGT à architecture CORBA: extensions pour la prise en charge des interfaces à granularité grossière*.

Si l'architecture CORBA est utilisée dans les interfaces entre éléments NE/MS, il convient d'appliquer les mécanismes de sécurité CORBA. Le niveau de sécurité de l'architecture CORBA implémentée devrait être clair. Dans la suite, des indications sont fournies concernant la sécurité CORBA. Elles ne visent pas à tenter d'identifier des normes. Lors de la fourniture de produits ou de systèmes fondés sur l'architecture CORBA, les niveaux de sécurité de base sont les suivants:

– niveau 0: aucune sécurité n'est assurée au niveau des applications et les programmes ne sont pas sécurisés. Il convient de prévoir une authentification, un chiffrement, une protection de l'intégrité des données, une autorisation d'invocation d'objet, des traces d'audit et une administration du domaine de sécurité;

– niveau 1: les programmes sont sécurisables, ce qui signifie qu'ils peuvent appeler une interface de programmation d'application pour accéder à des services additionnels tels que la vérification des signatures, le contrôle d'accès aux objets et l'enregistrement d'audit;

– niveau 2: une prise en charge des signatures numériques est assurée, permettant la signature et la non-répudiation des transactions. Ceci est particulièrement important en cas de collaborations entre diverses organisations (par exemple, dans un contexte interentreprises ou dans le cadre d'accords entre homologues pour la gestion de réseau).

La Spécification CSI (*common secure interoperability*) définit plusieurs niveaux d'interopérabilité sécurisée associés à l'utilisation du protocole inter-ORB général ou du protocole inter-ORB Internet:

– Niveau 1 CSI: l'identité de la partie initiatrice est communiquée au récepteur par l'émetteur.

– Niveau 2 CSI: l'identité de la partie initiatrice est communiquée au récepteur par l'émetteur, mais cette identité peut être déléguée à d'autres objets de manière à ce que ces derniers puissent se faire passer pour l'utilisateur.

– Niveau 3 CSI: en plus de la transmission de l'identité, les attributs de la partie initiatrice transmis du client à la cible peuvent inclure d'autres informations d'autorisation (appartenance à un rôle ou à un groupe par exemple).

Il appartient aux fournisseurs de:

– bien connaître toutes les capacités de sécurité de la technologie ORB choisie;

– vérifier que cette technologie satisfait aux prescriptions de sécurité formulées dans la présente Recommandation.

Comme son nom l'indique, l'architecture CORBA se rapporte à des objets. Assurer la sécurité des objets consiste à empêcher leur utilisation non autorisée en appliquant un ensemble de règles de contrôle d'accès. La sécurité CORBA permet de garantir que les actions des utilisateurs relatives à un objet leur sont imputables et de garantir la disponibilité des objets.

La sécurité des objets diffère de la sécurité par de nombreux autres aspects. Souvent, le développeur n'a pas besoin de connaître les détails relatifs à la sécurité car la sécurité est appliquée à une étape ultérieure par exemple avec un enveloppeur. Certains aspects sont extrêmement importants. Dans l'architecture CORBA, les noms peuvent être multiples ou peuvent ne pas exister du tout, auquel cas seuls les numéros de référence existent. Il faut donc pouvoir définir une politique relative à des objets sans connaître le nom des objets. De même, il faut pouvoir définir une politique relative à des objets ayant de nombreux noms et pouvoir appliquer la politique indépendamment du nom utilisé pour sécuriser un objet donné.

Les systèmes orientés objet comportent généralement des dizaines de milliers d'objets, et il n'est pas raisonnable de s'attendre à ce que la sécurité soit définie individuellement pour chaque objet. Il faut donc pouvoir regrouper les objets et définir une politique pour chaque groupe d'objets dont les besoins de protection sont analogues.

– *Authentification de bout en bout:* l'architecture CORBA permet la transmission du contexte de l'utilisateur à une autre application. Lorsqu'une relation de confiance forte a été établie entre les systèmes considérés, il peut être possible d'accepter ces informations sans autre vérification. Toutefois, lorsque ce n'est pas le cas, il peut être nécessaire de coupler étroitement la sécurité des systèmes et la sécurité CORBA. L'authentification de bout en bout est très importante et il est utile de vérifier si le fournisseur la prend en charge.
– *Contrôle d'accès:* l'architecture CORBA prend en charge le principe de la connexion fondée sur le rôle. Les systèmes devraient toujours être développés sur la base de ce principe, qui permet non seulement de réduire les coûts d'administration mais aussi de simplifier cette administration, ce qui signifie que la configuration est moins susceptible de comporter des erreurs.
– *Chiffrement:* l'utilisation du chiffrement dans l'architecture CORBA doit être conforme aux prescriptions formulées dans la présente Recommandation. Il convient d'utiliser toutes les fonctionnalités CORBA relatives à l'intégrité, à la confidentialité et à l'authentification de l'origine, notamment pour les communications sur un réseau de n'importe quel type.
– *Administration des politiques:* l'administration des politiques CORBA est chargée de définir les informations relatives à la politique d'accès aux objets, à la politique de protection des messages et à la politique d'audit, pour les domaines, les utilisateurs et les rôles. Tous les aspects de nommage des domaines et des objets doivent être spécifiés clairement. Les rôles doivent être définis clairement de façon à pouvoir séparer correctement les tâches.

I.2.2 Sécurité SNMP

Le protocole SNMP, qui est largement utilisé pour l'administration de divers équipements avec processeur, permet:

– d'obtenir des paramètres de configuration de dispositif;
– de fixer des paramètres de configuration de dispositif;
– d'envoyer des alertes depuis le dispositif géré vers un système d'analyse central.

Bon nombre de mises en œuvre du protocole SNMP présentent des vulnérabilités de sécurité importantes. Dans les versions 1 et 2 du protocole SNMP, le mot de passe (appelé chaîne de communauté) est transmis en clair. De plus, bien que des contrôles puissent être faits pour valider l'adresse IP du client, un attaquant modérément déterminé peut usurper des adresses IP. 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. La Commission d'études 4 de l'UIT-T étudie actuellement l'établissement de deux nouvelles piles de protocoles:

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

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. Il convient d'envisager de prendre les mesures suivantes pour sécuriser l'accès SNMPv3 aux éléments de réseau:

– un agent SNMP devrait envoyer une alerte à un gestionnaire s'il reçoit une commande provenant d'une source inconnue;
– il convient d'utiliser des contrôles d'accès afin d'autoriser uniquement les messages SNMP provenant d'un gestionnaire autorisé. Les messages SNMP provenant de toutes les autres sources devraient être refusés et traités conformément à des politiques de sécurité appropriées. Il peut être souhaitable de bloquer les demandes non autorisées au niveau du dispositif et au niveau du périmètre de réseau;
– il convient de ne pas utiliser la chaîne de communauté par défaut;
– il convient de journaliser les transgressions d'accès et les erreurs d'accès;
– par défaut, le protocole SNMPv3 utilise l'algorithme (DES, *data encryption standard*), mais des algorithmes davantage sécurisés peuvent être utilisés;
– 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;
– la journalisation par agents SNMP devrait être activée;
– tout service ou toute capacité qui n'est pas explicitement requis devrait être désactivé, y compris le protocole SNMP s'il est activé.

I.2.3 XML

La norme XML spécifie un langage pour la définition de structures de données. La version actuelle est la version 1.0. La version 1.1 fait l'objet d'une Recommandation actuellement à l'état de projet. Le Comité technique relatif aux services de sécurité d'OASIS (*Organization for the Advancement of Structured Information Standards*) cherche à élargir la fonctionnalité de sécurité sur la base du langage XML. OASIS finalise actuellement la définition du langage SAML (*security assertion markup language*), qui est fondé sur quatre assertions:

– *authentification* – authentification de l'objet par l'émetteur;
– *attribut* – identificateur uniforme de ressource ou schéma d'extension particulier;
– *décision* – indication de validité de l'authentification;
– *autorisation* – permission d'accéder à la ou aux ressources.

Les assertions XML doivent comprendre les éléments suivants:

– *information de base* – identificateur ou nom unique donné à l'assertion, comprenant généralement les dates et heure de création et la durée de validité;
– *déclaration* – document décrivant l'utilisation de l'assertion;
– *condition* – conditions éventuelles de validité de l'assertion;

– *avis* – informations additionnelles, par exemple assertions utilisées pour arrêter une décision politique.

I.2.4 SOAP

La version 1.1 du protocole SOAP est la version actuellement recommandée par le World Wide Web Consortium. Elle spécifie un format de message qui n'est pas lié à un protocole particulier. Le protocole de transfert hypertexte (HTTP, *hypertext transfer protocol*) est le protocole le plus souvent utilisé, mais d'autres protocoles peuvent être utilisés (SMTP ou FTP par exemple). Lorsque le protocole SOAP est utilisé avec le protocole HTTP, le pare-feu voit le protocole SOAP comme s'il s'agissait du protocole HTTP et l'autorisera généralement à passer. Le pare-feu pourrait filtrer le protocole SOAP, même s'il ne le connaît pas. Toutefois, ce filtrage est difficile et source d'erreurs. La difficulté vient du fait que le chiffrement peut cacher le contenu et le contexte des données transportées (autrement dit XML) et que le protocole SOAP ne possède pas de mécanisme d'adressage ou de structure interne uniforme (autrement dit, les en-têtes et les noms de méthode sont facultatifs).

I.3 Surveillance électronique autorisée légalement

Les exploitants de télécommunications devraient tenir compte des considérations de sécurité suivantes en ce qui concerne l'implémentation de la surveillance électronique autorisée légalement (LAES, *lawfully authorized electronic surveillance*).

Les prescriptions de sécurité pour les activités de surveillance LAES devraient être rigoureuses et identiques à celles qui sont formulées pour les éléments de réseau, systèmes support d'exploitation (OSS) et systèmes de gestion essentiels, aux exceptions près qui suivent. Ces prescriptions se rapportent à la nécessité de maintenir la confidentialité des activités LAES.

– seuls les employés autorisés participeront aux activités LAES;
– les informations liées à la surveillance LAES (identité de la cible, autorités de police impliquées, contenu de l'appel et identification de l'appel, etc.) seront protégées contre toute divulgation au personnel non autorisé;
– seul le personnel autorisé aura accès aux commandes et processus de surveillance LAES;
– une liste du personnel autorisé à accéder aux activités, processus et procédures de surveillance LAES, à les mettre à jour, à les administrer et à les gérer sera tenue à jour;
– les activités, politiques et procédures liées à la sécurité dans le cadre de la surveillance LAES feront l'objet d'une documentation appropriée, qui sera transmise au personnel autorisé;
– les journaux de sécurité et enregistrements d'activité liés à la surveillance LAES seront mis à jour et stockés dans une installation sécurisée;
– un processus documenté rigoureux sera implémenté pour identifier et authentifier les autorités de police et traiter les demandes de surveillance LAES.

I.4 Considérations relatives à la sécurité physique

Il convient de tenir compte des considérations suivantes en matière de sécurité physique. Lors de l'établissement des prescriptions de sécurité, la sécurité physique est une composante importante. Dans la plupart des architectures de sécurité, il est supposé que l'environnement physique est protégé. Par le passé, tous les éléments de réseau étaient contenus dans les bâtiments des centres de commutation. Dans ces bâtiments, les employés chargés de l'exploitation de la fourniture, de l'administration et de la maintenance de ces équipements assuraient une permanence 24 heures sur 24. Ils se connaissaient et les étrangers ne pouvaient pas accéder aux sites sans que quelqu'un les remarque et les questionne. A l'heure actuelle, l'environnement est très différent. Les équipements hertziens ont tendance à être installés à l'extérieur dans un environnement peu sûr. Par ailleurs, de

nombreux centraux, si ce n'est tous, sont sans personnel et sombres la plupart du temps. Des équipes et des individus itinérants sont chargés par un établissement central d'effectuer les améliorations et les tâches de maintenance programmées. Aujourd'hui, il est rare que des gardes de sécurité assurent une permanence 24 heures sur 24 et 7 jours sur 7. Le personnel s'occupant des installations extérieures utilise également les centraux pour se réunir et pour stocker outils et équipements. Les caractéristiques d'une installation sécurisée sont les suivantes:

– toutes les entrées et sorties de personnel sont journalisées et enregistrées.
– les fournisseurs et le personnel colocalisé sont contrôlés et leurs entrées et sorties sont journalisées et enregistrées;
– l'accès physique aux éléments de réseaux est restreint aux employés autorisés;
– le personnel colocalisé est assujetti aux mêmes conditions d'accès que le fournisseur de services d'origine;
– toute personne qui bénéficie d'un accès physique légitime au bâtiment ne dispose d'un accès logique aux éléments de réseau, consoles et systèmes OSS des dispositifs d'accès au réseau qu'après avoir procédé à une authentification protégée;
– les accès non autorisés feront l'objet d'une détection et d'une réaction rapides;
– des services tels qu'eau, électricité et télécommunications seront disponibles;
– les sites sont surveillés par un personnel de sécurité itinérant aléatoire, par des systèmes d'alarme qui surveillent et enregistrent les ouvertures et fermetures de portes et de fenêtres, par des détecteurs de mouvement et des détecteurs infrarouge ainsi que par des systèmes de télévidéosurveillance des endroits critiques;
– la conservation des données et des journaux de surveillance devrait être documentée, la durée de conservation étant fonction du niveau de risque.

Les paragraphes qui suivent contiennent des informations additionnelles concernant la sécurité physique. On trouvera une description détaillée des questions relatives à la sécurité physique dans le document *Public Switched Network Security Assessment Guidelines* de septembre 2000 du National Communication System.

I.4.1 Sécurité physique des locaux

Généralement, les organisations implémenteront divers niveaux de contrôle d'accès aux bâtiments en fonction de l'importance des ressources présentes dans l'installation considérée. Souvent, les grandes entreprises construiront des installations distinctes hautement sécurisées pour les composants de réseau critiques (commutateurs ou centres de données par exemple). Le niveau de sécurité est déterminé en fonction de l'importance des ressources présentes, pendant une phase de découverte et d'évaluation des ressources. Les paragraphes qui suivent portent sur les éléments à évaluer pour une installation hébergeant des ressources critiques ou très importantes. Une évaluation moins poussée sera faite pour les installations moins sensibles. L'évaluation globale de la sécurité physique doit permettre de déterminer le niveau de protection nécessaire et la qualité relative des mécanismes de protection en place.

I.4.1.1 Sécurité générale des bâtiments

Même si les portes et les fenêtres d'un bâtiment sont généralement considérées comme étant ses points d'accès principaux, d'autres points (par exemple, trous d'aération, points d'entrée pour l'eau, le gaz, les télécommunications et l'électricité, conduits d'écoulement des eaux) doivent être pris en considération, en fonction du type de menaces. D'autres points d'entrée encore (chambres de câbles de centre de commutation, par exemple) doivent être pris en considération, s'il y a un risque que des dommages puissent être causés. En outre, il faut s'intéresser à l'espace tampon autour du bâtiment qui n'est pas accessible au public et qui constitue la première couche de défense du périmètre. Des pelouses, des aménagements paysagers, un éclairage et des clôtures peuvent être envisagés dans cet

espace afin de ralentir ou d'empêcher les approches clandestines. Des barrières physiques (poteaux en béton ou grands pots d'aménagements paysagers en béton, par exemple) peuvent être utilisées pour empêcher l'approche de voitures, de camions ou d'autres véhicules avec intention de nuire. Des caméras extérieures et d'autres matériels de surveillance permettent d'améliorer encore ou d'élargir cet espace tampon.

I.4.1.2 Gardes, fermetures à clé et badges d'identification

Des gardes protègent le périmètre extérieur du bâtiment et parfois des zones intérieures. Pour les installations critiques, les vérifications à faire sont les suivantes:

- toutes les portes donnant accès à l'installation sont en permanence fermées à clé ou gardées;
- toutes les portes qui ne sont normalement pas utilisées (sorties d'urgence, par exemple) sont pourvues d'une alarme. Il convient de s'assurer que les alarmes fonctionnent correctement et qu'il existe des procédures de réaction en cas d'alarme;
- les portes sont installées correctement de manière à ne pas pouvoir être retirées de l'extérieur (par exemple, les gonds et les verrous sont protégés contre tout sabotage depuis l'extérieur);
- pendant les périodes de pointe d'entrée et de sortie, un garde est présent aux entrées et sorties. En dehors de ces périodes, les portes devraient être surveillées et une autre forme de contrôle d'accès devrait être appliquée (cartes magnétiques, cartes de proximité, clés, par exemple);
- pour l'accès par les portes non gardées, un mécanisme d'identification est en place;
- les portes non gardées pourvues d'une fermeture à clé ou d'un autre moyen de fermeture ont des mécanismes permettant d'empêcher le "passage en double"[5]. On peut utiliser des pièges à homme, des portes tournantes et des détecteurs pour empêcher le passage en double et envoyer une alarme lorsqu'un passage en double a lieu;
- les compétences et la formation requises pour les gardes ainsi que les méthodes utilisées pour les stabiliser dans leur emploi sont adéquates et appropriées. Ceci est particulièrement important pour les services de garde sous contrat, qui sont monnaie courante;
- les employés, les fournisseurs présents sur le site, les personnes sous contrat et les autres individus autorisés possèdent un badge et le portent en permanence lorsqu'ils sont à l'intérieur du bâtiment;
- un identificateur temporaire (par exemple un laissez-passer) est remis aux visiteurs, qui sont tenus de le porter de manière visible;
- il existe des procédures et des conditions applicables aux visiteurs qui peuvent entrer et travailler sans escorte et des conditions applicables à ceux qui doivent être escortés;
- les badges des employés comportent une photo en couleur. La photo doit être suffisamment grande pour que l'employé n'ait pas à tendre le badge à un garde pour que celui-ci puisse la voir. Les badges doivent être établis de manière à ne pas pouvoir modifier ou remplacer la photo. La photo doit être suffisamment claire pour que le garde puisse la comparer au visage du porteur du badge;
- le nom de l'employé et d'autres informations d'identification éventuelles (numéro ou code barre par exemple) figurent clairement sur le badge;
- les badges comportent un signe ou une indication permettant de faire la distinction entre les employés et les autres personnes qui ont accès au bâtiment;

---

5 Le passage en double est le franchissement d'une porte par une personne non autorisée juste derrière une personne autorisée qui a ouvert la porte.

– les badges sont, autant que possible, durables et résistants à l'usure, aux endommagements et aux altérations;
– les badges contiennent les informations électroniques ou magnétiques éventuellement nécessaires aux lecteurs de cartes;
– les badges peuvent inclure une puce contenant des informations additionnelles (données biométriques ou certificats X.509, par exemple);
– les systèmes d'authentification et d'autorisation de badge devraient être reliés à un répertoire de sécurité central de manière à pouvoir modifier ou supprimer immédiatement des privilèges d'accès;
– les badges permettent de limiter l'accès à certaines parties de l'enceinte de l'entreprise et non à la totalité, lorsque c'est utile;
– les badges comportent une adresse à laquelle ils peuvent être envoyés par la poste sans affranchissement, au cas où ils seraient perdus par leur porteur et retrouvés par quelqu'un d'autre;
– les services de sécurité de l'entreprise ou des bâtiments peuvent désactiver ou annuler la validité de tout badge qui a été perdu ou dont le porteur n'est plus autorisé à pénétrer dans les bâtiments ou dans l'enceinte de l'entreprise;
– lorsque le porteur d'un badge est arrivé en fin de contrat, une personne (gestionnaire, garde de bâtiment, services de sécurité de l'entreprise) conservera ou détruira le badge de manière à ce qu'il ne puisse pas être utilisé illégalement.

Les gardes ne sont pas les seules personnes chargées de préserver la sécurité à l'intérieur d'un bâtiment. Les occupants autorisés permettent souvent d'améliorer la sécurité grâce à leur vigilance et à leur surveillance passive. L'évaluation doit permettre de déterminer si le personnel a été habilité à interroger le personnel non autorisé dans les zones surveillées. Un test de pénétration peut être utile pour déterminer dans quelle mesure les gardes et les employés sont correctement formés à l'importance de la sécurité physique. Les examinateurs peuvent tenter de passer furtivement ou en parlant entre eux devant les gardes ou encore de ruser auprès d'employés pour que ceux-ci leur permettent d'entrer par des accès non gardés.

I.4.1.3 Administration des clés physiques et des clés logiques

Les clés physiques traditionnelles sont rarement utilisées dans les installations sensibles car elles sont difficiles à inventorier et à récupérer et elles ne permettent pas de fournir une trace d'audit de l'utilisateur. Souvent, l'utilisation de clés physiques est limitée à l'accès à certaines parties du bâtiment (débarras, salles d'entrepôt et armoires de câbles par exemple). Mais certaines entreprises et installations continuent à utiliser des serrures avec clé comme moyen principal d'entrée dans les bâtiments ou d'accès dans des zones critiques des bâtiments. Dans ce cas, il faut s'assurer:

– qu'il existe des procédures relatives à l'autorisation de la distribution de clés aux individus, y compris le contrôle des clés et la journalisation de l'accès et de la distribution;
– que les clés sont numérotées individuellement;
– qu'un inventaire complet des clés et de leur propriétaire est tenu à jour et fait l'objet d'audits;
– que des critères sont définis pour le remplacement de serrures lorsque des clés sont perdues;
– que des audits de l'inventaire des clés sont réalisés périodiquement et qu'il existe des procédures permettant de remédier aux problèmes;
– qu'il existe des procédures permettant de récupérer les clés lorsque l'accès n'est plus nécessaire ou que les autorisations ont changé.

Les procédures associées aux clés logiques (cartes de proximité, par exemple) doivent être évaluées par rapport aux mêmes critères. La récupération des clés, l'enregistrement des entrées et des sorties

et les procédures d'autorisation sont simplifiés avec les systèmes de clés logiques car ceux-ci permettent une centralisation de la surveillance des utilisations, de l'assignation des autorisations et de la désactivation des clés. Mais des procédures restent nécessaires pour faire en sorte que les personnes chargées de la tenue à jour de l'inventaire des clés et de la base de données des autorisations reçoivent une notification lorsque des individus partent ou que leurs prescriptions d'accès changent. Les serrures à combinaisons, qui constituent un cas particulier de serrures logiques, doivent être évaluées afin de vérifier que les combinaisons ne peuvent pas être devinées du fait d'usures ou de combinaisons écrites. Les combinaisons doivent être modifiées si les autorisations d'entrée changent.

I.4.1.4 Séparation fonctionnelle des installations et contrôle d'accès multiniveaux

La sécurité physique s'applique aux parties à l'intérieur d'un bâtiment ainsi qu'au périmètre extérieur. L'accès aux parties intérieures qui sont considérées comme sensibles ou critiques sur le plan de l'exploitation doit être contrôlé lorsqu'il est limité pour une raison ou pour une autre (par exemple, lorsque des données ou des équipements sensibles sont contenus dans ces parties intérieures ou que des expériences sensibles y sont menées). D'une manière générale:

– les installations informatiques et de réseau critiques devraient être mises dans des zones pourvues de mécanismes de contrôle d'accès physique distincts. L'accès ne devrait être accordé qu'à ceux qui en ont besoin;
– il devrait exister des procédures permettant de garantir que les informations propriétaires sont conservées dans des installations sécurisées lorsqu'elles ne sont pas utilisées. Les bureaux et les salles de fichiers où ces informations sont conservées devraient être fermés à clé, de même que les armoires qui contiennent de telles informations;
– tous les points d'accès potentiels aux installations informatiques et de réseau critiques (consoles, centres d'exploitation, par exemple) devraient faire l'objet d'un contrôle proportionné au contrôle mis en place pour les installations proprement dites;
– il convient d'enregistrer les accès à tous ces espaces contrôlés;
– les supports de stockage contenant des informations critiques devraient être chiffrés ou placés dans des zones à accès limité et fermées à clé;
– l'adresse physique d'un système critique ne doit pas être divulguée à ceux qui n'ont pas besoin de la connaître.

La surveillance des zones à l'intérieur d'un bâtiment peut être améliorée par le recours à différents rôles et différentes responsabilités. A titre d'exemple, le personnel administratif n'a pas besoin d'accéder aux salles informatiques d'une organisation. De même, les ingénieurs n'ont généralement pas besoin d'accéder à la salle de contrôle des documents. L'évaluation doit permettre de déterminer si la séparation fonctionnelle existante est appropriée. De plus, une clé d'entrée double ou des serrures à combinaisons peuvent être utilisées en fonction du niveau de risque.

I.4.2 Services disponibles dans les bâtiments

Le fonctionnement d'une organisation dépend très fortement de la disponibilité de services comme l'eau, l'électricité, les télécommunications et l'évacuation des déchets.

I.4.2.1 Services d'utilité publique (eau, électricité, télécommunications et évacuation des déchets)

Sans les services d'eau, électricité, télécommunications et évacuation des déchets, une organisation ne peut pas fonctionner efficacement, voire ne peut pas fonctionner du tout. La dépendance vis-à-vis de ces services est souvent sous-estimée. Les réactions prévues par l'organisation en cas d'interruption de l'un de ces services doivent être évaluées. En ce qui concerne les services indispensables pour que l'organisation puisse remplir en permanence sa fonction, les étapes suivantes sont essentielles:

– les alimentations électriques devraient être doublées et placées dans des endroits géographiques différents pour éviter toute interruption de courant accidentelle;
– une alimentation électrique de secours devrait être disponible pour permettre à l'organisation de continuer à fonctionner pendant les longues pannes d'électricité. Une capacité de production d'énergie électrique devrait pouvoir être opérationnelle avant que les réserves d'urgence ne soient épuisées. (L'organisation peut posséder des groupes électrogènes mobiles ou en disposer contractuellement.);
– il convient de disposer sur le site de réservoirs d'eau suffisants (ou de services de fourniture appropriés) pour que les composants critiques de l'installation puissent fonctionner en permanence;
– les systèmes de communications avec l'extérieur doivent comporter des moyens de secours actifs, ou doivent être suffisamment robustes pour pouvoir fonctionner en période de crise, tout comme les systèmes de communications internes. La capacité devrait être suffisante pour pouvoir traiter le trafic lié aux crises;
– toilettes et égouts doivent fonctionner pendant les crises ou des arrangements temporaires doivent être prévus (au moins contractuellement) et doivent pouvoir être activés rapidement;
– il faut prévoir un système de secours pour la climatisation des salles informatiques et des autres zones nécessitant un environnement contrôlé afin d'éviter que des machines ne tombent en panne ou soient endommagées par une surchauffe;
– des conteneurs fermant à clé pour l'évacuation et la destruction d'informations propriétaires devraient être disponibles facilement quel que soit l'endroit où ces informations sont utilisées. Au cours de l'évaluation, il convient d'établir le chemin d'évacuation de ces informations et de vérifier qu'il est bien fermé.

Dans le cadre de l'évaluation, on s'intéresse aussi à la distribution de ces services à l'intérieur des bâtiments. Il convient d'évaluer la résistance globale des installations à une interruption de service, depuis l'origine du service chez le fournisseur jusqu'aux conduits de distribution à l'intérieur des bâtiments.

I.4.2.2 Installations d'urgence

Au cours de l'évaluation, il convient d'évaluer l'adéquation des installations d'urgence (détection et suppression des incendies, par exemple), des systèmes de conditionnement d'énergie, de climatisation et de ventilation ainsi que des autres systèmes de protection de l'environnement nécessaires au fonctionnement permanent des systèmes critiques. La réaction de ces systèmes doit être telle que

– les personnes puissent évacuer les locaux;
– les équipements puissent être protégés (au moins jusqu'à l'arrivée de pompiers ou d'autres personnes);
– les installations puissent conserver leur intégrité structurelle;
– le contenu du bâtiment puisse être protégé de l'environnement extérieur, autant que possible.

Cela met en évidence le fait que les installations d'urgence sont tout aussi importantes en ce qui concerne les conséquences d'une atteinte à la sécurité qu'en ce qui concerne les accidents et les catastrophes naturelles.

I.4.2.3 Redondance pour le transport et protection physique des installations critiques

Les systèmes informatiques et de communications critiques devraient être dispersés géographiquement dans la mesure du possible sans que les répercussions sur les coûts

d'exploitation, sur la performance et sur la sécurité, ne soient trop importantes. De plus, les liaisons de communication critiques (par exemple, les circuits intercentraux importants, les liaisons de signalisation) devraient être redondantes et dispersées géographiquement à l'intérieur et à l'extérieur des installations de sorte que les communications puissent immédiatement être reroutées sur des routes de secours empruntant des chemins physiques différents lorsque c'est nécessaire. Les réseaux de communications requis pour le maintien du service devraient être conçus de manière à ce qu'une défaillance ponctuelle n'entraîne pas d'interruption étendue ou grave.

I.4.3 Menaces environnementales et géographiques

Il convient d'examiner les sites critiques afin d'évaluer les risques résultant de leur emplacement dans des zones dans lesquelles des catastrophes naturelles, des accidents graves (déversement accidentel de produits chimiques, explosion de gazoduc, par exemple), des interruptions de courant ou des problèmes du même ordre sont susceptibles de se produire. Il convient aussi de s'intéresser aux effets de facteurs environnementaux simples (chaleur ou froid extrême, dommages dus aux sels et à la pollution, conditions climatiques rigoureuses, par exemple).

Les questions à prendre en considération sur le plan géographique sont les réactions de la population locale (actes d'hostilité, par exemple), la réactivité des services d'urgence locaux et le niveau de sûreté offert au personnel, sur le site et en route vers les installations. Comme les activités et les motivations humaines peuvent varier dans le temps par suite de troubles, de problèmes politiques, de points de vue religieux ou d'autres facteurs, il convient de faire périodiquement des évaluations conformément à un calendrier prédéterminé. Il est souvent difficile d'abandonner des installations à haut risque, mais il peut être judicieux de dupliquer ou de relocaliser les systèmes et ressources critiques contenus dans de telles installations.

Il convient d'élaborer des plans de continuité d'exploitation et de rétablissement en cas de catastrophe afin de pouvoir réagir aux événements résultant de ces menaces et de ces questions. Ces plans devraient inclure des procédures de commande, de contrôle et de communications et devraient être testés régulièrement. Les plans de rétablissement de l'exploitation devraient aussi inclure des dispositions et des contrats pouvant être exécutés rapidement en réponse à des incidents liés à des matières dangereuses (HAZMAT). Il convient, dans ces plans, de tenir compte du fait que le rétablissement complet d'un environnement sûr risque d'empêcher l'accès normal aux installations pendant une grande période. On peut alors procéder à une relocalisation dans des installations de secours ou faire appel à du personnel formé et équipé concernant les matières dangereuses pour exploiter les installations dans l'attente du rétablissement complet.

I.4.4 Procédures relatives à la colocalisation

La colocalisation est une situation dans laquelle des installations appartenant à plusieurs fournisseurs sont présentes en un même endroit physique. Pour les évaluations de la sécurité physique, il est particulièrement important d'avoir à l'esprit que souvent, dans cette situation, les concurrents (parfois nombreux) auront besoin d'un accès aux composants et installations physiques du fournisseur hôte. Pour les évaluations, il convient de noter que:

– des barrières physiques devraient isoler les équipements critiques; toutefois, les prescriptions d'accès s'appliquant au personnel colocalisé sont les mêmes que celles qui s'appliquent au fournisseur de services hôte;

– des procédures existent pour la distribution de clés, la comptabilité et l'audit. Des processus devraient exister pour permettre de surveiller globalement les changements de personnel dans l'une ou l'autre des entreprises colocalisées;

– les équipements et les installations critiques n'attirent pas les regards. La méthode traditionnelle consistant à marquer clairement les équipements et les installations de transport cruciaux (appelée "marquage à l'encre rouge"[6]) présente un risque potentiel dans un environnement ouvert et il convient de l'éviter.

I.5 Processus de développement

I.5.1 Démarrage, installation et défaillances

Il convient de tenir compte des considérations suivantes concernant les procédures de sécurité applicables au démarrage, à l'installation et aux défaillances.

Plusieurs tâches doivent être effectuées pour sécuriser une implémentation depuis une "nouvelle installation" et tout au long de sa durée de vie. Pour cela, il est important de commencer par identifier les menaces qui pèsent sur l'implémentation. Ces menaces sont décrites dans les normes ANSI T1.233-2004, *Operations, Administration, Maintenance, and Provisioning – Security Framework for Telecommunications Management Network Interfaces* et ISO/CEI 10181, *Interconnexion de systèmes ouverts – Cadre de sécurité pour les systèmes ouverts*. La connectivité générale aux systèmes ouverts élargit le champ des menaces, qui sont notamment les suivantes:

– virus de démarrage;
– accès non autorisé;
– usurpation d'identité;
– menaces contre l'intégrité des données;
– menaces contre la confidentialité;
– déni de service (DoS);
– répudiation.

I.5.2 Processus de correction de programme

Les fournisseurs de services concluent des contrats avec des fournisseurs informatiques qui développent et fournissent à la fois une application et une plate-forme sur laquelle l'application est installée ou uniquement des logiciels d'application. Dans le deuxième cas, les fournisseurs de services installent les logiciels sur une plate-forme qu'ils ont achetée précédemment.

Les fournisseurs informatiques développent des programmes de correction visant à corriger ou à modifier les logiciels de système d'exploitation (OS) ou d'application, ou les deux, qu'ils distribuent aux fournisseurs de services entre deux versions officielles, après des tests appropriés. Dans certains cas, ils peuvent distribuer des programmes de correction par "lots", éventuellement selon une certaine régularité définie dans les contrats. Des distributions bisannuelles sont courantes.

D'une manière générale, un programme de correction de système d'exploitation ne devrait pas affecter la manière dont une application fonctionne, mais ce n'est pas toujours le cas. Par conséquent, lorsqu'un fournisseur de plate-forme distribue un programme de correction de système d'exploitation, il appartient au fournisseur de services de vérifier avec le fournisseur de l'application que ledit programme de correction distribué n'aura pas d'incidence négative sur le fonctionnement de l'application.

Lorsqu'un fournisseur d'application fournit à la fois une application et une plate-forme matérielle mais qu'il n'est pas le fabricant de la plate-forme d'origine, et qu'un programme de correction de sécurité de système d'exploitation est distribué par le fabricant de la plate-forme d'origine, il appartient à la fois au fournisseur de l'application et au fournisseur de services de se tenir au courant

---

6 Le marquage à l'encre rouge sert à avertir le personnel d'appui du fait que le circuit est particulièrement important et qu'il faut veiller à ne pas le perturber accidentellement.

de la distribution du programme de correction de sécurité et de prévoir de le tester rapidement afin de vérifier qu'il n'aura pas d'incidence négative sur l'application.

L'examen de l'application de programmes de correction de sécurité doit faire partie des priorités du fournisseur de l'application (quelques semaines et non quelques mois). A cet effet, il faut établir un processus général visant à ce que le fournisseur de l'application prenne rapidement les mesures qui s'imposent lorsqu'un fournisseur de services lui communique un problème concernant un programme de correction de sécurité. Par ailleurs, le fournisseur de l'application s'assurera que l'installation du programme de correction n'altérera pas les programmes de correction de sécurité déjà installés.

Si le test d'un programme de correction de sécurité révèle une incidence sur une application, des mesures correctives doivent être prises rapidement afin d'identifier le problème, de le résoudre et d'appliquer ensuite le programme de correction de sécurité.

Il convient de tenir compte des considérations de sécurité suivantes lors de l'installation de programmes de correction du système d'exploitation ou des logiciels d'application.

– Les fournisseurs d'équipements ou les intégrateurs de systèmes devraient fournir aux administrateurs des manuels de référence et de formation en matière de sécurité, contenant des détails sur les fonctions et procédures de sécurité pour le système d'exploitation et les applications ainsi que sur les procédures d'accès par les utilisateurs.
– Il convient de vérifier que les programmes de correction (de sécurité ou autres de système d'exploitation) sont compatibles avec les applications des éléments de réseau et des systèmes de gestion.
– Logiciels de système d'exploitation: seuls les programmes de correction approuvés par le fabricant du système d'exploitation d'origine devraient être appliqués à un système d'exploitation opérationnel de plate-forme de gestion ou d'élément de réseau.
– Logiciels d'application de gestion: seuls les programmes de correction approuvés par le fournisseur de l'application de gestion d'origine devraient être appliqués à une application de gestion opérationnelle.
– Les programmes de correction aux conséquences majeures devraient être distribués rapidement, sans tenir compte des processus de distribution périodique.
– Tous les téléchargements de logiciels ou de données de configuration doivent être sécurisés au moyen d'une authentification forte de l'origine des données et d'une forte protection de l'intégrité, qui, idéalement, devraient être assurées toutes les deux par le biais de la signature numérique du fournisseur de logiciels. De plus, le fournisseur de logiciels peut choisir de chiffrer les logiciels ou les données de configuration.
– Au moment de la distribution d'un programme de correction de sécurité, il convient de fournir une description de la ou des procédures d'acquisition et d'incorporation des programmes de correction de sécurité les plus récents pour les logiciels de système ou d'application présents dans chaque élément.
– Au moment de la distribution d'un programme de correction de sécurité, il convient de fournir une description du processus de test de ce programme qui a précédé l'approbation de la distribution du programme au fournisseur de services.
– Au moment de la distribution d'un programme de correction pour le maintien de la sécurité, il convient de spécifier le niveau de compatibilité amont avec les logiciels de système.
– Les programmes de correction et les mises à jour appliqués devraient être répertoriés, par exemple dans les logiciels de système. Le statut des programmes de correction et des mises à jour devrait pouvoir faire l'objet d'un audit.

I.5.3 Sécurité tout au long du cycle de vie du développement

La sécurité d'un produit ou d'un service dépend de l'ensemble de son cycle de vie. La sécurité est une question à prendre en considération aussi bien pendant la conception des grandes lignes que pendant la conception détaillée, l'élaboration, la mise en place et le retrait d'un produit. En ce qui concerne les produits et les services traitant des informations sensibles, la sécurité peut être requise au-delà de leur retrait. Des contrôles et des tests appropriés tout au long du cycle de vie sont cruciaux pour offrir des niveaux de sécurité acceptables.

I.5.3.1 Gestion du personnel

Le fait que le personnel soit digne de confiance est fondamental sur le plan de la sécurité mais cette question est souvent négligée. L'ensemble du personnel ayant accès à la conception, au développement et au test doit être digne de confiance.

– Il faut vérifier les antécédents de l'ensemble du personnel, des personnes sous contrat, des sous-traitants, des consultants et des employés participant au développement et au test des composants logiciels critiques.

I.5.3.2 Connaissances et formation en matière de sécurité

L'ensemble du personnel doit connaître les politiques et procédures de sécurité et être conscient de la nécessité de protéger les ressources en informations. C'est souvent le personnel qui constitue le maillon faible en termes de sécurité. Les connaissances et la formation en matière de sécurité permettent de renforcer considérablement ce maillon faible. Les connaissances permettent de réduire le nombre d'actions non autorisées tentées par le personnel et d'augmenter l'efficacité des contrôles de protection et contribuent à éviter les fraudes, les gaspillages et les abus concernant les ressources informatiques.

– Des connaissances et une formation en matière de sécurité devraient être dispensées à l'ensemble du personnel, y compris les personnes sous contrat, les sous-traitants, les consultants et les employés.

I.5.3.3 Gestion des risques

La gestion des risques est fondamentale pour la sécurité des informations. Par gestion des risques, on entend leur identification, leur analyse, leur contrôle et la réduction des pertes associées à un "événement". Les principales étapes de l'identification des risques consistent à déterminer les menaces réelles, les conséquences d'une menace réelle, la fréquence potentielle d'occurrence d'une menace et la probabilité pour qu'une menace réelle soit mise à exécution. La gestion des risques ne comporte pas uniquement une analyse des risques avec analyse du rapport coûts/avantages des protections mais également l'implémentation, l'examen et le maintien de protections.

Une analyse des risques consiste à identifier les risques et à exposer le bien-fondé de mesures de protection sur la base d'une analyse du rapport coûts/avantages. Cette analyse est utile pour la prise de décisions dans toutes les phases du cycle de vie (choix du site, conception des bâtiments, construction, etc.). Pour déterminer si des mesures de protection sont justifiées, on calcule une estimation des pertes annuelles (ALE). (ALE avant implémentation des mesures de protection) – (ALE après implémentation des mesures de protection) = valeur des mesures de protection. Il est à noter que l'implémentation des mesures de protection doit inclure le coût annuel de l'exploitation et de la maintenance.

– Une analyse des risques doit être faite pour chaque nouveau produit ou service et doit conduire à l'élaboration d'un document officiel exposant l'approche utilisée et les résultats de l'analyse. Au minimum, le rapport devrait identifier toutes les données accessibles et le propriétaire des données (à savoir l'entreprise, un fournisseur de services Internet), déterminer la quantité et l'importance des données ou des services présentant des risques et

établir les incidences potentielles en amont et en aval de la menace pour les éléments de réseau ou les systèmes OSS.

I.5.3.4 Prescriptions

– Les prescriptions de sécurité devraient être documentées pendant la phase de regroupement des prescriptions pour le produit ou le service.

I.5.3.5 Conception

– Les prescriptions de sécurité devraient être examinées pendant la phase de conception, et non pas être ajoutées une fois que le développement a commencé.

– Il convient de procéder à un examen de sécurité de la conception afin de localiser les défauts de conception qui ont une incidence sur la sécurité.

– Tous les points d'accès au système doivent faire l'objet d'une documentation détaillée et doivent pouvoir prendre en charge l'identification et l'authentification.

– Les trappes ou portes dérobées pour la maintenance qui transgressent la politique de sécurité ne doivent PAS être autorisées.

I.5.3.6 Séparation des fonctions

Des fonctions qui sont inoffensives dans un environnement sécurisé peuvent créer des vulnérabilités de sécurité lorsqu'elles sont utilisées dans des environnements non sécurisés. Donnons l'exemple d'un interpréteur postscript conçu pour visualiser des documents et dont les fonctions pourraient être utilisées de façon malveillante pour un document non sécurisé, par exemple pour faire des copies ou pour supprimer des fichiers.

– Le système devrait prendre en charge au moins trois niveaux d'utilisateur: utilisateur, administrateur/opérateur de système et administrateur de sécurité.

– Chaque utilisateur devrait disposer du niveau minimal de privilèges requis pour remplir sa fonction.

I.5.3.7 Implémentation

– Les ressources réutilisables devraient être vidées de toute information avant d'être réutilisées (c'est-à-dire les fichiers, les mémoires et les zones de stockage temporaires).

– Les développeurs devraient appliquer les meilleures pratiques de programmation sécurisée (autrement dit, les tampons devraient être gérés de manière à ce qu'ils ne puissent pas déborder).

– Il convient de procéder à des audits de sécurité périodiques dans les environnements de développement, de test et de prise en charge.

– Les environnements de développement ne devraient pas être utilisés pour des activités autres que celles de l'entreprise.

– Les logiciels du domaine public ne devraient pas être importés, employés ou distribués en vue d'une utilisation dans les systèmes de développement, de test ou de prise en charge sauf s'ils sont disponibles en code source et que l'absence de code malveillant dans le code source a été vérifié.

I.5.3.8 Documentation

– La documentation devrait être marquée avec des marquages propriétaires, lorsque c'est utile.

– La documentation destinée aux utilisateurs finals doit décrire la fonctionnalité de sécurité qui n'est pas transparente pour l'utilisateur, expliquer sa fonction et fournir des indications sur son utilisation.

– Le guide destiné aux administrateurs de système devrait inclure ce qui suit:
  - des avertissements concernant les fonctions et les privilèges qui doivent être contrôlés lors d'un fonctionnement en mode sécurisé;
  - une documentation concernant l'utilisation des fonctions d'audit;
  - des procédures d'examen et de mise à jour des journaux d'audit;
  - les structures détaillées des journaux d'audit;
  - des procédures de sauvegarde et de suppression des journaux d'audit;
  - des procédures de vérification de l'espace disponible pour les journaux d'audit.

I.5.3.9 Système d'exploitation

Le système d'exploitation doit permettre de contrôler efficacement les matériels et les logiciels afin d'assurer une protection adaptée à l'importance des données et des ressources qui sont gérées. En ce qui concerne l'architecture de sécurité proposée, le système d'exploitation est censé offrir le niveau de sécurité requis pour les données et les ressources qui sont gérées. Il peut être nécessaire de vérifier que le niveau de sécurité offert par le système d'exploitation répond aux besoins spécifiques du fournisseur de services. Si ce n'est pas le cas, il peut alors être nécessaire de porter les logiciels vers un autre système d'exploitation qui prend en charge des niveaux de sécurité plus élevés.

– Les programmes de correction de sécurité applicables doivent être installés dans le système d'exploitation.

– Le système d'exploitation doit présenter une configuration sécurisée et doit être fourni avec une configuration de privilèges d'accès de sécurité restrictifs. Il existe plusieurs documents et sites Web qui portent sur la sécurité du système d'exploitation. Leur énumération sort du cadre de la présente Recommandation, mais on peut citer la norme *common criteria* et les profils de protection de système d'exploitation (*operating system protection profiles*)[7, 8, 9].

– Seul l'ensemble minimal de services requis pour le fonctionnement par défaut sera activé.

I.5.3.10 Ingénierie logicielle

La sécurité fait partie intégrante de l'ingénierie logicielle. Pour élaborer un produit sécurisé, il faut utiliser des techniques de programmation sécurisée et des protocoles sécurisés. Des techniques de programmation non sécurisée peuvent mettre en échec les meilleurs protocoles et mécanismes de sécurité. A titre d'exemple, si un programmeur ne gère pas les tampons correctement, un débordement de tampon risque de se produire et de faire bénéficier un utilisateur de privilèges qui ne devraient pas lui être assignés.

– Les fournisseurs devraient appliquer des processus de développement documentés formels, comme le modèle de maturité de la capacité élaboré par le Software Engineering Institute. Il convient d'appliquer les meilleures pratiques de programmation sécurisée lors de la conception, du développement, du test et de la distribution des logiciels.

---

7 La norme Common Criteria devient une norme reconnue à l'échelle internationale concernant l'évaluation formelle de la sécurité (http://www.commoncriteria.org/).

8 Profils de protection de système d'exploitation du Forum Information Assurance Technical Framework, http://www.iatf.net/protection_profiles/operating_systems.cfm.

9 National Institute of Standards and Technology, Computer Security Resource Center, http://csrc.nist.gov/.

I.5.3.11 Disponibilité et performance

La disponibilité et la performance font partie intégrante d'un système sécurisé. La dégradation de la performance peut être telle que le système ne puisse plus être utilisé.

– Au cours de la conception, du développement et de l'implémentation, il convient de réduire autant que possible les effets d'une attaque de type DoS.
– Au cours de la conception, du développement et de l'implémentation, il convient de garantir une grande disponibilité.
– L'architecture et l'implémentation du réseau ne devraient présenter aucun point de défaillance.

I.5.3.12 Logiciels système

Les logiciels utilisés pour assurer l'exploitation et la maintenance des systèmes informatiques (systèmes d'exploitation, utilitaires et systèmes de gestion) doivent pouvoir être configurés et mis à jour de façon sécurisée. Des tests devraient être pratiqués pour garantir que les composantes et les fonctionnalités de sécurité ont été implémentées de façon robuste et configurées correctement.

– L'installation et la configuration des logiciels système et des intergiciels doivent se faire de façon sécurisée, y compris l'installation des programmes de correction de sécurité. Les logiciels doivent être fournis avec une configuration de privilèges d'accès de sécurité restrictifs.

I.5.3.13 Transmission

– L'option de sécurisation des transmissions de données doit être disponible et doit pouvoir être utilisée à la discrétion du fournisseur de services. Cette option devrait être disponible à la fois pour les transmissions client-serveur et système-système.

I.5.3.14 Stockage sécurisé

– Des options configurables par le fournisseur de services permettant de stocker des données de façon sécurisée devraient être prévues. Le fournisseur de services devrait pouvoir spécifier les champs qui sont stockés de façon sécurisée.

I.5.3.15 Assurance des logiciels

Dans le cadre de l'assurance des logiciels, il convient, d'une part, de tester les fonctionnalités de sécurité et, d'autre part, de rechercher les éventuelles transgressions de la politique de sécurité.

– Les fonctions des groupes de développement des logiciels et des groupes de test des logiciels doivent être séparées.
– Le plan des tests de sécurité, les procédures de test et les résultats devraient faire l'objet d'une documentation.
– Toutes les fonctionnalités de sécurité doivent être testées.
– Les tests doivent inclure des tentatives de localisation de transgressions de la politique de sécurité (c'est-à-dire des vulnérabilités, au niveau du contrôle d'accès, par exemple).
– Dans le cadre des tests, il faut vérifier que l'application ou le système nouvellement développé n'introduit pas de vulnérabilités dans les structures, les réseaux généraux et les systèmes existants.
– Il faut vérifier les techniques de programmation sécurisée, au moyen d'examens du code ou d'outils logiciels, par exemple.
– Tous les défauts de sécurité doivent être corrigés, supprimés ou neutralisés et le système doit ensuite être testé à nouveau.

I.5.3.16 Conditionnement et fourniture

Tout au long du cycle de vie d'un produit, il faut utiliser un système de gestion de la configuration des logiciels permettant de contrôler les modifications du code source et de conserver la documentation.

- Les développeurs ne devraient pas mettre à jour le système de gestion de la configuration des logiciels.
- Les développeurs ne devraient pas avoir accès aux systèmes de production sauf dans le cadre de dispositions d'urgence limitées qui sont approuvées et journalisées.
- Seuls un code et des modifications de code autorisés devraient être ajoutés au code source de base.
- Toutes les modifications doivent être documentées et examinées.
- Des outils ou des procédures doivent être prévus pour créer une nouvelle version du système à partir du code source.
- Des outils ou des procédures doivent être prévus pour protéger le code source contre les modifications non autorisées.
- Des outils ou des procédures doivent être prévus pour vérifier que les versions et les niveaux des modules source constitutifs utilisés sont appropriés.
- Le produit doit contenir des mécanismes de contrôle de l'intégrité de manière à pouvoir vérifier que les logiciels installés sont conformes aux logiciels fournis (autrement dit qu'aucune modification non autorisée n'a été apportée).
- Lorsqu'un outil de balayage automatique est disponible, il convient de procéder à un balayage pour rechercher les vulnérabilités après avoir procédé à des mises à jour ou à d'autres modifications importantes des logiciels d'application ou de système d'exploitation.
- Il convient de remédier aux défauts de sécurité d'autant plus rapidement que la menace est grande.
- Il faut prévoir une base de données principale contenant une copie de tous les logiciels fournis. A chaque logiciel doivent être associés un numéro de version et des spécifications relatives aux systèmes d'exploitation et aux matériels appropriés.

I.5.3.17 Installation, configuration et exploitation sécurisées

- Des paramètres de configuration sécurisée devraient être définis pour les logiciels.
- Des procédures d'exploitation sécurisée devraient être définies et documentées pour les logiciels.
- Toute la prise en charge à distance des logiciels devrait être faite de manière sécurisée.
- Toutes les identités d'utilisateur par défaut fournies avec le système devraient être fournies dans un état inactif nécessitant une action explicite de l'administrateur ou de l'installateur de logiciels pour pouvoir être utilisées.
- Tous les processus d'installation devraient être sécurisés et ne devraient pas reposer sur des relations de confiance (disques partagés, par exemple).

Appendice II

Cadre et directives de conception

II.1 Cadre et modèle

Dans le contexte de la présente Recommandation, par sécurisation – des ordinateurs, des réseaux, des données ou d'autres ressources – on entend leur protection contre les accès, les utilisations et les activités non autorisés. La perte de données, le déni de service (DoS) et le vol de service ne sont que quelques exemples de résultats d'incidents de sécurité. Les administrateurs de système et de réseau doivent protéger les systèmes et leurs éléments vis-à-vis des utilisateurs internes et des utilisateurs externes ainsi que des attaquants. La sécurité présente de nombreux aspects (couvrant l'exploitation, la sécurité physique, les communications, le traitement et le personnel), mais on s'intéresse ici aux problèmes de sécurité résultant des faiblesses inhérentes aux configurations et technologies couramment employées. Les menaces comprennent notamment la divulgation, l'utilisation non autorisée, les modifications d'éléments d'information et le déni de service. Le Tableau II.1 énumère quelques menaces de sécurité.

Tableau II.1/M.3016.1 – Menaces

Catégories de menaces (Note)	Exemples de menaces
Accès non autorisé	Piratage Accès non autorisé à un système pour lancer des attaques Vol de service
Usurpation d'identité	"Rejeu" de session Détournement de session Attaques de l'homme au milieu
Menaces contre l'intégrité du système	Manipulation non autorisée de fichiers de configuration de système Manipulation non autorisée de données de système
Menaces contre l'intégrité des communications	Manipulation non autorisée de données en transit
Menaces contre la confidentialité	Ecoute indiscrète Enregistrement et divulgation de session Transgressions de la confidentialité
Déni de service	Inondation SYN du protocole de commande de transmission (TCP) Attaques par paquets mal formés Déni de service réparti
NOTE – Déterminées à partir de la norme T1.233-1993 (R1999) de l'ANSI, *Operations, Administration, Maintenance, and Provisioning – Security Framework for Telecommunications Management Network Interfaces* et de l'ISO 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité*.	

Ces menaces de sécurité peuvent être réduites le plus possible ou atténuées dans un système de réseau, dans une plate-forme d'éléments de réseau ou dans une application grâce à l'inclusion de services de sécurité (comme défini dans l'ISO 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité*) permettant de prendre en charge ce qui suit:

– l'identification et l'**authentification**;
– des niveaux d'autorisation et de **contrôle d'accès**;
– l'intégrité des données;
– le respect de la vie privée et la confidentialité;
– la non-répudiation.

La présente Recommandation porte sur la sécurité pour le plan de gestion – autrement dit, sur les fonctionnalités de sécurité qui permettent de faire en sorte que le réseau puisse être administré et géré de façon sécurisée. Certaines vulnérabilités peuvent persister, même si les recommandations formulées dans la présente Recommandation ont été suivies. Les risques suivants sont des exemples de risques qui peuvent compromettre le plan de gestion:

– actions inappropriées lancées par des utilisateurs autorisés ou par des attaquants. Ces actions peuvent être malveillantes ou accidentelles;
– pontage de la sécurité du plan de commande (par exemple protocoles de signalisation, de routage, de nommage et de découverte);
– effets de vulnérabilités dans certains protocoles;
– logiciels malveillants ou maliciels (par exemple virus, chevaux de Troie, vers ou autre code imbriqué). Une fois qu'un maliciel a réussi à compromettre un élément NE/MS, il peut utiliser les liaisons de communication de réseau sécurisées pour transmettre des attaques à d'autres éléments NE/MS. Ces attaques peuvent continuer jusqu'à ce que les gestionnaires de réseau les détectent et prennent des mesures pour les éliminer.

La présente Recommandation porte sur la sécurité du trafic de gestion, notamment lorsque ce trafic est mélangé au trafic des utilisateurs finals pour traverser les réseaux. La Figure II.1 illustre un modèle de référence qui est utilisé pour spécifier des solutions de sécurité de gestion de réseau. On utilise ce modèle pour examiner les trajets de communication logiques dans l'ensemble du réseau et pour déterminer quels sont les protocoles qui sont utilisés pour les communications sur chaque trajet. Ce modèle permet d'examiner les menaces et les vulnérabilités pour chaque trajet et d'appliquer les mécanismes de sécurité appropriés.

Les éléments de réseau multifournisseurs sont représentés au bas du modèle de la Figure II.1. Le système de gestion d'élément (EMS) qui assure des fonctions de gestion spécifiques pour l'élément de réseau (NE) particulier est illustré au-dessus de l'élément de réseau. Le système de gestion de réseau (NMS) proprement dit se trouve en haut du modèle. Il assure une gestion d'ensemble de l'élément de réseau et du système EMS et contient les applications de gestion de service et les applications de gestion commerciale spécifiques (systèmes de configuration et de facturation, par exemple). Dans le modèle sont également représentés un opérateur local et un opérateur distant ainsi que les trajets de communication avec tous les autres éléments de système.

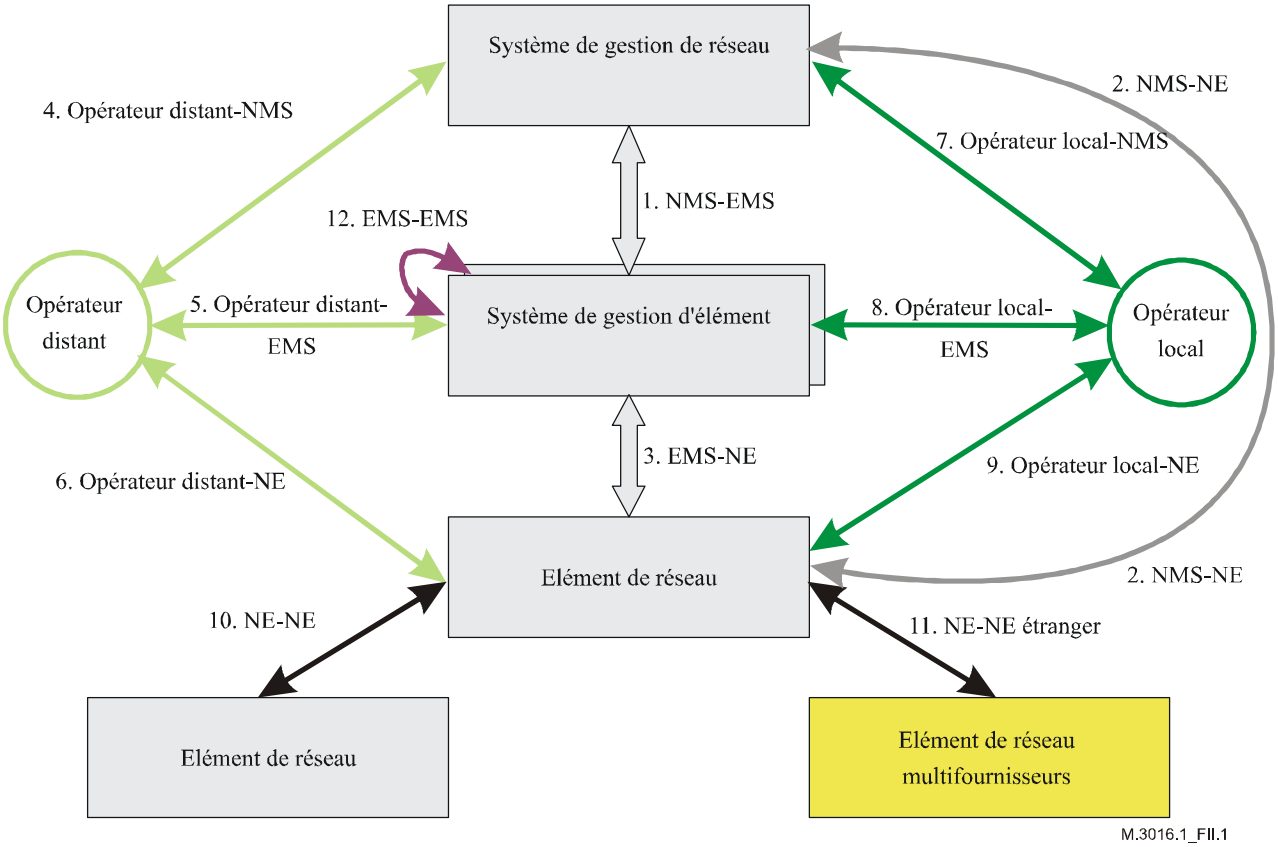

Figure II.1/M.3016.1 – Modèle de référence pour la sécurité de gestion de réseau

Le modèle de référence pour la sécurité (Figure II.1 ci-dessus) peut également être utile pour corréler les interfaces définies dans le réseau de gestion des télécommunications (RGT) avec le modèle de sécurité. Le RGT est défini dans la Rec. UIT-T M.3010, *Principes des réseaux de gestion des télécommunications*. Il est défini comme une architecture pour la gestion – y compris la planification, la fourniture, l'installation, la maintenance, l'exploitation et l'administration des équipements, des réseaux et des services de télécommunication.

II.2 Directives de conception

Le Tableau II.2 présente des directives de conception visant à satisfaire aux prescriptions définies au § 6 afin d'atténuer les menaces énumérées dans le Tableau II.1.

Tableau II.2/M.3016.1 – Directives de conception considérées

Directive	Description
Isolement	Isolement du trafic de gestion par rapport au trafic des clients
Politiques de sécurité efficaces	Les prescriptions et les architectures support doivent permettre de définir des politiques souples, fiables, facilement applicables et utilisables et qui puissent faire l'objet d'audits et de vérifications.
Authentification forte, autorisation et comptabilité (AAA)	Comptabilité fiable de sessions correctement autorisées entre entités authentifiées
Meilleur avantage possible pour un coût donné	Améliorer la sécurité en mettant en œuvre des mécanismes de sécurité normalisés et largement déployés, de manière à pouvoir évaluer ces mécanismes sur la base des historiques d'utilisation.

Tableau II.2/M.3016.1 – Directives de conception considérées

Directive	Description
Voie d'amélioration	Envisager les prochaines étapes de renforcement et d'amélioration de la sécurité de gestion de réseau afin de continuer à satisfaire à des prescriptions données avec de nouvelles technologies et de nouveaux mécanismes ou de satisfaire à des prescriptions de sécurité nouvellement définies.
Faisabilité technique	Les prescriptions doivent pouvoir être satisfaites avec les produits, solutions et/ou technologies disponibles actuellement.
Gestion interne	Les prescriptions devraient être cohérentes avec les procédures normalisées d'une gestion de réseau efficace.
Normes ouvertes	Utiliser des idées et des concepts qui sont déjà normalisés ou qui sont en cours de normalisation par des organismes de normalisation (par exemple, sécurité IP (IPsec), signatures numériques). Il convient de s'intéresser à tous les aspects des normes ouvertes (système, protocoles, modes, algorithme, option, longueur de clé, codage, etc.).

Appendice III

Sens des termes employés dans la série M.3016.x

Les termes qui suivent apparaissent en **gras** lorsqu'ils sont employés dans la définition d'une prescription.

III.1 Contrôle d'accès: précaution prise contre l'utilisation non autorisée d'une ressource, y compris l'utilisation d'une ressource d'une façon non autorisée[10].

III.2 Serveur de contrôle d'accès (ACS, *access control server*): élément de réseau auxiliaire qui est installé pour authentifier l'accès à un système de gestion sur la base de **mots de passe complexes**, si un élément de réseau ne peut pas mettre en application directement cette fonctionnalité.

III.3 Administrateur d'application: rôle dont le détenteur est chargé d'assurer l'activation, le maintien et l'utilisation appropriés d'une application d'entité NE/MS. Les tâches comprennent la mise à jour des logiciels d'application[11].

III.4 Administrateur de sécurité d'application: rôle dont le détenteur est chargé d'assurer l'activation, le maintien et l'utilisation appropriés des fonctionnalités de sécurité de la couche application d'une entité NE/MS. Cet administrateur constitue le niveau le plus élevé d'autorité de sécurité pour une instance d'application d'entité NE/MS. Les tâches peuvent être les suivantes:

– définir et assigner de nouveaux privilèges d'utilisateur ou de groupe au niveau de l'application;

---

[10] Voir le § 3.1 de la norme ANSI T1.233-1993 (R1999), *Operations, Administration, Maintenance, and Provisioning – Security Framework for Telecommunications Management Network Interfaces*.

[11] Cette tâche peut relever de l'**administrateur de système**, si l'autorité de **superutilisateur** est nécessaire pour effectuer cette tâche. Des processus peuvent être élaborés afin de contrôler l'accès au compte de **superutilisateur**.

– conserver un enregistrement de toutes les demandes d'identité de connexion relatives à l'application;
– ajouter et supprimer des utilisateurs au niveau de l'application;
– surveiller tous les journaux de sécurité de l'application;
– configurer la journalisation de sécurité et les alarmes de sécurité de l'application;
– gérer les processus de journalisation de sécurité de l'application;
– terminer les sessions d'application d'utilisateur.

III.5 Authentification: vérification d'une identité déclarée.

III.6 Mots de passe complexes: un mot de passe est dit "complexe" lorsqu'il est constitué d'une combinaison de caractères alphabétiques, numériques et spéciaux, rendant difficile, voire improbable, son extorsion par la méthode de l'ingénierie sociale ou par des moyens automatisés.

III.7 Plan de commande: le **plan de commande** assure les fonctions de commande d'appel et de commande de connexion. Il utilise la signalisation pour établir et libérer des connexions et éventuellement pour rétablir une connexion en cas de défaillance[12].

III.8 Actions d'administration de sécurité essentielles: c'est l'**administrateur de sécurité de système** qui est responsable des actions d'administration de sécurité essentielles, permettant d'assurer l'activation, le maintien et l'utilisation appropriés des fonctionnalités de sécurité d'un système (NE/MS). Les **actions d'administration de sécurité essentielles** sont notamment les suivantes:
– définir et assigner des privilèges d'utilisateur;
– ajouter et supprimer des identités d'utilisateur;
– désactiver l'utilisation d'identités d'utilisateur particulières comme identités de connexion;
– initialiser et réinitialiser des mots de passe de connexion;
– initialiser et modifier des clés de chiffrement;
– fixer, pour le système, la durée de validité des mots de passe de connexion;
– fixer, pour le système, le nombre maximal d'échecs de connexion pour chaque identité de connexion;
– supprimer un verrouillage ou modifier la valeur de temporisation de verrouillage du système;
– fixer la valeur de temporisation d'inactivité du système;
– configurer la journalisation de sécurité et les alarmes de sécurité du système;
– gérer les processus de journalisation de sécurité;
– mettre à jour les logiciels de sécurité;
– terminer les sessions d'utilisateur ou de système.

III.9 Désactivé: pour une identité d'utilisateur, état dans lequel l'identité d'utilisateur ne peut pas être utilisée comme identité de connexion tant qu'elle n'a pas été activée par une action spécifique d'un autre utilisateur possédant les privilèges d'autorisation appropriés (par exemple, **administrateur de sécurité de système** ou **administrateur de sécurité d'application**).

III.10 Système de gestion d'élément (EMS, *element management system*): système qui assure la fonction de système d'exploitation dans la couche de gestion d'élément.

---

[12] Recommandation UIT-T G.8080/Y.1304, *Architecture du réseau optique à commutation automatique (ASON)*, novembre 2001 (disponible dans la libraire électronique de l'UIT).

III.11 Force de clé: les algorithmes cryptographiques présentent des degrés de sécurité variables, qui sont fonction de la difficulté à les briser. On considère qu'un algorithme cryptographique est fort s'il est impossible de le briser par des calculs – autrement dit, il est suffisamment complexe pour ne pas pouvoir être brisé en un temps "raisonnable" avec les ressources disponibles actuellement ou dans un futur proche. La plupart du temps, la complexité des calculs est mesurée en termes de complexité de traitement, autrement dit en termes de temps et d'espace mémoire nécessaires pour effectuer une attaque. La complexité d'une attaque reste constante pour un algorithme et une longueur de clé donnés, mais la puissance de calcul ne cesse d'augmenter. Les bons systèmes de cryptographie sont ceux qui sont conçus comme étant impossibles à briser avec la puissance de calcul qui devrait être disponible dans un grand nombre d'années. Compte tenu de la rapidité avec laquelle les nouvelles technologies et les méthodes d'analyse cryptographique se développent, la longueur de clé correcte pour une application particulière change constamment.

III.12 Verrouillé: pour une identité d'utilisateur, état dans lequel l'identité d'utilisateur ne peut pas être utilisée comme identité de connexion tant que cet état n'a pas été supprimé par une ou plusieurs actions appropriées. Les actions appropriées sont notamment les suivantes:

– réinitialisation automatique après une durée fixée (par exemple, après 60 minutes);
– réinitialisation automatique après l'aboutissement d'un processus de réinitialisation prédéfini (par exemple, après que le détenteur de l'identité a répondu correctement à un ensemble de questions);
– réinitialisation par suite d'une action spécifique d'un autre utilisateur possédant les privilèges d'autorisation appropriés (par exemple, **administrateur de sécurité de système** ou **administrateur de sécurité d'application**).

III.13 Action de gestion: action entreprise par l'**administrateur de système** ou au nom de celui-ci.

III.14 Communication de gestion: toute communication d'une **action de gestion**.

III.15 Plan de gestion: le **plan de gestion** assure les fonctions de gestion pour le **plan de transport**, le **plan de commande** et le système dans sa totalité. Il assure aussi la coordination entre tous les plans. Les domaines fonctionnels de gestion de la performance, des dérangements, de la configuration, de la comptabilité et de la sécurité définis dans la Rec. UIT-T M.3010 (*Principes des réseaux de gestion des télécommunications*) font partie du **plan de gestion**[13].

III.16 Elément de réseau (NE, *network element*): voir la Rec. UIT-T M.3010.

III.17 Système de gestion de réseau (NMS, *network management system*): système qui assure la fonction de système d'exploitation dans la couche de gestion de réseau.

III.18 Elément de réseau/système de gestion (NE/MS, *network element/management system*): terme désignant collectivement la totalité des éléments d'un réseau de télécommunication (NE, EMS, NMS et OSS, par exemple).

III.19 Authentification protégée: désigne l'**authentification forte**, l'**authentification à double facteur**, l'**authentification par connexion sécurisée**, l'authentification par un tiers fondée sur une cryptographie (par exemple, Kerberos) ou l'authentification avec mot de passe à utilisation unique.

III.20 Session: séquence d'opérations, machine-machine ou homme-machine, qui sont associées à un processus ou à une identité d'utilisateur unique.

---

[13] L'architecture du RGT est décrite dans la Rec. UIT-T M.3010, *Principes des réseaux de gestion des télécommunications* et d'autres détails concernant le PLAN DE GESTION figurent dans les Recommandations de la série M. Rec. UIT-T G.8080/Y.1304, *Architecture du réseau optique à commutation automatique (ASON)*, novembre 2001 (disponible dans la librairie électronique de l'UIT).

III.21 Authentification forte: **Authentification** qui repose sur l'utilisation de techniques cryptographiques (par exemple, chiffrement à clé publique, chiffrement à clé symétrique, signatures numériques et techniques de hachage numérique). L'**authentification forte** devrait inclure une authentification dans les deux sens, qui peut être utilisée pour la prévention des attaques actives.

III.22 Chiffrement fort: une attaque par force brute se produit lorsqu'un attaquant essaie toutes les combinaisons de clé possibles en utilisant les ressources de calcul disponibles pour découvrir un message chiffré. De cette façon, l'attaquant trouve la clé correcte après avoir essayé, en moyenne, la moitié de toutes les combinaisons de clé possibles. Le temps requis pour tester la moitié des combinaisons de clé est une mesure de la force du chiffrement. Les mécanismes de **chiffrement fort** sont ceux qui utilisent des algorithmes et des clés qui ne peuvent pas être brisés en moins de deux ans par n'importe quel attaquant qui utilise les technologies du moment, quel que soit le moment considéré.

III.23 Administrateur de système: rôle dont le détenteur est responsable des processus et des procédures au niveau du système d'exploitation concernant l'installation, l'exploitation, la maintenance de la plate-forme d'exploitation, l'installation de logiciels sur la plate-forme et le contrôle de l'autorité de **superutilisateur**. Les tâches peuvent être les suivantes:

– coordonner l'installation d'une nouvelle plate-forme;
– définir et assigner de nouveaux privilèges d'utilisateur ou de groupe au niveau du système d'exploitation;
– conserver un enregistrement de toutes les demandes d'identités de connexion au système d'exploitation;
– ajouter et supprimer des utilisateurs au niveau du système d'exploitation;
– désactiver l'utilisation d'identités d'utilisateur particulières comme identités de connexion (bin, sys, uucp);
– installer des mises à jour et des programmes de correction du système d'exploitation;
– installer des logiciels d'application et de base de données pour le système d'exploitation;
– surveiller tous les journaux du système;
– conserver le mot de passe de **superutilisateur** et contrôler l'accès à ce mot de passe et ses modifications;
– contrôler l'accès au compte de **superutilisateur**, en autorisant un accès approprié en fonction des besoins de l'entreprise;
– gérer les processus de journalisation du système;
– déléguer des autorisations d'administration à des personnes particulières assurant d'autres fonctions (**administrateurs d'application**, par exemple);
– terminer les sessions d'utilisateur ou de système.

III.24 Administrateur de sécurité de système: rôle dont le détenteur est chargé de l'activation, du maintien et de l'utilisation appropriés des fonctionnalités de sécurité de système d'un élément NE/MS. Cet administrateur constitue le niveau le plus élevé d'autorité de sécurité pour une instance d'application de système. Les tâches peuvent être les suivantes:

– définir et assigner de nouveaux privilèges d'utilisateur ou de groupe au niveau du système d'exploitation;
– conserver un enregistrement de toutes les demandes d'identités de connexion au système d'exploitation;
– ajouter et supprimer des utilisateurs au niveau du système d'exploitation;
– désactiver l'utilisation d'identités d'utilisateur particulières comme identités de connexion (bin, sys, uucp);

– surveiller tous les journaux de sécurité de système;
– initialiser et modifier les clés de chiffrement;
– fixer, pour le système, la durée de validité des mots de passe de connexion;
– fixer, pour le système, le nombre maximal d'échecs de connexion pour chaque identité de connexion;
– supprimer un verrouillage ou modifier la valeur de temporisation de verrouillage du système;
– fixer la valeur de temporisation d'inactivité du système;
– configurer la journalisation et les alarmes du système;
– gérer les processus de journalisation de sécurité du système;
– déléguer des autorisations de sécurité à des personnes particulières assurant d'autres fonctions (**administrateurs de sécurité d'application**, par exemple);
– terminer les sessions d'utilisateur ou de système.

III.25 Plan de transport: assure le transfert bidirectionnel ou unidirectionnel d'informations d'utilisateur d'un élément de réseau à un autre. Il peut aussi assurer le transfert de certaines informations de commande et de gestion de réseau. Le **plan de transport** est stratifié; il est équivalent au réseau de transport défini dans la Rec. UIT-T G.8080/Y.1304, *Architecture du réseau optique à commutation automatique (ASON)*.[12]

III.26 Connexion sécurisée: mécanisme permettant de sécuriser les interactions utilisateur/opérateur-système ou système-système. Il ne peut être activé que par l'utilisateur/opérateur ou le système et ne peut pas être imité. Une **connexion sécurisée** peut être une connexion physique dédiée (autrement dit une connexion directe entre un terminal et un système) ou une connexion chiffrée, sur laquelle protection de l'intégrité et protection "antirejeu" sont assurées (réseau privé virtuel "sécurisé", tunnel (SSL, *secure socket layer*), protocole SSH (*secure shell*))[14].

III.27 Authentification à double facteur: terme généralement employé pour décrire un processus d'**authentification** pour lequel il faut à la fois posséder une entité physique (par exemple, un jeton ou une carte) et connaître un secret (par exemple, un mot de passe ou une phrase de passe).

[14] Adapté de National Computer Security Center, NCSC-TG-004-88, *Glossary of Computer Security Terms*, octobre 1998 (disponible à l'adresse http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf).

BIBLIOGRAPHIE

Les références citées ici donnent des informations complémentaires sur bon nombre des sujets abordés dans les Appendices I et II.

– ANSI J-STD-025-A-2003, *Lawfully Authorized Electronic Surveillance.*

– ANSI X9.52-1998, *Triple Data Encryption Algorithm Modes of Operation,* (disponible dans la boutique de normes électroniques de l'ANSI X9, http://webstore.ansi.org/ansidocstore/ dept.asp?dept_id=80).

– ANSI X9.62-1998, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),* (disponible dans la boutique de normes électroniques de l'ANSI X9, http://webstore. ansi.org/ansidocstore/dept.asp?dept_id=80).

– ANSI T1.210-2004, *OAM&P – Principles of Functions, Architectures, and Protocols for Telecommunications Management Network (TMN) Interfaces.*

– ANSI T1.233-2004, *OAM&P – Security Framework for Telecommunications Management Network (TMN) Interfaces*.

– ANSI T1.252-1996 (R2002), *Operations, Administration, Maintenance and Provisioning OAM&P – Security for the Telecommunications Management Network (TMN) Directory.*

– ANSI T1.261-1998 (R2004), *OAM&P – Security for TMN Management Transactions over the TMN Q3 Interface.*

– ANSI T1.268-2000, *TMN – PKI – Digital Certificates and Certificate Revocation Lists Profile*.

– ANSI X9.31-1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*.

– ATM Forum. AF-SEC-0179.000 (avril 2002), *Methods of Securely Managing ATM Network Elements – Implementation Agreements Version 1.1,* (disponible à l'adresse ftp://ftp.atmforum.com/pub/approved-specs/af-sec-0179.000.pdf).

– BARRETT (D.), SILVERMAN (R.): SSH, The Secure Shell: The Definitive Guide, *O'Reilly*, janvier 2001.

– BELLOVIN (S.): An Issue With DES-CBC When Used Without Strong Integrity, *Proceedings of the 32nd Internet Engineering Task Force*, Danvers, MA, avril 1995.

– BLEICHENBACHER (D.): Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1, *Advances in Cryptology-Crypto '98*, Springer LNCS Vol. 1462, pp. 1-12, 1998.

– BONEH (D.): Twenty Years of Attacks on the RSA Cryptosystem, *Notices of the American Mathematical Society (AMS)*, Vol. 46, No. 2, pp. 203-213, février 1999, (disponible à l'adresse http://www.ams.org/notices/199902/boneh.pdf).

– BONEH (D.), JOUX (A.), NGUYEN (P.): Why Textbook RSA and ElGamal Encryption Are Insecure, *Advances in Cryptology-Asiacrypt 2000*, Springer LNCS Vol. 1976, pp. 30-43, 2000.

– Federal Communications Commission Docket Number 97-213 *Implementation of the Communications Assistance for Law Enforcement Act*, septembre 1999.

– General Requirements (GR)-815, *Generic Requirements for Network Element/Network System Security*, mars 2002 (disponible dans la superboutique informationnelle de Telcordia, à l'adresse http://telecom-info.telcordia.com/site-cgi/ido/index.html).

– GR-1194, *Bellcore Operations Systems Security Requirements*, décembre 1998, (disponible dans la superboutique informationnelle de Telcordia, à l'adresse http://telecom-info.telcordia.com/site-cgi/ido/index.html).

– GUTMANN (P.): Software Generation of Practically Strong Random Numbers, *Seventh USENIX Security Symposium Proceedings*, The USENIX Association, pp. 243-257, 1998, (disponible à l'adresse http://www.usenix.org/publications/library/proceedings/sec98/full_papers/gutmann/gutmann.pdf).

– Information Assurance Technical Framework Forum (IATF), http://www.commoncriteria.org/ and http://www.iatf.net/protection_profiles/profiles.cfm.

– IEEE 1363-2000, *IEEE Standard Specifications for Public Key Cryptography*, (disponible dans la boutique électronique des normes de l'IEEE, à l'adresse http://standards.ieee.org/catalog/olis/ busarch.html).

– IETF RFC 768, *User Datagram Protocol*, J. Postel, août 1980, (disponible à l'adresse http://www.ietf.org/rfc/rfc0768.txt?number=768).

– IETF RFC 791 (1981), *Internet Protocol – DARPA Internet Program Protocol Specification*, (disponible à l'adresse http://www.ietf.org/rfc/ rfc0791.txt?number=791).

– IETF RFC 792 (1981), *Internet Control Message Protocol – DARPA Internet Program Protocol Specification*, (disponible à l'adresse http://www.ietf.org/rfc/rfc0792.txt?number=792).

– IETF RFC 793 (1981), *Transmission Control Protocol – DARPA Internet Program Protocol Specification*, (disponible à l'adresse http://www.ietf.org/rfc/rfc0793.txt?number=793).

– IETF RFC 826 (1982), *An Ethernet Address Resolution Protocol – or – Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*, (disponible à l'adresse http://www.ietf.org/rfc/rfc0826.txt?number=826).

– IETF RFC 859 (1983), *Telnet Status Option,* (disponible à l'adresse http://www.ietf.org/rfc/rfc0859.txt?number=859).

– IETF RFC 959 (1985), *File Transfer Protocol (FTP),* (disponible à l'adresse http://www.ietf.org/rfc/rfc0959.txt?number=959).

– 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 1288 (1991), *The Finger User Information Protocol,* (disponible à l'adresse http://www.ietf.org/rfc/rfc1288.txt?number=1288).

– 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).

– IETF RFC 2045 (1996), *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies,* (disponible à l'adresse http://www.ietf.org/rfc/rfc2045.txt?number=2045).

– IETF RFC 2202 (1997), *Test Cases for HMAC-MD5 and HMAC-SHA-1,* (disponible à l'adresse http://www.ietf.org/rfc/rfc2202.txt?number=2202).

– IETF RFC 2222 (1997), *Simple Authentication and Security Layer (SASL),* (disponible à l'adresse http://www.ietf.org/rfc/rfc2222.txt?number=2222).

– IETF RFC 2246 (1999), *The TLS Protocol Version 1.0,* (disponible à l'adresse http://www.ietf.org/rfc/rfc2246.txt?number=2246).

– IETF RFC 2271 (1998), *An Architecture for Describing SNMP 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 (SNMP),* (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 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, (disponible à l'adresse http://www.ietf.org/rfc/rfc3414.txt?number=3414).

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

– IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*, (disponible à l'adresse http://www.ietf.org/rfc/rfc2401.txt?number=2401).

– IETF RFC 2402 (1998), *IP Authentication Header,* (disponible à l'adresse http://www.ietf.org/rfc/rfc2402.txt?number=2402).

– IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*, (disponible à l'adresse http://www.ietf.org/rfc/rfc2406.txt?number=2406).

– IETF RFC 2451 (1998), *The ESP CBC-Mode Cipher Algorithms,* (disponible à l'adresse http://www.ietf.org/rfc/rfc2451.txt?number=2451).

– IETF RFC 2616 (1999), *Hypertext Transfer Protocol (HTTP) – HTTP/1.1,* (disponible à l'adresse http://www.ietf.org/rfc/rfc2616.txt?number=2616).

– IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method,* (disponible à l'adresse http://www.ietf.org/rfc/rfc2631.txt?number=2631).

– IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core,* (disponible à l'adresse http://www.ietf.org/rfc/rfc3080.txt?number=3080).

– IETF RFC 3081 (2001), *Mapping the BEEP Core onto TCP,* (disponible à l'adresse http://www.ietf.org/rfc/rfc3081.txt?number=3081).

– ISO 7498-2:1989, *Systèmes de traitement de l'information – Interconnexion de systèmes ouverts – Modèle de référence de base – Partie 2: Architecture de sécurité* (disponible dans la boutique électronique de l'ISO, à l'adresse http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=14256&ICS1 =35&ICS2=100&ICS3=1).

– Recommandation UIT-T M.3010 (2000), *Principes du réseau de gestion des télécommunications* (disponible dans la librairie électronique de l'UIT).

– Recommandation UIT-T M.3013 (2000), *Considérations relatives aux réseaux de gestion des télécommunications* (disponible dans la librairie électronique de l'UIT).

– JANSEN (W.A.): A Revised Model for Role Based Access Control, *NIST-IR 6192*, juillet 1998, (disponible à l'adresse http://csrc.nist.gov/rbac/jansen-ir-rbac.pdf).

– JONSSON (J.), KALISKI (B.): On the Security of RSA Encryption in TLS, *Advances in Cryptology-Crypto 2002*, Springer LNCS Vol. 2442, pp. 127-142, août 2002.

– KELSEY (J.), SCHNEIER (B.), FERGUSON (N.): Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator, *Sixth Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, août 1999, (disponible à l'adresse http://www.counterpane.com/yarrow-notes.html).

– KRAWCZYK (H.): Security Analysis of the Internet Key Exchange's Signature-Based Key Exchange Protocol, *Advances in Cryptology-Crypto 2002*, Springer LNCS Vol. 2442, pp. 143-161, août 2002.

– LENSTRA (A.), VERHEUL (E.): Selecting Cryptographic Key Sizes, *Journal of Cryptology*, Vol. 14, No. 4, pp. 255-293, 2001.

– National Computer Security Center, NCSC-TG-004-88, *Glossary of Computer Security Terms*, octobre 1988, (disponible à l'adresse http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf).

– National Communications System, *Public Switched Network Security Assessment Guidelines*, septembre 2000, (disponible à l'adresse http://www.ncs.gov/ncs/Reports/NCS_Security_Assessment_Guidelines_Version1_sep00.pdf).

– Object Management Group, *Common Object Request Broker Architecture Security Service Specification*, *Version 1.8*, mars 2002, (disponible à l'adresse http://cgi.omg.org/docs/formal/02-03-11.pdf).

– Object Management Group, *Common Object Request Broker Architecture Security Service Specification, Version 1.7,* mars 2001, (disponible à l'adresse http://cgi.omg.org/docs/formal/01-03-08.pdf).

– Partnership for Critical Infrastructure Security, *Partnership for Critical Infrastructure Security Common Reference Glossary of Terms, Version 2001-09*, septembre 2001, (disponible à l'adresse http://www.pcis.org/library.cfm?urlSection=WG).

– RESCORLA (E.): SSL and TLS, Addison-Wesley, 2001.

– SCHNEIER (Bruce.): Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

– SILVERMAN (R.): The Mythical MIPS Year, *IEEE Computer*, août 1999.

– SILVERMAN (R.): A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths, *RSA Laboratories Bulletin*, No. 13, avril 2000.

– VAUDENAY (S.): Security Flaws Induced by CBC Padding – Applications to SSL, IPsec, WTLS, *Advances in Cryptology-Eurocrypt 2002*, Springer LNCS Vol. 2332, pp. 534-545, avril-mai 2002.

– World Wide Web Consortium, *Extensible Markup Language (XML) 1.0*, février 1998, (disponible à l'adresse http://www.w3.org/TR/1998/REC-xml-19980210).

– World Wide Web Consortium, *Simple Object Access Protocol 1.1*, D. Box et al, mai 2000, (disponible à l'adresse http://www.w3.org/TR/SOAP/).

– WU (T.): The Secure Remote Password Protocol, *Proceedings of the 1998 Internet Society Symposium on Network and Distributed Systems Security*, San Diego, California, pp. 97-111, mars 1998, (disponible à l'adresse http://www.isoc.org/isoc/conferences/ndss/98/wu.pdf)

– YLÖNEN, T.: SSH – Secure Login Connections Over the Internet, *Sixth USENIX Security Symposium Proceedings*, pp. 37-42, juillet 1996, (disponible à l'adresse http://www.usenix.org/publications/library/proceedings/sec96/full_papers/ylonen/index.html).

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, 2005