الاتحـــــاد الـــدولـــــي للاتصـــــــالات

ITU-T M.3016.0

(2005/05)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة M: إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات

شبكة إدارة الاتصالات

الأمن لمستوي الإدارة: عرض عام

التوصية ITU-T M.3016.0

الاتحاد الدولي للاتصالات

توصيات السلسلة M الصادرة عن قطاع تقييس الاتصالات

إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات

مقدمة ومبادئ عامة بشأن الصيانة وتنظيمها	M.10 – M.299
أنظمة الإرسال الدولية	M.300 – M.559
الدارات الهاتفية الدولية	M.560 – M.759
أنظمة التشوير على قناة مشتركة	M.760 – M.799
أنظمة الإبراق الدولية وإرسال الصور برقياً	M.800 – M.899
وصلات الزمر والزمر الثانوية المؤجرة الدولية	M.900 – M.999
الدارات الدولية المؤجرة	M.1000 – M.1099
أنظمة وخدمات الاتصالات المتنقلة	M.1100 – M.1199
الشبكة الدولية للهواتف العمومية	M.1200 – M.1299
الأنظمة الدولية لإرسال المعطيات	M.1300 – M.1399
تبادل التسميات والمعلومات	M.1400 – M.1999
شبكة النقل الدولية	M.2000 – M.2999
شبكة إدارة الاتصالات	**M.3000 – M.3599**
الشبكات الرقمية متكاملة الخدمات	M.3600 – M.3999
أنظمة التشوير على قناة مشتركة	M.4000 – M.4999

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

الأمن لمستوي الإدارة: عرض عام

ملخص

تقدم هذه التوصية عرضاً عاماً وإطاراً يحددان التهديدات التي يتعرض لها أمن أي شبكة لإدارة الاتصالات، ويعرضان بإيجاز الكيفية التي يمكن بها تطبيق خدمات الأمن في سياق المعمارية الوظيفية لشبكة إدارة الاتصالات.

المصدر

وافقت لجنة الدراسات 4 (2005-2008) لقطاع تقييس الاتصالات بتاريخ 22 مايو 2005 على التوصية ITU-T M.3016.0 بموجب الإجراء المحدد في التوصية A.8.

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات. وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA)، التي تجتمع مرة كل أربع سنوات، المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB).

المحتويات

الصفحة

الأمن لمستوي الإدارة: عرض عام

1 مجال التطبيق

تقدم هذه التوصية عرضاً عاماً وإطاراً يحددان التهديدات التي يتعرض لها أمن أي شبكة لإدارة الاتصالات، ويعرضان بإيجاز الكيفية التي يمكن بها تطبيق خدمات الأمن ضمن سياق المعمارية الوظيفية لشبكة إدارة الاتصالات على النحو المبين في التوصية ITU-T M.3010.

وهذه التوصية عامة بطبيعتها، كما لا تحدد أو تتناول المتطلبات الخاصة لسطح بيني محدد لشبكة لإدارة الاتصالات.

ولا تنشد هذه التوصية تحديد خدمات أمنية جديدة لكنها تستخدم خدمات الأمن القائمة المحددة في توصيات أخرى لقطاع تقييس الاتصالات وفي معايير المنظمة الدولية للتوحيد القياسي.

وهذه التوصية جزء من توصيات السلسلة M.3016.x الصادرة عن قطاع تقييس الاتصالات والغرض منها هو تقديم إرشادات وتوصيات لتأمين مستوي إدارة الشبكات المتطورة:

التوصية ITU-T M.3016.0 – *الأمن لمستوي الإدارة: عرض عام.*

التوصية ITU-T M.3016.1 – *الأمن لمستوي الإدارة: متطلبات الأمن.*

التوصية ITU-T M.3016.2 – *الأمن لمستوي الإدارة: خدمات الأمن.*

التوصية ITU-T M.3016.3 – *الأمن لمستوي الإدارة: آلية الأمن.*

التوصية ITU-T M.3016.4 – *الأمن لمستوي الإدارة: نموذج الملامح العامة.*

وتحدد التوصيات ITU-T M.3016.1 وITU-T M.3016.2 وITU-T M.3016.3 مجموعة من المتطلبات والخدمات والآليات لضمان الأمن الملائم للوظائف الإدارية الضرورية لدعم البُنى التحتية للاتصالات. وبالنظر إلى أن الإدارات والمنظمات المختلفة تتطلب سويات مختلفة فيما يتعلق بالدعم الأمني، لا تحدد التوصيات ITU-T M.3016.1 وITU-T M.3016.2 وITU-T M.3016.3 ما إذا كان متطلب/خدمة/آلية إلزامياً أم اختيارياً.

والهدف من النموذج المحدد في التوصية ITU-T M.3016.4 هو مساعدة المنظمات والإدارات وغيرها من المنظمات الوطنية/الدولية على تحديد الدعم الإلزامي والاختياري للمتطلبات وكذلك مدى القيم والقيم ذاتها، إلخ. من أجل مساعدة هذه المنظمات والإدارات في تنفيذ سياساتها الأمنية.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، نحث جميع المستعملين لهذه التوصية على السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

- التوصية ITU-T E.408 (2004)، *متطلبات أمن شبكات الاتصالات.*
- التوصية ITU-T M.3010 (2000)، *مبادئ شبكة إدارة الاتصالات.*
- التوصية ITU-T M.3400 (2000)، *وظائف إدارة شبكة إدارة الاتصالات.*
- التوصية ITU-T X.509 (2000)، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – الدليل: أطر التصديق العمومية الرئيسية وتصديق النعوت.*

- التوصية ITU-T X.741 (1995)، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – إدارة الأنظمة: مواضيع ونعوت مراقبة النفاذ.*
- التوصية ITU-T X.800 (1991)، *معمارية الأمن للتوصيل البيني للأنظمة المفتوحة من أجل تطبيقات اللجنة الاستشارية الدولية للبرق والهاتف.*
- التوصية ITU-T X.802 (1995)، *تكنولوجيا المعلومات – نموذج الأمن في الطبقات السفلى.*
- التوصية ITU-T X.803 (1994)، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – نموذج الأمن في الطبقات العليا.*
- التوصية ITU-T X.810 (1995)، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: عرض عام.*
- التوصية ITU-T X.812 (1995)، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: إطار مراقبة النفاذ.*
- التوصية ITU-T X.813 (1996)، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: إطار عدم الإنكار.*
- التوصية ITU-T X.814 (1995)، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: إطار السرية.*
- التوصية ITU-T X.815 (1995)، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: إطار التكاملية.*
- التوصية ITU-T X.816 (1995)، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: إطار تدقيق الأمن والإنذارات.*
- الوثيقة ISO/IEC 9979:1999، *تكنولوجيا المعلومات – تقنيات الأمن – إجراءات تسجيل خوارزميات التشفير.*

3 التعاريف

لا تتضمن هذه التوصية أية مصطلحات جديدة.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات التالية:

CCITT اللجنة الاستشارية الدولية للبرق والهاتف *(International Telegraph and Telephone Consultative Committee)*

DCN شبكة توصيل المعطيات *(Data Communication Network)*

FC الأصناف الوظيفية *(Functional classes)*

ISO المنظمة الدولية للتوحيد القياسي *(International Organization for Standardization)*

ITU-T قطاع تقييس الاتصالات في الاتحاد *(Telecommunication Standardization Sector)*

LLA المعمارية المنطقية المبنية حسب الطبقات *(Logical Layered Architecture)*

MF وظيفة وساطة *(Mediation Function)*

NEF وظيفة عنصر الشبكة *(Network Element Function)*

OSF وظيفة نظام التشغيل *(Operation System Function)*

OSI التوصيل البيني للنظام المفتوح *(Open System Interconnection)*

PIN الرقم الشخصي لتعرف الهوية *(Personal Identification Number)*

TF وظيفة تحويل *(Transformation Function)*

TMN شبكة إدارة الاتصالات *(Telecommunications Management Network)*

TTP طرف ثالث موثوق به *(Trusted Third Party)*

WSF وظيفة محطة التشغيل *(WorkStation Function)*

5 الأسباب الجوهرية لمتطلب الأمن

يعود منشأ متطلبات الأمن في شبكة إدارة الاتصالات إلى مصادر مختلفة:

- **العملاء/المشتركون** يحتاجون إلى الثقة في الشبكة وفي الخدمات المقدمة، بما في ذلك الإعداد السليم للفواتير.
- **المجتمع/السلطات العامة** يتطلبان توفير الأمن بموجب قرارات رسمية وقوانين بغية ضمان تيسر الخدمات وحماية الخصوصية.
- **مشغلو الشبكات/مقدمو الخدمات** أنفسهم يحتاجون إلى الأمن للمحافظة على مصالح عملياتهم وأعمالهم التجارية وللوفاء بالتزاماتهم تجاه الزبائن وعامة الناس.

والغرض من شبكة إدارة الاتصالات هو إدارة شبكة الاتصالات التحتية؛ ومن ثم، فإن أمن شبكة إدارة الاتصالات ضروري للأداء السليم لشبكة الاتصالات. وبالإضافة إلى ذلك، فإن شبكة الاتصالات يمكن أن تتضمن ملامح أمنية بارزة تحتاج أن تديرها شبكة إدارة الاتصالات. وتسرد التوصية ITU-T M.3400 وظائف إدارة الأمن هذه.

ومن الأفضل أن تستند معايير الأمن المستخدمة في شبكة إدارة الاتصالات إلى معايير الأمن المتفق عليها دولياً لأنه من المفيد إعادة استخدام المعايير القائمة بدلاً من إيجاد معايير جديدة. فتوفير خدمات وآليات الأمن واستعمالهما يمكن أن يكونا غالي التكلفة تماماً بالقياس إلى قيمة المعاملات التي يجري حمايتها. ولذلك من المهم أن يكون في الإمكان تحديد الأمن المقدم وفقاً لمعاملات شبكة إدارة الاتصالات التي يجري حمايتها. وينبغي أن توفر خدمات وآليات الأمن المستخدمة لتأمين معاملات شبكة إدارة الاتصالات على نحو يسمح بإجراء هذه المواءمة. ونظراً للعدد الكبير من ملامح الأمن التي يمكن الجمع بينها فإن المستصوب هو توفير **ملامح أمنية** (انظر التذييل I) تغطي مجموعة عريضة من التطبيقات الخاصة بأمن شبكة إدارة الاتصالات.

وسيسهّل التقييس **استخدام الحلول والنواتج من جديد** مما يعني أن الأمن يمكن أن يتحقق بوتيرة أسرع وبتكلفة أخفض.

وتتمثل فوائد هامة للحلول المقيسة بالنسبة لبائعي ومستعملي الأنظمة أيضاً في وفورات الحجم الكبير فيما يتعلق بتطوير المنتج وفي التشغيل البيني للمكونات داخل نظام شبكة إدارة الاتصالات فيما يتعلق بالأمن.

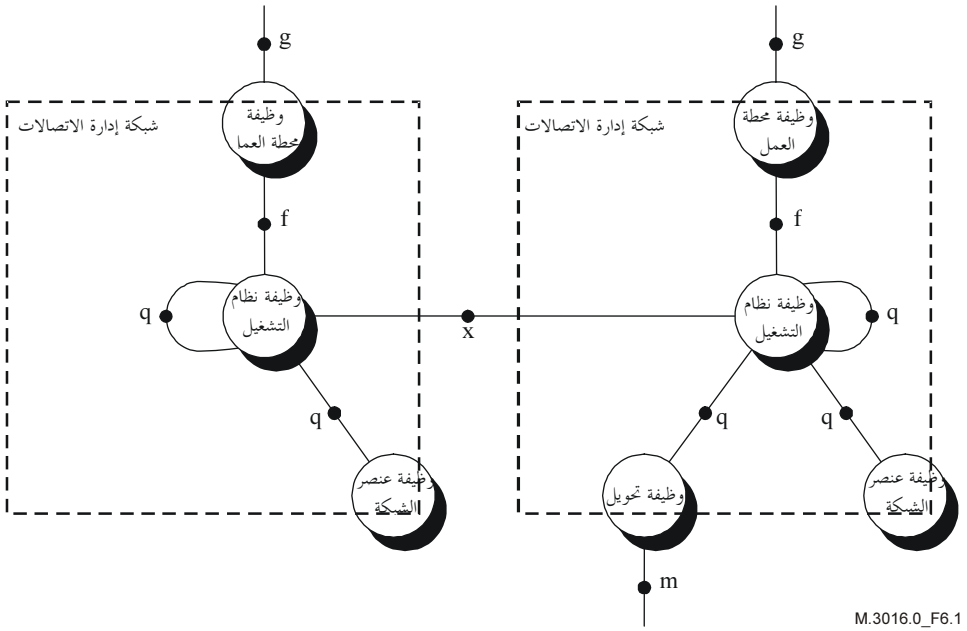
ومن الضروري توفير خدمات وآليات الأمن لحماية معاملات شبكة إدارة الاتصالات بين كيانات الشبكة، (حسبما تحددها التوصية ITU-T M.3010) من الهجمات الخبيثة مثل التنصت الخفي على الرسائل أو تزويرها أو التلاعب بها (تعديل الرسائل، أو تأخيرها، أو الحذف منها، أو الإدراج فيها، أو تكرارها، أو إعادة تسييرها، أو تسييرها على نحو خاطئ، أو إعادة ترتيبها)، أو إنكارها أو تزييفها. وتشمل الحماية الوقاية من الهجمات وكشفها واسترجاع الأمن، بالإضافة إلى إدارة المعلومات المتعلقة بالأمن. وينبغي للمعايير أن تغطي كلا السطوح البينية داخل المجالات (Q وF) وبين المجالات (X).

6 وصف النظام

إن الهدف المنشود من هذه التوصية هو تجريد يجعل في الإمكان تفادي الكثير من تفاصيل التنفيذ، والاتفاق على النتائج التي قد تكون مفيدة عندما يجري تقابلها فيما بعد مع أهداف تنفيذية محددة.

وتوصف شبكة إدارة الاتصالات على أساس معمارية وظيفية ومعمارية معلومات ومعمارية مادية (التوصية ITU-T M.3010).

ويسلّم في التوصية ITU-T M.3010 بأن الأبنية الفدرية لشبكة إدارة الاتصالات يمكن أن تدعم سطوح بينية أخرى بالإضافة إلى السطوح البينية Q وX وF. وبالمثل، يمكن أن يكون للتجهيزات المادية عناصر وظيفية أخرى بالإضافة إلى العناصر الوظيفية المرتبطة بالمعلومات الواردة عن طريق السطوح البينية Q وX وF. وتقع هذه السطوح البينية الإضافية والعناصر الوظيفية المرتبطة بها خارج نطاق شبكة إدارة الاتصالات ومن ثم، خارج نطاق تقييس الأمن الخاص بشبكة إدارة الاتصالات.



الشكل M.3016.0/1 – المعمارية الوظيفية لشبكة إدارة الاتصالات

1.6 الجهات الفاعلة والأدوار

لغرض تقييس أمن شبكة إدارة الاتصالات، لن يولى الاهتمام إلاّ للأمن التقني مما يعني أن الجهات الفاعلة ذات الصلة وموضع الاهتمام هم مستعملو شبكة إدارة الاتصالات. ومستعمل شبكة إدارة الاتصالات هو شخص أو عملية تطبق خدمات إدارة شبكة إدارة الاتصالات لغرض إنجاز عمليات الإدارة. ويمكن أيضاً تصنيف مستعملي شبكة إدارة الاتصالات في فئات تبعاً لما إذا كانوا ينتمون إلى المنظمة التي تدير شبكة إدارة الاتصالات (مستعملون داخليون) أو ما إذا كانوا ينفذون إلى شبكة إدارة الاتصالات بوصفهم مستعملين خارجيين.

وكل مرة ينفذ فيها مستعمل لشبكة إدارة الاتصالات إلى إحدى خدمات الإدارة، فإن هذا المستعمل سيضطلع بدور. وفي بعض الحالات تنشأ علاقة تلازم بين مستعمل شبكة إدارة اتصالات ودور ما، أي أن هذا المستعمل للشبكة سيظل دائماً يضطلع بالدور ذاته. وفي حالات أخرى تنشأ علاقة كثيرة الأدوار بين مستعمل محدد لشبكة إدارة الاتصالات والأدوار الممكنة التي يستطيع هذا المستعمل أداءها.

ويرد فيما يلي تصنيف عالي المستوى لبعض الأدوار المشتركة:

- مشغلو الشبكة (*من القطاع الخاص أو القطاع العام*)؛
- مقدمو الخدمات (*مقدمو خدمات الحمالة أو مقدمو خدمات قيمة مضافة*)؛
- المشتركون في الخدمة/زبائن الخدمة؛
- المستعملون النهائيون للخدمة؛
- بائعو التجهيزات/البرمجيات؛

– طرف ثالث موثوق به (أي طرف ثالث موضع ثقة كلا الطرفين ويعمل وفقاً للقوانين واللوائح الوطنية ذات الصلة من أجل تيسير إصدار الشهادات والاستيقان والخدمات المتعلقة بهما).

وعند تأمين شبكة إدارة الاتصالات، لا يكفي مراقبة سلوك مستعملين معروفين لشبكة إدارة الاتصالات. وينبغي للمرء أن يبحث أيضاً إمكانية محاولة مقتحم النفاذ على نحو غير قانوني إلى شبكة إدارة الاتصالات.

وتتطلب بعض التدابير الأمنية أن تؤدي الجهات الفاعلة دور الطرف الثالث الموثوق به (TTP). وتتمثل مسألة أمنية أهم في كيفية السماح لهذه الجهات الفاعلة بالتفاعل مع شبكة إدارة الاتصالات.

2.6 مجالات الأمن

تستحدث التوصية ITU-T M.3010 مفهوم معمارية منطقية مبنينة حسب الطبقات (LLA) تنقسم فيها العناصر الوظيفية للإدارة إلى طبقات. وتُعنى كل طبقة بمجموعة فرعية واضحة التحديد من أنشطة الإدارة الشاملة. وتصبح كل طبقة وظيفية *مجال إدارة* مستقل تحت مراقبة وظيفة نظام التشغيل (OSF)، ويطلق عليها مجال وظيفة نظام التشغيل. وستشكل وظائف عنصر الشبكة (NEFs) التي تراقبها وظيفة نظام التشغيل جزءاً من مجال وظيفة نظام التشغيل. وبذا تكون شبكة إدارة الاتصالات بصفتها هذه مؤلفة من مجال أو عدة مجالات لوظيفة نظام التشغيل حيث تكون مختلف هذه المجالات إما منفصلة أو متفاعلة أو متراكبة أو محتواة.

ويعرَّف *مجال الأمن* بأنه مجموعة من الكيانات والأطراف التي تخضع لسياسة أمنية منفردة ولإدارة أمنية منفردة. ووفق أي افتراض عادي تعتبر شبكة إدارة الاتصالات بمثابة مجال أمن واحد. وغالباً ما ستكون الحالة كذلك، بيد أنه قد لا يكون من السليم جعله افتراضاً عاماً. ففي شبكة إدارة الاتصالات الكبيرة التي تتألف من كثير من أنظمة الإدارة المختلفة، فقد يخضع مختلف أجزاء الشبكة لسياسات أمنية مختلفة ومتطلبات أمنية مختلفة. لذلك يبدو من الأكثر ملائمة القول بأن المجال الأمني لشبكة إدارة الاتصالات يشمل مجالاً واحداً منفرداً لوظيفة نظام التشغيل أو مجموعة من مجالات وظيفة نظام التشغيل.

وباستخدام هذا الافتراض، ستطبق العلاقات التالية بين مجالات الأمن وداخل مجالات الأمن:

العلاقات الممكنة داخل مجالات الأمن:

– q (OSF-NEF, OSF-OSF).

العلاقات الممكنة بين مجالات الأمن:

– x (OSF-OSF)؛

– f (WSF-OSF, WSF-MF)؛

– q (OSF-OSF, OSF-TF).

لاحظ أن العلاقات المشار إليها آنفاً تشير إلى مجالات أمن لا إلى مجالات إدارة. وثمة مسألة هامة ينبغي ملاحظتها هي أن النقطة المرجعية q يمكن أن تنخرط في كلا العلاقات داخل مجالات الأمن والعلاقات بين مجالات الأمن. ويتمثل فارق رئيسي بين العلاقات داخل المجالات والعلاقات بين المجالات في درجة الثقة القائمة بين الكيانات المعنية.

7 الأهداف الأمنية التنوعية لشبكة إدارة الاتصالات

يتمثل الغرض من هذه الفقرة في وصف الهدف الأساسي من التدابير الأمنية التي تتخذ في بيئة خاضعة لشبكة إدارة اتصالات. وينصب مجال التركيز على ماهية الأمن الذي يتحقق لا على الكيفية التي سيتحقق بها.

ويجب أن تُستَمَد الأهداف الأمنية من المصالح وعلاقات الأعمال التجارية للمشغل والجهات الفاعلة الأخرى ومن القيود القانونية والتنظيمية والقيود التعاقدية، إلخ.

وتتمثل الأهداف الأمنية لشبكة إدارة الاتصالات فيما يلي:

– يجب أن تكون الجهات الفاعلة الشرعية فقط هي التي يمكنها النفاذ إلى الأصول الكائنة في شبكة إدارة الاتصالات وتشغيلها.

– يجب أن تكون الجهات الفاعلة الشرعية قادرة على النفاذ إلى الأصول المصرح لها بالنفاذ إليها، وتشغيلها.

- يجب اعتبار جميع الجهات الفاعلة مسؤولة عن أفعالها الخاصة في شبكة إدارة الاتصالات، وفقط عن أفعالها الخاصة.
- ينبغي حماية تيسُّر شبكة إدارة الاتصالات من النفاذ غير المتطلب أو العمليات غير المتطلبة.
- يجب أن يكون في الإمكان استرجاع المعلومات المتعلقة بالأمن من شبكة إدارة الاتصالات.
- إذا كشفت انتهاكات الأمن، ينبغي أن تعالج على نحو مراقب، وبذلك يقل إلى أدنى حد الضرر الناجم عن الانتهاكات.
- بعد كشف خرق للأمن، يجب أن يكون في الإمكان استعادة سويات الأمن العادية.
- ويجب أن توفر معمارية أمن شبكة إدارة الاتصالات قدراً من المرونة لكي تدعم السياسات الأمنية المختلفة، على سبيل المثال، قوة آليات الأمن المختلفة.

ولا يفهم من تعبير "النفاذ إلى الأصول" فقط إمكانية أداء الوظائف وإنما أيضاً إمكانية قراءة المعلومات.

ويتم التعبير عن الأهداف التنوعية وفقاً لرأي وأسلوب إدارة المؤسسة. ويتعين التعبير عن الفقرات التالية بمصطلحات أكثر تقنية تؤدي إلى خدمات ووظائف أمنية قابلة للتنفيذ. والتقابل بين الأسلوبين ليس واضحاً دائماً.

ويمكن الإشارة إلى أنه بتحقيق مجموعة الأهداف الأمنية التالية ستتحقق الأهداف الأمنية الخمسة الأولى لشبكة إدارة الاتصالات المذكورة آنفاً في هذه الفقرة:

- السرية؛
- تكاملية المعطيات؛
- المسؤولية؛
- التيسر.

وستستند التهديدات والمخاطر المحددة في الفقرة 9 والمتطلبات الوظيفية الواردة في الفقرة 6 إلى هذه المصطلحات الأكثر اتساماً بالصبغة الرسمية. وللاطلاع على التعاريف، انظر الفقرة 9.

8 المسائل التشريعية

ينبغي أن يكون بوسع البنية التحتية للأمن في شبكة إدارة الاتصالات مراعاة القيود التي تفرضها القوانين الحكومية، والتشريعات التعاقدية والمعاهدات والقواعد التنظيمية. وقد تشمل هذه القيود خدمات أمنية إلزامية (من مثل ضمان سرية المعلومات المتعلقة بالزبائن) أو استبعاد بعض آليات الأمن (من مثل بعض أنماط التشفير) و/أو تقديم الدعم لوكالات إنفاذ القوانين في إجراء التنصت الهاتفي السري.

9 التهديدات والمخاطر

يتمثل الغرض من هذه الفقرة في استكشاف التهديدات والمخاطر التي تتعرض لها شبكة إدارة الاتصالات. وليس القصد هنا هو تحديد تقييم للمخاطر أو تحليل للتهديدات التي تتعرض لها فرادى حالات شبكات إدارة اتصالات فهذه المسائل محلية ويمكن معالجتها بطرق مختلفة من قبل كل مقدم للخدمة بدون التأثير على قابلة التشغيل البيني.

ويمثل أي تهديد انتهاكاً محتملاً للأمن. ووفقاً للأهداف الأمنية التنوعية المحددة فيما يتعلق بشبكة إدارة الاتصالات، فإن التهديدات يمكن أن توجه إلى أربعة أنواع مختلفة من الأهداف:

- **السرية** (سرية المعلومات المخزونة والمنقولة)؛
- **تكاملية المعطيات** (حماية المعلومات المخزونة والمنقولة)؛
- **المسؤولية** (يجب أن يكون أي كيان مسؤولاً عن أي أفعال يشرع في تنفيذها)؛
- **التيسر** (يجب على جميع الكيانات الشرعية أن تمارس نفاذاً سليماً إلى مرافق شبكة إدارة الاتصالات).

وتميز هذه التوصية بين ثلاثة أنواع من التهديدات:

- التهديد غير المقصود: هو تهديد لا ينطوي منشؤه على أي قصد خبيث؛
- التهديد الإداري: هو تهديد ينشأ من قصور في إدارة الأمن؛
- التهديد المقصود: هو تهديد يصدر عن كيان خبيث قد يهاجم إما الاتصال ذاته أو موارد الشبكة.

ويمكن في العمل التقييسي لشبكة إدارة الاتصالات أن تؤخذ التهديدات غير المقصودة والتهديدات الإدارية في الاعتبار طالما كانت عواقبهما تماثل عواقب التهديدات المقصودة. وبغية تقديم تحليل أكثر دقة للتهديدات يراعي معمارية شبكة إدارة الاتصالات، تركز هذه التوصية على التهديدات المقصودة التي تتعرض لها الاتصالات بين جهات فاعلة مختلفة في شبكة إدارة الاتصالات. والغرض من هذا النهج هو تقديم قائمة مختصرة بالتهديدات التي يمكن أن تستعمل مباشرة في العمل التقييسي لشبكة إدارة الاتصالات. ومن ثم فإن أي تحليل للتهديدات التي تتعرض لها شبكة إدارة الاتصالات ينبغي أن يتناول البنود التالية التي تستند إلى التوصية ITU-T X.800:

- **التنكر** (**"التزوير"**): ادعاء أي كيان بأنه كيان مختلف؛
- **التنصّت الخفي**: هو خرق للسرية من خلال مراقبة الاتصال؛
- **النفاذ غير المسموح**: هو أن يحاول كيان النفاذ إلى المعطيات منتهكاً السياسة الأمنية المنفذة؛
- **فقدان المعلومات أو خطؤها**: تتعرض تكاملية المعطيات المنقولة للخطر من جرّاء عمليات الشطب أو الإدراج أو التعديل أو إعادة الترتيب أو التكرار أو التأخير غير المصرّح بها؛
- **الإنكار**: يتمثل في كيان يتبادل اتصالاً ثم ينكر واقعة حدوث ذلك؛
- **التزوير**: يتمثل في كيان يلفق معلومات ويدعي أنه تلقى هذه المعلومات من كيان آخر أو أرسلت إلى كيان آخر؛
- **رفض الخدمة**: يحدث هذا عندما يقصر كيان عن أداء وظيفته أو يمنع كيانات أخرى من أداء وظائفها. وقد يشمل هذا رفض النفاذ إلى شبكة إدارة الاتصالات والحيلولة دون الاتصال عن طريق إغراق شبكة إدارة الاتصالات بالاتصالات. وفي شبكة متقاسمة، يمكن إدراك هذا التهديد على أنه بمثابة اختلاق حركة إضافية تغمر الشبكة وتحول دون استعمال الآخرين للشبكة عن طريق تأخير حركتهم.

ويقدم الجدول 1 تقابلاً للتهديدات والأهداف.

الجدول M.3016.0/1 – تقابل التهديدات والأهداف

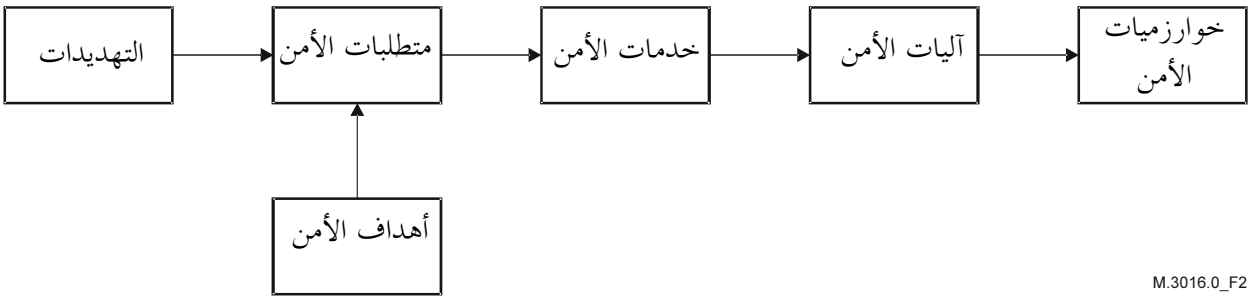
التهديد	السرية	تكاملية البيانات	المسؤولية	التيسر
التنكر	x	x	x	x
التنصت الخفي	x			
النفاذ غير المسموح	x	x	x	x
فقدان المعلومات (المنقولة) أو خطؤها		x		x
الإنكار			x	
التزوير		x	x	
رفض الخدمة				x

وإن أي تهديد محتمل لنظام ما لا ينجم عنه ضرر إلاّ إذا كان هناك ضعف مقابل في النظام وتوقيت زمني يمكن فيه استغلال هذا الضعف. وسينطوي كل تهديد على مخاطر. ويمكن أن ينقسم تقييم المخاطر إلى تقييم أرجحية حدوث كل تهديد وتقييم الأثر الذي يمكن أن يحدثه التهديد. وينبغي أن يكون تقييم التهديدات والمخاطر جزءاً من عملية تفاعلية: فالتهديدات الجديدة

يمكن أن تنشأ عندما تتخذ الإجراءات المضادة، على سبيل المثال التهديدات الموجهة إلى مفاتيح التجفير عندما تستعمل تدابير التجفير.

10 متطلبات الأمن وخدماته

يبين الشكل 2 العلاقات بين أهداف الأمن والتهديدات ومتطلبات الأمن وخدماته. وهو يصور كيفية اشتقاق "متطلبات الأمن" من "التهديدات" و"أهداف الأمن" التي ستتحقق بدورها من خلال مجموعة خدمات أمن. وستستعمل هذه "الخدمات" التي تقاوم التهديدات، "آليات" تستعمل هي ذاتها "خوارزميات أمن".



الشكل M.3016.0/2 – إطار الأمن

وتعدِّد الفقرة 1.10 متطلبات الأمن هذه. ولا تعني كلمة "متطلب" في هذه التوصية أن بعض العناصر الوظيفية إلزامي دائماً في كل شبكة لإدارة الاتصالات؛ وإنما تعني بالأحرى أن إدارة شبكة لإدارة الاتصالات يمكن أن تجعل عناصر وظيفية معينة إلزامية بالنسبة لبعض التطبيقات و/أو السطوح البينية المحددة لشبكة إدارة الاتصالات تلك. وسيتوقف الاختيار الفعلي على أهداف الأمن المعلنة في السياسة الأمنية للمشغل.

وبالإضافة إلى متطلبات الأمن وخدماته، تعرض هذه الفقرة أيضاً بعض المتطلبات التنوعية لإدارة خدمات الأمن (انظر الفقرة 2.10) وكذلك المتطلبات المعمارية الناظمة لتكاملية خدمات الأمن في معمارية شبكة إدارة الاتصالات (انظر الفقرة 3.10). وتتسم المتطلبات الإدارية ومتطلبات الدورة الحياتية بأهميتها لكنها لن تؤثر على المعمارية كما أنها غير مدرجة في هذه الفقرة.

1.10 متطلبات الأمن والخدمات المناسبة لها

تعرض هذه الفقرة مجموعة من المتطلبات الوظيفية التنوعية والخدمات المناسبة لها التي يمكن استعمالها في مقاومة التهديدات التي تتعرض لها شبكة إدارة الاتصالات.

1.1.10 تقابل المتطلبات الوظيفية والتهديدات وأهداف الأمن

ستحدد هذه الفقرة متطلبات الأمن الوظيفية لمواجهة التهديدات المذكورة في الفقرة 9. وقد تحقق ذلك في الجدول 2. ومن هذا الجدول، جرى وضع متطلبات الأمن في تقابل (الجدول 3) مع أهداف الأمن المبينة في الفقرة 7. وتقتصر هذه القائمة على المتطلبات التنوعية بطبيعتها والتي لها تأثير جوهري على المكونات والمعمارية.

الجدول M.3016.0/2 – تقابل المتطلبات الوظيفية والتهديدات

المتطلب الوظيفي	التنكر	التنصت الخفي	النفاذ غير المسموح	فقدان المعلومات أو خطؤها	الإنكار	التزوير	رفض الخدمة
التحقق من الهويات	x		x				
النفاذ والتخويل المراقبان			x				x
حماية السرية		x	x				
حماية تكاملية المعطيات				x			
المسؤولية					x	x	
تسجيل النشاط	x		x		x	x	x
الإخبار عن الإنذار	x		x	x			x
التدقيق	x		x		x	x	x

والأهداف المستعملة هي الأهداف الأربعة الرسمية المحددة في الفقرة 3، وكل منها وارد في عمود في الجدول 3، يبين مجموعة المتطلبات الوظيفية اللازمة لتحقيق الهدف المعني.

2.1.10 بيان المتطلبات الوظيفية والخدمات المناسبة لها

تناقش المتطلبات الوظيفية الواردة في الجدولين 2 و3 أيضاً في النص الذي يلي هذه الفقرة وتحدد بالنسبة لكل متطلب خدمات الأمن المناسبة له. والملاحظ أن متطلبات أي من هذه الوظائف لا يستدعي تلقائياً خدمة أمنية على النحو الذي تحدده المنظمة الدولية للتوحيد القياسي. غير أنه هناك في التطبيق توافقاً في بعض الحالات.

الجدول M.3016.0/3 – تقابل أهداف الأمن والمتطلبات الوظيفية

المتطلب الوظيفي	السرية	تكاملية المعطيات	المسؤولية	التيسر
التحقق من الهويات	x	x	x	
النفاذ والتخويل المراقبان	x	x	x	x
حماية السرية	x			
حماية تكاملية المعطيات		x		
المسؤولية			x	
تسجيل النشاط			x	x
الإخبار عن الإنذار	x	x	x	x
التدقيق			x	x

1.2.1.10 التحقق من الهويات

يجب على شبكة إدارة الاتصالات أن توفر المقدرة اللازمة لتحديد الهوية المُدعاة لأية جهة فاعلة في شبكة إدارة الاتصالات والتحقق من هذه الهوية.

ويمكن أن تكون الجهات الفاعلة مستعملين أو كيانات داخل شبكة إدارة الاتصالات. وتوفر الهويات المتحقق منها الأساس للمسؤولية، وتشكل عاملاً أساسياً في الوفاء بمعظم متطلبات الأمن الواردة في هذه الفقرة.

والخدمة الأمنية اللازمة لدعم المتطلب هي **الاستيقان**. وتقدم خدمة الاستيقان البرهان على أن هوية الكيان أو الشخص هي في الواقع الهوية التي يُدعى أن تكون. ورهناً بنوع الجهة الفاعلة وبالغرض من تعرف الهوية، يمكن طلب الأنواع التالية من الاستيقان:

- استيقان المستعمل الذي يوفر البرهان على هوية الإنسان المستعمل أو عملية التطبيق؛
- استيقان الكيان الند الذي يقدم البرهان على هوية الكيان الند أثناء علاقة الاتصال؛
- استيقان مصدر المعطيات الذي يقدم البرهان على الهوية المسؤولة عن وحدة معطيات محددة.

ويقدم استعمال خدمة الاستيقان البرهان بالنسبة لمرحلة زمنية معينة. ولضمان استمرار البرهنة، يتعين تكرار الاستيقان أو وصله بخدمة تكاملية.

والأمثلة على الآليات المستعملة لتنفيذ خدمة الاستيقان تتمثل في كلمات السر وأرقام الهوية الشخصية (PINs) (الاستيقان البسيط) والأساليب المستندة إلى التجفير (الاستيقان القوي).

2.2.1.10 النفاذ والتخويل المراقبان

يجب على شبكة إدارة الاتصالات أن توفر المقدرة اللازمة لضمان الحيلولة بين الجهات الفاعلة وبين إمكانية النفاذ إلى المعلومات أو الموارد غير المخول لهذه العناصر النفاذ إليها.

وتتمثل الخدمة الأمنية اللازمة للوفاء بهذا المتطلب في **مراقبة النفاذ**. فخدمة مراقبة النفاذ توفر وسائل ضمان أن الفاعلين لم ينفذوا إلى الموارد إلاّ بطريقة مخوَّلة. وقد تكون الموارد المعنية هي النظام المادي أو برمجيات أو تطبيقات أو معطيات النظام. ويمكن تحديد خدمة مراقبة النفاذ وتنفيذها على سويات مختلفة من التحبيبة في شبكة إدارة الاتصالات: على سوية الوكيل، أو سوية الموضوع أو سوية النعت. والقيود على النفاذ مبينة في المعلومات المتعلقة بمراقبة النفاذ التي تحدد ما يلي:

- وسائل تحديد أي الكيانات مخول للنفاذ؛
- أي نوع من النفاذ مسموح به (القراءة، الكتابة، التعديل، الابتكار، الشطب).

ويمكن تقسيم مراقبة أكثر تحديداً للنفاذ إلى شبكة إدارة الاتصالات إلى ثلاثة أنواع:

- *مراقبة النفاذ إلى تصاحب الإدارة*

  تمكن هذه الخدمة من مراقبة النفاذ عند سوية تصاحب الإدارة، الأمر الذي يعني أن حقوق النفاذ مرتبطة بالتصاحب ذاته، أي بالحق في إقامة التصاحب.
- *مراقبة النفاذ إلى تبليغات الإدارة*

  تمكن هذه الخدمة من مراقبة النفاذ فيما يتعلق بالتبليغات، أي ضمان عدم كشف التبليغات سوى للكيانات المسموح لها بتلقيها.
- *مراقبة النفاذ إلى الموارد المدارة*

  توفر هذه الخدمة مراقبة النفاذ فيما يتعلق بالموارد ذاتها.

ويتعين التحقق من هوية الكيان الذي يحاول النفاذ وذلك قبل منح حق النفاذ إلى الموارد. ويعني هذا أن استعمال مراقبة النفاذ يرتبط دائماً باستعمال خدمة الاستيقان.

3.2.1.10 حماية السرية

يجب على شبكة إدارة الاتصالات أن توفر المقدرة على ضمان سرية المعطيات المخزونة والمبلغة.

وتتمثل خدمات الأمن اللازمة لدعم هذا المتطلب في: **مراقبة النفاذ** إلى المعطيات المخزونة **وسرية المعطيات** بالنسبة للمعطيات المبلَّغة. وقد يلزم أيضاً متطلب **سرية المعطيات** بالنسبة لأنواع معينة من المعطيات المخزونة من مثل كلمات السر.

وتوفر خدمة السرية الحماية من الإفشاء غير المسموح للمعطيات المتبادلة.

والأنواع التالية من الخدمات المتعلقة بالسرية أنواع متميزة:

- السرية الانتقائية للمجالات؛

- سرية التوصيلات؛
- سرية تدفق المعطيات.

4.2.1.10 حماية تكاملية المعطيات

يجب أن تكون شبكة إدارة الاتصالات قادرة على ضمان تكاملية المعطيات المخزونة والمبلغة.

تتمثل خدمات الأمن اللازمة لدعم هذا المتطلب في: **مراقبة النفاذ** و**تكاملية المعطيات** بالنسبة للمعطيات المخزونة، و**تكاملية المعطيات** بالنسبة للمعطيات المبلغة.

وتوفر الخدمة الخاصة بالتكاملية الوسائل اللازمة لضمان صحة المعطيات المتبادلة كما تحمي هذه المعطيات من التعديل أو الشطب أو الابتكار (الإدراج) أو التكرار. والأنواع التالية من الخدمات الخاصة بالتكاملية هي أنواع متميزة:

- تكاملية المجالات الانتقائية؛
- تكاملية التوصيل بدون استرجاع؛
- تكاملية التوصيل مع استرجاع.

5.2.1.10 المسؤولية

يجب على شبكة إدارة الاتصالات أن توفر المقدرة على عدم تمكين أي كيان من إنكار مسؤوليته عن أيٍّ من الأفعال التي أداها وعما ترتب عليها من آثار أيضاً.

وتدعم هذا المتطلب خدمة **عدم الإنكار** الملزمة للشخص (أو الكيان) إزاء العملية المؤداة. وتوفر خدمات عدم الإنكار الوسيلة لإثبات أن تبادل المعطيات قد حدث فعلاً. وتتحقق هذه الخدمة في شكلين:

- عدم الإنكار: إثبات المصدر؛
- عدم الإنكار: إثبات التسليم.

وينجز تحقق آخر من المسؤولية أكثر عمومية وربما أضعف من خلال الجمع الملائم بين خدمات **الاستيقان** و**مراقبة النفاذ** و**تسجيل التدقيق**.

6.2.1.10 تسجيل النشاط والإخبار عن الإنذار وتدقيقه

تغطي هذه المتطلبات الاحتياجات اللازمة لتخزين المعلومات عن الأنشطة ذات الصلة بالأمن داخل شبكة إدارة الاتصالات وتحليل هذه المعلومات. وبالإضافة إلى ذلك، فإن التبليغات عن الإنذارات ينبغي توليدها بشأن أحداث معينة قابلة للضبط. والخدمات الملائمة هي **تسجيل التدقيق** و**الإخبار عن الإنذار**. ويناقش كل من المتطلبين أدناه ببعض التفصيل.

1.6.2.1.10 تسجيل النشاط

يجب على شبكة إدارة الاتصالات أن توفر المقدرة على تخزين المعلومات عن الأنشطة التي ينفذها النظام وكذلك إمكانية تتبع هذه المعلومات حتى الأشخاص أو الكيانات.

ويمثل السجل مستودعاً للسجلات: وهو تجريد التوصيل OSI لموارد التسجيل في الأنظمة المفتوحة الحقيقية. وتحتوي السجلات على المعلومات المسجلة.

ولأغراض وظائف إدارية كثيرة، من الضروري أن يكون في الإمكان حفظ المعلومات عن الأحداث التي حدثت أو العمليات التي أدتها أو حاولت أداءها موارد شتى، أو بشأن موارد شتى.

وبالإضافة إلى ذلك، عندما تسترجع هذه المعلومات من السجل ينبغي أن يكون المدير قادراً على تحديد ما إذا كانت أي سجلات قد فقدت، أو ما إذا كانت خواص السجلات المخزونة في السجل قد عدّلت في وقت ما.

2.6.2.1.10 الإخبار عن إنذار الأمن

يجب على شبكة إدارة الاتصالات أن توفر المقدرة على إصدار تبليغات بالإنذار بشأن أحداث منتقاة. ويجب أن يكون المستعمل قادراً على تحديد معايير الانتقاء.

وإن وظيفة مراقبة تدقيق الأمن هي وظيفة إدارة أنظمة تصف التبليغ من أجل تجميع أحداث الأمن. ويوفر التبليغ عن إنذار الأمن الذي تحدده وظيفة إدارة الأنظمة هذه معلومات تخص الشرط التشغيلي المتعلق بالأمن.

3.6.2.1.10 تدقيق الأمن

يجب على شبكة إدارة الاتصالات أن توفر المقدرة على تحليل المعطيات المسجلة بشأن الأحداث ذات الصلة بالأمن بغية التحقق من مدى انتهاكها لسياسة الأمن.

وينبغي النظر إلى التدقيق باعتباره مراجعة وفحص مستقلين لسجلات وأنشطة الأنظمة بغية اختبار مدى كفاية مراقبة الأنظمة ولضمان الامتثال للسياسة الأمنية والإجراءات التشغيلية الموضوعة، ولكشف ما يحدث للأمن من خروقات. وستحدد نتيجة التدقيق التغيرات اللازمة في المراقبة والسياسة العامة والإجراءات.

ويقدم الجدول 4 عرضاً عاماً للعلاقة بين متطلبات الأمن وخدماته. ولا تحدد هذه الفقرة سوى خدمات الأمن التي تغطيها حلول معيارية؛ أما الخدمات الممكنة الأخرى (على سبيل المثال، كشف رفض الخدمة،) فنُحِّيت جانباً.

الجدول M.3016.0/4 – التقابل بين متطلبات الأمن وخدماته

المتطلب الوظيفي	خدمة الأمن
التحقق من الهويات	استيقان المستعمل استيقان الكيان الند استيقان مصدر المعطيات
النفاذ والتخويل المراقبان	مراقبة النفاذ
حماية السرية – المعطيات المخزونة	مراقبة النفاذ السرية
حماية السرية – المعطيات المنقولة	السرية
حماية تكاملية المعطيات – المعطيات المخزونة	مراقبة النفاذ
حماية تكاملية المعطيات – المعطيات المنقولة	التكاملية
المسؤولية	عدم الإنكار
تسجيل الأنشطة	تسجيل التدقيق
الإخبار عن إنذار الأمن	إنذار الأمن
تدقيق الأمن	تسجيل التدقيق
حماية شبكة الواصل المتأخر	تفتيش الرزم

ملاحظة – إن المتطلبات التالية ليست من نمط المتطلبات المعبر عنها قبل الجدول 4، وقد لا ينظر إليها باعتبارها مرشحة للتقييس على نحو واضح. ومع ذلك ينبغي أن تؤخذ في الحسبان أثناء مرحلة التصميم جنباً إلى جنب مع تنفيذ المتطلبات الرئيسية لشبكة إدارة الاتصالات المعبر عنها آنفاً.

4.6.2.1.10 تكاملية النظام

من الضروري أن تحافظ بيئة البرمجيات وعتاد الحاسوب الخاصة بوظائف الأمن المنفذة على سوية الأمن المتطلبة.

ويشمل هذا التشكيل السليم للأنظمة التشغيلية وكذلك إزالة عيوب الأنظمة.

ولا تشكل هذه الجوانب جزءاً من ملمح الأمن الوظيفي ذاته لكن يتعين ذكرها معاً بتلك المواصفات من أجل ضمان قوة الوظائف في بيئة العالم الفعلي.

5.6.2.1.10 ملاحظات بشأن التيسر

إن أي متطلب بشأن التيسر ليس له مجموعة خدمات أمن منفردة أو محدودة قادرة على إنجاز هذا المتطلب. ويجب أن تشكل جميع خدمات الأمن الواردة هنا مجموعة متماسكة تستطيع معاً المحافظة على التيسر. إلاّ أن خدمات الأمن وحدها لن تستطيع على الإطلاق أن تضمن التيسر: وهذه المسألة هي أيضاً مسألة معولية العتاد والبرمجيات (سواء من ناحية التصميم أو من ناحية التنفيذ).

7.2.1.10 حماية شبكة الواصل المتأخر

يجب أن توفر شبكة إدارة الاتصالات الحماية لشبكة الواصل المتأخر من حركة شبكة العملاء وشبكة الأنداد.

ويجب أن توفر شبكة إدارة الاتصالات عزل شبكة الواصل المتأخر عن أنماط الحركة الأخرى، ولا سيما في شبكة واصل متأخر تستند إلى الرزم.

2.10 المتطلبات الخاصة بإدارة الأمن

يجب أن تحتوي شبكة إدارة الاتصالات على نماذج معلومات وقدرات إدارية بالنسبة للخدمات المستعملة في تأمين شبكة إدارة الاتصالات.

تحدد المتطلبات المفصلة بشأن إدارة الأمن أي تطبيقات إدارية يجب إدخالها والكيفية التي يجب تصميم هذه التطبيقات وفقها. ويحدث هذا من أجل تزويد مدير الأمن بالأدوات المناسبة اللازمة له لرصد ومراقبة خدمات الأمن بطريقة فعالة وسليمة. وتقدم غايات وأهداف إدارة الأمن على ثلاث سويات مختلفة لأي نظام للاتصالات، تناسب وظائف: إدارة أمن الأنظمة، وخدمات الأمن، وآليات الأمن، على التوالي.

وتحتاج العمليات والمعلومات المتعلقة بإدارة خدمات الأمن في شبكة لإدارة الاتصالات إلى عناية خاصة من وجهة النظر الأمنية. وتشكل مفاتيح التشفير السرية، ومعلومات الاستيقان، وقوائم مراقبة النفاذ أمثلة على الأمكنة التي ينبغي أن تكون قوة الحماية المطلوبة فيها أعلى مما هي عليه بالنسبة لإدارة الشبكة.

ويجب أن تكون إدارة الأمن متسقة مع وظائف إدارة الأمن المحددة في التوصية ITU-T M.3400.

ينبغي دعم استرجاع حالة الأمن في النظام بعد حدوث خرق للأمن.

عندما يحدث خرق للأمن، يجب أن تكون شبكة إدارة الاتصالات قادرة على معالجة هذه المحاولة بطريقة مراقبة بمعنى أن المحاولة ينبغي ألاّ تفضي إلى انحطاط شديد لشبكة إدارة الاتصالات من حيث التيسر.

3.10 المتطلبات المعمارية

إن أهم المتطلبات التي يتعين أن تلبيها تدابير الأمن التي تتخذ لتناسب إطار شبكة إدارة الاتصالات هي التالية:

- يجب أن تستند التدابير إلى مبادئ النموذج الوظيفي لشبكة إدارة الاتصالات.
- يجب أن تتوافق التدابير مع المعطيات الموجهة نحو الموضوع ونموذج معلومات شبكة إدارة الاتصالات.
- يجب أن تكون التدابير قابلة للتطبيق على جميع مجالات شبكة إدارة الاتصالات في القطاعين العام والخاص.
- يجب أن تكون الحلول قابلة للتنفيذ التدريجي لتلائم شبكات إدارة الاتصالات الصغيرة والكبيرة.
- يجب أن تكون الحلول متلائمة مع المعمارية الداخلية لنقاط شبكة إدارة الاتصالات المرجعية المعنية.
- يجب أن تتناول الحلول شواغل جميع مستعملي شبكة إدارة الاتصالات الداخليين والخارجيين.
- يجب أن تعنى الحلول بالجوانب المتعلقة بالمتانة والقوة.
- يجب أن تدعم الحلول إعادة التشكيل من خلال إضافة أو شطب مستعملين أو تطبيقات.

ولا بد أن تظهر نزاعات بين مجال الأمن والمجالات الوظيفية الأخرى. وعلى سبيل المثال، يتعين تحقيق التوازن بين تكاملية وسرية معطيات الترسيم وبين المتطلبات الخاصة بكل القدر الكبير من المعلومات اللازمة لإصدار بطاقات الترسيم. وينبغي في أي مجموعة من متطلبات الأمن المعتمدة أن تأخذ في الاعتبار الآثار المترتبة على خواص المجالات الوظيفية الأخرى.

وقد تنشأ متطلبات معمارية أخرى عندما يجري تحليل سيناريوهات محددة لشبكة إدارة الاتصالات.

4.10 خدمات الأمن وطبقات التوصيل OSI

تبين هذه الفقرة أي طبقات التوصيل OSI يستعمل في توفير خدمات الأمن، ومن ثم يبين الكيفية التي يمكن بها توفير هذه الطبقات لشبكة إدارة الاتصالات بطريقة ذات جدوى.

ويفترض أنه إذا قدمت طبقة ما خدمة أمن، فإن هذه الخدمة تقدم إلى الطبقة الأعلى من الطبقة المعنية. ويستخدم توفير الطبقات للخدمات المبينة في التوصية ITU-T X.800 بمثابة أساس للحد من الإمكانيات.

1.4.10 استيقان المستعملين

تتوقف هذه الخدمة على التفاعل مع المستعمل. ومن ثم فهي تقع خارج نطاق نموذج التوصيل OSI.

2.4.10 استيقان (الكيان الند ومصدر المعطيات)

يمكن للطبقات التالية توفير هذه الخدمة (وفقاً للتوصية ITU-T X.800):

- طبقة الشبكة (إثبات هوية أنداد طبقة النقل)؛
- طبقة النقل (إثبات هوية أنداد طبقة الدورة)؛
- طبقة التطبيق (إثبات هوية عمليات التطبيق)؛
- خارج التوصيل OSI: في عملية التطبيق ذاتها.

ونظراً لأن المتطلب الخاص بشبكة إدارة الاتصالات سيكون هو تعرف هوية المديرين والموظفين والاستيقان منهم وكذلك وصلة الاستيقان عن طريق مراقبة النفاذ، فإن المواضع الموصى بها فيما يتعلق ببطارية التوصيل OSI تتمثل في طبقة التطبيق وعملية التطبيق.

3.4.10 مراقبة النفاذ

- *مراقبة النفاذ إلى تصاحب الإدارة*

تستعمل هذه الخدمة في السويات التي يوجد بها تصاحب؛ وسيكون ذلك في طبقة التطبيق (مراقبة النفاذ إلى عمليات التطبيق) أو في عملية التطبيق ذاتها.

ويمكن توفير مراقبة النفاذ إلى التصاحب في طبقة الشبكة، على سبيل المثال خدمة زمرة مغلقة X.25 من المستعملين. وبالإضافة إلى ذلك، يمكن توفير مراقبة النفاذ إلى التصاحب في طبقة التطبيق أو في عملية التطبيق ذاتها.

- *مراقبة النفاذ إلى تبليغات الإدارة*

يمكن استعمال هذه الخدمة في طبقة التطبيق أو في عملية التطبيق ذاتها لأن عملية التطبيق ذاتها هي التي يمكنها التمييز بين كيانات (عملية التطبيق) مثل المديرين والموظفين.

- *مراقبة النفاذ إلى الموارد المدارة*

يمكن استعمال هذه الخدمة في طبقة التطبيق أو في عملية التطبيق ذاتها، إذ إن عملية التطبيق ذاتها هي التي يمكن أن تميز بين كيانات (عملية التطبيق) مثل المديرين والموظفين.

4.4.10 إنذار الأمن وتسجيل التدقيق والاسترجاع

ترتبط هذه الخدمات بخدمات أخرى، ولذلك فهي توجد في الطبقات التي توجد فيها الخدمات الأخرى.

5.4.10 التكاملية

- *التكاملية الانتقائية للمجالات*

يمكن استعمال هذه الخدمة في طبقة التطبيق أو في عملية التطبيق ذاتها نظراً لأن عملية التطبيق هي التي يمكنها التمييز بين المجالات.

- *تكاملية التوصيلات مع استرجاع*

يمكن توفيرها عند طبقة النقل وعند طبقة التطبيق أو في عملية التطبيق.

- *تكاملية التوصيلات بدون استرجاع*

يمكن توفيرها عند طبقة الشبكة وطبقة النقل وطبقة التطبيق أو في عملية التطبيق.

6.4.10 السرية

- *السرية الانتقائية للمجالات*

يمكن أن تستعمل هذه الخدمة في طبقة التطبيق أو في عملية التطبيق ذاتها نظراً لأن عملية التطبيق هي التي يمكنها التمييز بين المجالات.

- *سرية التوصيلات واللاتوصيلات*

نظراً للحاجة إلى توفير السرية من طرف إلى طرف، الأمر الذي يستبعد الطبقة المادية وطبقة وصلة المعطيات، يمكن توفير السرية في طبقة الشبكة، وطبقة النقل، وطبقة التقديم، وطبقة التطبيق أو في عملية التطبيق.

- *سرية تدفق الحركة*

يمكن توفير هذه الخدمة في الشبكة أو النقل أو في طبقات التطبيق أو في عملية التطبيق.

7.4.10 عدم الإنكار

- عدم الإنكار – إثبات الإرسال؛
- عدم الإنكار – إثبات التسليم.

يمكن استعمال هذه الخدمة في طبقة التقديم أو طبقة التطبيق أو في عملية التطبيق ذاتها.

ويرد تلخيص هذه المعلومات في الجدول 5.

الجدول M.3016.0/5 – وصل خدمات الأمن والنموذج المرجعي للتوصيل OSI

الخدمة	الطبقة						
	1	2	3	4	5	6	7
استيقان المستعمل	–	–	–	–	–	–	+
استيقان الكيان الند	–	–	+	+	–	–	+
استيقان مصدر المعطيات	–	–	+	+	–	–	+
مراقبة النفاذ إلى تصاحب الإدارة	–	–	+	–	–	–	+
مراقبة النفاذ إلى تبليغات الإدارة	–	–	–	–	–	–	+
مراقبة النفاذ إلى الموارد المدارة	–	–	–	–	–	–	+
إنذار الأمن وتسجيل التدقيق واسترجاعه	+	+	+	+	+	+	+

الخدمة	الطبقة						
	1	2	3	4	5	6	7
التكاملية الانتقائية للمجالات	–	–	–	–	–	–	+
تكاملية التوصيلات مع استرجاع	–	–	–	+	–	–	+
تكاملية التوصيلات بدون استرجاع	–	–	+	+	–	–	+
السرية الانتقائية للمجالات	–	–	–	–	–	–	+
سرية التوصيلات/اللاتوصيلات	–	–	+	+	–	+	+
سرية تدفق الحركة	–	–	+	+	–	+	+
عدم الإنكار – إثبات الإرسال	–	–	–	–	–	+	+
عدم الإنكار – إثبات التسليم	–	–	–	–	–	+	+

5.10 إدارة الأمن

تتألف إدارة الأمن من جميع الأنشطة اللازمة لتحقيق جوانب الأمن في أي نظام والمحافظة عليها وإنهائها.

وتتمثل المواضيع التي يجري تغطيتها فيما يلي:

- إدارة خدمات الأمن؛
- إنشاء آليات الأمن؛
- إدارة المفاتيح (جزء الإدارة)؛
- التثبت من الهويات والمفاتيح ومعلومات مراقبة النفاذ، وما إلى ذلك؛
- إدارة تسجيل تدقيق الأمن وإنذارات الأمن.

التذييل I

الأصناف الوظيفية والملامح الفرعية للأمن

1.I تجميع التدابير الأمنية

يمكن تجميع التدابير الأمنية في "أصناف وظيفية" (FC). ولا يتضمن التعريف التالي شدة تدبير الأمن:

ويمثل الصنف الوظيفي مجموعة متسقة من تدابير الأمن الرامية إلى تلبية متطلبات السويات الوظيفية المختلفة.

1.1.I استعمال الأصناف الوظيفية في حالة ما بين المجالات

يجب ألاّ يتأثر أمن شبكة إدارة الاتصالات على نحو سلبي نتيجة للأنشطة بين المجالات. وينبغي أن تحدد قواعد تفاعل المجالات في سياسة للأمن بين المجالات. وستحدد هذه القواعد أي تدابير أمن يجب استخدامها في الحالة المعينة. ولتسهيل الاتفاق بين المجالات المتفاعلة، يمكن الإشارة إلى تدابير الأمن هذه باعتبارها أصناف وظيفية خاصة.

2.1.I استعمال الأصناف الوظيفية في حالة داخل المجالات

في الحالة الناشئة داخل المجالات، يمكن للأصناف الوظيفية أن تسهل تحديد الأمن ويمكن أيضاً استخدام الأصناف الوظيفية لغرض ضمان الأمن. ولتحقيق هذا الغرض، يجب أن تكون الأصناف الوظيفية مصحوبة بسوية ضمان يدَّعيها مصنِّع منتجات الإدارة. ولهذا الموضوع علاقات قوية بمعايير التقييم الرسمية.

ولعله من الممكن لأغراض التفاعل بين المجالات أن يطلب مشغِّل تطبيق صنف وظيفي معين لحالة داخل مجال المشغل الآخر. وقد يكون سبب هذا هو أنه لا يمكن معالجة جميع التهديدات بكفاءة في السطح البيني فيما بين المجالين. وقد يتمثل حل لذلك في ضمان توافر حد أدنى لسوية الأمن الداخلي من أجل التفاعل بين شبكات إدارة الاتصالات. ويجب ألاّ يقضي أي معيار لأمن شبكة إدارة الاتصالات بأن الأصناف الوظيفية لازمة وإنما يجب أن يتيح إمكانية طلب بعض الأصناف الوظيفية من خلال تحديد بنود ملائمة للانتقاء.

2.I الأصناف الوظيفية

تستخدم الأصناف الوظيفية في تحديد مجموعة مختصرة من خدمات الأمن الرامية إلى تحقيق سوية أمن معينة. وتتناول هذه الفقرة مجموعة من الأصناف الوظيفية التي تستخدم كمثال على الكيفية التي يمكن بها تحديد الأصناف الوظيفية. ويقترح أن تكون الأصناف الوظيفية الخاصة *بالسطح البيني–X* في ثلاث سويات أمن متميزة:

1) الصنف الوظيفي الأدنى: (FC 1)؛

2) الصنف الوظيفي الأساسي: (FC 2)؛

3) الصنف الوظيفي المتقدم: (FC 3).

وللأغراض العملية، ينبغي ألاّ يكون عدد الأصناف الوظيفية كبيراً أكثر من اللازم. ومن ناحية أخرى، يجب أن يكون في إمكان الأصناف الوظيفية أن تلائم متطلبات منظمات كثيرة مختلفة. ويمكن تغيير الأصناف الوظيفية بالطرق التالية:

- يمكن للأصناف الوظيفية المحددة للسطح البيني–X فقط أن تشمل أيضاً السطوح البينية Q.
- يفترض أن تكون السرية سمة خيارية بالنسبة لجميع الأصناف وذلك لسببين:
  - إنها متطلب أقل صرامة؛
  - قد يكون للإدراج الإلزامي في صنف وظيفي آثار قانونية على إمكانية استعمال هذا الصنف.

ويقدم الجدول 1.I عرضاً عاماً للأصناف الوظيفية.

الجدول M.3016.0/1.I – الأصناف الوظيفية لخدمات الأمن

FC 1	FC 2	FC 3
التشديد على تكاملية الموارد المخزونة المدارة	التشديد على تكاملية الموارد المخزونة المدارة وعلى تكاملية المعطيات المنقولة	FC 2 بالإضافة إلى المسؤولية عن عمليات الإدارة
• استيقان (الكيان الند والمستعمل) • مراقبة نفاذ تصاحب الإدارة • مراقبة نفاذ الموارد المدارة • إنذار وتدقيق واسترجاع الأمن	• استيقان (الكيان الند والمستعمل) • مراقبة نفاذ تصاحب الإدارة • مراقبة نفاذ الموارد المدارة • استيقان مصدر المعطيات • التكاملية الانتقائية للمجالات • تكاملية التوصيلات • إنذار وتدقيق واسترجاع الأمن	• استيقان (الكيان الند والمستعمل) • مراقبة نفاذ تصاحب الإدارة • مراقبة نفاذ الموارد المدارة • استيقان مصدر المعطيات • التكاملية الانتقائية للمجالات • تكاملية التوصيلات • مصدر عدم الإنكار • عدم إنكار المقصد • إنذار وتدقيق واسترجاع الأمن
سمات خيارية: • تكاملية التوصيلات • سرية التوصيلات	سمات خيارية: • سرية التوصيلات • السرية الانتقائية للمجالات	سمات خيارية: • سرية التوصيلات • السرية الانتقائية للمجالات

وبالإضافة إلى ذلك، يجب التمييز بين الأصناف الوظيفية المطبقة فيما يتعلق بالحالة بين المجالات والأصناف الوظيفية المطبقة في الحالة داخل المجالات. فالمتطلب سيكون مختلفاً في كلتا الحالتين، ولهذا السبب ينبغي أن تكون تدابير الأمن مختلفة.

ويقدم الجزء التالي عرضاً عاماً لمختلف الحالات بحيث يمكن للمرء أن يكتشف أي الأصناف الوظيفية هو اللازم وأيها هو الملائم.

افتراض

وتوجد بالنسبة لكل مجال سلطة هي المسؤولة عن البت في أي تدابير أمن يجب أن تطبق في المجال.

وثمة ثلاث حالات متميزة في هذا الصدد:

1) الأصناف الوظيفية التي تحددها سلطة مجال وتطبق على المجال ذاته (داخل المجال)؛

2) الأصناف الوظيفية التي تحددها سلطة مجال وتطبق على تفاعلات المجالات (بين المجالات). وستكون الأصناف الوظيفية هذه نتيجة اتفاق بين سلطات المجالات المتفاعلة؛

3) الأصناف الوظيفية التي تحددها سلطة مجال بوصفها متطلبات للأمن الداخلي للمجال الآخر.

وفي كل حالة يمكن تحديد عدد الأصناف الوظيفية الخاصة بمختلف سويات الأمن.

ويحتاج عدد سويات الأمن إلى مزيد من الدراسة.

كما تحتاج مجموعة التدابير الأمنية التي تشكل صنفاً وظيفياً إلى مزيد من الدراسة.

ويمكن أن تكون الأصناف الوظيفية في الحالات المختلفة متساوية ومن ثم، تخفض العدد الإجمالي للأصناف الوظيفية.

ويمكن للمرء أيضاً أن ينظر في وجود علاقة تبادلية بين الحالات المختلفة، على سبيل المثال، عندما يكون الأمن بين المجالات على سوية عالية فإن متطلبات الأمن الداخلي في المجال الآخر تكون منخفضة، والعكس صحيح. وقد تتمثل إمكانية أخرى في أن صنفاً وظيفياً يمثل مجموعة دنيا من تدابير الأمن التي يمكن تقديمها مع تدابير إضافية، حسب الاقتضاء.

3.I ملامح الأمن العامة

لا تتطلب الأصناف الوظيفية استخدام آليات أمن مقيسة؛ فأي آليات تنجز المتطلبات يمكن تطبيقها.

وللتمكين من تحقيق التفاعل بين تدابير الأمن في مختلف المجالات، يجب أن تتطابق التدابير مع المعايير. وأي توجيه يقضي باستخدام معايير خاصة توفر معاً صنفاً وظيفياً، يطلق عليه ملمح أمني.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية وتعدد الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات البرامج الإذاعية الصوتية والتلفزيونية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	**إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات**
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	شبكات البيانات والاتصالات بين الأنظمة المفتوحة
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	لغات البرمجة والخصائص العامة للبرمجيات في أنظمة الاتصالات

طبعت في سويسرا
جنيف، 2005