الاتحاد الدولي للاتصالات

الأمن في الاتصالات وتكنولوجيا المعلومات

نظرة عامة على القضايا ذات الصلة وعلى تطبيق توصيات قطاع تقييس الاتصالات الحالية من أجل تحقيق أمن الاتصالات

قطاع تقييس الاتصالات في الاتحاد

ITU-T

2006

الاتحاد الدولي للاتصالات

ITU-T

ITU – مكتب تقييس الاتصالات (TSB)
Place des Nations – CH-1211 Geneva 20 – Switzerland
E-mail: tsbmail@itu.int Web: www.itu.int/ITU-T

الأمـــن
في الاتصـــالات
وتكنولوجيـــا المعلومـــات

نظرة عامة على القضايا ذات الصلة
وعلى تطبيق توصيات قطاع تقييس الاتصالات الحالية
من أجل تحقيق أمن الاتصالات

يونيو 2006

شكـــر وتقديـــر

أعد هذا الكتيب بمساهمة من مؤلفين عديدين ممن شاركوا في وضع توصيات قطاع تقييس الاتصالات المتصلة بهذا الموضوع أو شاركوا في اجتماعات لجان دراسات وحلقات العمل والحلقات الدراسية التي نظمها قطاع تقييس الاتصالات في هذا الخصوص. وينبغي توجيه الشكر، بصورة خاصة، إلى المساهمين التالي ذكرهم: هيرب بيرتين، دافيد شادويك، مارتين إيشنر، مايك هاروب، ساندور مازغون، ستيفين ميتلر، كريس رادلت، لاكشمي رامان، إريك روزنفيلد، نيل سايتز، راو فازيريدي، تيم والكر، هوينغ-يول يوم، جو زيبارت، والمستشارون لدى مكتب تقييس الاتصالات في الاتحاد.

المحتويات

الصفحة

الصفحة

تمهيـــد

كان أمن الاتصالات وتكنولوجيا المعلومات، حتى عهد قريب نسبياً، يحظى أساساً باهتمام مجالات معينة مثل الصيرفة والفضاء والتطبيقات العسكرية. ولكن سرعة النمو وسعة الانتشار في استعمال اتصالات البيانات، وخصوصاً شبكة الإنترنت، جعل من الأمن مسألة تكاد تهم كل الناس.

ولعل تزايد الاهتمام بأمن تكنولوجيا المعلومات والاتصالات يُعزى في جزء منه إلى الحوادث التي ينتشر الحديث عنها على نطاق واسع، ومنها مثلاً الفيروسات والديدان والمحتالون وما يهدد خصوصية الأفراد. وبما أن الحوسبة والتواصل بالشبكات يشغلان اليوم قدراً لا بأس به من الحياة اليومية فإن الحاجة إلى تدابير أمن فعالة لحماية أنظمة الحواسيب والاتصالات لدى الحكومات ودوائر الصناعة والتجارة والبنى التحتية الأساسية والمستهلكين عموماً غدت حاجة لا مناص منها. أضف إلى ذلك أن عدداً متزايداً من البلدان لديها اليوم تشريعات لحماية البيانات تستوجب الامتثال لمعايير أثبتت جدواها في مجال سرية البيانات وسلامتها.

ومن الضروري أن يكون الأمن عملية مدروسة بكل عناية في جميع المراحل، بدءاً من تصور النظام وتصميمه حتى تنفيذه ونشره. ولدى وضع المعايير لا بد من أن يكون الأمن دوماً عنصراً من عناصر العمل الأساسي وليس مجرد فكرة طارئة في مرحلة لاحقة. فالتقصير في دراسة الأمن بصورة وافية أثناء مرحلة تصميم المعايير وتطوير الأنظمة سرعان ما يسفر عن مواطن ضعف في عملية التنفيذ. ولجان المعايير تقوم بدور حيوي في حماية أنظمة الاتصالات وتكنولوجيا المعلومات بإذكاء الوعي بمسائل الأمن وبالحرص على أن تكون اعتبارات الأمن جزءاً أساسياً من المواصفات وبتوفير الإرشاد لمساعدة المنفذين والمستعملين على جعل أنظمة الاتصالات وخدماتها متينة بما فيه الكفاية.

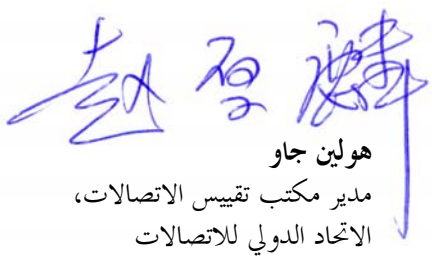
لقد كان قطاع تقييس الاتصالات نشطاً في جوانب الأمن التي تخص الاتصالات وتكنولوجيا المعلومات طوال سنوات عديدة. ومع ذلك لم يكن من اليسير دائماً الوقوف على ما أنجز ومعرفة السبيل إليه. ويسعى هذا الكتيب إلى تجميع كل المعلومات المتاحة عما يقوم به قطاع تقييس الاتصالات.

والغرض من هذا الكتيب أن يكون دليلاً للعاملين في مجال التكنولوجيات وفي الإدارة المتوسطة وكذلك للهيئات التنظيمية ليساعدهم على تنفيذ وظائف الأمن عملياً. وهو يستند إلى عدد من أمثلة التطبيقات في شرح مسائل الأمن ويركز على كيفية تناول توصيات القطاع لها.

وقد نشرت الطبعة الأولى من هذا الكتيب، طبعة عام 2003، في ديسمبر من ذلك العام، أي قبيل المرحلة الأولى من القمة العالمية لمجتمع المعلومات (WSIS). وقد لقيت الطبعة الأولى قبولاً حسناً في أوساط تكنولوجيا المعلومات والاتصالات في شتى أنحاء العالم كما تلقينا مقترحات وردود فعل قيّمة من جانب القراء الأمر الذي دفعنا إلى إعداد طبعة ثانية. واتخذت الطبعة التي نُشرت في أكتوبر 2004 شكلاً جديداً بنية جديدة وتعززت بإضافة مواد جديدة إليها والتوسع في بعض المجالات. أما هذه الطبعة الثالثة، طبعة عام 2006، فإنها تأخذ في الحسبان البنية الجديدة للجان الدراسات ومختلف المسائل التي تمخضت عنها الجمعية العالمية لتقييس الاتصالات التي عُقدت في فلوريانوبوليس في الفترة 5-14 أكتوبر 2004 (WTSA-04).

وأود في هذه المناسبة أن أعرب عن تقديري لمهندسي مكتب تقييس الاتصالات في الاتحاد الذين استكملوا، بالتآزر مع خبراء من مختلف أعضاء الاتحاد، القسط الأكبر من الطبعة الأولى. كما أود أن أعرب عن تقديري أيضاً لكل من زودنا بمقترحات قيّمة ولكل من ساهم في هذه الطبعة الجديدة. وأخص بالتقدير السيد هيربرت بيرتين، رئيس لجنة الدراسات 17 في القطاع وهي لجنة الدراسات الرائدة في مجال الأمن، وأعضاء فريقه من لجنة الدراسات 17، وغيرها من لجان الدراسات في القطاع.

وإنني على ثقة من أن هذا الكتيب سيكون دليلاً مفيداً لمن يسعون إلى تناول مسائل الأمن وإنني أرحب بأي تعليقات من القراء للاستئناس بها في طبعات قادمة.



هولين جاو
مدير مكتب تقييس الاتصالات،
الاتحاد الدولي للاتصالات
جنيف، يونيو 2006

ملخص تنفيذي

لقد أسهمت صناعة الاتصالات بنصيب وافر في تحسين الإنتاجية والكفاءة على صعيد العالم وذلك بتطوير البنى التحتية للاتصالات التي تمد الجسور بين المجتمعات في كل ركن من أركان الصناعة وفي كل قطر من أقطار العالم تقريباً. وقد أمكن ذلك، إلى حد كبير، من خلال الأخذ بالمعايير التي تضعها منظمات من قبيل قطاع تقييس الاتصالات في الاتحاد. وتكفل هذه المعايير إمكانية التشغيل البيني والكفاءة في عمليات الشبكات كما أنها ترسي الأسس لشبكات الجيل التالي (NGN). ومع ذلك، وإذا كانت المعايير لا تزال تلبي احتياجات المستعمل النهائي ودوائر الصناعة، فإن تزايد استعمال السطوح البينية المفتوحة والبروتوكولات وتعدد المشاركين الجدد ومجرد تنوع التطبيقات والمنصات وشتى عمليات التنفيذ التي لا تخضع دوماً للقدر الكافي من الاختبار، كل هذه العوامل زادت من فرص استعمال الشبكات لمآرب شريرة. وقد شهدت السنوات الأخيرة موجة من انتهاكات الأمن (في شكل فيروسات واعتداءات أسفرت عن خرق حجاب السرية والكتمان الذي يصون البيانات المخزّنة) عبر مختلف الشبكات العالمية الأمر الذي كثيراً ما أدى إلى تكبد تكاليف باهظة. والسؤال المطروح إذن كيف لنا بناء بنية تحتية مفتوحة للاتصالات دون أن تتعرض للخطر المعلومات التي يجري تبادلها على هذه الشبكات؟ وإلى حد كبير يكمن الرد على هذا السؤال في وضع مواصفات تقوم على أساس متين للتأكد من إمكانية صد أي تهديدات قد تنال من أي مجال في البنية التحتية للاتصالات. وتحقيقاً لهذه الغاية، فإن الجهود التي تبذلها هيئات التقييس تشتمل على تطوير معماريات وهياكل أمنية موحدة قياسياً وعلى معايير لإدارة الأمن وعلى بروتوكولات وأساليب تختص بالأمن والتقنيات وذلك للحفاظ على أمن بروتوكولات الاتصالات، إلى جانب الخطوات المتخذة التي ترمي إلى تقليص مواطن الضعف المحتملة إلى الحد الأدنى في المعايير القياسية للاتصالات عموماً.

والغرض من هذا الكتيب هو عرض صورة مجملة للتوصيات العديدة التي وضعها قطاع تقييس الاتصالات – بالتعاون في بعض الأحيان مع منظمات أخرى معنية بوضع المعايير – لتأمين البنى التحتية للاتصالات والخدمات والتطبيقات المرتبطة بها.

وإذا أردنا معالجة الجوانب المتعددة للأمن فلا بد لنا من وضع هيكلية ومعمارية لكي تكون لدينا مصطلحات موحدة يمكن بناءً عليها مناقشة المفاهيم المختلفة.

ويعرض القسم 2 معماريات الأمن الأساسية والعناصر المعرّفة في توصيات قطاع تقييس الاتصالات (ITU-T) إلى جانب أبعاد الأمن الثمانية التي تم تحديدها للتعامل مع مسألة الأمن من طرف إلى طرف في تطبيقات الشبكات – وهي الخصوصية، وسرية البيانات، والاستيقان، وسلامة البيانات، وعدم التنصل، والتحكم في النفاذ، وأمن الاتصالات، والتيسر. وتستخدم هذه المبادئ العامة بمثابة أساس يقوم عليه العديد من معايير خدمة الأمن وآلية عملها.

ويقدم القسم 3 مفاهيم الأمن الرئيسية، من تهديدات ومواطن ضعف ومخاطر، ويوضح العلاقة ما بين هذه المفاهيم وأهميتها في نظر هيئات وضع المعايير.

ويستند القسم 4 إلى المعلومات الواردة في الأقسام السابقة لكي يضع متطلبات الأمن لشبكات الاتصالات. وعلى وجه التحديد يناقش هذا القسم أهداف أمن شبكة الاتصالات والخدمات التي يمكن اللجوء إليها لتحقيق هذه الأهداف.

ويقدم القسم 5 المفاهيم الهامة لهياكل إدارة المفاتيح العمومية وإدارة الامتيازات. وتتسم هذه الآليات وما تنطوي عليه من بنى تحتية بأهمية خاصة في دعم خدمات الاستيقان والترخيص.

وقد قام قطاع تقييس الاتصالات بوضع أحكام للأمن في أنظمة وخدمات عديدة حددها في توصياته، وينصب اهتمام جزء كبير من هذا الكتيب على التطبيقات، كما نرى في القسم 6. وهي تشمل التطبيقات الصوتية والتطبيقات متعددة الوسائط عبر بروتوكول الإنترنت (التوصية H.323 والمعمارية الكبلية على أساس بروتوكول الإنترنت IPCablecom) والرعاية الصحية والفاكس. وهذه التطبيقات موصوفة على أساس معمارية النشر وعلى أساس كيفية وضع البروتوكولات لتلبية احتياجات الأمن. وبالإضافة إلى توفير الأمن للمعلومات ذات الصلة بالتطبيقات، هناك حاجة أيضاً

لتأمين البنية التحتية للشبكة وإدارة خدمات الشبكة. ويتضمن القسم 6 أيضاً أمثلة للمعايير التي تحددت بناء عليها الأحكام المتصلة بالأمن للتعامل مع الجوانب المتصلة بإدارة الشبكة.

ويتناول القسم 7 بُعد التيسر وطبقة الأمن في البنية التحتية. وهما يمثلان اثنين من الاختصاصات الأساسية لقطاع تقييس الاتصالات على الرغم من أنهما لا يُعتبران دوماً أنهما يسهمان في مجال الأمن. وثمة معلومات عن كيفية حساب التيسر وأساليب لتعزيز تيسر شبكة للنقل. وينتهي هذا القسم بتوفير الإرشاد فيما يتعلق بتأمين المنشآت الخارجية.

ويوجز القسم 8 مبادئ توجيهية أقرها مؤخراً قطاع تقييس الاتصالات بشأن تنظيم التحسب لما قد يقع من حوادث ومعالجة حوادث الأمن. ومن المتفق عليه عموماً أن لهذه المسألة أهمية عالية نظراً لتطور تهديدات الأمن في البنية التحتية لأنظمة الاتصالات والمعلومات.

وبالإضافة إلى ذلك، يتضمن هذا الكتيب القائمة الحالية لتوصيات القطاع فيما يتعلق بجوانب الأمن – والقائمة الواردة في الملحق "ألف" قائمة مستفيضة توضح أيضاً مدى اتساع أعمال قطاع التقييس في مجال الأمن. ويتضمن هذا الكتيب أيضاً قائمة بالمختصرات والتعاريف المتصلة بالأمن والموضوعات الأخرى التي تعالجها هذه الوثيقة، وهي مقتبسة من توصيات القطاع ذات الصلة ومصادر أخرى (مثل قاعدة بيانات SANCHO للقطاع وتجميع تعاريف الأمن التي أقرها القطاع والتي وضعتها لجنة الدراسات 17 التابعة له). وهذا ما يأتي بيانه في الملحق "باء". ويلخص الملحق "جيم" الأعمال المتصلة بالأمن التي يقوم بها كل من لجان الدراسات التابعة للقطاع. والمواد الواردة في هذه الملحقات يتم تحديثها باستمرار، ويمكن الاطلاع عليها في الموقع التالي: www.itu.int/ITU-T.

وخلاصة القول، إن قطاع تقييس الاتصالات يواكب التطورات ليس فيما يتعلق بالتكنولوجيات القائمة على بروتوكول الإنترنت فحسب وإنما في تلبية احتياجات قطاعات كثيرة مختلفة في صناعة الاتصالات تتفاوت فيها متطلبات الأمن تفاوتاً كبيراً. ويبين هذا الكتيب كيف أن توصيات القطاع تتضمن حلولاً لا تقتصر على الهياكل والمعماريات عموماً وإنما تتناول أيضاً أنظمة وتطبيقات محددة – وهي منتشرة عالمياً يستفيد منها مقدمو الشبكات والخدمات.

1 نطاق الكتيب

يتناول هذا الكتيب إجمالاً مسألة الأمن في الاتصالات وتكنولوجيا المعلومات ويصف الجوانب العملية ويوضح كيف يتناول قطاع تقييس الاتصالات في الاتحاد مختلف جوانب الأمن في التطبيقات المستخدمة في الوقت الحاضر. ويتسم الكتيب بطابع تعليمي، فهو يجمع في مكان واحد المواد المتعلقة بالأمن الواردة في توصيات قطاع تقييس الاتصالات ويشرح العلاقات فيما بينها. وهو يشمل جوانب إضافية في مجال الأمن ولا سيما تلك التي تتصل بالتيسر – والتي يسهم فيها القطاع بنصيب وافر – أو بالأضرار البيئية وهو مجال ينشط فيه القطاع. كما يشمل أيضاً ما أحرزه، منذ الطبعة الثانية، من نتائج بخصوص مسائل التقييس المتصلة بالأمن. وفضلاً عن ذلك، فإنه يستند إلى الأعمال المنجزة، وليس إلى الأعمال الجارية والتي ستتناولها الطبعات المقبلة من هذا الكتيب.

وهذا الدليل موجه إلى جمهور يشمل المهندسين ومديري المنتجات والطلاب والأكاديميين، كما يشمل الهيئات التنظيمية التي تحرص على تحقيق فهم أفضل للقضايا المتصلة بالأمن في التطبيقات العملية.

2 معماريات الأمن وخدماته الأساسية

برزت الحاجة إلى تناول عناصر معمارية الأمن في سياق أعمال تقييس الاتصالات في أوائل الثمانينات. وقد أدى ذلك إلى وضع معمارية أمن الأنظمة المفتوحة (التوصية ITU-T X.800). بيد أنه أصبح من الواضح أيضاً أن تلك ما هي إلا المرحلة الأولى في وضع سلسلة من المعايير لتدعيم خدمات الأمن وآلياته. وأفضى هذا العمل، ومعظمه جرى بالتعاون مع المنظمة الدولية للتوحيد القياسي (ISO)، إلى وضع مزيد من التوصيات، شاملة نماذج أمن وهياكل أمن تحدد كيف يمكن تطبيق أنماط محددة من الحماية في بيئات معينة. وعلاوة على ذلك، تجلت الحاجة إلى معماريات أخرى للأمن، ومنها مثلاً معماريات الأمن من أجل المعالجة الموزعة المفتوحة ومن أجل الأنظمة التي توفر الاتصالات من طرف إلى طرف. وتتناول التوصية ITU-T X.805، الصادرة حديثاً، هذه الحاجة وتستكمل توصيات أخرى في السلسلة X.800 بتقديم حلول أمن ترمي إلى توفير أمن الشبكة من طرف إلى طرف.

1.2 معمارية أمن الأنظمة المفتوحة (X.800)

كانت أولى معماريات أمن الاتصالات التي خضعت للتقييس في إطار التوصية ITU-T X.800 هي معمارية أمن الأنظمة المفتوحة. وتحدد هذه التوصية العناصر المعمارية العامة المتصلة بالأمن والتي يمكن تطبيقها تبعاً للظروف التي تكون الحماية مطلوبة لها. وعلى وجه التحديد، تقدم التوصية X.800 وصفاً عاماً لخدمات الأمن والآليات المتصلة بذلك التي يمكن استعمالها لتوفير تلك الخدمات. وتحدد أيضاً، من حيث النموذج المرجعي الأساسي سباعي الطبقات للتوصيل ما بين الأنظمة المفتوحة (OSI)، أكثر المواقع ملاءمة لتنفيذ خدمات الأمن.

وتقتصر التوصية ITU-T X.800 على تلك الجوانب المرئية من مسار الاتصالات والتي تمكّن الأنظمة الطرفية من تحقيق النقل الآمن للمعلومات فيما بينها. وهي لا تسعى إلى تقديم أي نوع من مواصفات التنفيذ كما أنها لا توفر وسائل تقييم امتثال أي تنفيذ لهذا المعيار أو لغيره من معايير الأمن. ولا تشير كذلك، بأي درجة من التفصيل، إلى تدابير الأمن الإضافية التي قد تلزم في الأنظمة الطرفية لتوفير ملامح الأمن في التوصيل ما بين الأنظمة المفتوحة (OSI).

وعلى الرغم من أن التوصية X.800 صممت تحديداً بمثابة معمارية أمن للتوصيل OSI فقد تبين أن المفاهيم التي تنطوي عليها تتمتع بقدر أوسع من القبول وإمكانية التطبيق. ومعيار التوصية على جانب من الأهمية من حيث إنه يمثل أول توافق في الآراء عالمياً بشأن تعاريف خدمات الأمن الأساسية (أي *الاستيقان والتحكم في النفاذ وسرية البيانات وسلامة البيانات وعدم التنصل*) إلى جانب خدمات أكثر عمومية من قبيل *الوثوق بالوظيفة والكشف عن الحدث والتحقق من الأمن واستعادته*. وقبل اعتماد التوصية X.800 كانت هنالك طائفة واسعة من وجهات النظر بشأن تحديد ما هي خدمات الأمن الأساسية المطلوبة وما هو بالضبط الدور الذي يؤديه كل منها. وتعبّر التوصية X.800 عن توافق قوي في الآراء دولياً بصدد هذه الخدمات. (تستعرض خدمات الأمن الأساسية بمزيد من التفصيل في القسم 3.2).

وتُعزى قيمة التوصية X.800 وإمكانية تطبيقها عموماً إلى أنها تمثل توافقاً هاماً في الآراء بشأن مدلول المصطلحات المستخدمة لوصف جوانب الأمن وبشأن مجموعة خدمات الأمن اللازمة لتوفير الحماية لعمليات توصيل البيانات وبشأن طبيعة خدمات الأمن تلك.

وقد برزت الحاجة، أثناء وضع التوصية X.800، إلى معايير أمن إضافية فيما يتعلق بالاتصالات. وتبعاً لذلك، وبعد الانتهاء من وضع التوصية X.800، انصبّت الجهود على عدد من المعايير الداعمة والتوصيات المعمارية التكميلية. ويناقش بعض هذه التوصيات فيما يلي أدناه.

2.2 نموذج أمن كل من الطبقتين السفلى والعليا (X.802 وX.803)

إن الغرض من نموذج أمن كل من الطبقتين السفلى والعليا (X.802 وX.803 على التوالي) هو بيان كيف يمكن تطبيق مفاهيم الأمن المطورة في هياكل الأمن على مناطق محددة في معماريات الأنظمة المفتوحة.

والغرض من نموذج أمن الطبقات العليا (X.803) هو تزويد واضعي المعايير بالنموذج المعماري من أجل تطوير خدمات الأمن وبروتوكولاته المستقلة عن التطبيقات في الطبقات العليا من نموذج التوصيل OSI سباعي الطبقات. وتوفر التوصية الإرشاد فيما يتعلق بمواقع خدمات الأمن والعلاقات فيما بينها وذلك في طبقات الجلسة والتقديم والتطبيق. وعلى وجه الخصوص، تصف التوصية كيفية تناول وظائف التحويل الأمنية (كالتجفير مثلاً) في كل من طبقتي التطبيق والتقديم. وعلاوة على ذلك، تتحدث التوصية عن مفهوم *تبادل الأمن* كما تصف *سياسة الأمن* و*حالة الأمن*.

ويوفر نموذج أمن الطبقات السفلى (X.802) الإرشاد فيما يتعلق بوضع البروتوكولات المتصلة بالأمن وعناصر البروتوكولات الملائمة للطبقات السفلى من نموذج التوصيل OSI. ويصف أساس التفاعلات الأمنية بين الطبقات السفلى وكذلك مواقع بروتوكولات الأمن.

3.2 هياكل الأمن (X.810 إلى X.816)

وضعت هياكل الأمن لتقديم توصيفات شاملة ومتسقة لخدمات الأمن المعرفة في التوصية X.800. والغرض منها تناول جميع جوانب كيفية تطبيق خدمات الأمن في سياق معمارية أمن معينة، بما في ذلك معماريات أمن ممكنة في المستقبل. وتركز الهياكل على توفير الحماية للأنظمة وللكيانات ضمن الأنظمة والتفاعل ما بين الأنظمة. وهي لا تتناول منهجية بناء الأنظمة أو آلياتها.

وتتناول الهياكل كلاً من عناصر البيانات وتعاقب العمليات (باستثناء عناصر البروتوكولات) المستخدمة للحصول على خدمات أمن معينة. وتنطبق هذه الخدمات على كيانات الاتصال في الأنظمة كما تنطبق على البيانات المتبادلة بين الأنظمة والبيانات التي تديرها الأنظمة.

1.3.2 المنظور الإجمالي لهيكل الأمن (X.810)

يقدم المنظور الإجمالي لهيكل الأمن الهياكل الأخرى ويصف مفاهيم مشتركة تشمل ميادين الأمن وسلطات الأمن وسياسات الأمن المستخدمة في جميع الهياكل. كما يصف نسق بيانات عمومياً يمكن استعماله لنقل كل من معلومات الاستيقان ومعلومات التحكم في النفاذ نقلاً آمناً.

2.3.2 هيكل الاستيقان (X.811)

الاستيقان هو توفير الضمان بصحة هوية الكيان الذي يدّعيها. ولا تقتصر الكيانات على المستعملين البشر وإنما تشمل الأجهزة والخدمات والتطبيقات. ويوفر الاستيقان أيضاً الضمان بأن أي كيان لا يحاول التنكر في هيئة اتصال سابقة أو في هيئة استعادة تسجيل غير مرخص به لاتصال سابق. وتتحدث التوصية X.800 عن شكلين من أشكال الاستيقان: *الاستيقان من أصل البيانات* (أي البرهان على أن مصدر البيانات المتلقاة هو المصدر المزعوم) و*الاستيقان من الكيان الند* (أي البرهان على أن الكيان الند في ترابط ما هو الكيان المزعوم).

ويحتل هيكل الاستيقان مرتبة على رأس هرم معايير الاستيقان التي توفر المفاهيم والتسميات كما توفر تصنيفاً لطرائق الاستيقان. ويقوم هذا الهيكل بما يلي: يعرّف مفاهيم الاستيقان الأساسية؛ ويحدد الأصناف الممكنة من آليات الاستيقان؛ ويحدد الخدمات من أجل هذه الأصناف من الآليات؛ ويحدد المتطلبات الوظيفية للبروتوكولات التي تدعم أصناف الآليات هذه؛ ويحدد متطلبات الإدارة عموماً من أجل الاستيقان.

والاستيقان يعقب عموماً تعرّف الهوية. وينبغي حماية المعلومات المستعملة من أجل تعرّف الهوية والاستيقان والترخيص.

3.3.2 هيكل التحكم في النفاذ (X.812)

التحكم في النفاذ هو الحيلولة دون استعمال غير مرخص به لمورد ما، بما في ذلك الحيلولة دون استعمال مورد ما على نحو غير مرخص به. ويضمن التحكم في النفاذ أن الأفراد المرخص لهم أو الأجهزة المرخص لها فقط يمكنهم ويمكنها النفاذ إلى عناصر الشبكة والمعلومات المخزنة وتدفقات المعلومات والخدمات والتطبيقات.

ويصف هيكل التحكم في النفاذ نموذجاً يشكل كل جوانب النفاذ في الأنظمة المفتوحة، والعلاقة بوظائف الأمن الأخرى (مثل الاستيقان والتحقق)، ومتطلبات الإدارة من أجل التحكم في النفاذ.

4.3.2 إطار عدم التنصل (X.813)

عدم التنصل هو القدرة على الحيلولة دون إنكار كيانات ما لاحقاً أنها قامت بأداء إجراء ما. ويعنى مفهوم عدم التنصل بإقامة الدليل الذي يمكن استخدامه لاحقاً لدحض أي مزاعم كاذبة. وتصف التوصية X.800 شكلين من أشكال خدمة عدم التنصل، ألا وهما *عدم التنصل مع برهان التسليم*، ويُستعمل لدحض إنكار كاذب من قبل كيان مقصود يدّعي أنه لم يتلق البيانات، و*عدم التنصل مع برهان المصدر*، ويُستعمل لدحض إنكار كاذب من قبل كيان مصدر يدّعي أنه لم يرسل البيانات. ولكن من الممكن، بصفة أعم، تطبيق مفهوم عدم التنصل على سياقات مختلفة عديدة بما فيها عدم التنصل من استحداث المحتوى أو تقديمه أو تخزينه أو إرساله أو تسلّم البيانات.

ومن شأن هيكل عدم التنصل أن يوسع مفاهيم عدم التنصل من خدمات الأمن كما هي موصوفة في التوصية X.800 وأن يوفر إطاراً لتطوير هذه الخدمات. كما أنه يحدد آليات ممكنة لتوفير هذه الخدمات ومتطلبات الإدارة عموماً فيما يتعلق بعدم التنصل.

5.3.2 هيكل السرية (X.814)

السرية هي خاصية عدم إتاحة المعلومات أو الكشف عنها لأفراد أو كيانات أو عمليات غير مرخص لهم أو لها بذلك.

والغرض من خدمة السرية هو حماية المعلومات من الكشف عنها لمن لا يُرخص له بذلك. ويتناول هيكل السرية مسألة سرّية المعلومات من حيث الاستقاء والنقل والإدارة وذلك بتعريف المفاهيم الأساسية للسرية، وتحديد الأصناف الممكنة من السرية والمرافق المطلوبة لكل صنف من آليات السرية، وتحديد خدمات الإدارة والخدمات الداعمة المطلوبة، وتناول مسألة التفاعل مع خدمات الأمن الأخرى.

6.3.2 هيكل السلامة (X.815)

سلامة البيانات هي الخاصية التي تفيد بأن البيانات لم تخضع لأي تغيير على نحو غير مرخص به. وبصفة عامة، تتناول خدمة السلامة الحاجة إلى ضمان عدم تحريف البيانات أو إذا حدث أن حرّفت أن يكون المستعمل على علم بذلك. وعلى الرغم من وجود جوانب مختلفة للسلامة (سلامة البيانات وسلامة الأنظمة مثلاً) فإن التوصية X.800 تكاد تركز على سلامة البيانات دون غيرها.

ويتناول هيكل السلامة سلامة البيانات في مجال استقاء المعلومات ونقلها وإدارتها. وهو يحدد المفاهيم الأساسية للسلامة ويحدد الأصناف الممكنة من السلامة والمرافق المطلوبة لكل صنف من الآليات، ويحدد الإدارة المطلوبة لكل صنف منها، ويتناول التفاعل ما بين آلية السلامة والخدمات الداعمة من جهة وخدمات الأمن الأخرى وآلياتها من جهة ثانية.

7.3.2 هيكل التحقق والإنذارات (X.816)

عملية *التحقق من الأمن* هي مراجعة مستقلة وتمحيص لسجلات النظام وأنشطته لاختبار كفاية عمليات التحكم في النظام، ولضمان الامتثال للسياسة المقررة والإجراءات التشغيلية، وللكشف عن أي ثغرات في الأمن، وللتوصية بأي تغييرات يشار بها في مجالات التحكم والسياسات والإجراءات. و*إنذار الأمن* رسالة تتولد عندما يكتشف حدث متصل بالأمن معرّف بسياسة أمن على أنه حالة إنذار.

ويعرّف هيكل التحقق والإنذارات المفاهيم الأساسية ويقدم نموذجاً عاماً للتحقق من الأمن والإنذارات، ويحدد المعايير من أجل التحقق من الأمن في حالة ما ومن أجل إطلاق الإنذارات، ويحدد أصنافاً ممكنة من آليات التحقق والإنذارات، ويعرّف الخدمات لهذه الأصناف من الآليات، ويحدد المتطلبات الوظيفية لتوفير هذه الآليات، ويحدد متطلبات الإدارة عموماً من أجل التحقق من الأمن والإنذارات.

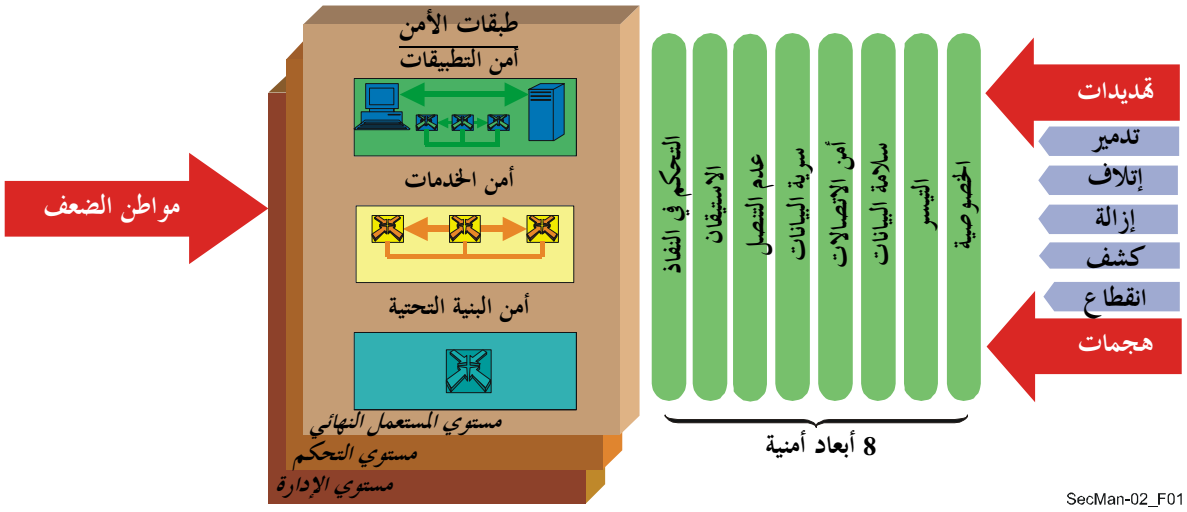
4.2 معمارية الأمن من أجل الأنظمة التي توفر الاتصالات من طرف إلى طرف (X.805)

ألقيت مؤخراً نظرة جديدة على معمارية الأمن من أجل الشبكات. وكانت النتيجة التوصية ITU-T X.805 التي ترسم معيارية أمن لضمان أمن الشبكة من طرف إلى طرف. ويمكن تطبيق المعمارية على مختلف أنواع الشبكات حيث يكون الأمن من طرف إلى طرف موضع اهتمام بصرف النظر عن التكنولوجيا التي تنطوي عليها الشبكة. وتنطبق المبادئ العامة والتعاريف على جميع التطبيقات على الرغم من أن التفاصيل مثل التهديدات وجوانب الضعف وتدابير التغلب عليها أو منع حدوثها تتفاوت تبعاً لاحتياجات التطبيق.

وتعرّف معمارية الأمن هذه على أساس مفهومين رئيسيين، هما الطبقات والمستويات. ويتناول المحور الأول، وهو طبقات الأمن، الشروط التي تنطبق على عناصر الشبكة والأنظمة التي تشكل الشبكة من طرف إلى طرف. ويُعتمد في ذلك منهج تراتبـــي في تقسيم المتطلبات عبر الطبقات حتى يمكن تحقيق الأمن من طرف إلى طرف بناءً على كل طبقة. وهذه الطبقات الثلاث هي طبقة "البنية التحتية"، وطبقة "الخدمات"، وطبقة "التطبيقات". ومن بين مزايا تحديد الطبقات أنه يسمح بإعادة الاستخدام عبر تطبيقات مختلفة عند توفير الأمن من طرف إلى طرف. وتختلف جوانب الضعف في كل طبقة، وبالتالي يجب تحديد تدابير التغلب عليها لتلبية حاجات كل طبقة. وتتألف طبقة البنية التحتية من مرافق الإرسال في الشبكة وكذلك من العناصر المنفردة للشبكة. ومن أمثلة العناصر التي تتكون منها طبقة البنية التحتية أجهزة التسيير والبدالات والمخدمات وكذلك وصلات الاتصال فيما بينها. وتتناول طبقة الخدمات أمن خدمات الشبكة التي تقدم إلى الزبائن. وتتراوح هذه الخدمات بين مرافق التوصيلية الأساسية مثل خدمات الخطوط المؤجرة وخدمات القيمة المضافة مثل التبادل الفوري للرسائل. أما طبقة التطبيق فتتناول متطلبات التطبيقات القائمة على الشبكة التي يستخدمها الزبائن. وقد تكون هذه التطبيقات بسيطة مثل البريد الإلكتروني أو متطورة مثل التطبيقات المرئية المتآزرة التي تستخدم فيها تقنيات راقية للنقل بالفيديو في استكشاف النفط أو تصميم السيارات، وما إلى ذلك.

ويتناول المحور الثاني أمن الأنشطة التي يجري أداؤها داخل الشبكة. وتتضمن معمارية الأمن هذه ثلاثة "مستويات أمنية" تمثل ثلاثة أنواع من الأنشطة المحمية التي تجري على شبكة ما، وهي: (1) مستوي "الإدارة"، (2) ومستوي "التحكم"، (3) ومستوي "المستعمل النهائي". وتتناول مستويات الأمن هذه حاجات الأمن المحددة المرتبطة بأنشطة إدارة الشبكة، أو التحكم في الشبكة أو أنشطة التشوير، وأنشطة المستعمل النهائي. ويتعلق مستوي الإدارة، الذي يناقش في القسم 4.6 بمزيد من التفاصيل، بأنشطة العمليات والإدارة والصيانة وتوفير الخدمات (OAM&P)، مثل توفير الخدمات اللازمة لمستعمل أو لشبكة، وما إلى ذلك. ويرتبط مستوي التحكم بجوانب التشوير لإقامة (وتعديل) الاتصالات من طرف إلى طرف عبر الشبكة، بغض النظر عن الوسط والتكنولوجيا المستخدمة في الشبكة. ويتناول مستوي المستعمل النهائي أمن النفاذ واستعمال الزبائن للشبكة، وكذلك حماية تدفق بيانات المستعمل النهائي.

وانطلاقاً من محوري طبقات الأمن ومستويات الأمن (3 طبقات أمن و 3 مستويات أمن)، تعرّف المعمارية أيضاً ثمانية أبعاد أمن مصممة لتناول أمن الشبكة. ويرد تعريف هذه الأبعاد فيما يلي. وتطبق هذه الأبعاد، من منظور معماري، على كل خلية من خلايا مصفوفة 3 × 3 مشكّلة بين الطبقات والمستويات حتى يمكن تحديد التدابير المضادة الملائمة. ويبين الشكل 2-1 مستويات معمارية الأمن وطبقاتها وأبعادها. ويبين القسم 4.6 حيث يتناول مستوى الإدارة كيف تتناول توصيات أخرى في قطاع تقييس الاتصالات الخلايا الثلاث لمصفوفة 3 × 3 بالنسبة إلى مستوى الإدارة.



الشكل 2-1 – عناصر معمارية الأمن في التوصية ITU-T X.805

وتعتمد التوصية X.805 على بعض مفاهيم التوصية X.800 وهياكل الأمن (X.810 إلى X.816) التي نوقشت أعلاه. وعلى وجه الخصوص، تطابق وظائف خدمات الأمن الأساسية في التوصية X.800 (*التحكم في النفاذ*، *والاستيقان*، *وسرية البيانات*، *وسلامة البيانات*، *وعدم التنصل*) وظائف أبعاد الأمن المقابلة في التوصية X.805 (المرسومة في الشكل 2-1). وعلاوة على ذلك، فإن أبعاد الأمن في التوصية X.805، أي *أمن الاتصال* و*التيسر* و*الخصوصية*، توفر أنماطاً جديدة من حماية الشبكات. وتستعرض أدناه أبعاد الأمن الثمانية.

- البعد الأمني *للتحكم في النفاذ* يحمي من استخدام موارد الشبكة دون ترخيص. ويضمن التحكم في النفاذ أن يقتصر النفاذ إلى عناصر الشبكة والمعلومات المخزنة وتدفقات المعلومات والخدمات والتطبيقات على الأشخاص أو الأجهزة المرخص لهم أو لها بذلك.

- البعد الأمني *للاستيقان* يؤكد صحة هويات الكيانات لدى الاتصال. ويضمن الاستيقان صلاحية الهويات التي تدعيها الكيانات المشاركة في الاتصال (كالأشخاص أو الأجهزة أو الخدمات أو التطبيقات) ويوفر الضمان بأن أي كيان لا يحاول التنكر في هيئة اتصال سابق أو في هيئة استعادة تسجيل غير مرخص به لاتصال سابق.

- البعد الأمني *لعدم التنصل* يوفر سبل الحيلولة دون إنكار فرد أو كيان أنه قام بأداء إجراء ما يتعلق بالبيانات وذلك بإتاحة البرهان عن مختلف الإجراءات المتصلة بالشبكة (من قبيل البرهان على الالتزام أو القصد أو الواجب، والبرهان على منشأ البيانات، والبرهان على الملكية، والبرهان على استعمال المورد). وهو يضمن تيسر الإثبات الذي يمكن تقديمه إلى طرف ثالث واستخدامه برهاناً على أن حدثاً ما، أو إجراءً ما قد حدث فعلاً.

- البعد الأمني *لسرية البيانات* يحمي البيانات من الكشف عنها لمن لا يرخص له بذلك. وتضمن سرية البيانات أن محتوى البيانات لا تستطيع أن تفهمه كيانات غير مرخص لها بذلك. وكثيراً ما تستخدم طرائق التجفير وقوائم التحكم في النفاذ وتصاريح الاطلاع على الملفات لضمان سرية البيانات.
- البعد الأمني *لأمن الاتصال* يضمن أن المعلومات تتدفق حصراً بين النقاط الطرفية المرخص لها بذلك (أي أن المعلومات لا يحدث تحويلها أو اعتراضها عندما تتدفق بين هذه النقاط).
- البعد الأمني *لسلامة البيانات* يضمن صحة أو دقة البيانات. وتكون البيانات محمية من أي تعديل أو حذف أو استحداث أو استنساخ، وتوفر دليلاً على أي من هذه الأنشطة غير المرخص بها.
- البعد الأمني *للتيسر* يضمن عدم رفض النفاذ المصرح به إلى عناصر الشبكة والمعلومات المخزنة وتدفق المعلومات والخدمات والتطبيقات نتيجة أحداث تؤثر على الشبكة. وتشمل هذه الفئة حلول إعادة الشبكة إلى ما كانت عليه قبل الحدث.
- البعد الأمني *للخصوصية* يؤمن حماية المعلومات التي يمكن أن تُستخلص من مراقبة أنشطة الشبكة. ومن أمثلة هذه المعلومات مواقع شبكة الويب التي يكون قد زارها المستعمل، والموقع الجغرافي للمستعمل، وعناوين بروتوكول الإنترنت وأسماء ميادين الأجهزة في شبكة مقدم خدمات ما.

وبإمكان معمارية أمن التوصية X.805 أن توجه عملية وضع تعاريف سياسة أمن شاملة، وخطط الاستجابة لأي حدث والتغلب عليه، ومعماريات التكنولوجيا وذلك بأن تأخذ في الحسبان كل بعد من أبعاد الأمن عند كل طبقة أمن ومستوي أمن أثناء مرحلة التعريف والتخطيط. كما يمكن استعمال معمارية أمن X.805 أساساً لتقييم حالة أمن ما حيث ينظر في كيفية تناول تنفيذ برنامج الأمن الأبعاد والطبقات والمستويات الأمنية عندما تبدأ عملية تنفيذ السياسات والإجراءات ونشر التكنولوجيا. وحالما ينشر برنامج أمن ما يتعين صيانته لكي يبقى صالحاً في بيئة أمن ما فتئت تتغير. وبإمكان معمارية أمن X.805 أن تساعد في إدارة سياسات الأمن وإجراءاته وفي خطط الاستجابة إلى الحدث والتغلب عليه وفي معماريات التكنولوجيا وذلك بالحرص على أن التعديلات التي تطرأ على برنامج الأمن تتناول كل بعد من أبعاد الأمن في كل طبقة ومستوي من طبقات ومستويات الأمن.

3 مبادئ الحماية: التهديدات ومواطن الضعف والمخاطر

لدى وضع أي نوع من هياكل الأمن من الضرورة بمكان أن يكون هنالك فهماً واضحاً للأصول التي تحتاج إلى الحماية، وللتهديدات التي ينبغي حماية تلك الأصول منها، ولمواطن الضعف المرتبطة بالأصول، ولمدى المخاطرة إجمالاً التي تتعرض لها الأصول من جراء تلك التهديدات ومواطن الضعف.

وبصفة عامة، قد نحتاج، في مجال أمن تكنولوجيا المعلومات والاتصالات، إلى حماية الأصول التالية:

- خدمات الاتصالات والحوسبة؛
- المعلومات والبيانات، بما فيها البرمجيات والبيانات المتصلة بخدمات الأمن؛
- التجهيزات والمرافق.

وتبعاً للتوصية X.800 فإن *تهديد الأمن* هو خرق محتمل للأمن. ومن أمثلة التهديد:

- كشف عن معلومات غير مرخص به؛
- إتلاف أو تبديل البيانات أو التجهيزات أو الموارد الأخرى غير مرخص به؛
- سرقة المعلومات أو الموارد الأخرى أو إزالتها أو فقدانها؛
- انقطاع في الخدمات أو رفض تقديمها؛
- تقمص أو انتحال هوية كيان مرخص له.

وقد تكون التهديدات *عرضية* أو *متعمدة* وقد تكون *نشيطة* أو *خاملة*. والتهديد العرضي لا يكون عن سابق تعمد كأن يحدث خلل في نظام أو برمجية ما أو أن يحدث عطل مادي. والتهديد المتعمد يقوم به فرد بممارسة عمل مقصود. (عندما يتحقق تهديد متعمد يدعي *هجمة*). والتهديد النشيط يسفر عن تغيير ما في الحالة مثل تحوير البيانات أو إتلاف تجهيزات مادية. أما التهديدي الخامل فلا ينطوي على أي تغيير في الحالة. والتنصت مثال للتهديد الخامل.

و*مواطن الضعف في الأمن* عيب أو مأخذ يمكن استغلاله لانتهاك نظام ما أو ما يحويه من معلومات (X.800). وموطن الضعف يمكّن من تحقيق التهديد.

وهنالك أربعة أنماط من مواطن الضعف: مواطن ضعف *نموذج التهديد* الناشئة عن صعوبة التنبؤ بالتهديدات المحتملة؛ ومواطن ضعف *التصميم والمواصفات* الناجمة عن أخطاء أو إغفال في تصميم نظام أو بروتوكول ما يجعله عرضة للتأثر في حد ذاته؛ ومواطن ضعف *التنفيذ* بسبب أخطاء تُرتكب أثناء تنفيذ نظام أو بروتوكول ما؛ ومواطن ضعف *التشغيل والتشكيل* التي تنشأ عن استعمال الخيارات على نحو غير ملائم في عمليات التنفيذ أو عن ضعف سياسات النشر (من قبيل عدم فرض استعمال التجفير في شبكة WiFi).

و*الخطر الأمني* يمثل مقدار الآثار الضارة التي قد تحدث إذا ما استغل موطن ضعف أمني ما، أي إذا ما نفذ التهديد. ولئن كان مستحيلاً إزالة الخطر فإن واحداً من أهداف الأمن يكمن في خفض الخطر إلى سوية مقبولة. ولتحقيق ذلك لا بد من فهم التهديدات ومواطن الضعف ومن تطبيق التدابير المضادة الملائمة (أي خدمات الأمن وآلياته).

وبينما تتغير التهديدات وعوامل التهديد تلازم مواطن الضعف الأمنية حياة نظام أو بروتوكول ما، إلا إذا اتخذت خطوات معينة للتغلب على مواطن الضعف. وفي حالة البروتوكولات التي تمتثل لمعايير التقييس، قد تكون مخاطر الأمن التي يتعرض لها البروتوكول كبيرة جداً وعالمية في نطاقها. ولذلك، فمن المهم فهم مواطن الضعف في البروتوكولات وتحديدها واتخاذ الخطوات اللازمة للتغلب على مواطن الضعف عندما تُعرف.

وتقع على عاتق الهيئات المعنية بوضع المعايير مسؤولية فضلاً عن أنها في وضع فريد يمكّنها من التصدي لمواطن الضعف الأمنية التي قد تكون متأصلة في مواصفات من قبيل المعماريات والهياكل والبروتوكولات. ولا يمكن توفير القدر الكافي من الأمن، وإن توفر القدر الكافي من معرفة المخاطر ومواطن الضعف والتهديدات المرتبطة بمعالجة المعلومات وشبكات الاتصالات، ما لم تطبق تدابير الأمن منهجياً بموجب السياسات ذات الصلة والتي ينبغي استعراضها وتحديثها دورياً. وعلاوة على ذلك، لا بد من أن يؤخذ في الحسبان القدر الكافي من إدارة الأمن وإمكانية التعامل مع الأحداث. وهذا يشمل تحديد المسؤولية والتدابير المعنية لمنع وقوع أي حادث أمني، أو التصدي له (أي الاشتراطات وعمليات المراقبة والتدابير المضادة والاحتياطات الواجبة أو الإجراءات التي يتعين الاضطلاع بها). ويعكف القطاع ITU-T على صياغة توصيات جديدة تشمل مثل هذه الجوانب من إدارة الأمن.

4 متطلبات الأمن من أجل شبكات الاتصال

يتناول هذا القسم الاعتبارات الأساسية بشأن الحاجة إلى جوانب الأمن وخصائصها من منظور المستعملين، بمن فيهم مشغلو شبكات الاتصالات. وهذه الاعتبارات مستمدة من المتطلبات التي أعربت عنها أطراف شتى في أسواق الاتصالات. وهو يشير بالدرجة الأولى إلى الأعمال التي تحققت لدى اعتماد التوصية ITU-T E.408، بعنوان *متطلبات أمن شبكات الاتصالات*. وتوفر هذه التوصية نظرة عامة تشمل متطلبات الأمن وهيكلاً يحدد ما هي تهديدات الأمن التي تتعرض لها شبكات الاتصالات عموماً (الثابتة منها والمتنقلة، سواء للصوت أو البيانات) وتحتوي على إرشادات بغية التخطيط لتدابير مضادة يمكن اتخاذها لتقليل المخاطر الناجمة عن التهديدات.

والتوصية عمومية في طابعها ولا تحدد أو تتناول متطلبات من أجل شبكات معينة.

ولم ينظر في أي خدمات أمن جديدة وإنما في استعمال خدمات الأمن القائمة المعرّفة في توصيات أخرى صادرة عن القطاع ITU-T وفي المعايير القياسية ذات الصلة التي وضعتها هيئات أخرى.

ومن شأن تنفيذ المتطلبات الواردة أن يسهل تعاوناً دولياً في المجالات التالية فيما يتعلق بأمن شبكات الاتصالات:

- تقاسم المعلومات وتعميمها؛
- تنسيق الأحداث والاستجابة إلى الأزمات؛
- استقدام المهنيين في مجال الأمن وتدريبهم؛
- تنسيق إنفاذ القوانين؛
- حماية البنى التحتية الحساسة والخدمات الحساسة؛
- وضع التشريعات الملائمة.

وتحقيقاً لمثل هذا التعاون لا بد من تنفيذ متطلبات المكونات الوطنية للشبكة على الصعيد الوطني.

1.4 الأسباب الموجبة

ترجع الأسباب الموجبة لوضع هيكل عمومي لأمن الشبكات في الاتصالات الدولية إلى مصادر مختلفة:

- يحتاج *الزبائن/المستعملون* إلى الثقة في الشبكة والخدمات التي تقدمها بما في ذلك تيسر الخدمات (وخاصة خدمات الطوارئ) في حالة الكوارث الكبرى، بما في ذلك أحداث العنف الأهلية.
- يطالب *الجمهور والسلطات العامة* بتوافر الأمن بموجب توجيهات وتشريعات، وذلك لضمان تيسر الخدمات والمنافسة الشريفة وحماية الخصوصية.
- يحتاج *مشغلو الشبكات ومقدمو الخدمات* بالذات إلى الأمن للحفاظ على عملياتهم ومصالحهم التجارية، وتلبية التزاماتهم تجاه الزبائن والجمهور، على الصعيدين الوطني والدولي.

وينبغي أن تقوم متطلبات أمن شبكات الاتصالات على أساس معايير أمن متفق عليها دولياً حيث من الأفضل استعمال المعايير الموجودة بدلاً من استحداث معايير جديدة. وقد يكون توفير خدمات وآليات الأمن واستخدامها عملية باهظة التكاليف مقارنة بقيمة المعاملات المطلوب حمايتها. ولهذا من المهم التمكن من تفصيل الأمن تبعاً للخدمات المطلوب حمايتها، وبالتالي ينبغي توفير خدمات الأمن وآلياته بحيث يمكن تفصيلها. ونظراً لضخامة عدد التشكيلات الممكنة من مجموعات خصائص الأمن، من المستصوب أن تغطي *مواصفات الأمن* طائفة واسعة من خدمات شبكات الاتصالات.

ويساعد التقييس على تيسير *إعادة استخدام الحلول والمنتجات*، أي أن من الممكن توفير الأمن بشكل أسرع وبتكاليف أقل.

ومن الفوائد المهمة للحلول التي تمتثل لمعايير التقييس سواء بالنسبة إلى بائعي الأنظمة أو مستعمليها تحقيق وفورات الحجم عند تطوير المنتجات وتوفير إمكانية التشغيل البيني للمكونات ضمن شبكات الاتصالات فيما يتعلق بالأمن.

ومن الضروري توفر خدمات الأمن وآلياته لحماية شبكات الاتصالات من أي هجوم مؤذ مثل إنكار الخدمة أو التنصت أو الخداع أو التلاعب بالرسائل (التعديل أو التأخير أو الحذف أو الإضافة أو استعادة التسجيل أو إعادة التسيير أو التسيير الخاطئ أو إعادة ترتيب الرسائل) أو التنصل أو التزوير. وتشمل الحماية جوانب الوقاية واكتشاف وقوع الهجمات والتغلب عليها، وكذلك إدارة المعلومات المتصلة بالأمن. وينبغي أن تشتمل الحماية أيضاً على تدابير للحيلولة دون توقف الخدمة نتيجة أحداث طبيعية (حالة الطقس مثلاً) أو هجمات مؤذية (أعمال عنف). وينبغي وضع أحكام تسمح بالتنصت والرقابة بناء على طلب سلطات قانونية مُخوّلة بذلك.

2.4 أهداف الأمن العامة من أجل شبكات الاتصالات

يتناول هذا القسم بالوصف الهدف البعيد من تدابير الأمن التي تتخذ في شبكات الاتصالات ويركز على ما تحققه متطلبات الأمن أكثر مما يركز على كيفية عملها.

وأهداف الأمن من أجل شبكات الاتصالات هي:

أ) ينبغي أن يقتصر النفاذ إلى شبكات الاتصالات واستعمالها على المستعملين المرخص لهم بذلك.

ب) ينبغي أن تقتصر قدرة المستعملين المرخص لهم بذلك على النفاذ إلى الأصول المرخص لهم بالنفاذ إليها وإمكانية تشغيلها.

ج) ينبغي أن توفر شبكات الاتصالات الخصوصية عند السوية التي تحددها سياسات أمن الشبكة.

د) ينبغي أن يتحمل جميع المستعملين مسؤولية ما يقومون به فقط لا غير في شبكات الاتصالات.

هـ) حرصاً على ضمان التيسر، ينبغي حماية شبكات الاتصالات من النفاذ أو العمليات الاقتحامية.

و) ينبغي أن يكون في الإمكان استقاء معلومات متصلة بالأمن من شبكات الاتصالات (ولكن ينبغي أن تقتصر إمكانية استقاء هذه المعلومات على المستعملين المرخص لهم بذلك دون غيرهم).

ز) إذا ما اكتشفت انتهاكات أمنية، ينبغي عندئذ أن تعالج بشكل محكم وفقاً لخطة محددة مسبقاً وذلك لتخفيف الضرر المحتمل.

ح) بعد اكتشاف أي إخلال بالأمن ينبغي أن يكون من الممكن استعادة سويات الأمن الاعتيادية.

ط) ينبغي أن توفر معمارية أمن شبكات الاتصالات قدراً من المرونة بغية تقبل سياسات أمنية مختلفة، مثال ذلك آليات أمن متفاوتة الشدة.

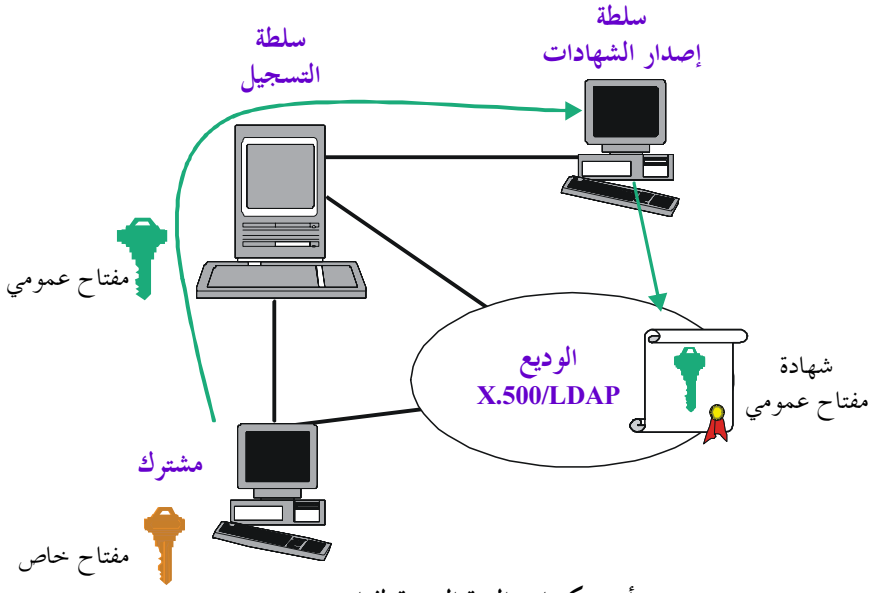
وعبارة "النفاذ إلى الأصول" لا تقتصر على إمكانية أداء وظائف ما وإنما تشمل أيضاً قراءة المعلومات.

ويمكن التدليل على أن تنفيذ تدابير الأمن الوارد ذكرها أدناه يحقق الأهداف الخمسة الأولى من أهداف أمن شبكات الاتصالات آنفة الذكر أعلاه:

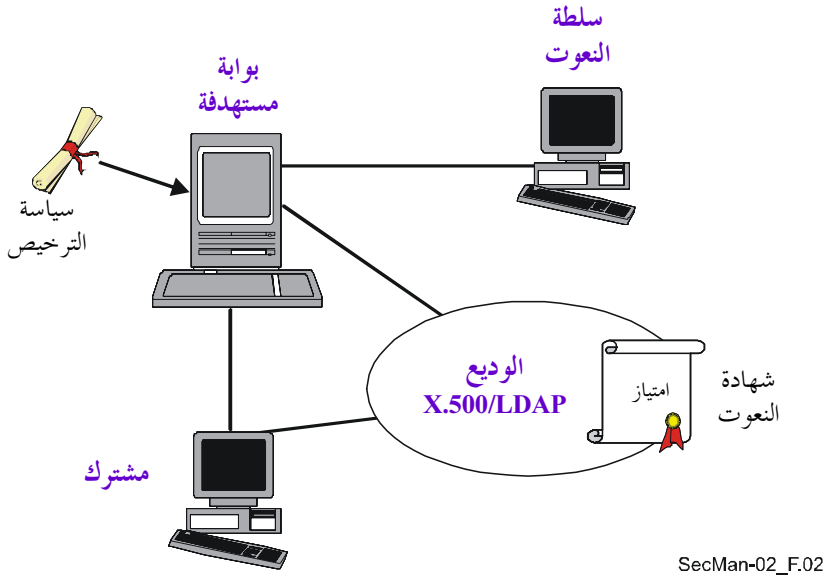
- السرّية؛
- سلامة البيانات؛ (لا شك في أن سلامة برامج الأنظمة مطلوبة أيضاً)
- المساءلة، بما فيها الاستيقان وعدم التنصل والتحكم في النفاذ؛
- التيسر.

5 البنى التحتية لكل من المفاتيح العمومية وإدارة الامتيازات

توفر التوصية ITU-T X.509 بعنوان *الدليل: هياكل المفاتيح العمومية وشهادات النعوت* معيار بنية تحتية للمفاتيح العمومية (PKI) لاستيقان قوي قائم على أساس شهادات المفاتيح العمومية وسلطات إصدار الشهادات. وتوفر البنية التحتية (PKI) إمكانية إدارة المفاتيح العمومية لتمكين خدمات الاستيقان والتجفير والسلامة وعدم التنصل. والتكنولوجيا الأساسية في البنية التحتية PKI هي تجفير المفاتيح العمومية الموصوفة أدناه. وبالإضافة إلى تحديد هيكل استيقان من أجل البنية التحتية PKI تتناول التوصية X.509 أيضاً بنية تحتية لإدارة الامتيازات (PMI) والتي تُستخدم للتأكد من حقوق ومزايا المستعملين في سياق الاستيقان القوي الذي يقوم على أساس شهادات النعوت وسلطات النعوت. ويتضمن الشكل 5-1 مكونات البنية التحتية للمفاتيح العمومية (PKI) والبنية التحتية لإدارة الامتيازات (PMI).



(أ) مكونات البنية التحتية لمفتاح عمومي



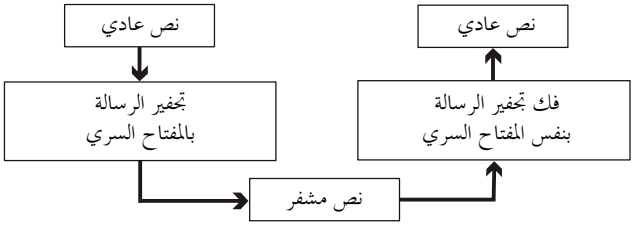
(ب) مكونات البنية التحتية لإدارة الامتيازات

الشكل 5-1 – مكونات البنية التحتية للمفاتيح العمومية (PKI) والبنية التحتية لإدارة الامتيازات (PMI)

1.5 تجفير المفاتيح السرية والمفاتيح العمومية

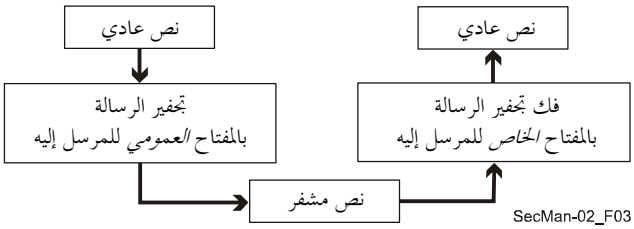
يشير التجفير *التناظري* (أو تجفير *المفتاح السري*) إلى نظام تجفير يُستخدم فيه نفس المفتاح لكل من عملية التشفير وفك التشفير على السواء كما يوضح الشكل 5-2(أ). وتقتضي أنظمة التجفير التناظرية أن تكون الترتيبات الأولية لأفراد يتقاسمون مفتاحاً سرياً واحداً. وينبغي أن يكون المفتاح موزعاً على الأفراد عبر وسائل آمنة لأن معرفة مفتاح التشفير تعني معرفة مفتاح فك التشفير والعكس بالعكس.

ويقوم نظام التجفير *اللاتناظري* (أو تجفير *المفتاح العمومي*) على زوج من المفاتيح كما هو مبين في الشكل 5-2(ب) – مفتاح عمومي ومفتاح خاص. ويمكن توزيع المفاتيح العمومية على نطاق واسع ولكن المفتاح الخاص يجب أن يبقى سرياً دوماً. ويُحتفظ بالمفتاح الخاص عادة في بطاقة ذكية أو في علامة خاصة. ويتولد المفتاح العمومي انطلاقاً من المفتاح الخاص، وعلى الرغم من أن هذين المفتاحين مترابطان رياضياً، ليس هنالك من وسيلة ممكنة بغية عكس العملية لاشتقاق المفتاح الخاص من المفتاح العمومي. ولإرسال بيانات سرية إلى شخص ما على نحو آمن باستعمال تجفير المفاتيح العمومية يقوم المرسل بتجفير البيانات مستعملاً المفتاح العمومي لدى المرسل إليه. ثم يقوم المرسل إليه بفك تجفير البيانات مستعملاً المفتاح الخاص المقابل. ومن الممكن أيضاً استعمال تجفير المفاتيح العمومية لوسم بيانات معينة بتوقيع رقمي للتأكيد على أن وثيقة أو رسالة ما قد صدرت عن الشخص الذي يدّعي أنه المرسل (أو مصدر الرسالة). والتوقيع الرقمي هو في الواقع خلاصة للبيانات المنتجة باستعمال المفتاح الخاص لصاحب التوقيع وهي تذيّل الوثيقة أو الرسالة. أما المرسل إليه فيستعمل المفتاح العمومي لصاحب التوقيع لكي يتأكد من صحة التوقيع الرقمي. (**ملاحظة** – تستخدم بعض أنظمة المفاتيح العمومية زوجين من أزواج المفاتيح العمومية/الخاصة، زوج للتجفير/لفك التجفير، والآخر للتوقيع/للتحقق الرقمي).



– يتقاسم الطرفان مفتاحاً سرياً واحداً
– المشكلة: تبادل المفاتيح بسرية كاملة صعب ولا يقبل اتساع النطاق، أي غير عملي لمجموعة كبيرة من المستعملين.
– أفضل مثال معروف: معيار تجفير البيانات (DES)

(أ) تجفير المفتاح التناظري (أو السري)



– يوجد لدى كل مشارك
– مفتاح خاص لا يتقاسمه أحد، إضافة إلى
– مفتاح عمومي معروف للجميع
– المشكلة: أبطأ من تجفير المفتاح السري
– أفضل مثال معروف: خوارزمية ريفست وشامير وأدلمان (RSA)

(ب) تجفير مفتاح لا تناظري (أو عمومي)

الشكل 5-2 – مخطط عملية تجفير مفتاح تناظري (أو سري) وعملية تجفير لا تناظري (أو عمومي) مع إبراز الخصائص

في حالة التجفير التناظري يجب أن يكون لدى كل زوج من المستعملين زوج مختلف من المفاتيح ويجب أن توزع أزواج المفاتيح هذه ويُحتفظ بها على نحو آمن. أما في حالة التجفير اللاتناظري فيمكن نشر مفاتيح التجفير العمومية في دليل ويمكن لأي طرف أن يستعمل نفس مفتاح التجفير (العمومي) لكي يرسل بيانات إلى أي مستعمل يريد. وهذا ما يجعل التجفير اللاتناظري أكثر قابلية لإمكانية اتساع النطاق مما هو الحال في التجفير التناظري. بيد أن التجفير اللاتناظري مكلف من حيث زمن الحوسبة ولذلك ليس من الكفاءة تجفير رسائل بأكملها باستخدام التجفير اللاتناظري. ومن ثم فإن التجفير اللاتناظري يُستخدم عملياً لتبادل المفاتيح المتناظرة التي تستخدم بعدئذ لتجفير متن الرسالة باستخدام خوارزمية تناظرية أكثر كفاءة من حيث زمن الحوسبة. وعندما يتطلب الأمر توقيعاً رقمياً تُفرم الرسالة باستخدام وظيفة فرم آمنة في اتجاه واحد مثل خوارزمية الفرم الآمنة SHA1 أو خوارزمية تلخيص الرسالة MD5 ويتم تجفير البتات الناتجة وعددها 160 أو 128 لا تناظرياً باستخدام المفتاح الخاص لدى المرسل وتذيّل الرسالة بهذا التوقيع.

وجدير بالإشارة، سواء استخدم التجفير التناظري أم اللاتناظري، فإنه ليس من الممكن تسيير الرسائل إلى أصحابها إذا كانت الرسالة مجفرة بأكملها، إذ إن العقد الوسيطة لن تكون قادرة على معرفة عنوان المرسل إليه. ولذلك لا بد من أن تكون رأسيات الرسائل غير مجفرة عموماً.

ويعتمد التشغيل الآمن لأي نظام من أنظمة المفاتيح العمومية كل الاعتماد على صلاحية هذه المفاتيح العمومية. وتنشر المفاتيح العمومية عادة في شكل شهادات رقمية يُحتفظ بها في دليل بموجب التوصية X.500. ولا تحتوي الشهادة على مفتاح التجفير العمومي، وعند الاقتضاء مفتاح التحقق من توقيع فرد ما، فحسب وإنما تحتوي على معلومات إضافية ومنها صلاحية الشهادة. والشهادات التي تبطل لأي سبب كان تُدرج عادة في الدليل في قائمة إبطال الشهادات (CRL). وقبل استخدام المفاتيح العمومية يجري التحقق عادة من صلاحيتها باستشارة القائمة CRL.

2.5 شهادات المفاتيح العمومية

شهادة المفتاح العمومي (التي تسمى أحياناً "الشهادة الرقمية") هي إحدى طرق التحقق من أهلية صاحب زوج من المفاتيح اللاتناظرية. وتقيم هذه الشهادة رابطة وثيقة بين المفتاح العمومي واسم صاحبه، وهي موقّعة رقمياً من قبل سلطة موثوق بها تشهد على هذه الرابطة. وتعرف هذه السلطة باسم سلطة إصدار الشهادات (CA). وتحدد التوصية ITU-T X.509 نسق المعيار القياسي المعترف به دولياً لشهادات المفاتيح العمومية. وباختصار، تتألف شهادة المفتاح العمومي بموجب التوصية X.509 من مفتاح عمومي ومُعرِّف للخوارزمية اللاتناظرية التي يتعين أن يستخدم معها المفتاح، واسم صاحب زوج المفاتيح واسم سلطة إصدار الشهادات التي تشهد بهذه الملكية والرقم المسلسل ومدة صلاحية الشهادة ورقم صيغة التوصية X.509 التي تمتثل لها هذه الشهادة ومجموعة اختيارية من مجالات فرعية تحتوي معلومات عن السياسة التي تطبقها سلطة إصدار الشهادات. ثم يتم توقيع الشهادة بأكملها رقمياً باستخدام المفتاح الخاص لدى سلطة إصدار الشهادات. ويمكن نشر أي شهادة بموجب التوصية X.509 على نطاق واسع، كأن تنشر مثلاً على موقع الويب، في دليل بروتوكول النفاذ السريع (LDAP)، أو في البطاقة Vcard المرفقة برسائل البريد الإلكتروني. ويضمن توقيع سلطة إصدار الشهادات أن محتويات الشهادة لا يمكن تعديلها دون علمها.

وللتحقق من صلاحية شهادة المفتاح العمومي لدى مستعمل ما يحتاج الأمر إلى النفاذ إلى المفتاح العمومي الصالح لدى السلطة التي أصدرت الشهادة وذلك للتحقق من توقيع السلطة على الشهادة. ويجوز لسلطة ما أن تُشهد سلطة أخرى (أعلى منها) على مفتاحها العمومي بحيث يتناول التحقق من المفاتيح العمومية سلسلة من الشهادات. ولا بد أن تنتهي هذه السلسلة في نقطة ما، وذلك عندما نصادف شهادة من جانب سلطة تكون بمثابة "الأصل الموثوق". ويتم توزيع المفاتيح العمومية لدى هذه السلطة الأصل في شكل شهادات موقعة ذاتياً (يشهد فيها الأصل الموثوق بأن ذلك هو مفتاحه العمومي). ويضمن التوقيع التحقق من أن المفتاح واسم سلطة إصدار الشهادات لم يتم التلاعب فيهما منذ أن صدرت الشهادة. ومع ذلك، لا يمكننا الاطمئنان إلى اسم سلطة إصدار الشهادات المبيّن في شهادة موقعة ذاتياً لأن السلطة أدرجت الاسم في الشهادة بنفسها. ولذلك فإن المكون الحرج في البنية التحتية للمفاتيح العمومية هو التوزيع الآمن للمفاتيح العمومية من جانب سلطة الأصل الموثوق (في شكل شهادات موقعة ذاتياً)، بحيث نطمئن إلى أن المفتاح العمومي ينتمي حقاً إلى

سلطة الأصل الموثوق المبين اسمها في الشهادة الموقعة ذاتياً. ولولا ذلك، لا يمكننا أن نكشف عن انتحال كيان ما هوية سلطة الأصل الموثوق لإصدار الشهادات.

3.5 البنى التحتية للمفاتيح العمومية

الغرض الرئيسي من البنية التحتية للمفاتيح العمومية هو إصدار شهادات المفاتيح العمومية وإدارتها، بما في ذلك الشهادات الموقعة ذاتياً من قبل الأصل الموثوق لسلطة إصدار الشهادات. وتشمل إدارة المفاتيح استحداث أزواج المفاتيح، وإصدار شهادات المفاتيح العمومية، وإبطال شهادات المفاتيح العمومية (عندما تكون سرّية المفتاح الخاص موضع شك مثلاً)، وتخزين وأرشفة المفاتيح والشهادات، وإتلافها عندما ينقضي أجل استعمالها. وتعمل كل سلطة من سلطات إصدار الشهادات طبقاً لمجموعة من السياسات، وتحدد التوصية ITU-T X.509 آليات لتوزيع بعض معلومات هذه السياسات في مجالات التمديد في الشهادات X.509 التي تصدرها سلطة إصدار الشهادات. وتكون قواعد وإجراءات السياسات التي تتبعها سلطة إصدار الشهادات مبينة عادة في سياسة الشهادات وفي بيان ممارسات الإشهاد، وهما من الوثائق التي تنشرها السلطة. ومن شأن هاتين الوثيقتين ضمان أساس مشترك لتقييم درجة الثقة التي يمكن أن نضعها في شهادات المفاتيح العمومية التي تصدرها السلطات سواء على المستوى الدولي أم عبر القطاعات. كما توفران لنا (جزءاً من) الإطار القانوني الضروري لبناء الثقة فيما بين المنظمات وتضعان قيوداً على استخدام الشهادات الصادرة.

ولا بد من الإشارة، في حالة الاستيقان من استخدام شهادات المفاتيح العمومية، إلى أن النقاط الطرفية عليها أن تقدم توقيعات رقمية باستخدام قيمة المفتاح الخاص المرتبط بها، إذ إن تبادل شهادات المفاتيح العمومية لا يوفر بمفرده الحماية من هجمات طرف متوسط بين الطرفين.

4.5 البنية التحتية لإدارة الامتيازات

حددت الصيغ الأولى من التوصية ITU-T X.509 (1988 و1993 و1997)، *الدليل: هيكل استيقان* العناصر الأساسية اللازمة للبنى التحتية للمفاتيح العمومية. ويشمل ذلك تعريف شهادات المفاتيح العمومية. وتحتوي التوصية ITU-T X.509 المراجعة التي اعتُمدت في عام 2000 تعزيزاً هاماً لشهادات النعوت وإطاراً لبنية تحتية لإدارة الامتيازات (PMI). (وتقوم البنية PMI بإدارة الامتيازات للقيام بخدمة ترخيص شاملة فيما يتعلق ببنية PKI). وتسمح الآليات الموصوفة بتحديد امتيازات نفاذ المستعملين في بيئة متعددة البائعين والتطبيقات.

ومفاهيم البنية التحتية لإدارة الامتيازات (PMI) والبنية التحتية للمفاتيح العمومية (PKI) متماثلة، إلا أن PMI تتناول الترخيص بينما تركز PKI على الاستيقان. ويوضح الشكل 5-1 والجدول 5-1 التماثل بين البنيتين التحتيتين.

الجدول 5-1 – مقارنة بين خصائص البنية التحتية لإدارة الامتيازات والبنية التحتية للمفاتيح العمومية

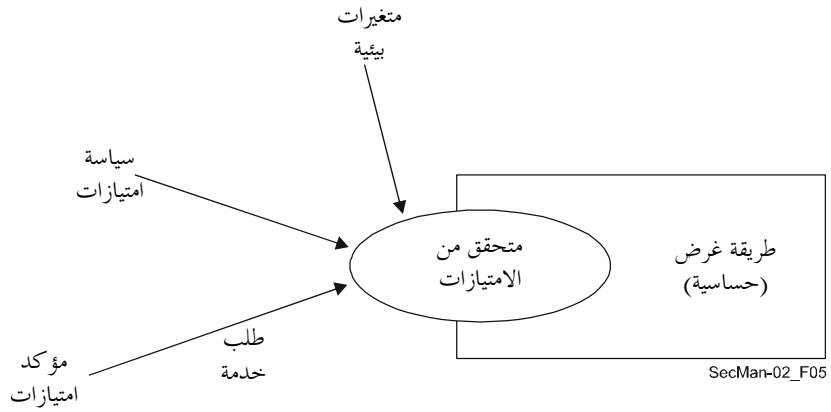
البنية التحتية لإدارة الامتيازات (PMI)	البنية التحتية للمفاتيح العمومية (PKI)
مصدر السلطة	السلطة الأصل لإصدار الشهادات (مرتكز الثقة)
سلطة تحديد النعوت	سلطة إصدار الشهادات
شهادة النعوت	شهادة المفتاح العمومي
قائمة إبطال شهادات النعوت	قائمة إبطال الشهادات
قائمة إبطال السلطات بالنسبة إلى PMI	قائمة إبطال السلطات بالنسبة إلى PKI

والغرض من تعيين امتيازات للمستعملين هو ضمان اتباعهم لسياسة أمن مقررة يضعها مصدر السلطة. وترتبط تلك المعلومات المتعلقة بالسياسة باسم المستعمل في شهادة النعوت، وتتألف من عدد من العناصر المبينة في الشكل 5-3.

الصيغة
صاحب الشهادة
جهة الإصدار
التوقيع (شفرة تعريف خوارزمية)
الرقم المسلسل للشهادة
مدة الصلاحية
النعوت
شفرة تعريف فريدة لجهة الإصدار
التمديدات

الشكل 5-3 – هيكل شهادة النعوت بموجب التوصية X.509

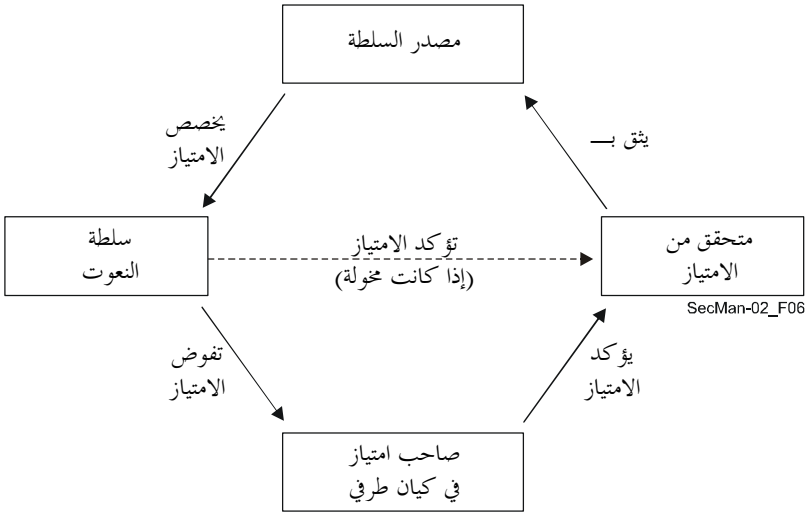
هنالك خمسة مكونات للتحكم في البنية التحتية لإدارة الامتيازات (PMI) موصوفة في التوصية ITU-T X.509، وهي: مؤكد الامتياز، والمتحقق من الامتياز، وطريقة الغرض[1]، وسياسة الامتيازات، والمتغيرات البيئية (انظر الشكل 5-4). وتمكّن التقنيات المتحقق من الامتياز من التحكم في النفاذ إلى طريقة الغرض بواسطة مؤكد الامتياز طبقاً لسياسة الامتيازات.



الشكل 5-4 – نموذج تحكم في البنية التحتية لإدارة الامتيازات بموجب التوصية ITU-T X.509

وعندما يكون تفويض الامتياز ضرورياً من أجل التنفيذ، هنالك أربعة مكونات لنموذج التفويض بالنسبة إلى البنية التحتية لإدارة الامتياز بُحثت في التوصية ITU-T X.509 وهي: متحقق من الامتياز، ومصدر السلطة، وسلطة النعوت، ومؤكد الامتياز (انظر الشكل 5-5).

[1] تعرّف طريقة الغرض على أنها إجراء يمكن تنفيذه على مورد (يمكن مثلاً أن يكون لنظام ملفات طرائق أغراض للقراءة والكتابة والتنفيذ).



الشكل 5-5 – نموذج تفويض البنية التحتية لإدارة الامتيازات بموجب التوصية ITU-T X.509

وتعتبر عمليات التنفيذ الحديثة لمخططات الترخيص طبقاً لنموذج التحكم في النفاذ القائم على الدور (RBAC) أن المستعمل له دور. وتربط سياسة الترخيص ما بين مجموعة من التصاريح ودور ما. وعند النفاذ إلى مورد يتم التأكد من دور المستعمل طبقاً للسياسة المقررة لتمكين أي إجراء لاحق. ويوضح تطبيق الوصفات الطبية الإلكترونية الموصوف في القسم 2.5.6 استخدام نظام التحكم في النفاذ القائم على الدور.

6 تطبيقات

تنتمي التطبيقات التي يتناولها هذا القسم إلى نوعين متميزين. يركز النوع الأول على تطبيقات المستعمل النهائي، ومنها مثلاً نقل الصوت بواسطة بروتوكول الإنترنت (VoIP) حيث توصف معمارية الشبكة ومكوناتها المستخدمة لتوفير هذا التطبيق من تطبيقات المستعمل النهائي. ويناقش هذا القسم اعتبارات الأمن وحلولها للمستويات الثلاثة التي تدعم تطبيقات متعددة الوسائط ويعامل نقل الصوت بواسطة بروتوكول الإنترنت كحالة خاصة. وتطبيقات المستعمل النهائي الأخرى التي يناقشها هذا القسم هي نظام الاتصالات الكبلية باستعمال بروتوكول الإنترنت (IPCablecom) الذي يوفر الخدمات القائمة على بروتوكول الإنترنت في الوقت الفعلي على شبكة كبلية، وإرسال الفاكس. وتشمل التطبيقات التي لا تنحصر في صناعة الاتصالات والتي تبحث هنا الرعاية الصحية الإلكترونية، ولا سيما نظام الوصفات الطبية الإلكترونية. ويركز النوع الثاني على تطبيقات إدارة الشبكة. ومسألة الأمن من الاعتبارات الهامة لضمان جودة الخدمات المقدمة وسلامتها. ولذلك، لا مناص من أداء أنشطة الإدارة على أساس الامتيازات الملائمة والترخيص الملائم.

1.6 نقل الصوت بواسطة بروتوكول الإنترنت باستخدام أنظمة التوصية H.323

إن نقل الصوت بواسطة بروتوكول الإنترنت (VoIP)، المعروف أيضاً باسم المهاتفة بواسطة بروتوكول الإنترنت، هو توفير الخدمات التي كانت تقدم تقليدياً عبر الشبكة الهاتفية العمومية التبديلية (PSTN) (بتبديل الدارة) عن طريق شبكة تستخدم بروتوكول الإنترنت (والتي تقوم على أساسها الإنترنت). وتشمل هذه الخدمات الصوت في المقام الأول ولكنها تشمل أيضاً أشكالاً أخرى من الوسائط، بما في ذلك الفيديو والبيانات، من قبيل تقاسم التطبيقات ووظيفة اللوح الأبيض الإلكتروني. ويشمل نقل الصوت VoIP أيضاً خدمات تكميلية مصاحبة مثل المؤتمرات الشبكية وإمكانية إحالة النداء والنداء قيد الانتظار والنداء المحوّل وتعدد الخطوط واستبقاء النداء للرد على نداء آخر والاطلاع على النداءات الواردة وإمكانية تتبع الجهة المطلوبة وغير ذلك من الخدمات الكثيرة الأخرى التي توفرها الشبكات الذكية، ومنها أيضاً بيانات النطاق الصوتي لبعض المستعملين. ونقل الصوت بواسطة الإنترنت حالة خاصة لنقل الصوت بواسطة بروتوكول الإنترنت، وفيها يتم ترحيل حركة الصوت عبر الشبكة الفقرية العمومية للإنترنت.

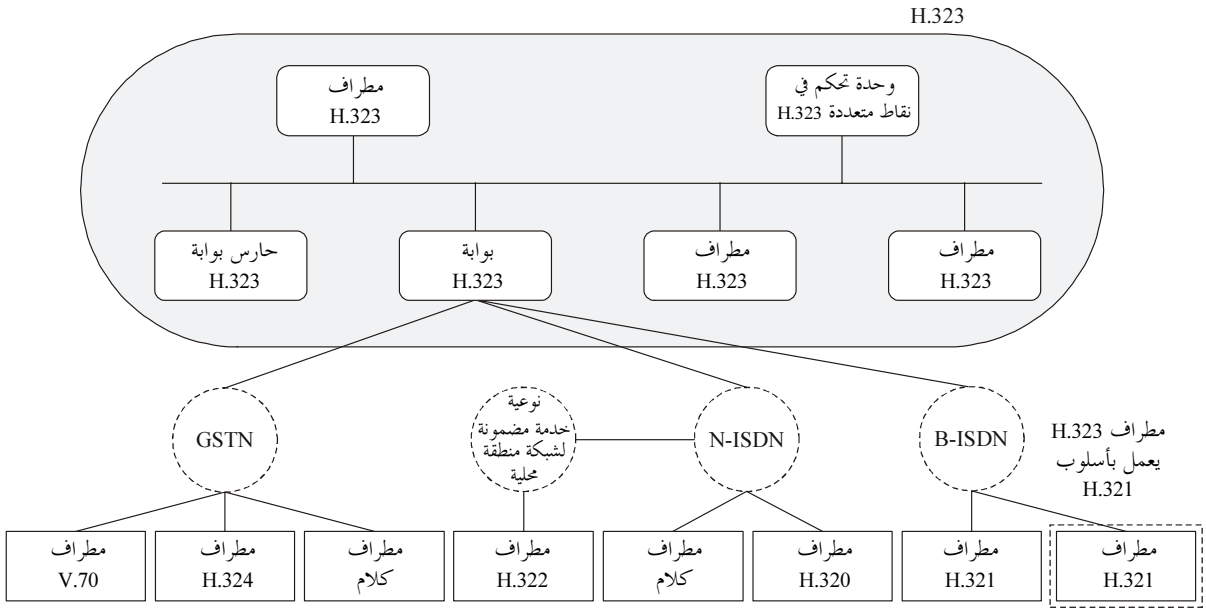
والتوصية H.323 توصية شاملة أصدرها قطاع تقييس الاتصالات لكي توفر أساساً لنقل الصوت والفيديو والبيانات عبر شبكات تبديلية بالرزم، بما في ذلك الإنترنت وشبكات المناطق المحلية (LAN) وشبكات المناطق العريضة (WAN)، والتي لا توفر نوعية خدمة مضمونة. وتسود هذه الشبكات الحواسيب المكتبية للمؤسسات وتشمل تكنولوجيات بروتوكول التحكم في الإرسال بتبديل الرزم/بروتوكول الإنترنت (TCP/IP) وتبادل بروتوكول الإنترنت عبر إثرنت، والإثرنت السريعة والعلامة الجوالة في شبكة حلقية. ومن شأن الامتثال للتوصية H.323 أن يمكّن تحقيق التشغيل البيني لمنتجات وتطبيقات متعددة الوسائط من بائعين متعددين بما يسمح للمستعملين بالاتصال دون قلق بشأن التوافق. وكانت التوصية H.323 أول بروتوكول لنقل الصوت بواسطة بروتوكول الإنترنت (VoIP) وتعتبر حجر الأساس للمنتجات القائمة على هذا البروتوكول للمستهلكين والمعاملات وتقديم الخدمات والتسلية والتطبيقات المهنية. وفيما يلي التوصيات الرئيسية التي هي جزء من نظام التوصية H.323:

- H.323 – وثيقة "شاملة" تصف استخدام التوصيتين H.225.0 وH.245 ووثائق أخرى تتناول تقديم خدمات المؤتمرات متعددة الوسائط والقائمة على الرزم.
- H.225.0 – تصف ثلاثة بروتوكولات تشوير (خوارزمية ريفست وأدلمان وشامير وتشوير النداء و"الملحق زاي").
- H.245 – بروتوكول مراقبة الوسائط المتعددة (مشترك بين H.310 وH.323 وH.324).
- H.235.x – الأمن ضمن الأنظمة القائمة على التوصية H.323.
- H.246 – التشغيل البيني مع الشبكات الهاتفية العمومية التبديلية.
- H.450.x – الخدمات التكميلية.
- H.460.x – تمديدات مختلفة لبروتوكول التوصية H.323.
- H.501 – بروتوكول للإدارة المتنقلة والاتصالات داخل الميدان وفيما بين الميادين.
- H.510 – تنقلية المستعملين والمطاريف والخدمات.
- H.530 – مواصفات الأمن للتوصية H.510.

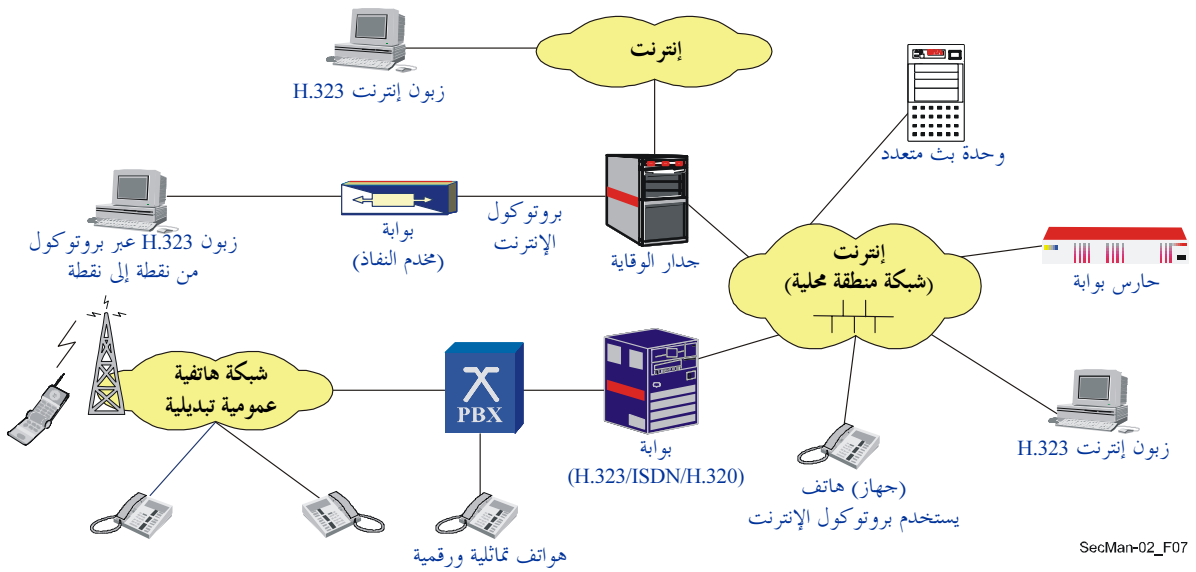
وقد اعتمد قطاع تقييس الاتصالات الصيغة الأولى للتوصية H.323 في عام 1996. واعتمدت الصيغة الثانية في يناير 1998، أما الصيغة الحالية رقم 6، فقد اعتمدت في عام 2006. والمعيار واسع في نطاقه ويشمل كلاً من الأجهزة التي تعمل بمفردها والتكنولوجيا المدمجة في الحاسوب الشخصي، وكذلك المؤتمرات من نقطة إلى نقطة والمؤتمرات متعددة النقاط. وتتناول التوصية ITU-T H.323 التحكم في النداءات، وإدارة الوسائط المتعددة، وإدارة عرض النطاق، وكذلك سطوح التماس بين مختلف الشبكات.

والتوصية H.323 جزء من سلسلة أكبر تشمل معايير الاتصالات التي تمكّن من عقد مؤتمرات فيديوية عبر طائفة من الشبكات. وهذه السلسلة من التوصيات تُعرف باسم H.32x، وتشمل التوصيتين H.320 وH.324 اللتين تتناولان الاتصالات عبر الشبكات الرقمية متكاملة الخدمات (ISDN) والشبكات الهاتفية العمومية التبديلية، على التوالي. وتتضمن الأولى نظرة إجمالية لمعيار التوصية H.323 وفوائده ومعماريته وتطبيقاته.

وتتضمن التوصية H.323 تعريف أربعة مكونات رئيسية لنظام الاتصالات القائم على الشبكات، وهي: المطاريف، والبوابات، وحراس البوابات، ووحدات التحكم متعددة النقاط. ويمكن أن تتناول أيضاً عناصر ترادف أو تماس. وتبدو هذه العناصر في الشكل 6-1.



(أ) نظام H.323 ومكوناته [Packetizer]



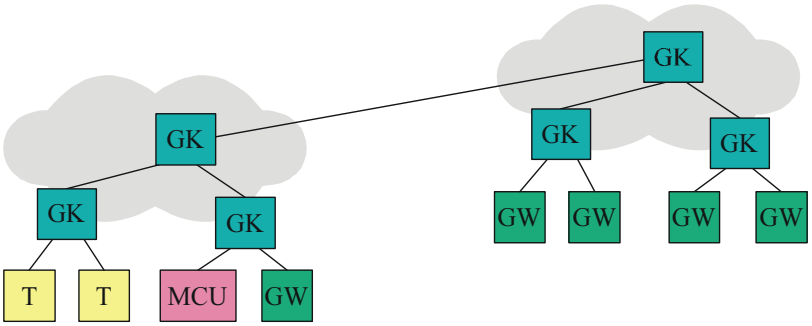
(ب) سيناريوهات التنفيذ H.323 [Euchner]

الشكل 6-1 – نظام التوصية H.323: مكونات وسيناريوهات التنفيذ

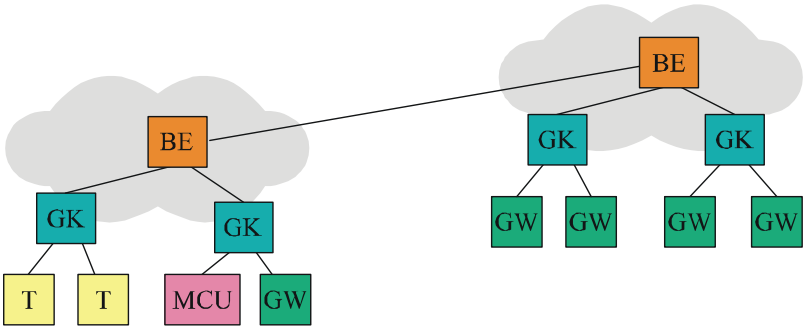
المطاريف هي نقاط طرفية يستخدمها الزبون على الشبكة الفقرية لبروتوكول الإنترنت الذي يوفر اتصالات ثنائية الاتجاه. ويجب أن تحمل المطاريف H.323 الاتصالات الصوتية ويمكنها أن تدعم أيضاً كودك الفيديو وبروتوكولات مؤتمرات البيانات T.120، ومقدرات وحدات التحكم متعددة النقاط. ومن أمثلة ذلك: الهواتف التي تستخدم بروتوكول الإنترنت والهواتف الفيديوية، وأجهزة النظام التفاعلي للاستجابة الصوتية (IVR)، وأنظمة البريد الصوتي و"برمجيات المهاتفة" (مثل NetMeeting™).

توفر *البوابة* خدمات كثيرة، أكثرها شيوعاً وظيفة ترجمة بين النقاط الطرفية H.323 وأنواع المطاريف الأخرى. وتشمل هذه الوظيفة الترجمة بين أنساق الإرسال (من H.225.0 إلى H.221 مثلاً) وبين إجراءات الاتصالات (من H.245 إلى H.242 مثلاً). وبالإضافة إلى ذلك، تترجم البوابة بين كودك الصوت والفيديو وتقوم بوظيفة إقامة النداء وتحريره على كل من جانب تبديل الرزم وجانب تبديل الدارة في الشبكة.

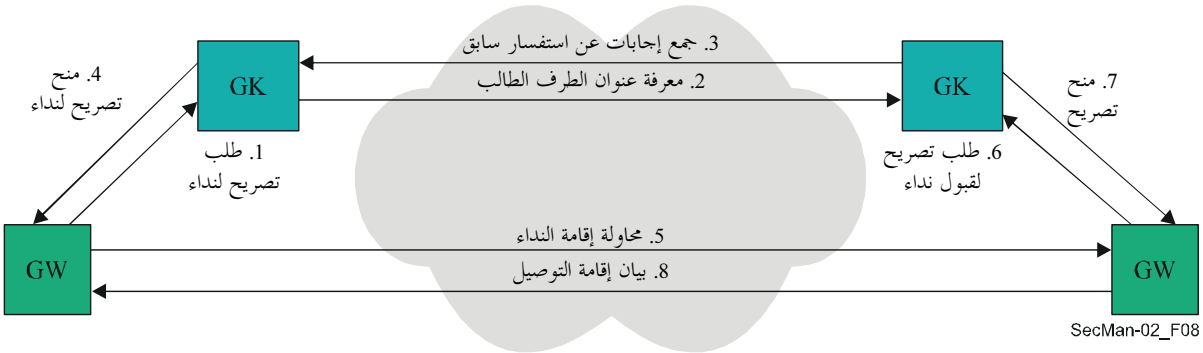
حارس البوابة مكون هام من مكونات أي شبكة تعمل بموجب H.323. وهو بمثابة نقطة مركزية لجميع النداءات داخل المنطقة التي يغطيها ويوفر للنقاط الطرفية المسجلة خدمات التحكم في النداءات. ويعمل حارس البوابة H.323 إلى حد كبير بمثابة بدالة تقديرية لأنه يتحكم في القبول ويستبين العنوان ويمكن أن يسمح بإقامة النداءات بين النقاط الطرفية المباشرة، أو يقوم ذاتياً بتسيير تشوير النداء لأداء وظائف من قبيل التتبع/العثور على الجهة المطلوبة، وتحويل النداء في حالة الانشغال، وما إلى ذلك. وتقترن بحراس البوابات *عناصر تماس* (أو ترادف) وهي مسؤولة عن تبادل معلومات العناوين وتشارك في ترخيص النداءات بين (أو داخل) الميادين الإدارية. وتمكّن هذه الوظيفة أيضاً من الاتصال ما بين مختلف "الجزر" أو الشبكات في ظل التوصية H.323. ويتم هذا من خلال تبادل سلسلة من الرسائل كما هو مبين في الشكل 6-2.



(أ) طوبولوجيا على أساس بروتوكول التسجيل والقبول والوضع الراهن (RAS)



(ب) طوبولوجيا على أساس الملحق زاي/H.225.0



(ج) تدفق نداء عالي المستوى

المختصرات: BE: عنصر تماس؛ GK: حارس بوابة؛ GW: بوابة؛ MCU: وحدة تحكم متعددة النقاط؛ T: مطراف

الشكل 6-2 – اتصالات بين ميادين إدارية

وحدة التحكم متعددة النقاط (MCU) تدعم المؤتمرات بين ثلاث نقاط طرفية أو أكثر. وفي إطار التوصية H.323 تتألف هذه الوحدة من جهاز تحكم لا بد منه ومن صفر أو أكثر من معالجات متعددة النقاط. ويدير جهاز التحكم متعدد النقاط تشوير النداء ولكنه لا يتعامل مباشرة مع أي من تدفقات الوسائط، فهذا متروك لمعالجات متعددة النقاط تخلط وتبدل وتعالج بتات صوتية و/أو فيديوية و/أو بيانات. وقد تتوفر مقدرات لوحدة التحكم متعددة النقاط ومعالجات متعددة النقاط في عنصر مخصص أو كجزء من المكونات الأخرى المشار إليها في التوصية H.323.

وتحمل الشبكات H.323 العاملة في الوقت الحاضر مليارات الدقائق من حركة الصوت والفيديو كل شهر؛ ويجري نقل معظم حركة نقل الصوت بواسطة بروتوكول الإنترنت (VoIP) اليوم طبقاً للتوصية H.323. وتشير التقديرات الحالية إلى أن VoIP يمثل أكثر من 10 في المائة من إجمالي دقائق المهاتفة الدولية طويلة المسافة. وكذلك ما فتئت تزداد الحركة الفيديوية بموجب التوصية H.323. والسبب الرئيسي لهذا النمو هو نضوج البروتوكول وأشكال تنفيذه، وأن التوصية H.323 أثبتت أنها تمثل حلاً قابلاً جداً للاتساع يلبي احتياجات مقدمي الخدمات والشركات على السواء، حيث تتراوح المنتجات في التوصية H.323 من أكداس ورقاقات إلى الهواتف اللاسلكية ومعدات المؤتمرات الفيديوية.

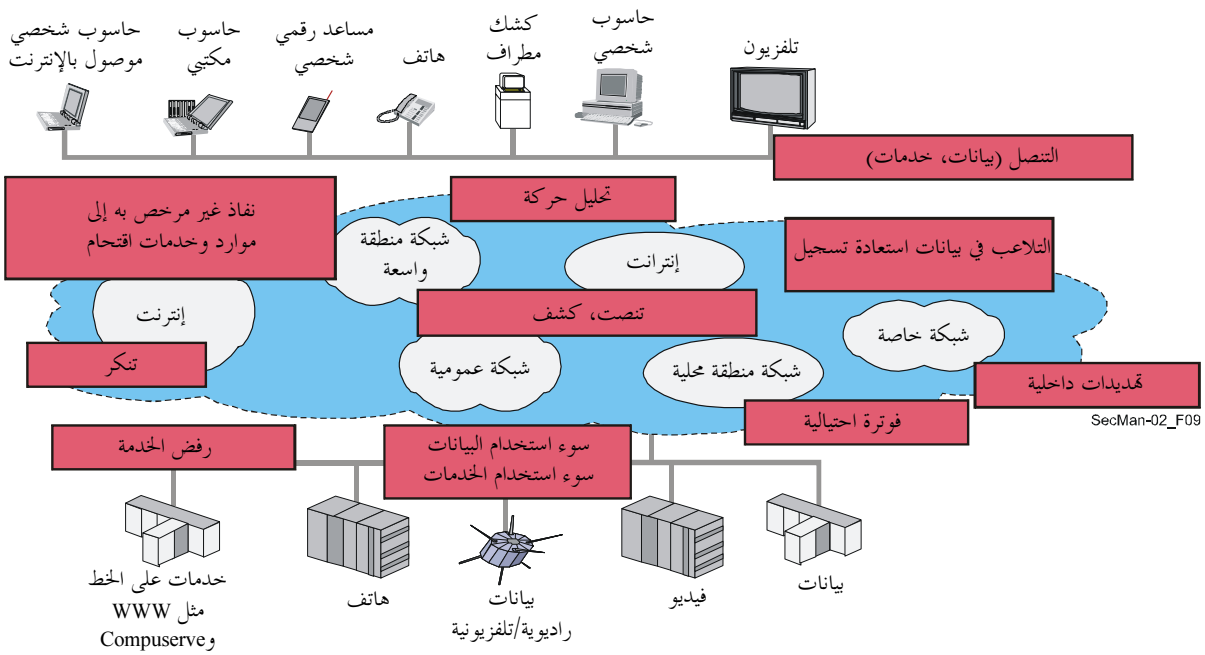
وفيما يلي قائمة بالوظائف التي توفرها الأنظمة المشار إليها في التوصية H.323:

- المقدرة على عقد مؤتمرات صوت وفيديو وبيانات؛
- الاتصال بين مختلف أنواع المطاريف، بما في ذلك من حاسوب شخصي إلى هاتف ومن فاكس إلى فاكس ومن هاتف إلى هاتف ونداءات عبر شبكة الويب؛
- تشغيل فاكس T.38 وإرسال النص والمودم بواسطة بروتوكول الإنترنت؛
- خدمات تكميلية كثيرة (إحالة النداء والرد نيابة عن الغير، وما إلى ذلك)؛
- قابلية تشغيل بيني قوية مع أنظمة أخرى في التوصية H.32x، بما في ذلك التوصية H.320 (الشبكات الرقمية متكاملة الخدمات) والتوصية H.323M (لا سلكي متنقل 3GPP)؛
- مواصفة لتجزئة بوابة وسائط (عبر بروتوكول التحكم في البوابة بموجب التوصية H.248)؛
- دعم التشوير وأمن الوسائط؛
- تنقلية المستعمل والمطراف ومطراف الخدمة؛
- دعم تشوير خدمات الطوارئ.

ومن أمثلة استخدام التوصية H.323 عبور بالجملة لوكالات التشغيل، ولا سيما عبر الشبكات الفقرية للمهاتفة بواسطة بروتوكول الإنترنت (مقارنة ببدالات من الفئة 4 لحركة الصوت) وخدمات بطاقات النداء. وفي اتصالات المؤسسات، تستخدم التوصية H.323 للبدالات الفرعية الخاصة بواسطة بروتوكول الإنترنت (IP-PBX) ونظام IP-Centrex – والشبكات الخاصة التقديرية (VPN) الصوتية والأنظمة المتكاملة للصوت والبيانات، وهواتف WiFi، وتنفيذ مراكز النداءات وخدمات التنقلية. وبالنسبة للاتصالات المهنية، تستخدم التوصية بشكل واسع في مجال المؤتمرات الصوتية (أو السمعية) والمؤتمرات الفيديوية، والتطبيقات التي تجمع بين الصوت/البيانات/الفيديو، وفي التعلم عن بُعد. وتشمل الاستعمالات في بيئة سكنية النفاذ السمعي البصري عريض النطاق، ومن حاسوب شخصي إلى هاتف، ومن هاتف إلى حاسوب، ومن حاسوب إلى حاسوب، ويمكن أن تستخدم أيضاً في تقديم الأخبار والمعلومات حسب الطلب.

1.1.6 قضايا الأمن في الوسائط المتعددة ونقل الصوت بواسطة بروتوكول الإنترنت

بما أن جميع عناصر النظام في التوصية H.323 يمكن أن تتوزع جغرافياً، وبحكم الطابع المفتوح لشبكات بروتوكول الإنترنت، ينشأ العديد من التهديدات للأمن، كما هو مبين في الشكل 6-3.



الشكل 6-3 – تهديدات الأمن في حالة الاتصالات متعددة الوسائط

والقضايا الرئيسية للأمن في الاتصالات متعددة الوسائط والمهاتفة بواسطة بروتوكول الإنترنت بصورة عامة مفصلة أدناه [Euchner]:

- الاستيقان من المستعمل والمطراف: يحتاج مقدمو خدمات نقل الصوت بواسطة بروتوكول الإنترنت إلى معرفة من يستخدم خدماتهم وذلك لأغراض المحاسبة وفوترة استخدام الخدمة. وكشرط أساسي للاستيقان ينبغي معرفة هوية المستعمل و/أو المطراف بأسلوب ما. ثم يتعين على المستعمل/المطراف أن يثبت صحة الهوية التي يدّعيها. ويحدث هذا عموماً من خلال إجراءات استيقان مجفرة (مثل كلمة سر محمية أو توقيعات رقمية طبقاً للتوصية X.509). وكذلك، قد يود المستعملون معرفة من يتهاتفون معهم.
- الاستيقان من المخدم: بما أن مستعملي نقل الصوت بواسطة بروتوكول الإنترنت يتصلون فيما بينهم من خلال بنية تحتية ما لنقل الصوت بواسطة بروتوكول الإنترنت تنطوي على مخدمات (حراس البوابات، وأجهزة تعدد البث، والبوابات)، يود المستعملون معرفة أنهم يتحدثون مع المخدم الصحيح و/أو مقدم الخدمة المقصود. ويشمل هذا الجانب مستعملي الخدمات الثابتة والمتنقلة.
- تهديدات أمن الاستيقان من المستعمل/المطراف والمخدم ، مثل التنكر والتدخل وخداع عناوين بروتوكول الإنترنت واختطاف التوصيل.
- الترخيص بالنداء هي عملية اتخاذ قرار لتقرير ما إذا كان المستعمل/المطراف مسموحاً له حقاً باستخدام موارد الخدمة (مثل النداء على الشبكات الهاتفية العمومية التبديلية) أو مصدر شبكة (نوعية الخدمة، وعرض النطاق، وأجهزة كودك، وما إلى ذلك). وغالباً ما تأتي وظائف الاستيقان والترخيص معاً لاتخاذ قرار التحكم في النفاذ. ويساعد الاستيقان والترخيص في إحباط الهجمات مثل التنكر وإساءة الاستخدام والغش والتلاعب ورفض الخدمة.
- تتناول حماية أمن التشوير حماية بروتوكولات التشوير من التلاعب وإساءة الاستخدام كما تتناول السرية والخصوصية. وتكون حماية بروتوكولات التشوير عموماً باستخدام وسائل التجفير فضلاً عن ضمان سلامة البيانات وحمايتها من استعادة التسجيل. وينبغي إيلاء عناية خاصة لتلبية متطلبات الأداء الحرج لإجراء الاتصالات في الوقت الفعلي بأقل الإجراءات وأقصر الطرق لتجنب الإطالة في إقامة النداء أو تدهور نوعية الصوت نتيجة التأخر في نقل الرزم أو ارتعاش الصوت نتيجة لتطبيق إجراءات الأمن.

- تتحقق سرية الصوت من خلال تجفير رزم الصوت، أي الحمولة النافعة لبروتوكول الوقت الفعلي (RTP) والحيلولة دون تنصت البيانات الصوتية. وبصورة عامة، يجري كذلك تجفير رزم الوسائط (مثل الفيديو) لتطبيقات الوسائط المتعددة. كذلك تشمل الحماية المتطورة لرزم الوسائط حماية الاستيقان وضمان سلامة بيانات الحمولة النافعة.
- لا تقتصر إدارة المفاتيح على جميع المهام الضرورية لتوزيع مواد المفاتيح بشكل آمن بين الأطراف على المستعملين والمخدمات فحسب، بل تشمل أيضاً مهام مثل تحديث المفاتيح التي انتهت صلاحيتها أو المفاتيح المفقودة. وقد تكون إدارة المفاتيح مهمة منفصلة عن تطبيق نقل الصوت بواسطة بروتوكول الإنترنت (توفير كلمة سر) أو قد تكون متكاملة مع التشوير عندما يتم التفاوض الدينامي بشأن أشكال الأمن التي تتوافر لها المقدرات اللازمة، ويتعين توزيع المفاتيح على أساس الجلسة.
- يتعامل الأمن فيما بين الميادين مع مشكلة أن الأنظمة في بيئات غير متجانسة تنفذ خصائص مختلفة للأمن بحكم اختلاف الاحتياجات وسياسات الأمن ومقدراته. وعليه تدعو الحاجة إلى التفاوض دينامياً بشأن مواصفات الأمن ومقدراته مثل الخوارزميات المجفرة ومعلماتها. ويتسم الأمر بأهمية خاصة عند عبور حدود بين الميادين واختلاف مقدمي الخدمات والشبكات. ومن المتطلبات الهامة لأمن الاتصالات بين الميادين إمكانية عبور الجدران الواقية بسهولة والتغلب على القيود التي تفرضها أجهزة ترجمة العناوين في الشبكة (NAT).

وهذه القائمة ليست شاملة ولكنها أساسية لمتطلبات الأمن بموجب التوصية H.323. ولكن قد يواجه المرء في مجال التطبيق قضايا أخرى متعلقة بالأمن تعتبر خارج نطاق التوصية H.323 (ومنها مثلاً سياسة الأمن أو أمن إدارة الشبكات أو توفير الأمن أو أمن التنفيذ أو أمن التشغيل أو التعامل مع حادث في مجال الأمن).

2.1.6 لمحة عن توصيات السلسلة الفرعية H.235.x

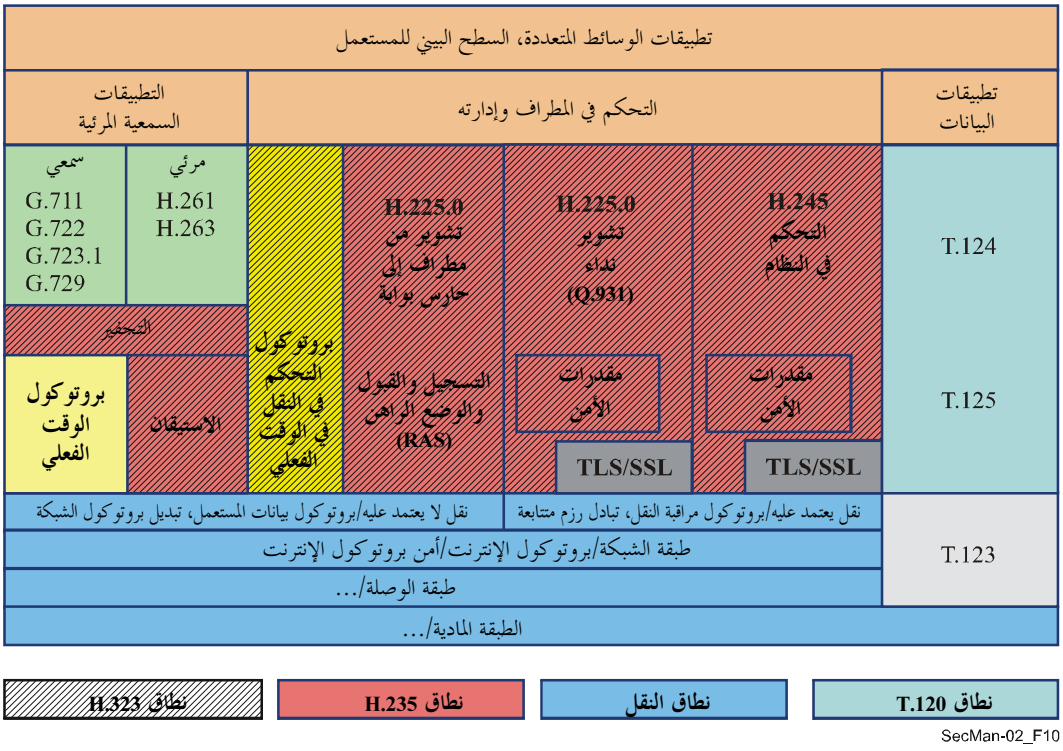
في نظام وسائط متعددة H.323، تحدد التوصية ITU-T H.235.0 إطار الأمن بما في ذلك مواصفة آليات الأمن وبروتوكولات الأمن من أجل H.323. وقدمت H.235 أنظمة الصيغة 2 من H.323 لأول مرة في عام 1998. ومنذ ذلك الحين تطورت H.235 من خلال تجميع آليات الأمن المعروضة وإضافة خوارزميات أمن أكثر تطوراً (مثل معيار التجفير المتطور (AES) على درجة عالية من الأمن والسرعة) وبوضع مواصفات مفيدة تتسم بالكفاءة لبعض حالات الاستخدام والبيئات. والصيغة 4 للسلسلة H.235.0-H.235.9 هي السلسلة الراهنة لتوصيات الأمن الصادرة عن قطاع تقييس الاتصالات للأنظمة القائمة على أساس H.323 التي توفر أمناً قابلاً للاتساع لمجموعات صغيرة من المؤسسات والشركات الناقلة التي تعمل على نطاق واسع.

خضعت الصيغة 3 السابقة للتوصية ITU-T H.235 لإعادة هيكلة شاملة لجميع أجزائها وملحقاتها بحيث أصبحت مجموعة كاملة من سلسلة H.235.x قائمة بذاتها من التوصيات حيث تشمل ITU-T H.235.0 "إطار الأمن لأنظمة تعدد الوسائط للسلسلة H (H.323 وأخرى قائمة على أساس H.245)". وتوفر هذه التوصية لمحة شاملة للسلسلة الفرعية H.235.x وتضم إجراءات مشتركة مع النص الأساس.

وباختصار فإن توصيات السلسلة ITU-T H.235.x توفر حماية مجفرة لبروتوكولات التحكم (H.225.0 التسجيل والقبول والوضع الراهن وتشوير النداء وH.245) وكذلك حماية مجفرة لبيانات تدفق وسائط سمعية/فيديوية. وخلال المراحل المختلفة لتشوير H.323، توفر التوصية H.235 وسائل للتفاوض بشأن خدمات مجفرة مرغوبة ومطلوبة وخوارزميات تجفير ومقدرات أمن. ووظائف إدارة المفاتيح لاستحداث مفاتيح جلسات دينامية مدمجة تماماً ضمن إجراءات التشوير مما يساعد على خفض فترة الانتظار في إقامة النداء. وإدارة مفاتيح H.235 تدعم الاتصالات "الكلاسيكية" من نقطة إلى نقطة، كما تدعم التشكيلات متعددة النقاط مع أجهزة البث المتعدد عندما تتصل عدة مطاريف متعددة الوسائط داخل مجموعة.

وتستخدم التوصية H.235 تقنيات أمن خاصة مثلى كتجفير منحني إهليلجي ومعيار التجفير المتطور لتلبية قيود الأداء الصارمة. ويكون التجفير الصوتي في طبقة التطبيقات حيث يتم تجفير أحمال نافعة لبروتوكول الوقت الفعلي. وهذا يسمح بتنفيذ مفيد باستخدام حيز صغير في النقاط الطرفية من خلال التفاعل المحكم مع معالج الإشارة الرقمية (DSP) وجهاز تفكيك انضغاط الصوت دون ضرورة الاعتماد على منصة نظام تشغيل محدد. ويمكن استخدام أدوات الأمن القائمة إذا كانت متاحة ومناسبة، مثل رزم ومعايير أمن الإنترنت المتاحة (أمن بروتوكول الإنترنت (IPSec) وطبقة مقبس آمن (SSL)/أمن طبقة نقل (TLS)) أو إعادة استخدامها في سياق التوصية H.235.

ويبين الشكل 6-4 نطاق التوصية H.235 التي تحتوي على أحكام لإقامة نداءات (فدرات H.225.0 وH.245) واتصالات في اتجاهين (تجفير أحمال نافعة لبروتوكول الوقت الفعلي (RTP) الذي يحتوي على صوت و/أو فيديو منضغط). وتشمل العناصر الوظيفية آليات الاستيقان وسلامة البيانات والخصوصية وعدم التنصل. وحراس البوابات مسؤولون عن الاستيقان عن طريق التحكم في القبول في النقاط الطرفية وعن توفير آليات عدم التنصل. أما الأمن على طبقة النقل والطبقات السفلية، على أساس بروتوكول الإنترنت، فيعد خارج نطاق أي من التوصيتين H.323 وH.235 ولكنه ينفذ عادة باستخدام أمن بروتوكول الإنترنت (IPSec) لفريق مهام هندسة الإنترنت (IETF) وبروتوكولات أمن طبقة النقل (TLS). وبصورة عامة، يمكن استخدام أمن بروتوكول الإنترنت (IPSec) أو أمن طبقة النقل (TLS) لتوفير الاستيقان أو، اختيارياً، لتوفير السرية (أي التجفير) عند طبقة بروتوكول الإنترنت الشفافة لأي (تطبيق) بروتوكول يجري فوقها. ولا حاجة إلى تحديث بروتوكول التطبيق للسماح بذلك وإنما يكفي تطبيق سياسة الأمن عند كل طرف.



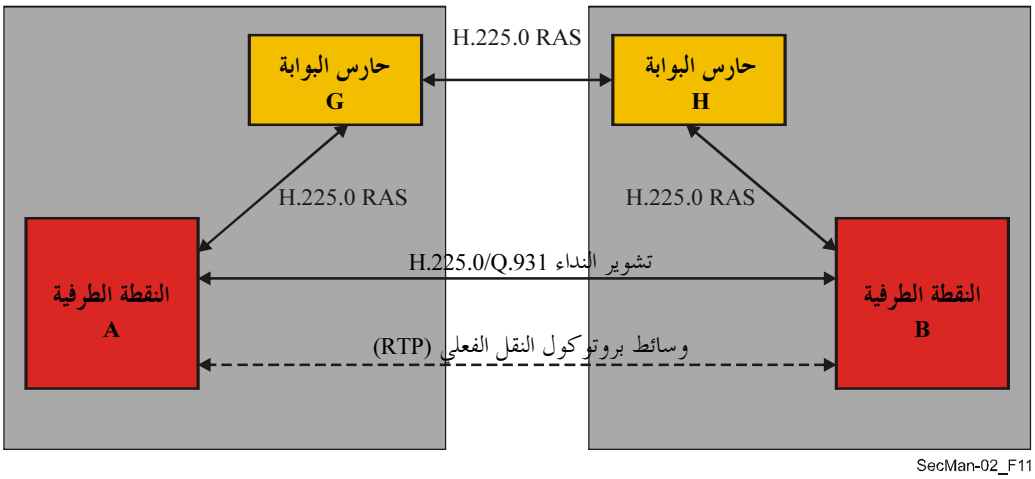
الشكل 6-4 – الأمن في التوصية H.323 كما يرد في التوصية H.235 [Euchner]

وتشمل سلسلة التوصيات ITU-T H.235.x طائفة واسعة من تدابير الأمن التي تتناول بيئات مستهدفة مختلفة كما في داخل المؤسسات/وفيما بينها وفي الشركات الناقلة. واستناداً إلى الافتراضات الخاصة بتوافر البنية التحتية للأمن وتوافر المقدرات الطرفية والمنصات، من نقاط طرفية بسيطة أو نقاط طرفية ذكية، تقدم التوصية H.235.x طائفة من مواصفات الأمن المتكيفة الخاصة بكل سيناريو والقابلة للتشغيل البيني. وتوفر مواصفات الأمن المتاحة تقنيات للأمن تتراوح من التقنيات البسيطة السرية المشتركة التي تنطوي على كلمة سر محمية (H.235.1 للاستيقان وسلامة الرسائل لتشوير H.225.0) إلى مواصفات متطورة تعمل بتوقيعات رقمية وشهادات البنى التحتية للمفاتيح العمومية بموجب X.509 (H.235.2). وهذه التقنيات تسمح إما بالحماية قفزة قفزة باستخدام تقنيات بسيطة ولكنها أقل قابلية للاتساع أو بالحماية من طرف إلى طرف باستخدام التقنيات القابلة للاتساع للبنى التحتية للمفاتيح العمومية. وتدعى H.235.3 مواصفة الأمن الهجينة إذ إن هذه التوصية تجمع ما بين إجراءات الأمن التناظرية من H.235.1 وباستعمال الشهادات والتواقيع القائمة على البنى التحتية للمفاتيح العمومية من H.235.2 تحقق أداء أمثل وزمن إقامة نداء أقصر. كما توفر H.235.3 إمكانية خيار تنفيذ عمليات كثيفة الحوسبة في كيان معالج آمن وظيفي يقوم على أساس التفويض.

وتتناول H.235.4 "أمن النداء المسيّر مباشرة وانتقائياً" بتخفيف الاعتماد الصارم على معمارية مركزها مخدم يسيّرها حارس بوابة وهي توفر تدابير أمن ترمي إلى تأمين نموذج الند إلى الند. وتعرّف هذه التوصية إجراءات لإدارة المفاتيح في بيئة مؤسسة أو في بيئة ما بين الميادين. وعلى وجه الخصوص، تشمل H.235.4 سيناريوهات معينة حيث يعمل حارس

البوابة بأسلوب تسيير مباشر أو حيث قد يقتصر حارس البوابة على القيام انتقائياً بتنفيذ تسيير بعض حركة تشوير النداء بموجب H.225.0.

ولئن كان العديد من مواصفات أمن H.235 يفترض نموذج تسيير حارس البوابة بموجب H.323 فإن H.235.4 تنـــزع أكثر نحو اتصالات آمنة من الند إلى الند بغية إعفاء حراس البوابات المعنيين من تسيير مهام تشوير H.323 وتوفير قدر أفضل من إمكانية الاتساع ومن الأداء بصفة عامة. وفي إطار H.235.4، في مجال تناول النداءات المسيّرة مباشرة، يعمل حراس البوابات في غالب الأحوال محلياً ضمن ميدانهم للقيام بعمليات الاستيقان من المستعمل/المطراف والتسجيل والقبول ومعرفة العناوين والتحكم في عرض النطاق. ومن جهة أخرى تقيم المطاريف نداءات H.323 مباشرة بين النقاط الطرفية بأسلوب من طرف إلى طرف، كما هو مبيّن في سيناريو الشكل 6-5.



الشكل 6-5 – سيناريو التسيير المباشر في إطار H.235.4

عندما تطلب النقطة الطرفية A من حارس البوابة G قبول النداء من أجل الاتصال بالنقطة B يقوم حارس البوابة (إما G في بيئة شركة أو H في بيئة بين الميادين) بتوليد مفتاح تشوير النداء من طرف إلى طرف لكلتا النقطتين A وB. وعلى غرار مماثل جداً لما يحدث في بروتوكول Kerberos (انظر تطبيقاً له في التوصية ITU-T J.191) تحصل النقطة A بشكل آمن على المفتاح المولّد ضمن علامة أمن واحدة كما تحصل في الوقت ذاته على علامة أمن أخرى تحتوي على نفس المفتاح من أجل النقطة B. ولدى إقامة النداء، تستعمل النقطة A، من جهة أولى، مباشرة المفتاح لتحمي تشوير النداء نحو النقطة B ولكنها، من جهة أخرى، ترسل علامة الأمن الأخرى مع المفتاح إلى النقطة B. وبإمكان H.235.4 أن تستعمل أياً من مواصفات أمن H.235.1 أو H.235.3 في إطار H.235.

ومن شأن مزيد من الدعم الإجرائي لسيناريوهات ما بين الميادين في إطار H.235.4 أن يمكّن من التمييز بين الحالات حيث لا تدعم النقاط الطرفية أو حراس البوابات المقدرة لتنفيذ اتفاق مفتاح ديفي–هيلمان، ومع ذلك فإن صافي النتيجة في نهاية المطاف هو حصول النقطتين A وB على سر جلسة مشترك يحمي من طرف إلى طرف التشوير H.323 من حيث الاستيقان أو السلامة أو السرية.

وسعياً إلى تعزيز أمن الأنظمة التي تستعمل أرقام تعرّف الهوية الشخصية (PINs) أو كلمات السر للاستيقان من المستعملين فإن H.235.5 توفر إطاراً آخر هو "*إطار لتأمين الاستيقان في عملية التسجيل والقبول والوضع الراهن RAS باستخدام أسرار متقاسمة ضعيفة*" وذلك باستخدام طرائق المفاتيح العمومية لتأمين استعمال الأرقام PIN أو كلمات السر. وثمة مواصفة معينة تحدد حالياً وهي تستغل طريقة تبادل المفاتيح المجفرة للتفاوض على سر متقاسم قوي يكون محمياً من أي هجمات منفعلة أو فاعلة (من جهة وسيطة). ويمكّن هذا الإطار من تعريف مواصفات جديدة باستعمال طرائق تفاوض أخرى على أساس المفاتيح العمومية.

وتضم التوصية ITU-T H.235.6 "*مواصفة تجفير الصوت على أساس إدارة المفتاح الأصلي H.245/H.235*" كل الإجراءات اللازمة لتجفير تدفق وسائط في بروتوكول الوقت الفعلي (RTP) بما في ذلك إدارة المفاتيح المحيطة المعبّر عنها كلياً ضمن حقول تشوير H.245.

وحرصاً على تقارب أفضل مع بروتوكول استهلال الجلسة (SIP) ومع بروتوكول النقل الآمن في الوقت الفعلي (SRTP) تعمد التوصية ITU-T 235.7 "*استخدام بروتوكول إدارة مفاتيح MIKEY من أجل بروتوكول النقل الآمن في الوقت الفعلي (SRTP) ضمن H.235*" إلى استعمال بروتوكول النقل (RFC 3711، SRTP) ضمن H.235. وتحدد هذه التوصية كيفية استعمال إدارة مفاتيح IETF MIKEY ضمن H.235.7 من أجل توزيع مفاتيح الوسائط من طرف إلى طرف باستعمال البروتوكول SRTP.

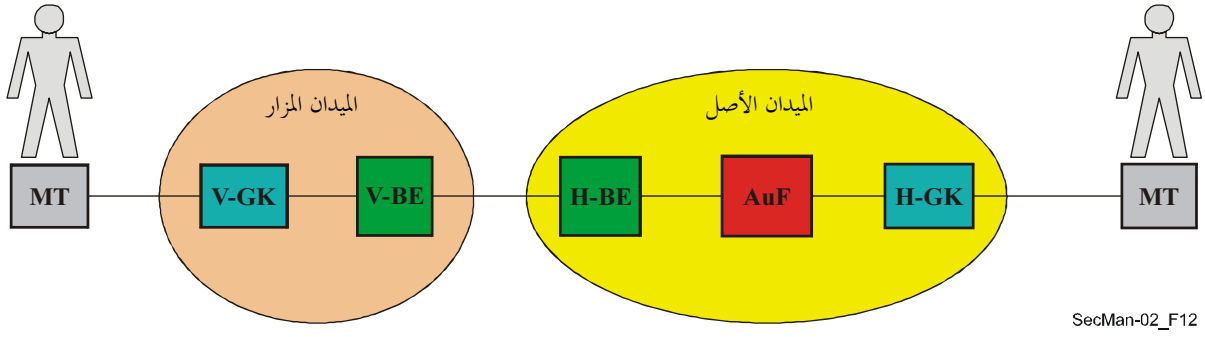
وثمة نهج تكميلي آخر وارد ضمن H.235.8 "*تبادل المفاتيح من أجل البروتوكول SRTP باستعمال قنوات التشوير*" حيث الغرض هو تشوير معلمات مفاتيح البروتوكول SRTP في الجزء الواضح من طرف إلى طرف بافتراض توفر نقل آمن في الجانب الأسفل، وهو مماثل للنهج المتبع في أوصاف بروتوكول وصف الجلسة (SDP) لدى فريق مهام هندسة الإنترنت (IETF). ويمكن تحقيق مثل قنوات نقل التشوير الآمن هذه باستخدام إما بروتوكول أمن الإنترنت (IPSec) أو بروتوكول أمن طبقة النقل (TLS) أو تركيب الرسائل المجفرة (CMS).

وكان ثمة عقبة هامة لوقت طويل في الواقع العملي وهي جعل التشوير H.323 يجتاز مرحلة ترجمة العناوين في الشبكة (NAT) ويجتاز مختلف جدران الوقاية (Firewalls). وتضم التوصية ITU-T H.235.9 "*دعم بوابات الأمن من أجل H.323*" إجراءات الأمن التي تمكّن أي نقطة طرفية/مطراف H.323 من اكتشاف بوابات الأمن H.323 حيث يفهم أن كياناً كهذا يشمل وظيفة بوابة طبقة تطبيقات (ALG) في إطار ترجمة عناوين شبكة/جدار وقاية (NAT/FW) ضمن H.323. وتتحرى بوابة التشوير H.323 المفترض الوثوق بها معاملات التشوير الجارية وتصبح ضالعة في إدارة المفاتيح من أجل التشوير H.225.0.

وبينما تتناول التوصية H.235.0 بالدرجة الأولى البيئات "الساكنة" H.323 مع أحكام تتناول قدراً محدوداً من التنقلية، فقد برزت الحاجة إلى توفير تنقلية آمنة للمستعملين والمطاريف في بيئات H.323 الموزعة تتجاوز حدود التوصيل فيما بين الميادين ومنطقة التنقلية المحدودة لحارس البوابة. وتشمل التوصية ITU-T H.530 حاجات الأمن من خلال تناوب جوانب أمن مثل:

- الاستيقان من مطراف/مستعمل متنقل والترخيص له في الميادين الأجنبية التي يزورها؛
- الاستيقان من الميدان موضع الزيارة؛
- تأمين إدارة المفتاح؛
- حماية بيانات التشوير بين مطراف متنقل وميدان موضع الزيارة.

يبيّن الشكل 6-6 السيناريو الأساسي الذي تتناوله H.530 حيث يمكن لمطراف متنقل (MT) في إطار H.323 إما أن يرتبط مباشرة بميدانه الأصل عبر حارس البوابة الأصل (H-GK) أو أن يرتبط بأي حارس بوابة أجنبي (V-GK) في الميدان الذي يزوره. وبما أن المطراف المتنقل وكذلك المستعمل غير معروفين في الميدان المزار فإن حارس البوابة المزارة عليه أولاً أن يستفسر لدى وظيفة الاستيقان (AuF) في الميدان الأصل حيث يكون المطراف المتنقل مشتركاً ومعروفاً. وهكذا فإن الميدان المزار يفوض مهمة الاستيقان إلى وظيفة الاستيقان في الميدان الأصل ويدعها تقوم بالاستيقان وتقرر في مسألة الترخيص. وإضافة إلى ذلك تزود وظيفة الاستيقان حارس البوابة المزارة برابط مجفر للمطراف المتنقل والمفتاح الدينامي لدى حارس البوابة المزارة وذلك باستخدام بروتوكول أمن تجفيري مندمج في إطار H.530. وتستجيب وظيفة الاستيقان على نحو آمن ببيان قرارها لحارس البوابة المزارة وهذا يحدث أثناء مرحلة تسجيل المطراف.



الشكل 6-6 – سيناريو H.530

يجري الاتصال بين الميدان المزار والميدان الأصل باستخدام بروتوكول H.501 النوعي من أجل إدارة التنقلية القائمة على أساس H.323 وكذلك الاتصال داخل الميدان وما بين الميادين. ولدى تلقي قرار الاستيقان والترخيص من الوظيفة AuF يتفق حارس البوابة المزارة والمطراف المتنقل على مفتاح وصلة دينامية جديد يتقاسمانه كلاهما أثناء ارتباطهما أمنياً. ويستعمل مفتاح الوصلة هذا لحماية أي اتصال تشوير H.323 إضافي بين المطراف المتنقل وحارس البوابة المزارة، ويحدث اتصال التشوير متعدد الوسائط محلياً في الميدان المزار ولا يتطلب أي تفاعل مع الميدان الأصل.

وتأخذ H.530 في الحسبان معمارية أمن مبسطة جداً حيث لا يتقاسم المطراف المتنقل سوى سراً متقاسماً مسبق التشكيل (كلمة سر اشتراك مثلاً) مع الوظيفة AuF التي ينتمي إليها في الميدان الأصل ولكنها لا تشترط على المطراف المتنقل أن يتقاسم أي روابط أمن مسبقة مع أي من الميادين المزارة. ولا تتطلب حماية الأمن بين الكيانات سواء داخل أي ميدان أو عبر الميادين سوى الأسرار المتقاسمة تناظرياً، مثلما يحدث مثلاً من خلال اتفاقات سوية الخدمة بين الميادين. وتقوم H.530 بإعادة استعمال مواصفات أمن H.235 قائمة، مثل H.235.1، لتأمين رسائل التشوير H.530/H.501 عبر الميادين.

وبالإضافة إلى أن التوصيات H.235.0 وH.350 و H.350.2 تمكّن الإدارة المتواسعة للمفاتيح باستخدام بروتوكول النفاذ السريع إلى الدليل (LDAP) وطبقة المقبس الآمن (SSL/TLS) فإن التوصية ITU-T H.350.x توفر مقدرات عديدة مهمة تمكّن المؤسسات وشركات الاتصالات من إدارة آمنة لأعداد كبيرة من مستعملي الخدمات الفيديوية وخدمات نقل الصوت بواسطة بروتوكول الإنترنت. وتوفر H.350 وسيلة لتوصيل H.323 وبروتوكول استهلال الجلسة (SIP) وH.320 وخدمات المراسلة المعتادة بخدمة دليل بحيث يمكن تطبيق الممارسات الحديثة لإدارة الهوية على الاتصالات متعددة الوسائط. وفضلاً عن ذلك، توفر المعمارية مكاناً معيارياً لتخزين شهادات الأمن لهذه البروتوكولات.

ولا تغير التوصية H.350 معماريات الأمن في أي بروتوكول بعينه. ومع ذلك، فإنها توفر مكاناً معيارياً لتخزين شهادات الاستيقان حسب مقتضى الحال. وينبغي ملاحظة أن كلاً من التوصية H.323 وبروتوكول استهلال الجلسة يتقبل الاستيقان من السر المتقاسم (H.235.1 وخلاصة بروتوكول HTTP، على التوالي). وتتطلب هذه المناهج أن يكون لمخدم النداء الحق في النفاذ إلى كلمة السر. وبالتالي، إذا تعرض مخدم النداء أو دليل H.350 لأي خلل فقد تتعرض كلمات السر أيضاً للعبث. وقد تكون مواطن الضعف هذه نتيجة لمواطن ضعف في الأنظمة (دليل H.350 أو مخدّمات النداء) وتشغيلها بدلاً من أن تُعزى إلى H.350 في حد ذاتها.

ويُستحسن جداً أن تعمد مخدمات النداء ودليل H.350 إلى الاستيقان المتبادل قبل تقاسم المعلومات. وفضلاً عن ذلك، من المستحسن جداً إقامة الاتصالات بين أدلة H.350 ومخدمات النداء أو النقاط الطرفية عبر قنوات اتصالات آمنة مثل طبقة مقبس الأمن (SSL) أو أمن طبقة النقل (TLS).

وينبغي ملاحظة أن قوائم التحكم في النفاذ إلى مخدمات بروتوكول النفاذ السريع إلى الدليل تندرج ضمن مسائل السياسات وليست جزءاً من المعيار. ومن المستصوب أن يستخدم مديرو الأنظمة الحصافة عند تحديد التحكم في النفاذ في نعوت H.350. إذ ينبغي مثلاً أن يقتصر النفاذ إلى نعوت كلمة السر على المستعمل المستيقن منه، بينما يمكن أن تكون نعوت العناوين متاحة لأي كان.

3.1.6 H.323 وأجهزة ترجمة عناوين الشبكة (NAT) وجدران الوقاية (FW)

لقد صممت الإنترنت بحيث تراعي مبدأ "من طرف إلى طرف". أي أن بإمكان أي جهاز على الشبكة الاتصال مباشرة بأي جهاز آخر على الشبكة. ومع ذلك، وبحكم اعتبارات الأمن ونظراً إلى النقص في عناوين الشبكات في برمجية IPv4، فإن أجهزة جدران الوقاية وترجمة عنوان الشبكة كثيراً ما تُستخدم عند حدود الشبكات. وتشمل هذه الحدود ميدان الإقامة وميدان مقدم الخدمة وميدان المؤسسة، وأحياناً ميدان البلد. ويُستخدم أحياناً أكثر من جهاز جدار وقاية أو ترجمة عناوين شبكة ضمن ميدان مفرد.

وأجهزة جدران الوقاية مصممة بحيث تتحكم بشكل صارم في كيفية انتقال المعلومات عبر حدود الشبكات وهي مشكّلة عادة بحيث تمنع مرور معظم اتصالات بروتوكول الإنترنت. ولذلك، وما لم يشكّل جدار الوقاية صراحة لتمرير حركة H.323 الآتية من الأجهزة الخارجية وتمكينها من العبور لكي تصل إلى أجهزة H.323 الداخلية فإن الاتصال غير ممكن إطلاقاً. وهذا يطرح مشكلة لكل من يستعمل تجهيزات H.323.

وتقوم أجهزة NAT بترجمة العناوين المستخدمة في الميدان الداخلي إلى عناوين مستخدمة في الميدان الخارجي والعكس بالعكس. وتكون العناوين المستخدمة ضمن ميدان سكني أو ميدان مؤسسة مخصصة عموماً وليس دوماً، من مساحات عناوين شبكات خاصة محددة في المعيار RFC 1597. وهي كما يلي:

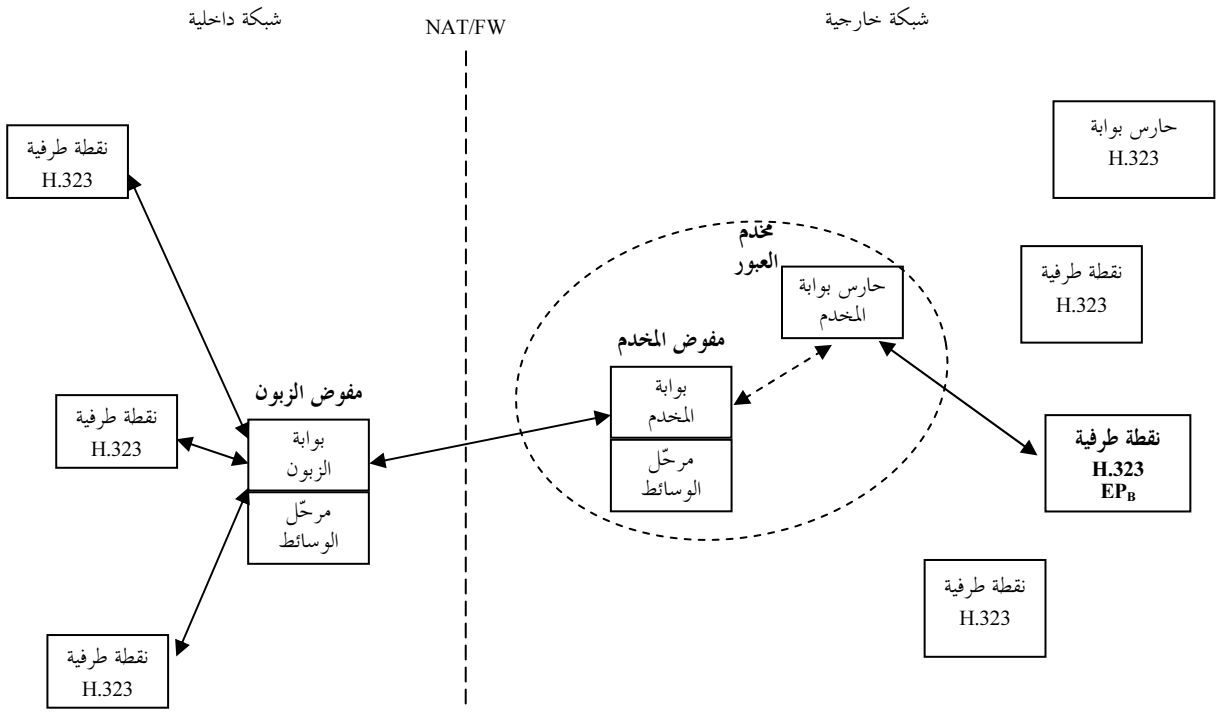
الصنف	مدى العنوان	عدد عناوين بروتوكول الإنترنت
A	10.0.0.0 – 10.255.255.255	16 777 215
B	172.16.0.0 – 172.31.255.255	1 048 575
C	192.168.0.0 – 192.168.255.255	65 535

وتنطوي أجهزة NAT على مشكلة عويصة لمعظم بروتوكولات الإنترنت، لا سيما تلك التي تحمل عناوين بروتوكول الإنترنت داخل البروتوكول. ولا بد لبروتوكولات H.323 وSIP وغيرها من بروتوكولات الاتصال في الوقت الفعلي التي تعمل عبر شبكات التبديل بالرزم من أن تقدم عنوان بروتوكول الإنترنت ومعلومات المنفذ لكي تعرف الأطراف الأخرى في الاتصال إلى أين ترسل تدفقات الوسائط (مثال ذلك التدفقات السمعية والمرئية).

وقد درس القطاع ITU-T مسائل عبور أجهزة NAT/FW ووضع سلسلة من ثلاث توصيات لأنظمة H.323 لتمكين هذه الأنظمة من عبور واحد أو أكثر من أجهزة NAT/FW بشكل انسيابي. وهذه التوصيات هي: H.460.17 ("*استعمال توصيل تشوير النداء H.225.0 كوسيلة نقل لرسائل التسجيل والقبول والوضع الراهن RAS في إطار H.323*") وH.460.18 ("*عبور تشوير H.323 من خلال أجهزة ترجمة عناوين الشبكة وجدران الوقاية*") وH.460.19 ("*عبور وسائط H.323 من خلال ترجمة عناوين الشبكة وجدران الوقاية*").

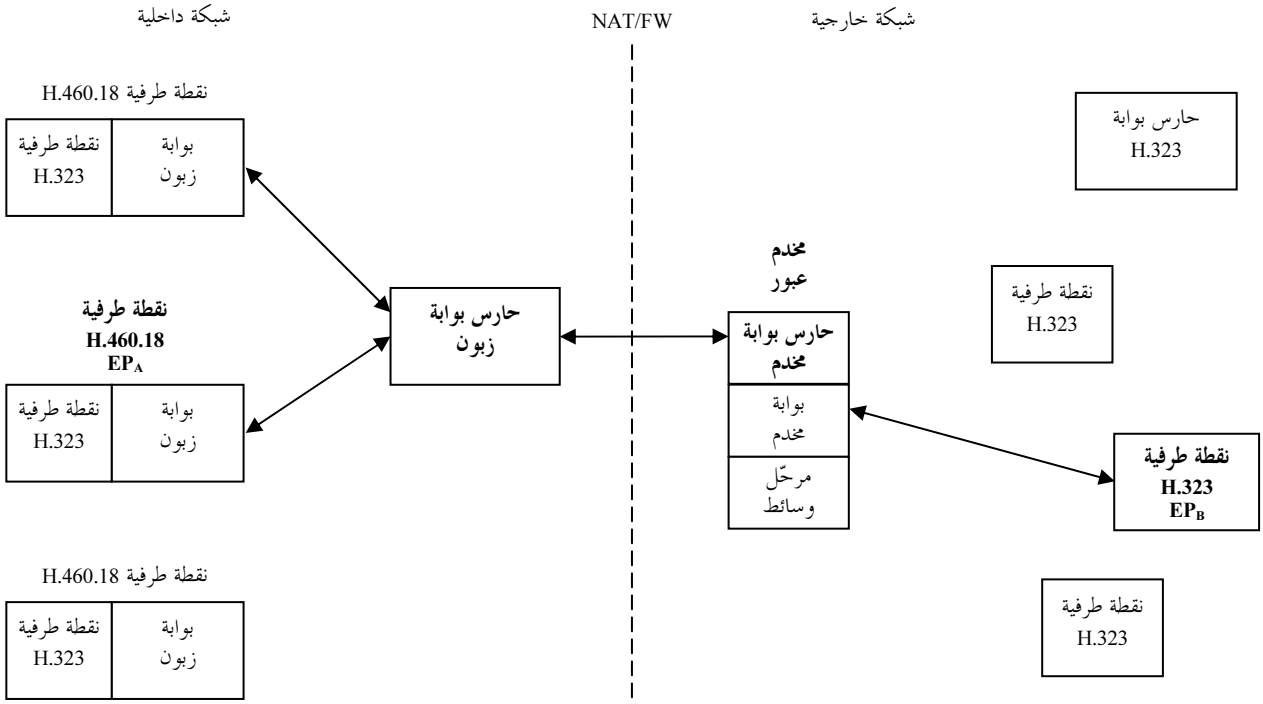
وجميع هذه التوصيات تستخدم إطار الامتدادية النوعي المدخل في الصيغة 4 من H.323، أي أن أي جهاز من سوية الصيغة 4 من H.323 فما فوق يمكن أن يتكيف للاضطلاع بإجراءات عبور NAT/FW هذه. وعلاوة على ذلك تنطوي H.460.18 على إجراءات من شأنها أن تمكّن الأجهزة الأقدم عهداً التي لا تمتثل لهذه التوصيات من أن تعبر حدود NAT/FW بمساعدة جهاز "مفوض".

ويصور الشكل 6-7 كيف يمكن استعمال جهاز "مفوض" خاص لمساعدة الأجهزة "الغافلة" عن NAT/FW على عبور حدود NAT/FW على نحو ملائم:



الشكل 6-7 – معمارية H.460.18، تنفيذ مفكك كلياً

وقد تكون الطوبولوجيا المصورة أعلاه مستصوبة أيضاً عندما ترغب مؤسسة مثلاً في التحكم في الطريق التي يمر فيها تشوير النداء وتدفقات الوسائط H.323 عبر الشبكة. غير أن H.460.17 وH.460.18 (اللتين تشملان جوانب التشوير في عبور NAT/FW) تمكنان النقاط الطرفية من عبور حدود NAT/FW دون المساعدة من أي أجهزة داخلية خاصة "مفوضة". ويصور الشكل 6-8 مثل هذه الطوبولوجيا:



الشكل 6-8 – معمارية الاتصال بين حراس البوابة

في الطوبولوجيا المصورة أعلاه القائمة على أساس H.460.18 تتصل النقاط الطرفية على الشبكة الداخلية مع حارس البوابة الذي يقيم أيضاً في الشبكة الداخلية لفك عنوان كيانات خارجية (رقم هاتف مثلاً أو معرف موارد موحّد H.323 URL لعنوان IP). ثم يتصل حارس البوابة في الشبكة الداخلية بحارس البوابة في الشبكة الخارجية لتبادل معلومات

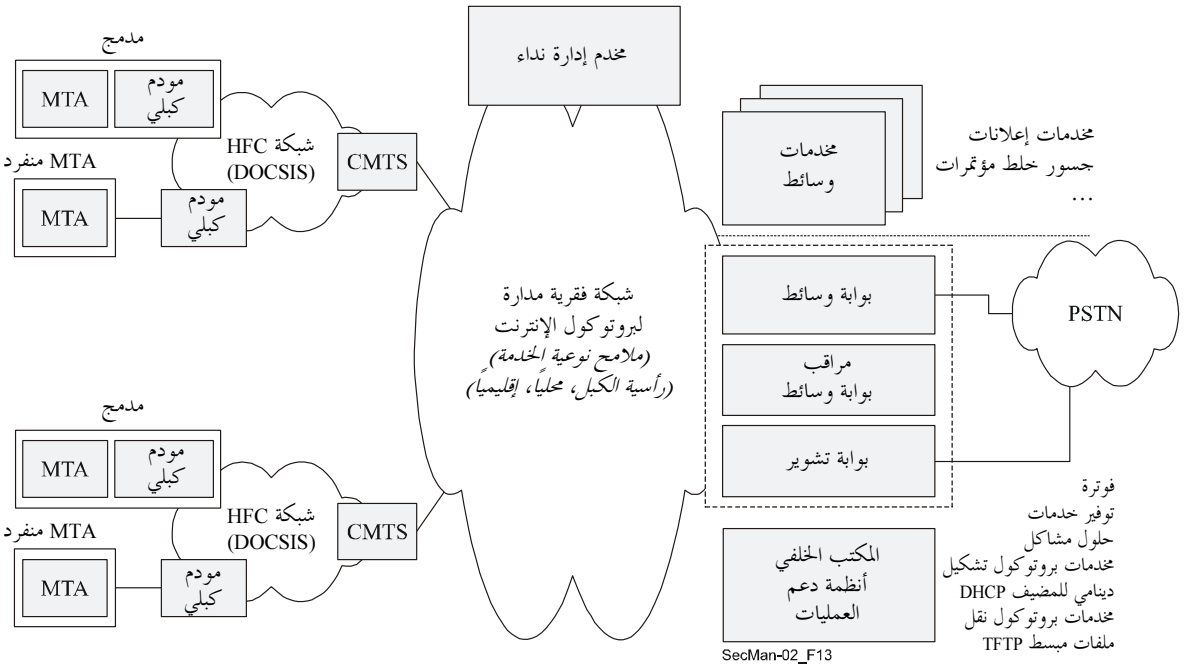
العناوين تلك وينقل تلك المعلومات إلى النقطة الطرفية صاحبة النداء. وعندما يباشر جهاز ضمن الشبكة الداخلية نداءً إلى جهاز في الشبكة الخارجية فإنه يستخدم الإجراءات المحددة في H.460.18 لكي يفتح ما يلزم من "ثقوب دبوس" عبر أجهزة NAT/FW للحصول على التشوير من الشبكة الداخلية إلى الشبكة الخارجية. وكذلك يستخدم الإجراءات المحددة في H.460.19 لكي يفتح ما يلزم من "ثقوب دبوس" لتمكين تدفقات الوسائط من العبور الملائم من الشبكة الداخلية إلى الشبكة الخارجية والعكس بالعكس.

وعندما تكون الأجهزة طالبة النداء والأجهزة المطلوبة واقعة في شبكتين خاصتين مختلفتين تفصل بينهما أجهزة NAT/FW وشبكة الإنترنت العمومية عندئذ يحتاج الأمر إلى ما لا يقل عن "بوابة مخدم" واحدة و"مرحل وسائط" واحد (محددين في H.460.18) وذلك لتسيير التشوير والوسائط على نحو ملائم بين الشبكتين الخاصتين. وكثيراً ما يشار إلى هذه التوليفة من الأجهزة باسم "مراقب حدود الجلسة". والسبب بكل بساطة أن ليس هنالك، بحكم التصميم، من وسيلة لأي رزمة IP ضمن شبكة خاصة أن تدخل شبكة خاصة أخرى دون مساعدة من كيان ما في الشبكة العمومية يضطلع بدور "المفوض" لتلك الرزمة.

وبطبيعة الحال فإن النداءات التي تنطلق وتنتهي ضمن نفس الشبكة الخاصة تعمل كما تعمل اليوم دون أي إجراءات خاصة لتناول النداء، أي أن H.460.17 وH.460.18 وH.460.19 لا تعرقل عملية التشغيل الملائمة لأجهزة H.323 ضمن نفس الشبكة الداخلية.

2.6 نظام الاتصالات الكبلية بواسطة بروتوكول الإنترنت (IPCablecom)

يُمكّن نظام IPCablecom مشغلي التلفزيون الكبلي من توفير خدمات في الوقت الفعلي تقوم على أساس بروتوكول الإنترنت (IP) (مثل الاتصالات الصوتية) عبر شبكاتهم المعزَّزة لدعم المودمات الكبلية. وتتضمن التوصية ITU-T J.160 تعريف معمارية نظام IPCablecom. وعلى سوية عالية جداً تتناول معمارية نظام IPCablecom ثلاث شبكات وهي: "شبكة النفاذ الهجينة من الألياف البصرية والكبلات متحدة المحور (HFC) طبقاً للتوصية J.112" و"شبكة بروتوكول الإنترنت المدارة" والشبكة الهاتفية العمومية التبديلية (PSTN). وتوفر عقدة النفاذ إمكانية التوصيل بين "شبكة النفاذ الهجينة من الألياف البصرية والكبلات متحدة المحور (HFC) طبقاً للتوصية J.112" و"شبكة بروتوكول الإنترنت المدارة". ويوفر كل من بوابة التشوير وبوابة الوسائط إمكانية التوصيل بين "شبكة بروتوكول الإنترنت المدارة" والشبكة الهاتفية العمومية التبديلية. ويوضح الشكل 6-9 المعمارية المرجعية لنظام الاتصالات IPCablecom.



الشكل 6-9 – معمارية مرجعية لنظام الاتصالات IPCablecom [J.165]

توفر شبكة النفاذ الهجينة (HFC) في إطار التوصية J.112 إمكانية نقل آمن يُعتمد عليه وبسرعة عالية بين مقر الزبون ورأسية الكبل. ويمكن أن توفر شبكة النفاذ هذه جميع مقدرات J.112 بما في ذلك نوعية الخدمة والسطوح البينية للطبقة المادية من خلال نظام انتهائية المودم الكبلي (CMTS).

وتقوم شبكة بروتوكول الإنترنت المدارة بعدة وظائف. أولاً، توفر التوصيل البيني للمكونات الوظيفية لنظام الاتصالات IPCablecom والمسؤولة عن التشوير والوسائط وتوفير الخدمة ونوعية الخدمة. وبالإضافة إلى ذلك، توفر شبكة بروتوكول الإنترنت المدارة توصيلية طويلة المسافة بين مختلف شبكات بروتوكول الإنترنت المدارة وشبكات النفاذ الهجينة (HFC) في إطار J.112. وتشمل شبكة بروتوكول الإنترنت المدارة المكونات الوظيفية التالية: مخدم إدارة النداء ومخدم الإعلان وبوابة التشوير وبوابة الوسائط ومراقب بوابة الوسائط وعدد من مخدمات المكتب الخلفي لأنظمة دعم العمليات.

يوفر *مخدم إدارة النداء* (CMS) مراقبة النداء وخدمات متعلقة بالتشوير من أجل مكيف مطراف الوسائط وعقدة النفاذ وبوابات الشبكة PSTN في شبكة الاتصالات IPCablecom. ومخدم إدارة النداء عنصر موثوق به من عناصر الشبكة ويكون في جزء بروتوكول الإنترنت المدار من شبكة IPCablecom. *ومخدمات الإعلان* هي مكونات منطقية في الشبكة تدير وترسل نغمات ورسائل معلومات استجابة لأحداث تقع في الشبكة. *وبوابة التشوير* ترسل وتستقبل تشوير شبكة تبديل الدارة عند حافة شبكة IPCablecom. وفي هذه الشبكة تقتصر وظيفة بوابة التشوير على تشوير غير مرتبط بأي مرفق في شكل تشوير النظام SS7 (أما التشوير المرتبط بمرفق ما في شكل نغمات متعددة التردد فتقوم به مباشرة وظيفة بوابة الوسائط). ويستقبل *مراقب بوابة الوسائط* (MGC) ويتواسط معلومات تشوير النداء بين شبكة IPCablecom وشبكة PSTN. كما يرصد ويراقب مجمل حالة النداءات التي تتطلب توصيلاً بينياً مع الشبكة PSTN. وتوفر *بوابة الوسائط* (MG) توصيلية الحمالة بين شبكة PSTN وشبكة IPCablecom. وتمثّل كل حمالة بنقطة طرفية، ويوعز المراقب إلى بوابة الوسائط بإقامة توصيلات الوسائط مع نقاط طرفية أخرى على شبكة IPCablecom والتحكم بها. كما يوعز إلى البوابة باكتشاف وتوليد أحداث وإشارات ذات صلة بحالة النداء المعروفة لمراقب بوابة الوسائط. ويحتوي *المكتب الخلفي لأنظمة دعم العمليات (OSS)* على مكونات أعمال وخدمة وإدارة شبكة تدعم العمليات الرئيسية. والمجالات الوظيفية الرئيسية لأنظمة دعم العمليات هي إدارة الأعطال وإدارة الأداء وإدارة الأمن وإدارة الحسابات وإدارة التشكيل. وتعرّف الشبكة IPCablecom مجموعة محدودة من المكونات الوظيفية والسطوح البينية لأنظمة دعم العمليات وذلك لتوفير الخدمة لمكيف مطراف الوسائط (MTA) وتنظيم رسائل الأحداث لحمل معلومات الفوترة.

1.2.6 مسائل الأمن في شبكة الاتصالات الكبلية بواسطة بروتوكول الإنترنت

يتعرض كل سطح بيني لبروتوكول شبكة الاتصالات الكبلية بواسطة بروتوكول الإنترنت IPCablecom لتهديدات قد تشكل مخاطر أمن لكل من المشترك ومقدم الخدمة على السواء. فقد يعبر مسير تدفق الوسائط مثلاً عدداً كبيراً غير معروف أصلاً من أسلاك مقدمي خدمات الإنترنت وخدمات الشبكات الفقرية. ونتيجة لذلك، قد يكون تدفق الوسائط معرضاً لتنصت مؤذ مما يؤدي إلى فقدان خصوصية الاتصالات.

2.2.6 آليات الأمن في شبكة الاتصالات الكبلية بواسطة بروتوكول الإنترنت

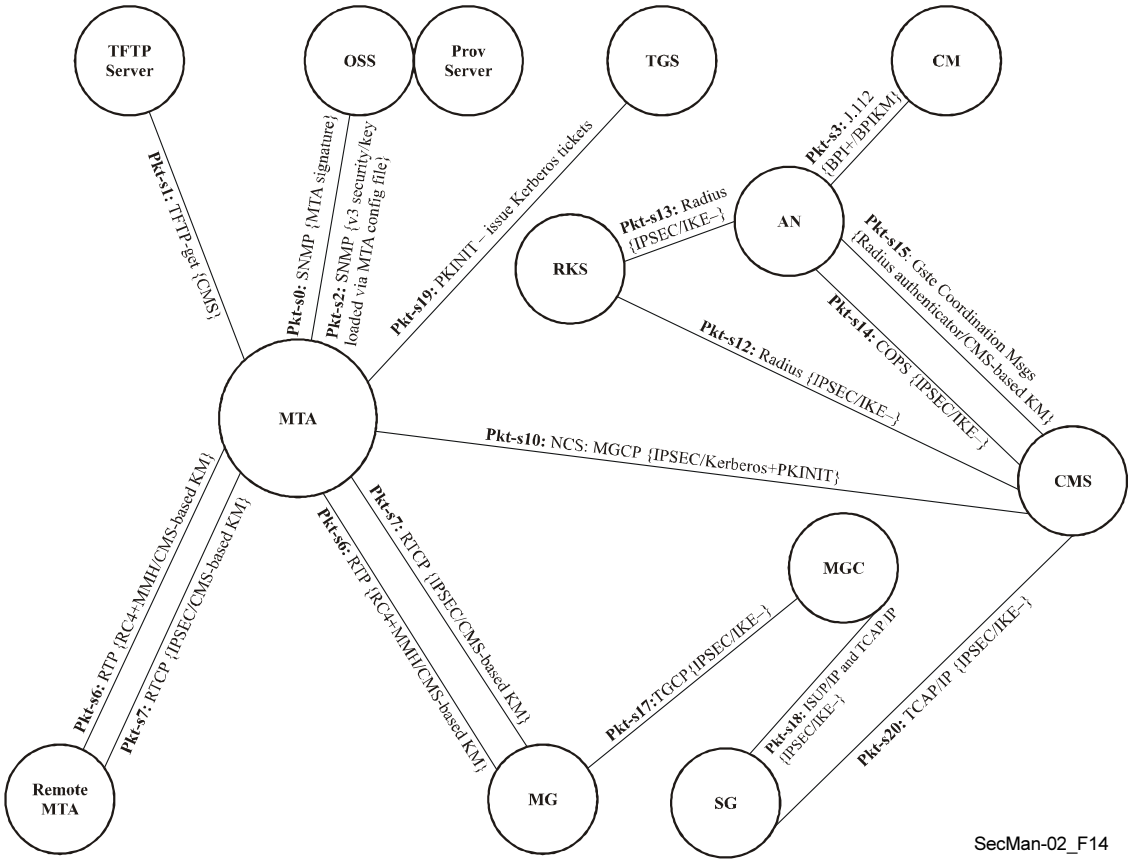
تتخذ تدابير الأمن في شبكة الاتصالات الكبلية بواسطة بروتوكول الإنترنت IPCablecom في عناصر الطبقة الأدنى ومن ثم فهي تستخدم غالباً الآليات التي عرّفها فريق مهام هندسة الإنترنت (IETF). وتتناول معمارية الاتصالات IPCablecom هذه التهديدات بأن تحدد، لكل سطح بيني لبروتوكول معيّن، آليات الأمن التي يقوم عليها (مثل أمن بروتوكول الإنترنت IPSec) التي تزود السطح البيني للبروتوكول بخدمات الأمن التي يتطلبها. وفي سياق معمارية التوصية X.805، يتناول مجمل خدمات الأمن بالنسبة إلى IPCablecom جميع الخلايا التسع الناتجة عن ثلاثة مستويات وطبقات مبينة في الشكل 2-1. مثال ذلك أن أمن بروتوكول الإنترنت IPSec يدعم خدمات بروتوكولات التشوير في مستوي التحكم. ويتحقق أمن البنية التحتية للإدارة باستخدام الصيغة 3 من بروتوكول إدارة الشبكة البسيطة (SNMP).

وتتكون خدمات الأمن المتاحة من خلال طبقة الخدمة الأساسية في IPCablecom هي الاستيقان والتحكم في النفاذ والسلامة والسرية وعدم التنصل. وقد لا يستخدم السطح البيني لبروتوكول IPcablecom أي خدمة أو يستخدم خدمة واحدة أو أكثر من هذه الخدمات للوفاء بمتطلبات الأمن الخاصة به.

ويلبي أمن الاتصالات IPCablecom المتطلبات الأمنية لكل سطح بيني من سطوح البروتوكولات في الشبكة بواسطة:

- تحديد نموذج التهديد الذي يتعرض له كل سطح بيني في كل بروتوكول؛
- تحديد خدمات الأمن (الاستيقان والترخيص والسرية والسلامة وعدم التنصل) المطلوبة للتعامل مع التهديدات المحددة؛
- تحديد آلية الأمن المعينة التي توفر خدمات الأمن المطلوبة.

وتشمل آليات الأمن كلاً من بروتوكول الأمن (مثل أمن بروتوكول الإنترنت (IPSec)، وأمن طبقة بروتوكول الوقت الفعلي (RTP)، وأمن بروتوكول إدارة الشبكة البسيطة (SNMP) v3 ودعم بروتوكول إدارة المفاتيح (مثل بدالة مفتاح الإنترنت (IKE) والاستيقان الأولي من تجفير المفاتيح العمومية /Kerberos) وكذلك تشمل خدمات الأمن الأساسية في الاتصالات IPCablecom آلية تجفير تدفقات الوسائط في بروتوكول الوقت الفعلي من طرف إلى طرف، ومن ثم تحول دون قدر كبير من تهديد الخصوصية. ويضم الشكل 6-10 موجزاً لجميع السطوح البينية لأمن الاتصالات IPCablecom. وإذا لم يكن بروتوكول إدارة المفاتيح وارداً، فإن ذلك يعني أن ذلك السطح البيني لا يحتاج إليه. ولا يتضمن الشكل 6-10 السطوح البينية للاتصالات IPCablecom التي لا تتطلب الأمن.



TFTP – [مخدم] بروتوكول نقل ملفات مبسط
TGS – مخدم مانح البطاقات
AN – شبكة النفاذ
MGC – مراقب بوابة الوسائط
SG – بوابة تشوير
IKE+ – تبادل مفاتيح إنترنت يتطلب شهادات مفاتيح عمومية

OSS – أنظمة دعم العمليات
CM – مودم كبلي
MTA – مكيف مطراف وسائط
MTA – مكيف مطراف وسائط [ناء]
IKE– – تبادل مفاتيح إنترنت على أساس مفاتيح متقاسمة مسبقاً
CMS-based KM – مفاتيح مولدة عشوائياً يوزعها نظام إدارة الزبائن

Prov Server – مخدم توفير الخدمات
RKS – مخدم الاحتفاظ بالسجلات
CMS – نظام إدارة الزبائن
MG – بوابة وسائط

الشكل 6-10 – السطوح البينية لأمن IPCablecom (معرفة على النحو التالي: (<label>: <protocol> { <security protocol> / <key management protocol> }

تقسم معمارية أمن الاتصالات IPCablecom تزويد الأجهزة بالخدمة إلى ثلاثة أنشطة متميزة وهي: اكتتاب المشترك وتزويد الجهاز بالخدمة وترخيص الجهاز. وتفتح عملية *اكتتاب المشترك* حساب فوترة دائم للمشترك يقوم بتعريف مكيف مطراف الوسائط تعريفاً فريداً لدى نظام إدارة الزبائن (CMS) عبر الرقم المسلسل للمكيف (MTA) أو عنوان شفرة

استيقان الرسالة (MAC). ويستخدم حساب الفوترة أيضاً لمعرفة الخدمات التي يشترك فيها المشترك لدى المكيف. وقد يحدث اكتتاب المشترك داخل النطاق أو خارج النطاق. وتقع المواصفة الفعلية لعملية اكتتاب المشترك خارج نطاق IPCablecom وقد تختلف باختلاف مقدمي الخدمات. أما بالنسبة *لتزويد الجهاز بالخدمة*، فإن المكيف MTA يتحقق من صحة ملف التشكيل الذي يقوم بتحميله أولاً بتطبيق إجراءات الأمن بموجب بروتوكول إدارة الشبكة البسيطة SNMP v3 (باستخدام الاستيقان وإدارة المفاتيح القائمين على نظام Kerberos) بينه وبين المخدم الذي يوفر الخدمة. ثم يقوم المخدم بتعريف المكيف MTA بمكان ملف التشكيل وبفرم لملف التشكيل. ويستجلب المكيف ملف التشكيل ويقوم بعملية فرم لملف التشكيل ويقارن النتيجة مع الفرم الذي قدمه مخدم توفير الخدمة. ويكون ملف التشكيل مستيقناً إذا كان الفرم مطابقاً. وقد يكون ملف التشكيل مجفراً اختيارياً من أجل الخصوصية (ينبغي أيضاً تفعيل سرية البروتوكول SNMP v3 من أجل إرسال مفتاح تجفير ملف التشكيل على نحو آمن إلى المكيف MTA). ويحدث *ترخيص الجهاز* عندما يستيقن جهاز MTA نفسه لدى مخدم إدارة النداء ويقيم علاقة أمن مع ذلك المخدم قبل أن يصبح قيد التشغيل بالكامل. ويسمح الاستيقان من الجهاز بتشوير النداء التالي الذي يتعين حمايته بناء على علاقة الأمن القائمة.

ويمكن حماية كل من حركة التشوير وتدفق الوسائط. ويجري تأمين كل حركة التشوير، التي تشمل تشوير نوعية الخدمة وتشوير النداء والتشوير مع السطح البيني لبوابة الشبكة PSTN، عبر أمن بروتوكول الإنترنت (IPsec). وتتم إدارة علاقة أمن IPsec باستخدام بروتوكولين لإدارة المفاتيح، هما: بروتوكول الاستيقان من الشبكة (Kerberos) بتجفير المفاتيح العمومية (PKINIT) وبروتوكول تبادل مفاتيح الإنترنت (IKE). ويستخدم البروتوكول Kerberos/PKINIT لتبادل المفاتيح بين زبائن MTA ومخدم نظام إدارة الزبائن (CMS)؛ ويستخدم البروتوكول IKE لإدارة جميع علاقات تشوير أمن IPsec الأخرى. وفيما يتعلق بتدفقات الوسائط، تجفر كل رزمة وسائط في بروتوكول الوقت الفعلي (RTP) من أجل الخصوصية ويتم الاستيقان منها للتحقق من سلامة البيانات وأصل الرزمة. وبإمكان أجهزة MTA التفاوض على خوارزمية تجفير معينة، على الرغم من أن خوارزمية التجفير الوحيدة المطلوبة هي خوارزمية معيار التجفير المتطور (AES). وقد تشمل كل رزمة في بروتوكول الوقت الفعلي (RTP) شفرة اختيارية للاستيقان من الرسالة. ويمكن أيضاً التفاوض بشأن خوارزمية شفرة استيقان من الرسالة (MAC)، على الرغم من أن الخوارزمية الوحيدة المحددة حالياً هي الفرم الزجلي متعدد الخطوط (MMH). ويغطي حساب شفرة الاستيقان من الرسالة (MAC) رأسية غير مجفرة وحمولة نافعة مجفرة للرزمة.

وتشتق المفاتيح من أجل التجفير وحساب شفرة الاستيقان MAC من السر من طرف إلى طرف ومن حشو اختياري يجري تبادلهما بين مكيف MTA المرسل والمستقبل كجزء من تشوير النداء. وهكذا تتم تبادلات المفاتيح لأمن تدفق الوسائط بشكل آمن بذاتها بواسطة أمن تشوير النداء.

ويتوفر الأمن أيضاً لأنظمة دعم العمليات (OSS) ولنظام الفوترة. وينفذ وكلاء بروتوكول إدارة الشبكة البسيطة (SNMP) في أجهزة IPCablecom الصيغة SNMP v3. ويوفر نموذج أمن مستعمل [RFC 2274] هذا لبروتوكول خدمات الاستيقان والخصوصية لحركة البروتوكول. وقد يستخدم التحكم في النفاذ القائم على الرؤية [RFC 2275] في البروتوكول SNMP v3 من أجل التحكم في النفاذ إلى أغراض قاعدة معلومات الإدارة (MIB).

ويستخدم بروتوكول إدارة تبادل مفاتيح الإنترنت (IKE) في إنشاء مفاتيح للتجفير والاستيقان بين مخدم حفظ السجلات (RKS) وكل عنصر في شبكة الاتصالات IPCablecom الذي يولد رسائل الأحداث. وعند إقامة علاقات أمن الشبكة IPsec، ينبغي استحداث هذه المفاتيح بين كل مخدم RKS (أولي أو ثانوي أو غيرهما) وكل من أنظمة إدارة الزبائن (CMS) وشبكة المنطقة. وقد يحدث تبادل المفاتيح بين مراقب بوابة الوسائط (MGC) والمخدم (RKS) ويترك لتنفيذ البائع في المرحلة الأولى من الاتصالات IPCablecom. وترسل رسائل الأحداث من نظام إدارة الزبائن (CMS) وشبكة المنطقة (AN) إلى المخدم RKS باستخدام بروتوكول نقل خدمة نفاذ المستعمل بالمراقمة عن بعد (RADIUS) الذي يؤمَّن بدوره بواسطة أمن بروتوكول الإنترنت (IPsec).

3.6 إرسال الفاكس الآمن

الفاكس تطبيق شائع جداً، وقد عرِّف في البداية للإرسال عبر الشبكات PSTN (التوصية ITU-T T.4) ثم للشبكات الرقمية متكاملة الخدمات (ISDN) (التوصية ITU-T T.6). وقد اتسع مؤخراً ليشمل النقل عبر شبكات بروتوكول الإنترنت (بما في ذلك الإنترنت) للإرسال في غير الوقت الفعلي (ترحيل بريد إلكتروني مثلاً) باستخدام التوصية ITU-T T.37، وفي الوقت الفعلي (باستخدام بروتوكول الوقت الفعلي RTP) باستخدام التوصية ITU-T T.38. ويواجه إرسال الفاكس عموماً – بغض النظر عما إذا كان عبر الشبكات PSTN أو الشبكات ISDN أو بروتوكول الإنترنت – مسألتين من مسائل الأمن

تتعلق الأولى بالاستيقان من توصيل ما (وفي بعض الأحيان بعدم التنصل منه) وتتعلق الثانية بسرية البيانات المرسلة. بيد أن التوصيتين T.37 وT.38 أبرزتا أهمية هاتين المسألتين نتيجة للطابع الموزع لشبكة بروتوكول الإنترنت.

وتتضمن التوصية ITU-T T.36 تعريف حلين تقنيين مستقلين يمكن استخدامهما في سياق إرسال آمن للفاكس لتجفير الوثائق التي يتم تبادلها. ويقوم الحلان التقنيان على أساس خوارزميات النظام HKM/HFX40 (الملحق ألف/T.36) وخوارزمية ريفست وشامير وأدلمان RSA (الملحق باء/T.36). وعلى الرغم من أن كلا الحلين يقصر مفاتيح الدورة على 40 بتة (بحكم القواعد التنظيمية الوطنية وقت الموافقة على التوصية في سنة 1997)، فقد تم تحديد آلية لتوليد مفتاح دورة بديلة (من مفتاح دورة طوله 40 بتة) للخوارزميات التي تتطلب مفاتيحاً أطول. ويوضح الملحق جيم بالتوصية T.36 استخدام نظام HKM لتوفير مقدرات إدارة المفاتيح بشكل آمن لمطاريف الفاكس بواسطة طريقة تسجيل وحيدة الاتجاه بين الكيانين X وY أو إرسال مفتاح سري بشكل آمن بين الكيانين X وY. ويشمل الملحق دال بالتوصية T.36 إجراءات استخدام نظام تجفير الموجة الحاملة لخوارزمية HFX40 لتوفير سرية الرسالة لمطاريف الفاكس. وأخيراً يوضح الملحق هاء بالتوصية T.36 خوارزمية فرم HFX40 من حيث استخدامها، والحسابات الضرورية والمعلومات الواجب تبادلها بين مطاريف الفاكس لتوفير سلامة رسالة الفاكس المرسلة إما كبديل مختار أو مسبق البرمجة لتجفير الرسالة.

وبالإضافة إلى ذلك، تتضمن التوصية T.36 تعريف خدمات الأمن التالية:

- الاستيقان المتبادل (إلزامي).
- خدمة أمن (اختيارية) تشمل الاستيقان المتبادل وسلامة الرسالة وتأكيد استلام الرسالة.
- خدمة أمن (اختيارية) تشمل الاستيقان المتبادل وسرية الرسالة (تجفير) وإقامة مفتاح الدورة.
- خدمة أمن (اختيارية) تشمل الاستيقان المتبادل وسلامة الرسالة وتأكيد استلام الرسالة وسرية الرسالة (تجفير) وإقامة مفتاح الدورة.

ويتم تحديد أربع مواصفات للخدمة على أساس خدمات الأمن هذه المعرفة أعلاه، كما هو مبين في الجدول 6-1 أدناه.

الجدول 6-1 – مواصفات الأمن المبينة في الملحق حاء بالتوصية T.30

خدمات الأمن	مواصفات الخدمة			
	1	2	3	4
الاستيقان المتبادل	X	X	X	X
• سلامة الرسالة • تأكيد استلام الرسالة		X		X
• سرية الرسالة (تجفير) • إقامة مفتاح الدورة			X	X

1.3.6 أمن الفاكس باستخدام خوارزمية هوثورن لإدارة المفاتيح (HKM) وخوارزمية هوثورن لشفرة الفاكس (HFX)

يوفر الجمع بين خوارزمية *هوثورن لإدارة المفاتيح* وخوارزمية *هوثورن لشفرة فاكس* المقدرات التالية لتوفير اتصالات الوثائق الآمنة بين كيانات (المطاريف أو مشغلي المطاريف):

- الاستيقان المتبادل من الكيانات؛
- إقامة مفتاح سري للدورة؛
- سرية الوثائق؛
- تأكيد الاستلام؛
- تأكيد أو رفض سلامة الوثائق.

يتم توفير إدارة المفاتيح باستخدام نظام هوثورن لإدارة المفاتيح (HKM) كما هو مبين في الملحق باء بالتوصية T.36. ويقوم ذلك على إجراءين: الأول هو التسجيل والثاني هو الإرسال الآمن للمفتاح السري. ويقيم التسجيل أسراراً متبادلة

ويمكّن توفير جميع عمليات الإرسال التالية بأمان. وفي عمليات الإرسال اللاحقة، يوفر نظام HKM استيقاناً متبادلاً ومفتاح دورة سرياً لضمان سرية الوثائق وسلامتها، وتأكيد الاستلام، وتأكيد أو رفض سلامة الوثائق.

وتتوفر سرية الوثائق باستخدام الشفرة المبينة في الملحق دال بالتوصية T.36. وتستخدم الشفرة مفتاحاً رقمياً يتألف من 12 رقماً عشرياً، وهو يكافئ تقريباً مفتاح دورة يتألف من 40 بتة.

وتتوفر سلامة الوثائق باستخدام النظام المبين في الملحق هاء بالتوصية T.36 وتوضح التوصية ITU-T T.36 خوارزمية الفرم، بما في ذلك الحسابات المرتبطة بها وتبادل المعلومات.

وفي أسلوب التسجيل، يتبادل المطرافان المعلومات التي تمكّن الكيانين من تعرف كل منهما على الآخر على نحو فريد. ويقوم ذلك على أساس اتفاق بين مستعملي مفتاح سري لمرة واحدة. ويقوم كل كيان بتخزين عدد يتكون من 16 رقماً يرتبط على نحو فريد بالكيان الذي قام معه بتنفيذ التسجيل.

وعندما يكون من المطلوب إرسال وثيقة على نحو آمن، يرسل المطراف المرسل عدداً سرياً يتكون من 16 رقماً مرتبطاً بالكيان المستقبل إلى جانب عدد عشوائي ومفتاح دورة مجفر بمثابة تحد للكيان المستقبل. ويستجيب المطراف المستقبل بإرسال مفتاح يتألف من 16 رقماً مرتبطاً بالكيان المرسل إلى جانب عدد عشوائي وصيغة معاد تجفيرها للتحدي الوارد من الكيان المرسل. ويرسل في نفس الوقت عدداً عشوائياً ومفتاح دورة مجفراً بمثابة تحد للكيان المرسل. ويستجيب المطراف المرسل بعدد عشوائي وصيغة معاد تجفيرها للتحدي الذي تلقاه من الكيان المستقبل. ويمكّن هذا الإجراء كلاً منهما من الاستيقان من الآخر. وفي نفس الوقت، يرسل المطراف المرسل عدداً عشوائياً ومفتاح الدورة المجفر الذي يتعين استخدامه في التجفير والفرم.

وبعد إرسال الوثيقة، يرسل المطراف المرسل عدداً عشوائياً ومفتاح دورة مجفراً بمثابة تحد للكيان المستقبل. وفي نفس الوقت، يرسل عدداً عشوائياً وقيمة الفرم المجفرة التي تمكّن الكيان المستقبل من ضمان سلامة الوثيقة الواردة. ويرسل المطراف المستقبل عدداً عشوائياً وصيغة التحدي المعاد تجفيرها من الكيان المرسل. وفي نفس الوقت، يرسل عدداً عشوائياً ووثيقة سلامة مجفرة لتكون بمثابة تأكيد أو رفض لسلامة الوثيقة الواردة. وتنفذ خوارزمية الفرم المستخدمة في تأكيد سلامة الوثيقة على الوثيقة بأكملها.

وثمة أسلوب أسبقية لا يتضمن تبديل أي إشارات أمن بين المطرافين. ويتفق الطرفان على مفتاح دورة سري لمرة واحدة يُدخل يدوياً. وهذا ما يستخدمه المطراف المرسل لتجفير الوثيقة وما يستخدمه المطراف المستقبل لفك تجفير الوثيقة.

2.3.6 أمن الفاكس باستخدام خوارزمية ريفست وشامير وأدلمان (RSA)

يحدد الملحق حاء بالتوصية T.30 الآليات التي توفر ملامح الأمن القائمة على أساس الآلية المجفرة RSA. وللاطلاع على مزيد من التفاصيل عن خوارزمية RSA يمكن الرجوع إلى *[ApplCryp، الصفحات من 466 إلى 474]*. وقد يكون مخطط تشفير الوثيقة المرسلة باستخدام ملامح الأمن من أي نوع من الأنواع المعرَّفة في التوصيتين ITU-T T.4 وITU-T T.30 (تشفير Huffman المعدل وأسلوب MR وMMR، وأسلوب السمة كما هو معرف في الملحق دال بالتوصية T.4، وأسلوب نقل ملف اثنيني BFT، وأسلوب نقل ملف آخر معرّف في الملحق جيم بالتوصية T.4).

والخوارزمية الأساسية المستخدمة للتوقيع الرقمي (من قبيل خدمات الاستيقان والسلامة) هي خوارزمية RSA باستخدام زوج "مفتاح عمومي"/"مفتاح سري".

وعند توفير خدمة السرية الاختيارية تجفر أيضاً العلامة التي تحتوي على مفتاح الدورة ("Ks") المستخدمة لتجفير الوثيقة بواسطة خوارزمية RSA. وزوج المفاتيح المستخدم لهذا الغرض المسمى ("المفتاح العمومي للتجفير"/"المفتاح السري للتجفير") ليس هو نفس زوج المفاتيح الذي يستخدم لخدمات من قبيل الاستيقان والسلامة، وذلك من أجل الفصل بين نوعي الاستخدام.

وتنفيذ خوارزمية RSA المستخدمة في الملحق حاء من التوصية T.30 موصوف في المعيار ISO/IEC 9796 (*مخطط توقيع رقمي يمكّن من استرجاع الرسالة*).

ولتجفير علامة تحتوي على مفتاح دورة تكون قواعد الإطناب عند معالجة خوارزمية RSA هي نفس الخوارزميات المحددة في المعيار ISO/IEC 9796. وينبغي ملاحظة أن بعض الإدارات قد تتطلب تنفيذ آلية *خوارزمية التوقيع الرقمي [ApplCryp، الصفحات من 483 إلى 502]* بالإضافة إلى خوارزمية RSA.

وكخيار تلقائي لا تُستخدم *سلطات إصدار الشهادات المبينة* في مخطط الملحق حاء بالتوصية T.30، ومع ذلك فإنها قد تستخدم اختيارياً للتصديق على صلاحية مفتاح عمومي لمرسل رسالة بالفاكس. وفي مثل هذه الحالة، قد يجري التصديق على المفتاح العمومي كما هو منصوص عليه في التوصية ITU-T X.509. ويرد وصف وسيلة إرسال شهادة المفتاح العمومي للمرسل في الملحق حاء بالتوصية T.30، ولكن نسق الشهادة على وجه الدقة متروك للدراسة في المستقبل بينما يجري التفاوض بشأن الإرسال الفعلي للشهادة في إطار البروتوكول.

ويمكن اعتماد *أسلوب التسجيل* كوظيفة إلزامية. وهو يسمح للمرسل والمستقبل بتسجيل وتخزين المفاتيح العمومية التي يستخدمها الطرف الآخر بطريقة سرية قبل أي اتصال آمن بالفاكس بين الطرفين. ويمكن لأسلوب التسجيل أن يجنب المستعمل الحاجة إلى إدخال المفاتيح العمومية لمراسليه يدوياً في المطراف (إذ إن المفاتيح العمومية طويلة بعض الشيء، 64 أثمونا أو أكثر).

وبما أن أسلوب التسجيل يسمح بتبادل المفاتيح العمومية ويمكّن من تخزينها في المطاريف، ليس من الضروري إرسالها عند إجراء اتصالات الفاكس.

وكما ورد في الملحق المذكور، تطبق بعض التوقيعات على نتيجة "وظيفة الفرم".

إن وظائف الفرم التي يمكن استخدامها هي إما (SHA-1، *خوارزمية الفرم الآمنة*) وهي خوارزمية من وضع المعهد الوطني للمعايير والتكنولوجيا في الولايات المتحدة (NIST) أو ملخص الرسالة رقم 5 (RFC 1321). وبالنسبة لخوارزمية الفرم الآمنة SHA-1، يكون طول نتيجة عملية الفرم على 160 بتة، وبالنسبة لملخص الرسالة رقم 5 يكون طول نتيجة عملية الفرم على 128 بتة. ويمكن لمطراف يمتثل للملحق حاء بالتوصية T.30 تنفيذ إما خوارزمية SHA-1 أو ملخص الرسالة رقم 5 أو كليهما. ويجري التفاوض بشأن استخدام خوارزمية أو أخرى في البروتوكول (كما سيأتي ذكره أدناه).

وعملية تجفير البيانات من أجل توفير السرية عملية اختيارية. ويجري تسجيل خمسة مخططات تجفير اختيارية في نطاق الملحق حاء بالتوصية T.30 وهي: FEAL-32 وSAFER K-64 وRC5 وIDEA وHFX40 (كما ورد وصفها في التوصية ITU-T T.36). وقد يخضع استخدامها في بعض البلدان لقواعد تنظيم وطنية.

ويمكن أيضاً استخدام خوارزميات اختيارية أخرى ، على أن يراعى في اختيارها سلسلة ISO/IEC 18033.

إن مقدرة المطراف على مناولة هذه الخوارزميات والاستخدام الفعلي لواحدة معينة خلال الاتصالات مسألة يجري التفاوض بشأنها في البروتوكول. ويستخدم مفتاح دورة للتجفير. والطول الأساسي لمفتاح دورة هو 40 بتة. وبالنسبة للخوارزميات التي تستخدم مفتاح دورة طوله 40 بتة (مثل HFX40)، يكون مفتاح الدورة ("Ks") هو المفتاح المستخدم فعلياً في خوارزمية التجفير، أما بالنسبة للخوارزميات التي تتطلب مفاتيح أطول من 40 بتة (مثل FEAL-32 وIDEA وSAFER K-64 التي تتطلب على التوالي: 64 بتة و128 بتة و64 بتة) فيتم تنفيذ آلية إطناب للحصول على الطول المطلوب. ويسمى المفتاح الناتج "مفتاح الدورة المطنب". وهذا المفتاح هو المفتاح الذي يستخدم فعلاً في خوارزمية التجفير.

4.6 تطبيقات إدارة الشبكة

انطلاقاً من معمارية الأمن التي بُحثت في القسم 4.2 من الضروري تأمين الحركة في مستوى الإدارة. وتستخدم هذه الحركة لرصد شبكة الاتصالات والتحكم فيها. وتقسم حركة الإدارة عادة إلى فئات على أساس المعلومات المطلوبة لوظائف التعامل مع الأعطال والتشكيل والأداء والمحاسبة وإدارة الأمن. ويتناول مجال إدارة الأمن كلاً من إقامة شبكة إدارة آمنة وكذلك إدارة أمن المعلومات المتصلة بالمستويات الثلاثة والطبقات الثلاث لمعمارية الأمن. ويرد وصف هذه الأخيرة في هذا القسم.

وفي شبكة الاتصالات، غالباً ما تُرسل حركة الإدارة على شبكة منفصلة لا تحمل سوى حركة إدارة الشبكة وليس حركة المستعملين. ويشار غالباً إلى هذه الشبكة باسم شبكة إدارة الاتصالات (TMN) الوارد وصفها في التوصية ITU-T M.3010. وتكون شبكة إدارة الاتصالات منفصلة ومعزولة عن البنية التحتية للشبكة العمومية بحيث لا ينتشر إليها أي انقطاع نتيجة تهديد أمني في مستوى المستعمل النهائي في الشبكة العمومية. ونتيجة لهذا الانفصال، من السهل نسبياً تأمين حركة شبكة الإدارة لأن النفاذ إلى هذا المستوى مقصور على مديري الشبكة المرخص لهم بذلك، ومن ثم

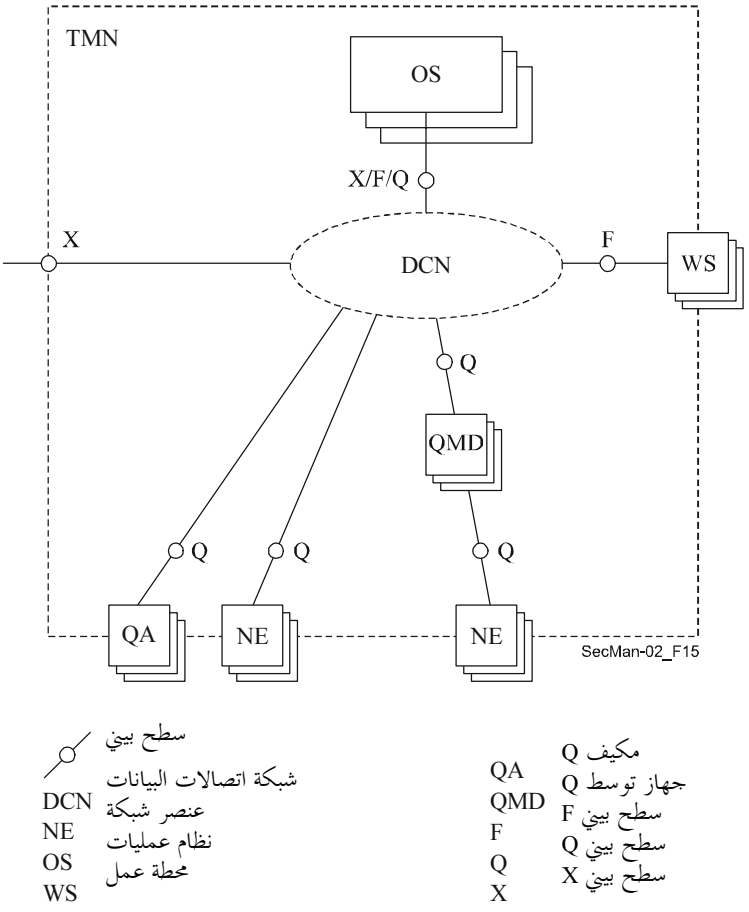
تقتصر الحركة على أنشطة الإدارة الصحيحة. ولكن في إطار شبكات الجيل التالي، قد يتم أحياناً الجمع بين تطبيق حركة المستعمل النهائي وتطبيق حركة الإدارة. ولئن كان هذا النهج يساعد على تقليل التكاليف إلى أدنى حد، لأنه لا يتطلب سوى بنية تحتية لشبكة متكاملة وحيدة، فإنه يؤدي أيضاً إلى ظهور كثير من تحديات الأمن الجديدة. إذ تصبح التهديدات في مستوى المستعمل النهائي تهديدات على مستويات الإدارة والتحكم. ويصبح مستوى الإدارة مفتوحاً لنفاذ العديد من المستعملين النهائيين، ومن ثم يصبح من الممكن حدوث أنواع كثيرة من الأنشطة المؤذية.

ولتوفير حل كامل من طرف إلى طرف، ينبغي أن تطبق جميع تدابير الأمن (مثل التحكم في النفاذ والاستيقان) على كل نوع من أنواع نشاط الشبكة (أي نشاط مستوي الإدارة ونشاط مستوي التحكم ونشاط مستوي المستعمل النهائي) للبنية التحتية للشبكة وخدمات الشبكة وتطبيقات الشبكة. وهنالك عدد من توصيات قطاع تقييس الاتصالات يركز بشكل محدد على جانب الأمن في مستوي إدارة عناصر الشبكة وأنظمة الإدارة التي هي جزء من البنية التحتية للشبكة.

وعلى الرغم من وجود معايير كثيرة لتأمين معلومات الإدارة المطلوبة للحفاظ على البنية التحتية للاتصالات، كما سيأتي بيانه فيا يلي، هناك مجال آخر يندرج ضمن الإدارة ويتصل بالبيئات التي يحتاج فيها مختلف مقدمي الخدمات للتفاعل من أجل تقديم خدمات من طرف إلى طرف، مثل الخطوط المؤجرة للزبائن التي تعبر الحدود الجغرافية أو الهيئات التنظيمية أو الحكومية التي تتدخل لدعم عمليات إعادة الخدمة إلى ما كانت عليه قبل وقوع أي كارثة.

1.4.6 معمارية إدارة الشبكات

تتضمن التوصية ITU-T M.3010 معمارية تحديد إدارة الشبكة في شبكة اتصالات ما، ويوضح الشكل 6-11 المعمارية المادية لهذا الغرض. وتحدد شبكة الإدارة السطوح البينية التي تقرر التبادلات المطلوبة لأداء وظائف العمليات والإدارة والصيانة وتوفير الخدمة في مستويات مختلفة.



الشكل 6-11 – مثال لمعمارية مادية في التوصية M.3010

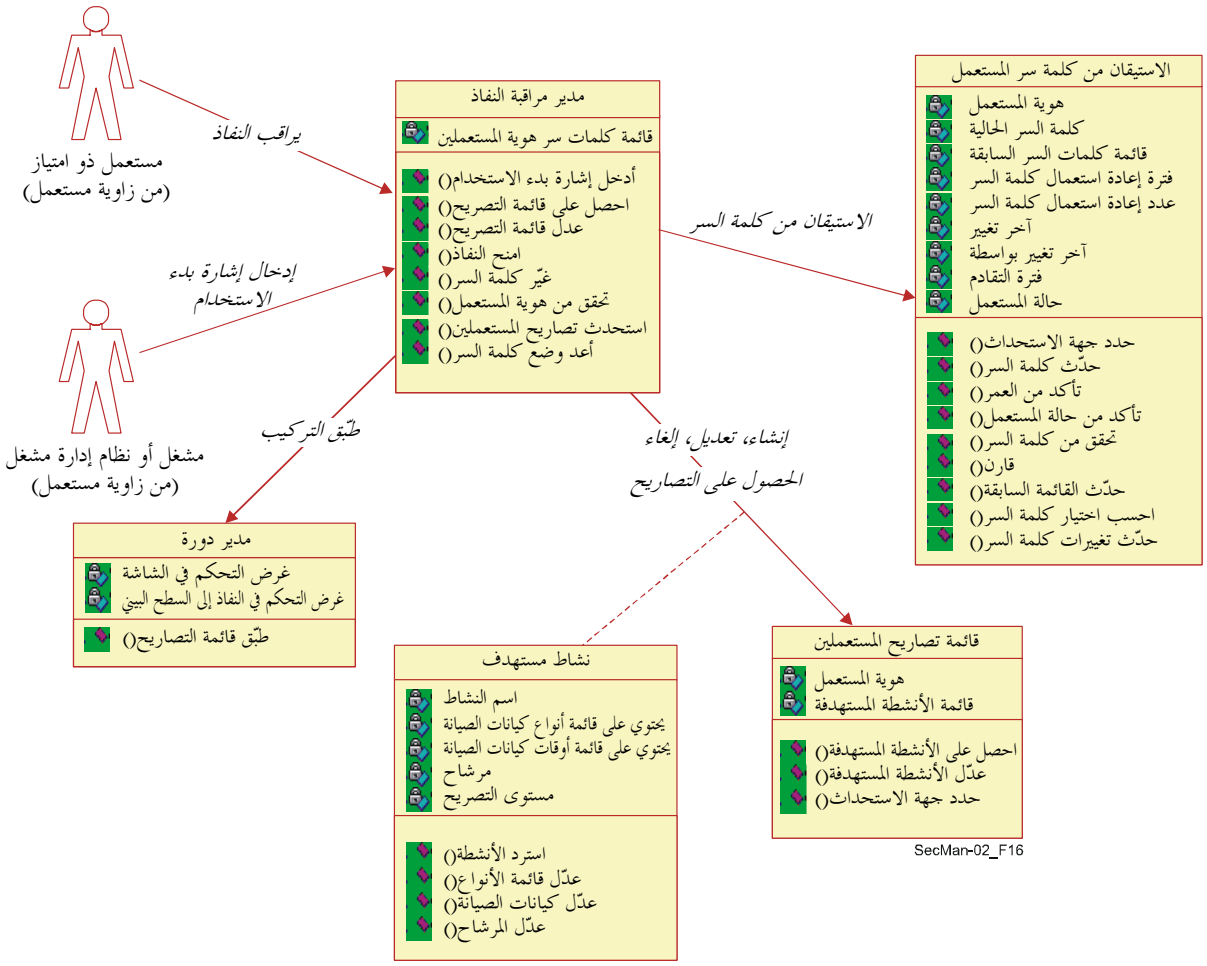
تتفاوت من منظور الأمن متطلبات مختلف السطوح البينية. ويقع السطح البيني Q ضمن ميدان إداري واحد، بينما يقع السطح البيني X بين ميادين إدارية مختلفة قد تمتلكها جهات مختلفة من مقدمي الخدمات. وبينما تدعو الحاجة إلى خدمات أمن في كل من Q وX، فإن الحاجة أشد إلى تدابير معاكسة قوية في حالة السطح البيني X. وتشتمل التوصية ITU-T M.3016.0 على لمحة عامة وهيكل يحدد محاذير الأمن التي تتهدد شبكة إدارة الاتصالات (TMN). وفي إطار سلسلة التوصيات M.3016 تحدد التوصية M.3016.1 المتطلبات المفصلة والتوصية M.3016.2 خدمات الأمن والتوصية M.3016.3 الآليات التي يمكن بها مواجهة التهديدات ضمن سياق المعمارية الوظيفية لشبكة TMN، كما هي موصوفة في التوصية M.3010. وبما أن مختلف منظمات وضع المعايير لا تحتاج إلى أن تضع جميع المتطلبات فإن التوصية M.3016.4 توفر قالباً لاستحداث مواصفات على أساس متطلبات الأمن والخدمات والآليات يمكن استخدامه من أجل الامتثال لسياسة الأمن التي تنفرد بها منظمة ما. وتتضمن التوصية ITU-T 3320 تفاصيل جوانب الأمن الخاصة بالسطح البيني X. وتتضمن التوصيتان ITU-T Q.811 وITU-T Q.812 جوانب البروتوكول لمختلف طبقات الاتصالات.

وهنالك وجهان لمناقشة الأمن في سياق الإدارة. يتعلق أحدهما بمستوي الإدارة لنشاط من طرف إلى طرف (مثل خدمات نقل الصوت بواسطة بروتوكول الإنترنت). وينبغي القيام بنشاط الإدارة الذي يتطلب إدارة المستعملين بطريقة آمنة. وهذا ما يشار إليه بعبارة تبادل *أمن معلومات الإدارة* عبر الشبكة لتنفيذ تطبيق من طرف إلى طرف. والوجه الآخر هو إدارة معلومات الأمن. وبغض النظر عن التطبيق، مثل نقل الصوت بواسطة بروتوكول الإنترنت أو نشاط الإبلاغ عن عطلٍ بين جهتين من مقدمي الخدمة، ينبغي كذلك إدارة تدابير الأمن، مثل استخدام مفاتيح التجفير. وهذا ما يشار إليه غالباً بعبارة *إدارة معلومات الأمن*. وتعتبر البنية التحتية للمفاتيح العمومية (PKI) المعرّفة في القسم السابق مثالاً لهذا الوجه. وتتضمن التوصية ITU-T M.3400 تعريف عدد من الوظائف المتعلقة بكلا الوجهين.

واستناداً إلى الإطار الوارد في التوصية X.805، وُضِعت عدة توصيات تتناول وظائف الإدارة بالنسبة إلى خلايا مستوي الإدارة الثلاث (انظر الشكل 2-1). وتوضح الأقسام الفرعية الواردة فيما يلي أدناه بعض هذه التوصيات وتبيّن كيف تتناول احتياجات الأمن. وبالإضافة إلى التوصيات بالنسبة إلى طبقات مستوي الإدارة الثلاث هنالك توصيات أخرى تتضمن تعريف الخدمات النوعية أو المشتركة مثل إطلاق الإنذارات عند حدوث انتهاك مادي للأمن، ووظائف التدقيق، ونماذج معلومات تعريف سويات الحماية لأهداف مختلفة (أي كيانات إدارة).

2.4.6 تقاطع مستوي الإدارة وطبقة البنية التحتية

تتناول هذه الخلية كيفية تأمين نشاط الإدارة لعناصر البنية التحتية للشبكة، أي عناصر الإرسال والتبديل والوصلات التي توصل بينها وكذلك الأنظمة الطرفية مثل المخدمات. وكمثال على ذلك فإن الأنشطة من قبيل توفير الخدمة لعنصر الشبكة ينبغي أن يقوم بها مستعمل مرخص له بذلك. ويمكن النظر في توصيلية من طرف إلى طرف على أساس شبكة (أو شبكات) نفاذ وشبكة (أو شبكات) أساسية. ويمكن استخدام تكنولوجيات مختلفة في هذه الشبكات. وقد تم وضع توصيات تتناول كلاً من شبكات النفاذ والشبكات الأساسية. وثمة حالة من هذا القبيل تناقش هنا هي الشبكة البصرية المنفعلة عريضة النطاق (BPON) المستخدمة في النفاذ. وتتضمن التوصية ITU-T Q.834.3 إدارة امتيازات مستعمل شبكة نفاذ باستخدام منهجية وضع النماذج الموحدة، بينما تتضمن التوصية Q.834.4 تعريف تبادل الإدارة باستخدام معمارية وسيط مشترك لطلب غرض (CORBA). والسطح البيني الموصوف في هذه التوصيات هو السطح البيني Q المبين في الشكل 6-11. وهو يطبق بين نظام إدارة العناصر وأنظمة إدارة الشبكات. ويستخدم الأول لإدارة عناصر الشبكة الفردية، وبالتالي يدرك التفاصيل الداخلية لمعماريات عتاد وبرمجيات العناصر الواردة من طرف واحد أو أكثر، بينما يقوم الثاني بالأنشطة على مستوى الشبكة من طرف إلى طرف ويشمل أنظمة إدارة العديد من الموردين. ويبين الشكل 6-12 الأغراض المختلفة المستخدمة لإنشاء وإلغاء وتخصيص واستخدام معلومات التحكم في النفاذ لمستعملي نظام إدارة العناصر. وتحتوي قائمة تصاريح المستعملين على قائمة بأنشطة الإدارة المسموح بها لكل مستعمل مرخص له بذلك. ويتحقق مدير التحكم في النفاذ من هوية المستعمل ومن كلمة السر الخاصة به لنشاط الإدارة ويمنحه حق النفاذ إلى العناصر الوظيفية المسموح بها والمدرجة في قائمة التصاريح.



الشكل 6-12 – إدارة امتيازات المستعمل بموجب التوصية Q.834.3

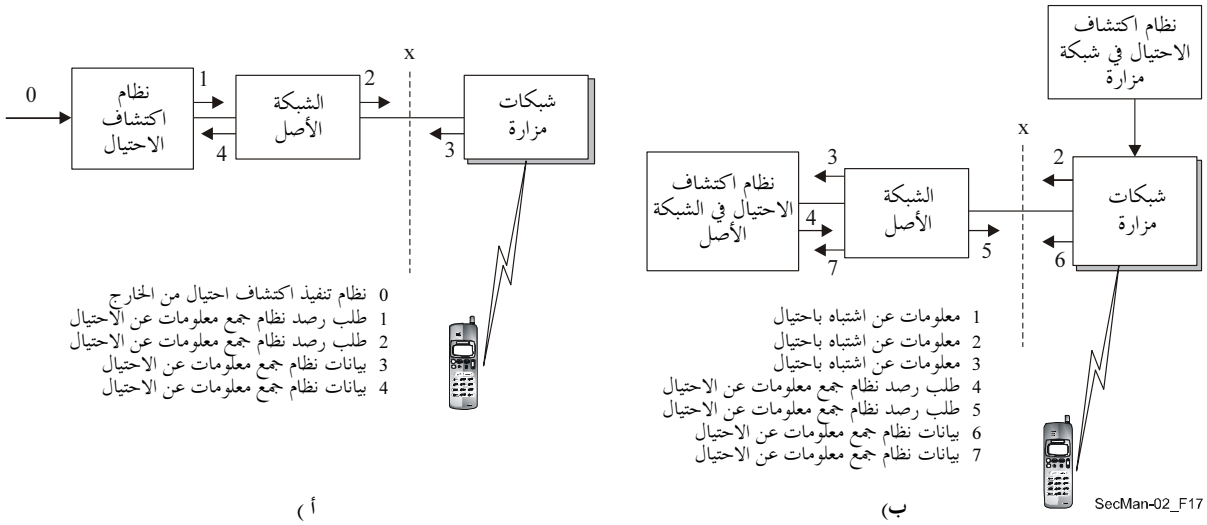
3.4.6 تقاطع مستوي الإدارة وطبقة الخدمات

يتعلق التقاطع بين مستوي الإدارة وطبقة الخدمات بتأمين الأنشطة في مجال رصد موارد الشبكة المخصصة لخدمات التسليم بواسطة مقدّم الخدمات والتحكم في هذه الموارد. وتتناول توصيات قطاع تقييس الاتصالات جانبين بخصوص هذا التقاطع، يضمن أحدهما توفير تدابير الأمن الملائمة للخدمات المتاحة في الشبكة. ومن أمثلة هذا الجانب الحرص على أن أداء العمليات المرتبطة بتوفير الخدمة يقتصر على المستعملين المخولين، بينما يتناول الجانب الثاني تعريف ما هي التبادلات الإدارية وتبادلات الإدارة الصحيحة. ويساعد مثل هذا التعريف على اكتشاف انتهاكات الأمن. وعندما توجد انتهاكات للأمن، يتم إدارتها غالباً باستخدام أنظمة إدارة محددة.

ومن أمثلة التوصيات التي تتناول الجانب الأول، وهو نشاط إدارة خدمة ما، التوصية ITU-T M.3208.2 بشأن إدارة التوصيل. ويستخدم زبون الخدمة، الذي يمتلك وصلات موفرة مسبقاً، هذه الخدمة في إنشاء توصيل من طرف إلى طرف على دارة مؤجرة. وتسمح خدمة إدارة التوصيل هذه للمشترك بإنشاء/تفعيل، أو تعديل أو إلغاء الدارات المؤجرة في نطاق حدود الموارد الموفرة مسبقاً. ولأن المستعمل هو الذي يوفر التوصيلية من طرف إلى طرف، فمن الضروري ضمان أن المستعملين المخولين فقط هم الذين يسمح لهم بأداء هذه العمليات. وأبعاد الأمن المعرفة لنشاط الإدارة المرتبط بهذه الخدمة هي مجموعة فرعية من أبعاد الأمن الثمانية التي نوقشت في القسم 4.2، وهي الاستيقان من كيان نظير، والتحكم في سلامة البيانات (لمنع التعديل غير المرخص به للبيانات أثناء العبور)، والتحكم في النفاذ (لضمان عدم نفاذ مشترك ما إلى بيانات مشترك آخر قصد الإيذاء أو بشكل عرضي).

والتوصية ITU-T M.3210.1 مثال لتوصية تتضمن تعريف الأنشطة الإدارية المرتبطة بمستوي الإدارة للخدمات اللاسلكية. وهذا يقابل الجانب الثاني الوارد ذكره أعلاه.

وفي الشبكة اللاسلكية، عندما يتحول المستعملون من الشبكة الأصل إلى الشبكة المزارة قد يعبرون ميادين إدارية مختلفة. وتصف الخدمات المعرّفة في التوصية ITU-T M.3210.1 كيف أن ميدان إدارة حالات الاحتيال في الموقع الأصل يقوم بجمع المعلومات الملائمة عن مشترك ما حالما يتسجل على الشبكة المزارة. ويوضح كل من السيناريو أ) والسيناريو ب) في الشكل 6-13 الشروع في نشاط رصد الإدارة سواء بواسطة الشبكة الأصل أو الشبكة المزارة. ويطلب نظام كشف الاحتيال في الشبكة الأصل معلومات عن الأنشطة عندما يتسجل مشترك ما لدى شبكة مزارة إلى أن يغادر هذه الشبكة عندما ينسحب من التسجيل فيها. وبعدئذ يمكن وضع مواصفات تتصل بالاستعمال على أساس سجلات تفاصيل النداءات والتعقب (التحليل) في سوية الخدمة أو من أجل مشترك ما. ومن ثم يستطيع نظام كشف الاحتيال القيام بعملية التحليل وتوليد الإنذارات الملائمة بشأن السلوك الاحتيالي.



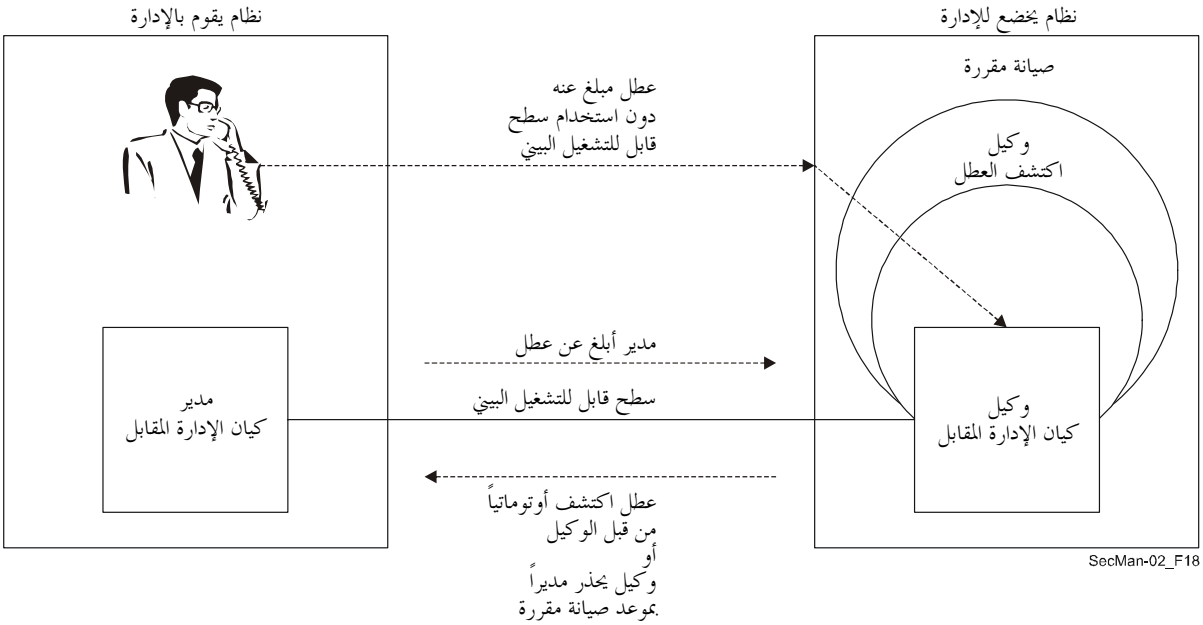
الشكل 6-13 – إدارة حالات الاحتيال في الخدمات اللاسلكية بموجب التوصية ITU-T M.3210.1

4.4.6 تقاطع مستوي الإدارة وطبقة التطبيق

تقوم الخلية الثالثة، وهي تقابل تقاطع مستوي الإدارة وطبقة التطبيق، بتأمين تطبيقات المستعمل النهائي القائمة على الشبكة. ويتضمن كل من سلسلة التوصيات X.400 وX.500 تعريف تطبيقات مثل إرسال الرسائل وتنظيم الدليل.

والنوع الآخر من التطبيقات التي يجري فيها تأمين أنشطة الإدارة هي تطبيقات الإدارة نفسها. وقد يبدو هذا القول دائري المنطق، ومن الأفضل شرحه باستخدام الأمثلة. فالمستعملون النهائيون لهذه التطبيقات هم موظفو (عمليات) الإدارة لدى مقدم الخدمة. ولننظر في حالة مقدم خدمات يستخدم خدمات توصيل يوفرها مقدم خدمات آخر من أجل توفير خدمة التوصيل من طرف إلى طرف. وتبعاً للبيئة التنظيمية أو بيئة السوق، قد يوفر بعض مقدمي الخدمات خدمات نفاذ، بينما يوفر مقدمو خدمات آخرون، يشار إليهم باسم *الشركات الناقلة فيما بين البدالات*، توصيلية مسافات بعيدة. وتستأجر هذه الشركات خدمات نفاذ من مقدم خدمات محلي للحصول على توصيلية من طرف إلى طرف عبر مواقع موزعة جغرافياً. وعندما تتعطل خدمة ما يستخدم تطبيق إدارة يسمى إدارة تقرير الأعطال للتبليغ عن الأعطال بين أنظمة الإدارة. ويتطلب مستعمل هذه الأنظمة وكذلك التطبيق نفسه ترخيصاً للإبلاغ عن حدوث أعطال في الخدمة. وينبغي للأنظمة المرخص لها والمستعملين المرخص لهم اتخاذ الإجراءات اللازمة لتدارك الأعطال المبلغ عنها.

ويوضح الشكل 6-14 التفاعلات التي ينبغي تنفيذها بطريقة آمنة. ومثل ما يحدث في إدارة صناديق البريد في التطبيق الخاص بالبريد الإلكتروني، تدار امتيازات النفاذ لمنع النفاذ غير المرخص به إلى تقارير الأعطال. ويسمح لمقدم الخدمة بالتبليغ فقط عن الأعطال في الخدمات التي يستأجرها وليس في الخدمات التي يستأجرها مقدم خدمة آخر.



الشكل 6-14 – وضع تقرير عن إدارة الأعطال بموجب التوصية ITU-T X.790

وتتضمن التوصية ITU-T X.790 تعريف تطبيق الإدارة هذا وتستخدم آليات مثل قائمة التحكم في النفاذ والاستيقان المتبادل لتأمين الأنشطة. وقد نُفذ هذا التطبيق إلى جانب آليات الأمن من أجل الاستيقان، باستخدام هذه التوصيات.

5.4.6 خدمات إدارة الأمن المشتركة

تتضمن التوصيات X.736 وX.740 وX.741 الصادرة عن القطاع ITU-T تعريف الخدمات المشتركة التي تطبق على جميع الخلايا الثلاث لمستوي الإدارة لدى استخدام بروتوكول معلومات الإدارة المشتركة (CMIP) عند السطح البيني. وفيما يلي أدناه وصف موجز للخدمات الواردة في هذه التوصيات. ويلاحظ أن جميع هذه الوظائف تُعتبر حقاً أنشطة في مستوي الإدارة.

1.5.4.6 وظيفة الإبلاغ عن إنذار أمن: الإبلاغ عن إنذار عموماً وظيفة أساسية في السطوح البينية للإدارة. وعندما يُكشف عن عطل إما ناتج من المنظور التشغيلي (عطل في رزمة الدارة) أو من انتهاك لسياسة الأمن يبلّغ عن إنذار إلى النظام القائم بالإدارة. ويحتوي بلاغ الإنذار على عدد من المعلمات بحيث يتمكن النظام القائم بالإدارة من معرفة سبب العطل واتخاذ تدابير تصحيحية. وتشمل معلمات أي حدث حقلاً إلزامياً يدعى نمط الحدث ومجموعة من الحقول الأخرى تشمل معلومات الحدث. وتتألف هذه المجموعة من معلومات تتناول مثلاً حدة الإنذار والأسباب المحتملة للإنذار وكاشف انتهاك الأمن وغير ذلك. وأسباب الإنذار مرتبطة بأنماط الأحداث كما هو مبين في الجدول 6-2.

الجدول 6-2 – أسباب إنذار الأمن

نمط الحدث	أسباب إنذار الأمن
انتهاك السلامة	معلومات مزدوجة معلومات ناقصة كشف عن تعديل معلومات معلومات في غير ترتيبها معلومات غير متوقعة
انتهاك التشغيل	رفض الخدمة تعطل الخدمة خطأ إجرائي سبب غير محدد
انتهاك مادي	تلاعب في الكبل كشف دخيل سبب غير محدد
انتهاك خدمة أمن أو آلية أمن	فشل الاستيقان انتهاك السرية فشل عدم التنصل محاولة نفاذ غير مرخص به سبب غير محدد
انتهاك ميدان زمني	معلومات متأخرة مفتاح انتهت صلاحيته نشاط خارج الساعات المحددة

وأسباب الإنذار هذه موضحة بشكل أوفى في التوصية X.736. ويتصل عدد من أسباب الإنذار بتهديدات جاء ذكرها في فقرات سابقة.

2.5.4.6 وظيفة سجل تدقيق الأمن: لتمكين مستعمل إدارة أمن ما من تسجيل انتهاكات الأمن ومتابعة تدقيقها تحدد التوصية ITU-T X.740 عدداً من الأحداث التي تخضع لسجل التدقيق. وهذه الأحداث هي عمليات الوصل والقطع واستعمالات آليات الأمن وعمليات الإدارة ومحاسبة الاستعمال. ويستخدم النموذج آلية التسجيل المعرّفة في التوصية ITU-T X.735 وهي سجل عام لتدوين أي حدث يتولد في النظام الخاضع للإدارة. وتؤدي وظيفة سجل التدقيق إلى تعريف حدثين يتصلان بانتهاكات الأمن. وهما تقرير الخدمة وتقرير الاستخدام. ويتناول تقرير الخدمة توفير الخدمة أو رفض الخدمة أو استعادة الخدمة. ويستخدم تقرير الاستخدام لبيان استحداث سجل يحتوي على بيانات إحصائية ذات صلة بالأمن. وكما هو الحال بالنسبة إلى أي حدث فقد جرى تعريف عدد من قيم الأسباب فيما يتعلق بتقرير الخدمة. ومن بينها مثلاً طلب الخدمة ورفض الخدمة وتعطل الخدمة واستعادة الخدمة وغيرها. ويمكن تعريف أنماط جديدة من الأحداث عند الاقتضاء لأن النمطين المذكورين في التوصية قد لا يكفيان في المستقبل.

3.5.4.6 تتضمن التوصية ITU-T X.741 وصفاً مفصلاً للنموذج المرتبط بتخصيص التحكم في النفاذ لمختلف الكيانات التي تخضع للإدارة. ومن المتطلبات التي تلبيها تعاريف التحكم في النفاذ في هذه التوصية حماية معلومات الإدارة من استحداث أو حذف أو تعديل غير مرخص به، وتكون العمليات المسموح بإجرائها على الكيانات متسقة مع حقوق النفاذ التي يتمتع بها مستهلو العمليات، وهي تمنع إرسال معلومات الإدارة إلى جهات غير مرخص لها بذلك. وثمة سويات مختلفة من التحكم في النفاذ معرّفة من أجل الوفاء بالمتطلبات آنفة الذكر. وبالنسبة إلى عمليات الإدارة فإن أحكام التوصية تحدد قيود النفاذ في سويات متعددة وهي: الكيان الخاضع للإدارة ككل، والنعوت المنسوبة إلى الكيان، وقيم النعوت، وسياق النفاذ، والإجراءات إزاء الكيان. وقد حُدد عدد من المخططات، مثل قائمة التحكم في النفاذ على أساس المقدرة أو الوسم أو السياق، ويمكن لسياسة تحكم في النفاذ أن تطبق واحداً أو أكثر من هذه المخططات. وفي هذا النموذج، القائم على أساس السياسة ومعلومات التحكم في النفاذ (ACI)، يُتخذ القرار بالسماح بإجراء العملية المطلوبة أم خلاف ذلك. وتشمل معلومات التحكم في النفاذ مثلاً القواعد وهوية الجهة التي تستهل العملية وهويات الجهات المقصودة المطلوب النفاذ إليها والمعلومات المتصلة بالاستيقان من الجهة مستهلة العملية، وما إلى ذلك. والنموذج غني جداً بالإمكانات وقد لا تكون كل المقدرات مطلوبة في أي تطبيق بعينه.

4.5.4.6 خدمات الأمن القائمة على أساس معمارية وسيط مشترك لطلب غرض (CORBA): ولئن كانت توصيات السلسلة X.700 تفترض استخدام بروتوكول معلومات الإدارة المشتركة (CMIP) بوصفه بروتوكول السطح البيني للإدارة فإن هنالك اتجاهات أخرى في دوائر الصناعة قد شرعت في استخدام بروتوكول يقوم على أساس معمارية وسيط مشترك لطلب غرض وما يتصل بها من خدمات ونماذج أغراض للسطوح البينية للإدارة. وتحدد التوصية ITU-T Q.816 إطاراً لاستعمال هذه الخدمات في سياق السطوح البينية للإدارة. وللقيام بمتطلبات الأمن لهذه السطوح البينية فإن هذه التوصية تشير إلى المواصفة التي وضعها فريق إدارة الأغراض (OMG) للخدمات المشتركة من أجل الأمن.

5.6 الوصفات الطبية الإلكترونية

يتطلب توفير الرعاية الصحية ويولّد مجموعة واسعة متنوعة من البيانات والمعلومات، ويحتاج الأمر إلى جمع هذه البيانات والمعلومات ومعالجتها وتوزيعها والنفاذ إليها واستخدامها، كل ذلك بشكل آمن يتمسك باحترام للقواعد الأخلاقية والتشريعية. ويتسم هذا بأهمية حيوية بصورة خاصة بالنسبة للمعلومات الإكلينيكية والإدارية، فضلاً عن أهميته لأنواع أخرى من المعلومات مثل معلومات قواعد البيانات الخاصة بالأوبئة والأدبيات والمعارف الأخرى.

وتقع مصادر هذه الأنواع من البيانات والمعلومات داخل البنية التحتية للرعاية الصحية وخارجها، وعلى مسافات متفاوتة من مستعمليها. وفي واقع الممارسة يتطلب المستعملون ويولدون مزيجاً من أنواع المعلومات هذه وفي مراحل مختلفة في وظائفهم، كأن يستشير طبيب ما قاعدة معارف بينما يقوم بفحص مريض ويُدخل معلومة ذات صلة في سجل المريض، وقد تستخدم هذه المعلومة في أغراض الفوترة.

واللقاءات والمعاملات المرتبطة بالرعاية الصحية متعددة الأوجه. فهي تحدث مثلاً بين مريض وطبيب؛ أو بين طبيبين؛ أو بين طبيب وخبير استشاري؛ أو بين مريض ومؤسسة صحية، كمختبر أو صيدلية أو مركز إعادة تأهيل. ويمكن أن تحدث هذه اللقاءات في مجتمع أو في جزء آخر من البلاد أو في الخارج. وجميع هذه اللقاءات تتطلب بيانات ومعلومات قبل أن تبدأ فعلاً كما أنها تولّد بيانات ومعلومات خلال اللقاء أو بعده مباشرة. وقد تكون هذه البيانات والمعلومات بأحجام مختلفة وفي أوقات مختلفة وفي أشكال مختلفة مثل الصوت والأرقام والنصوص والرسوم البيانية والصور الساكنة أو الدينامية، وغالباً ما تكون مزيجاً حصيفاً من كل ذلك.

وقد تنتشر مصادر ومخازن هذه البيانات والمعلومات في أماكن مختلفة وتتخذ أشكالاً مختلفة، مثل السجلات الكاملة للمرضى والوصفات الطبية بخط اليد وتقارير من طبيب أو خبير استشاري أو مختبر.

وفي الماضي، كانت جميع هذه اللقاءات تتم وجهاً لوجه، وكان الكلام والكتابة الأسلوبين الرئيسيين للاتصالات والاحتفاظ بالسجلات الطبية، أما عملية الانتقال فكانت تتم أساساً بواسطة الخدمات العامة والخاصة باستخدام الطرق البرية أو السكك الحديدية أو الطائرات. وعندما نمت شبكات الخدمات الهاتفية أصبحت شبكات الاتصالات وسيلة الاتصال بين المهنيين والمؤسسات الصحية، وطنياً ودولياً، إلى أن ظهرت الأدوات الحديثة لاستخدام التليماتية في مجال الصحة واتسع انتشارها.

وقد اتسع نطاق استخدامات التكنولوجيا بشكل مطرد في الجوانب الإكلينيكية/الطبية لخدمات الرعاية الصحية وشمل الأجهزة والمعدات، ولا سيما معدات الاستشعار والقياس وخدمات المختبرات والتصوير الساكن والدينامي. وإزاء نمو استخدامات هذه التكنولوجيات وتنوعها وتطورها، بات محتوماً أن تنفصل هذه الخدمات التكنولوجية عن صلب مؤسسات الرعاية الصحية، سواء من حيث المسافة أم من حيث الإدارة، وهذا هو الأهم. ولذلك، أصبحت الاتصالات بين هذه الخدمات القائمة على التكنولوجيا والخدمات المعهودة في مجال الرعاية الصحية من الاعتبارات الهامة في كفاءة هذه الخدمات واقتصادها.

وقد بدأ استخدام تكنولوجيا المعلومات والاتصالات في قطاع الصحة ينتشر منذ أكثر من 25 عاماً عن طريق المراسلات الإلكترونية البسيطة (البريد الإلكتروني) التي كانت تحمل مجرد مذكرات وتقارير ألفبائية رقمية. ومثلما كانت الاتصالات الصوتية الدافع الرئيسي لتركيب الهواتف في عيادات الأطباء ومؤسسات الرعاية الصحية، كان البريد الإلكتروني المبرر الرئيسي الأول لتركيب وصلات الاتصالات الحديثة. وبازدياد خدمات البريد الإلكتروني، ازدادت المطالبة بأداء مرتفع وزيادة تغطيتها الجغرافية: زيادة في عدد المواقع التي تتاح فيها هذه الخدمة بمزيد من السرعة وزيادة في عرض النطاق لمواجهة الزيادة في عدد مرفقات رسائل البريد الإلكتروني. وقد شهدت السنوات العشر الأخيرة نمواً مطرداً أضعافاً مضاعفة في استخدامات البريد الإلكتروني في قطاع الصحة في داخل البلدان وفيما بينها، حتى في أفقر البلدان، ولا سيما

عبر الإنترنت. فقد أصبحت المعاملات الإلكترونية مثلاً تحل محل الوظائف التي لا تتطلب المقابلة وجهاً لوجه، مثل إعداد الوصفات الطبية والتقارير وإرسالها، وتحديد مواعيد الاستشارة والخدمات، وإحالة المرضى، وكذلك حيثما كان أداء خدمات الاتصالات ملائماً، إرسال الصور الطبية وقراءات الخبراء المصاحبة لها، سواء كانت مكتوبة أم شفهية.

وثمة مستوى آخر في تطور استخدامات تكنولوجيا المعلومات والاتصالات هو ممارسة الطب عن بُعد، وهو "توفير الرعاية الطبية باستخدام الاتصالات الصوتية والمرئية والبيانات"، بما في ذلك التشخيص الفعلي والفحص وحتى العناية بالمريض الكائن في بقعة نائية. والطب عن بعد مجال هام ومتزايد الاتساع، ومن المتوقع أن يؤدي إلى تغيير مناهج تقليدية كثيرة في مجال الرعاية الصحية، بل إنه بداية لنموذج جديد في الرعاية الطبية.

وهنالك مجال آخر ليس حديث العهد نسبياً ولكنه يزداد اتساعاً بشكل مفيد بفضل انتشار التليماتية هو النفاذ إلى الأنظمة القائمة على المعرفة واستخدامها. وهذه الأنظمة، المعروفة أيضاً باسم الأنظمة الخبيرة وأنظمة دعم اتخاذ القرارات، هي أنظمة توفر المشورة المتخصصة والتوجيه بشأن المسائل والإجراءات الطبية العلمية. فإذا توفرت مثلاً المعلومات الخاصة بمريض ما والأعراض التي يعاني منها، يمكن لهذه الأنظمة أن تدعم عملية التشخيص وأن تقترح إجراء اختبارات إضافية أو أن تقترح علاجاً.

وجميع هذه التطورات لها تأثير كبير أيضاً على أنظمة معلومات الإدارة ذات الصلة المطلوبة والمستخدمة في قطاع الصحة، مثل أنظمة معلومات الإدارة في المستشفيات. وهذه ليست مجرد أنظمة لإدارة شؤون رعاية المرضى في المستشفى منذ الدخول إليها حتى الخروج منها أو الإحالة إلى غيرها ولكنها تشمل عدداً كبيراً من السطوح البينية الذكية ميسورة الاستعمال من قبل العاملين الطبيين للتفاعل مثلاً مع أنظمة دعم اتخاذ القرارات الإكلينيكية، ووصلات الطب عن بعد، وبوابات مواقع الويب، وما إلى ذلك.

ولا بد من ذكر مسألتين أخريين من واقع عمل موظفي الرعاية الصحية والمرضى وهما: قدرتهم على الحركة وحاجتهم إلى حرية استعمال اليدين، ومن ثم التركيز على الرعاية الطبية نفسها. وتعني القدرة على الحركة إمكانية حصولهم على المعلومات الطبية المطلوبة، مثل السجل الإلكتروني للمريض، أو الحصول على آلة أو أداة، من أي مكان بعيد وحيثما تدعو الحاجة رهناً بإمكانية التحقق منها، في مبنى أو مدينة، وكذلك داخل البلدان وفيما بينها. وتعني حرية استعمال اليدين ضرورة إيجاد حلول لتعرف الهوية والترخيص بالنفاذ لا تتطلب قيام المسؤول الطبي بتدخل يدوي، مثل فتح باب أو استعمال لوحة مفاتيح الحاسوب.

وهكذا، فإن الرعاية الصحية قطاع كثيف المعلومات إلى حد بعيد حيث يكون جمع البيانات والمعلومات الصحية والمتصلة بالصحة وتدفقها ومعالجتها وعرضها وتوزيعها من المقتضيات الأساسية لتحقيق الكفاءة والفعالية والاقتصاد في عمليات خدمات الرعاية الصحية وفي تطويرها داخل البلد وفيما بين البلدان.

والاشتراط الأساسي الحاسم هو أن تتحقق جميع هذه التدفقات بطريقة آمنة وسرية، مع الالتزام الصارم بالقواعد واللوائح الأخلاقية والقانونية.

1.5.6 اعتبارات البنية التحتية للمفاتيح العمومية (PKI) والبنية التحتية لإدارة الامتيازات (PMI) في تطبيقات الصحة الإلكترونية

تقوم البنية التحتية للمفاتيح العمومية (PKI) من خلال تسلسل سلطات إصدار الشهادات باستحداث بنية تراتبية للعالم الواقع، سواء كان تراتباً من حيث الجغرافيا السياسية (أقاليم – بلدان – دول – مواقع) أو من حيث الموضوع (صحة – طب – جراحة – جراحة متخصصة – جهات توريد، وغيرها). وفضلاً عن ذلك، وبما أن قطاع الصحة منتشر في كل مكان في آن واحد وبما أنه تراتبي بعيد الأثر ويتفاعل بشكل متزايد عبر الحدود، فإن وضع تعريف قياسي للبنية التحتية للمفاتيح العمومية والبنية التحتية لإدارة الامتيازات (PMI) في مجال الصحة قد أصبح ضرورة واضحة.

ويتعين ضمان قابلية التشغيل البيني التقني للأنظمة الصحية من خلال الاستخدام المكثف لمعايير التكنولوجيا. وقد اعتمد معظم جهات توفير الحلول الخاصة بالأمن معايير مثل معايير التوصية ITU-T X.509. ولما كان الاستيقان من المستعمل من التطبيقات شديدة الأهمية التي تعتمد على المعلومات المحلية فإن حرية اختيار بنية تحتية ما للمفاتيح العمومية (PKI) وبنية تحتية لإدارة الامتيازات (PMI) ينبغي ألا تؤثر على قدرة المستعمل على التشغيل البيني مع أشخاص تحققت منهم توليفة أخرى من PMI/PKI في قطاع الصحة (الأمر الذي يمتد طبعاً إلى ما لا يقل عن حد أدنى من التقييس فيما يتعلق

بالتحكم في النفاذ والسياسات الأخرى ذات العلاقة بقطاع الصحة). ولتحقيق ذلك، يمكن وضع استراتيجيات مختلفة قد تشمل الاعتراف المتبادل بالبنى التحتية المختلفة أو استخدام جذر مشترك. ومن شأن اعتماد معايير تكنولوجيا وإمكانية التشغيل البيني من الناحية التقنية للبنى التحتية المختلفة وتقييس سياسات معينة أن يضمن قيام بيئة كاملة الكفاءة ومتكاملة لمعاملات الصحة في جميع أنحاء العالم.

2.5.6 نظام سالفورد للوصفات الطبية الإلكترونية

إن نظام الوصفات الطبية الإلكترونية الموصوف في [*Policy*] مثال جيد على تطبيق البنية التحتية للمفاتيح العمومية (PKI) والبنية التحتية لإدارة الامتيازات (PMI) في مجال الصحة الإلكترونية. ونظراً لضخامة عدد المهنيين الذين يعملون في برنامج الإرسال الإلكتروني للوصفات الطبية (ETP) في المملكة المتحدة (500 34 طبيب و000 10 ممرض وممرضة يحق لهم وصف الأدوية سيرتفع عددهم إلى 000 120 خلال السنوات القليلة القادمة و000 44 صيدلي مسجل و000 22 طبيب أسنان) وضآلة عدد التراخيص المطلوبة حالياً (أي مختلف مستويات الترخيص لوصف العلاج وصرف الدواء واستحقاق الحصول على الوصفات الطبية المجانية)، يبدو أن التحكم في النفاذ القائم على الدور (RBAC) هو آلية الترخيص المثلى للاستخدام في الإرسال الإلكتروني للوصفات الطبية (ETP). وعندما يقترن ذلك بعدد المرضى المحتملين في المملكة المتحدة (60 مليوناً)، وبأن الوصفات الطبية المجانية [*FreePresc*] تمثل نسبة 85 في المائة من الوصفات الطبية، عندئذ ينبغي استخدام التحكم في النفاذ القائم على الدور (RBAC) أيضاً للتحكم في النفاذ إلى الوصفات الطبية المجانية إذا كان ذلك ممكناً. ونظراً لضخامة عدد الأشخاص الذين يتعين الترخيص لهم وأولئك ذوي الاستحقاق فمن الضروري توزيع إدارة الأدوار على السلطات المختصة بدلاً من محاولة إخضاعها لسلطة مركزية، وإلا سيكون من المتعذر إدارة النظام.

ولكل مهني هيئة رسمية تمنحه حق ممارسة المهنة. والمجلس الطبي العام في المملكة المتحدة هو المسؤول عن تسجيل الأطباء وشطبهم من قائمة الأطباء في حالة الإخلال بآداب المهنة. ويؤدي مجلس أطباء الأسنان العام نفس الدور لأطباء الأسنان، ويهتم مجلس التمريض والقبالة بالممرضين والممرضات والكلية الملكية للصيدلة بالصيادلة. وفي نظام الإرسال الإلكتروني للوصفات الطبية (ETP) المذكور، يكون تخصيص الأدوار شأن تلك الهيئات، لأنها وظيفة تؤديها أصلاً على ما يرام.

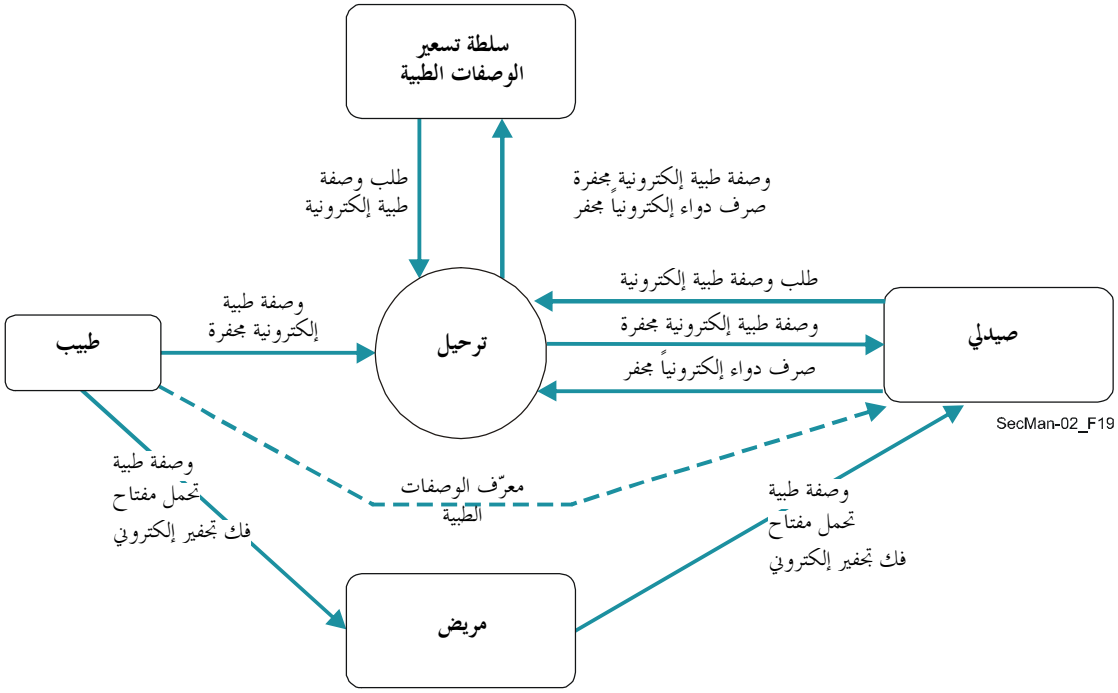
وقد تولت إدارة العمل والمعاشات التقاعدية (DWP) التي أنشئت في يونيو 2001، مسؤوليات الإدارتين السابقتين اللتين كانتا معنيتين بالضمان الاجتماعي وبالتعليم والعمالة. وهي مسؤولة عن دفع إعانات البطالة والمعاشات التقاعدية، كما أنها – بالإضافة إلى سلطة تسعير الوصفات الطبية (PPA) – مسؤولة أيضاً عن تحديد استحقاق الوصفات الطبية المجانية. ويستحق عدد كبير من الأشخاص الوصفات الطبية المجانية، ومنهم كل من تجاوز الستين والأطفال دون سن 16 سنة والشباب الذين تبلغ أعمارهم 16 أو 17 أو 18 سنة من المتفرغين للدراسة، ومن يتلقى هو أو شريكه دعماً للدخل أو إعانة للبحث عن عمل، ومن لديه شهادة المساعدة الكاملة لذوي الدخل المنخفض ضمن نظام الصحة الوطنية (NHS) الحالي، والحوامل والنساء اللاتي وضعن خلال الاثني عشر شهراً الماضية، والمتقاعدون المعوقون بسبب الحرب. وبناء على ذلك، توزع الإدارة هذه المستحقات بين مختلف فروع إدارة العمل والمعاشات التقاعدية وسلطة تسعير الوصفات الطبية.

وتخصص كل هيئة مهنية لكل مهني شهادة بالدور الذي يقوم به، وتخزن هذه الشهادات في دليل بروتوكول النفاذ السريع (LDAP) التابع لتلك الهيئة المهنية. وبوسع نظام الإرسال الإلكتروني للوصفات الطبية (ETP) اتخاذ قرارات بالترخيص بوصف العلاج وصرف الدواء إذا كان يستطيع النفاذ إلى أدلة بروتوكول النفاذ السريع. وبالمثل، فإذا خصصت إدارة العمل والمعاشات التقاعدية شهادات أدوار للأشخاص الذين يحق لهم الحصول على وصفات طبية مجانية لأسباب مختلفة، وخزنت هذه الشهادات في دليل (أو أدلة) بروتوكول النفاذ السريع، فسوف يتمكن النظام ETP من اتخاذ قرارات بشأن استحقاق الوصفات الطبية المجانية بواسطة النفاذ إلى دليل بروتوكول النفاذ السريع دون أن يحتاج الصيدلي إلى أن يسأل المريض ما إذا كان يستحق ذلك. وقد لا يحتاج الأمر إلى ذلك سوى في الحالات التي يصبح فيها المريض مستحقاً مؤخراً، عندما يُشخص الطبيب مثلاً أن امرأة حامل و لم يكن لدى إدارة العمل والمعاشات التقاعدية الوقت الكافي لإنشاء شهادة رسمية بذلك.

وتُستخدم هذه الأدوار فيما بعد في محرك اتخاذ قرار الترخيص (مثل PERMIS، انظر www.permis.org) لتقرير ما إذا كان الأطباء يُسمح لهم بوصف العلاج والصيادلة بصرف الدواء والمرضى بتلقي الوصفات الطبية مجاناً، طبقاً لسياسة الإرسال الإلكتروني للوصفات الطبية (ETP). ويقوم كل تطبيق في النظام ETP (نظام وصف العلاج ونظام صرف الدواء ونظام سلطة تسعير الوصفات الطبية) بقراءة سياسة النظام ETP في مرحلة تحديد المعلمات، وعندما يطلب مهني ما إجراءات مثل وصف علاج أو صرف دواء، يقوم محرك اتخاذ قرار الترخيص باستحضار دور كل شخص من

دليل بروتوكول النفاذ السريع (LDAP) الملائم، ويتخذ قراره طبقاً للسياسة المرعية. ومن ثم يمكن للمستعملين النفاذ إلى تطبيقات متعددة، وكل ما يحتاجونه هو زوج من مفاتيح البنية التحتية للمفاتيح العمومية (PKI). ويمكن إصدار شهادات الأدوار دون اشتراك المستعمل الذي لا يهمه كيف أو أين يجري تخزينها واستخدامها من قبل النظام.

يحتوي الشكل 6-15 على مثال لتنفيذ نظام الوصفات الطبية الإلكترونية في المملكة المتحدة، ويوضح العديد من مسائل الأمن الرئيسية المرتبطة بتنفيذها. وفي قلب النظام بنية تحتية للأمن لا توفر الاستيقان القوي فحسب (أي بنية تحتية للمفاتيح العمومية (PKI) باستخدام شهادات مفاتيح عمومية)، بل توفر أيضاً ترخيصاً قوياً (أي بنية تحتية لإدارة الامتيازات (PMI)) تمنح فيها الحقوق المحددة التي يتمتع بها المهنيون الطبيون بحكم أدوارهم المختزنة في شهادات الأدوار. وتستخدم النماذج التقليدية قوائم تحكم في النفاذ مبينة في كل تطبيق (مثل السجلات الطبية، وقواعد بيانات الوصفات الطبية، والتأمين، وما إلى ذلك)، وهي تتطلب من المستعملين (الأطباء والصيادلة والمرضى وغيرهم) الحصول على العديد من مختلف علامات الأمن وإدارتها (مثل اسم المستعمل/كلمات السر، والبطاقات، وغيرها). وفي النموذج الجديد الذي يضم البنية التحتية للمفاتيح العمومية (PKI) والبنية التحتية لإدارة الامتيازات (PMI)، يحتاج المستعمل إلى مجرد علامة واحدة – هي شهادة المفتاح العمومي للمستعمل – للاستفادة من مختلف الخدمات والموارد الموزعة جغرافياً و/أو طوبولوجياً. ويحتفظ بشهادات الأدوار الخاصة بالمستعمل داخل النظام وليس لدى المستعمل، وتنتقل هذه الشهادات بين المكونات حسبما يكون ملائماً لتوفير النفاذ. وبما أن شهادات الأدوار موقعة رقمياً من قِبل الجهات التي تُصدرها، فلا يمكن التلاعب فيها خلال عمليات الانتقال هذه.



الشكل 6-15 – نظام سالفورد للوصفات الطبية الإلكترونية

وفي المثال المبين في الشكل 6-15، يستحدث الطبيب الوصفة الطبية الإلكترونية ويوقع عليها رقمياً (لأغراض الاستيقان)، وبعدئذ تجفر تناظرياً باستخدام مفتاح دورة عشوائي (لضمان السرية) ثم تُرسَل إلى مكان التخزين المركزي. وتُعطى للمريض وصفة طبية ورقية تحتوي على شفرة قضبانية تحمل مفتاح تجفير تناظري. ثم يذهب المريض إلى الصيدلية التي يختارها ويقدم الوصفة الطبية، ويقوم الصيدلي بمسح الشفرة القضبانية ثم يستجلب الوصفة الطبية ويفك تجفيرها. ويقرر المريض في النهاية الجهة المرخص لها بصرف دواء وصفته الطبية، كما هو الحال في نظام الوصفة الطبية الورقية الحالي. إلا أن هذا لا يكفي، إذ من الضروري أيضاً التحقق من الجهة المرخص لها بوصف العلاج، وصرف أي أنواع من الأدوية، ومن يحق له الحصول على وصفات طبية مجانية.

ومع أن الوصف الوارد أعلاه يشير إلى نظام متكامل بإحكام فهو قابل بالفعل للتوزيع، بحيث يكون دليل أدوار الطبيب مختلفاً عن النظام المستخدم في الاستيقان من الصيادلة، أو النظام الذي يقوم بتخزين حقوق وسياسات صرف الأدوية،

وما إلى ذلك، وهو نظام يعتمد على أطراف أخرى موثوق بها للاستيقان من مختلف الأطراف والترخيص لها. وعلى الرغم من إمكانية تطبيق حلول غير قياسية في البنية التحتية للمفاتيح العمومية (PKI) والبنية التحتية لإدارة الامتيازات (PMI)، فإن استخدام حلول قياسية مثل الحلول التي تنطوي عليها التوصية ITU-T X.509 تمكن اليوم من تحقيق نفاذ أعم وأوسع إلى الوصفات الطبية الإلكترونية.

6.6 اتصالات بيانات متنقلة آمنة من طرف إلى طرف

لقد جرى توزيع المطاريف المتنقلة التي تنطوي على مقدرات اتصالات البيانات (ومنها الهاتف المتنقل في نظام IMT-2000 أو الحاسوب الشخصي المحمول أو المساعد الرقمي المحمول المجهزة ببطاقة راديوية) على نطاق واسع وبدأ يظهر توفير خدمات مختلف التطبيقات (ومنها مثلاً التجارة الإلكترونية المتنقلة) للمطاريف المتنقلة الموصولة بالشبكة المتنقلة. وفي بيئة التجارة الإلكترونية مسألة الأمن مسألة ضرورية، بل حيوية.

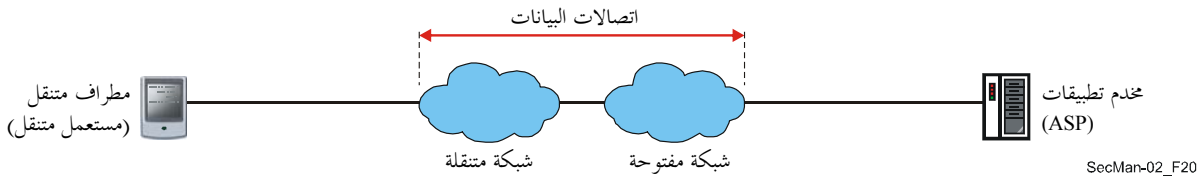
وهنالك العديد من مجالات الأمن قيد الدراسة من وجهة نظر مشغّل الخدمة المتنقلة (من ذلك مثلاً معمارية الأمن من أجل شبكة الهاتف المتنقلة IMT-2000). ولكن من الضروري أيضاً دراسة المسألة من وجهة نظر المستعمل المتنقل ومن وجهة نظر مقدم خدمات التطبيقات (ASP).

ولدى دراسة مسألة الأمن في الاتصالات المتنقلة ومن وجهة نظر كل من المستعمل المتنقل ومقدم خدمات التطبيقات فإن جانب الأمن في اتصالات البيانات المتنقلة من طرف إلى طرف بين المطراف المتنقل ومخدم ما من مخدم التطبيقات هو واحد من أكثر الجوانب أهمية.

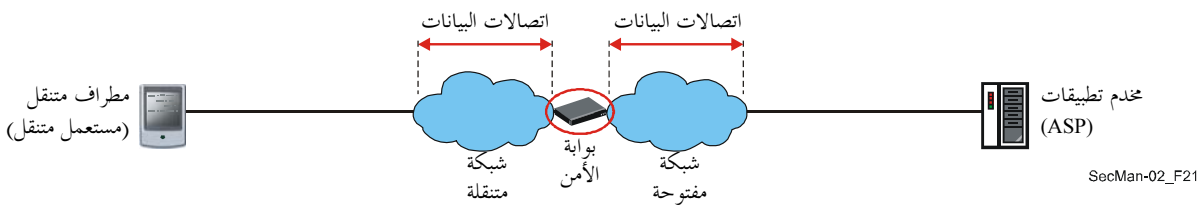
وعلاوة على ذلك، فإن دراسة الأمن، بالنسبة إلى النظام المتنقل الذي يصل شبكة متنقلة بشبكة مفتوحة، في الطبقات الأعلى (طبقات التطبيقات والتقديم والجلسات) في النموذج المرجعي في التوصيل البيني للأنظمة المفتوحة (OSI) ضرورية لأن هنالك عمليات تنفيذ ممكنة بالنسبة إلى الشبكات المتنقلة (من قبيل شبكة الهاتف المتنقلة IMT-2000 وشبكة المنطقة المحلية اللاسلكية ومواصفة "بلوتوث" لشبكات المنطقة الشخصية) أو إلى الشبكات المفتوحة.

1.6.6 هيكلية تكنولوجيات الأمن لاتصالات البيانات المتنقلة من طرف إلى طرف

تصف التوصية ITU-T X.1121 نماذج لاتصالات البيانات المتنقلة من طرف إلى طرف بين المطاريف المتنقلة ومخدمات التطبيقات في الطبقات الأعلى. ويحدد نمطان من نماذج الأمن من أجل هيكلية أمن لاتصالات البيانات المتنقلة من طرف إلى طرف بين مستعمل متنقل ومقدم خدمات تطبيقات (ASP) وهما: نموذج عام ونموذج بوابة. ويعمد المستعمل المتنقل إلى استخدام المطراف المتنقل للنفاذ إلى مختلف الخدمات المتنقلة الآتية من مقدمي خدمات التطبيقات. ويقوم مقدم هذه الخدمات بتوفير خدمة متنقلة إلى المستعملين المتنقلين من خلال مخدم تطبيقات. وتقوم بوابة الأمن المتنقلة بترحيل الرزم من المطاريف المتنقلة إلى مخدم التطبيقات، وتقوم بتحويل بروتوكول اتصالات متنقلة قائم على شبكة إلى بروتوكول مفتوح قائم على شبكة، والعكس بالعكس.

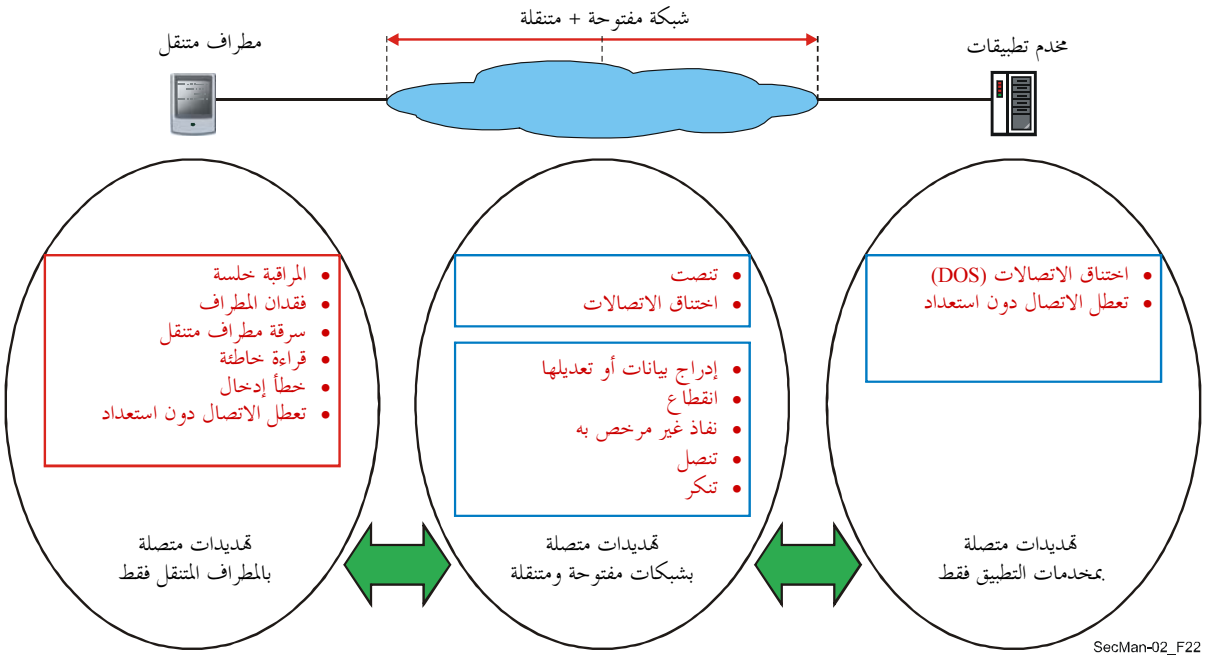


الشكل 6-16 – نموذج عام لاتصالات بيانات من طرف إلى طرف بين مستعمل ومخدم تطبيقات



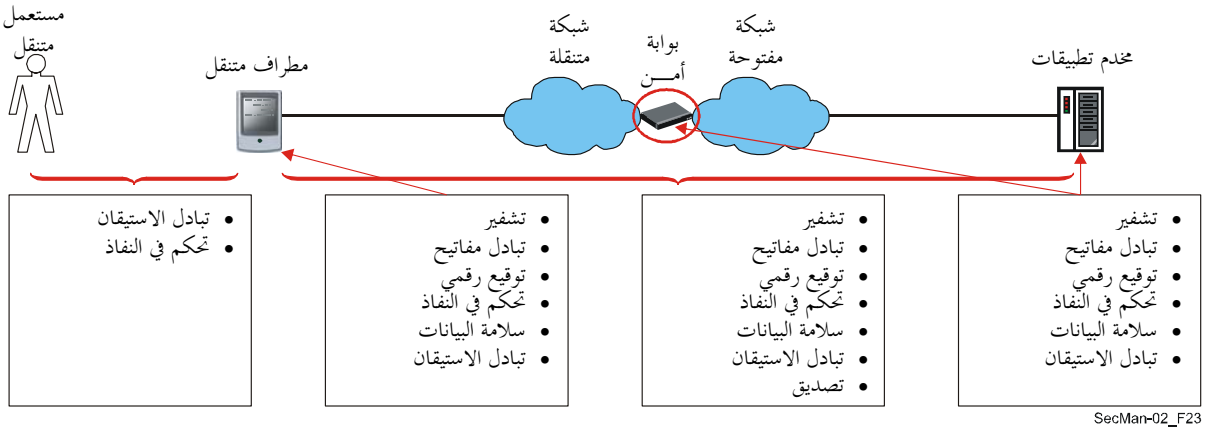
الشكل 6-17 – نموذج بوابة لاتصالات بيانات متنقلة من طرف إلى طرف بين مستعمل ومخدم تطبيقات

وتصف التوصية ITU-T X.1121 أيضاً تهديدات الأمن إزاء اتصالات بيانات متنقلة من طرف إلى طرف ومتطلبات الأمن من وجهة نظر كل من المستعمل المتنقل ومقدم خدمات التطبيقات (ASP) في كلا النموذجين. وهنالك نمطان من التهديدات: نمط عام موجود في أي شبكة مفتوحة ونمط آخر محدد من تهديدات الأمن متنقلة التوجه. ويصور الشكل 18-6 التهديدات في شبكة اتصالات بيانات متنقلة من طرف إلى طرف.



الشكل 6-18 – التهديدات في الاتصالات المتنقلة من طرف إلى طرف

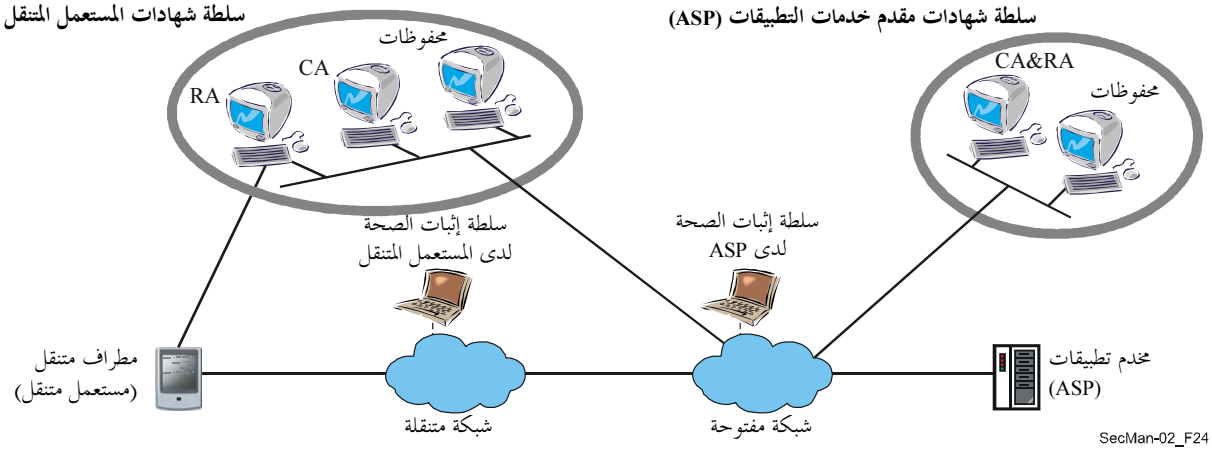
علاوة على ذلك، تحدد التوصية ITU-T X.1121 الأماكن حيث تنفذ تكنولوجيات الأمن، عند الاقتضاء، لكل كيان والعلاقة بين الكيانات في اتصال بيانات متنقلة من طرف إلى طرف (انظر الشكل 6-19).



الشكل 6-19 – وظيفة الأمن المطلوبة لكل كيان والعلاقة بين الكيانات

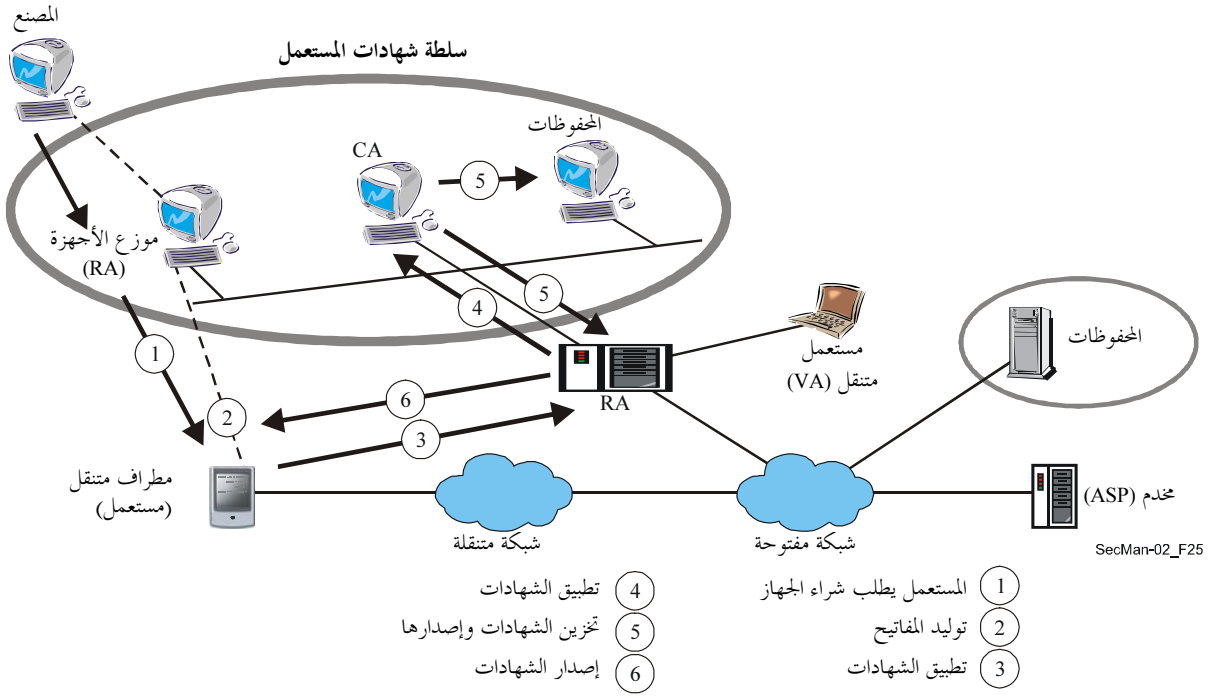
2.6.6 اعتبارات البنية التحتية للمفاتيح العمومية (PKI) من أجل اتصالات بيانات متنقلة آمنة من طرف إلى طرف

يتناول هذا القسم التوصية ITU-T X.1122. وعلى الرغم من أن تكنولوجيا PKI تكنولوجيا مفيدة جداً في حماية اتصالات البيانات المتنقلة من طرف إلى طرف فإن بعض الخصائص التي تتسم بها تحديداً اتصالات البيانات المتنقلة قد تتطلب تكييف تكنولوجيا PKI لدى بناء أنظمة متنقلة آمنة. وقد حدد نمطان من نماذج PKI لتوفير خدمات أمن في الاتصالات المتنقلة من طرف إلى طرف. ويتصل أحدهما بنموذج PKI عام حيث لا تتوفر وظيفة بوابة أمن في اتصالات بيانات متنقلة من طرف إلى طرف، أما الآخر فيتصل بنموذج PKI له بوابة، حيث هنالك بوابة أمن بمثابة سطح بيني تتوسط الشبكة المتنقلة والشبكة المفتوحة. ويصور الشكل 6-20 نموذج PKI العام من أجل الاتصالات المتنقلة من طرف إلى طرف. ويشمل هذا النموذج أربعة كيانات. وتصدر سلطة الشهادات (CA) لدى المستعمل المتنقل شهادة لذلك المستعمل وتقوم بإدارة مكان المحفوظات التي تخزن فيها قائمة إبطال الشهادات (CRL) التي سبق أن أصدرتها سلطة الشهادات لدى المستعمل. وتوفر سلطة إثبات الصحة (VA) لدى المستعمل المتنقل خدمة إثبات صحة شهادات على الخط لذلك المستعمل. وتصدر سلطة الشهادات (CA) لدى مقدم خدمات التطبيقات (ASP) شهادة لذلك المقدم وتقوم بإدارة مكان المحفوظات التي تخزن فيها قائمة إبطال الشهادات التي سبق أن أصدرتها سلطة الشهادات لدى المقدم. وتوفر سلطة إثبات الصحة (VA) لدى المقدم (ASP) خدمة إثبات صحة شهادات على الخط لذلك المقدم.



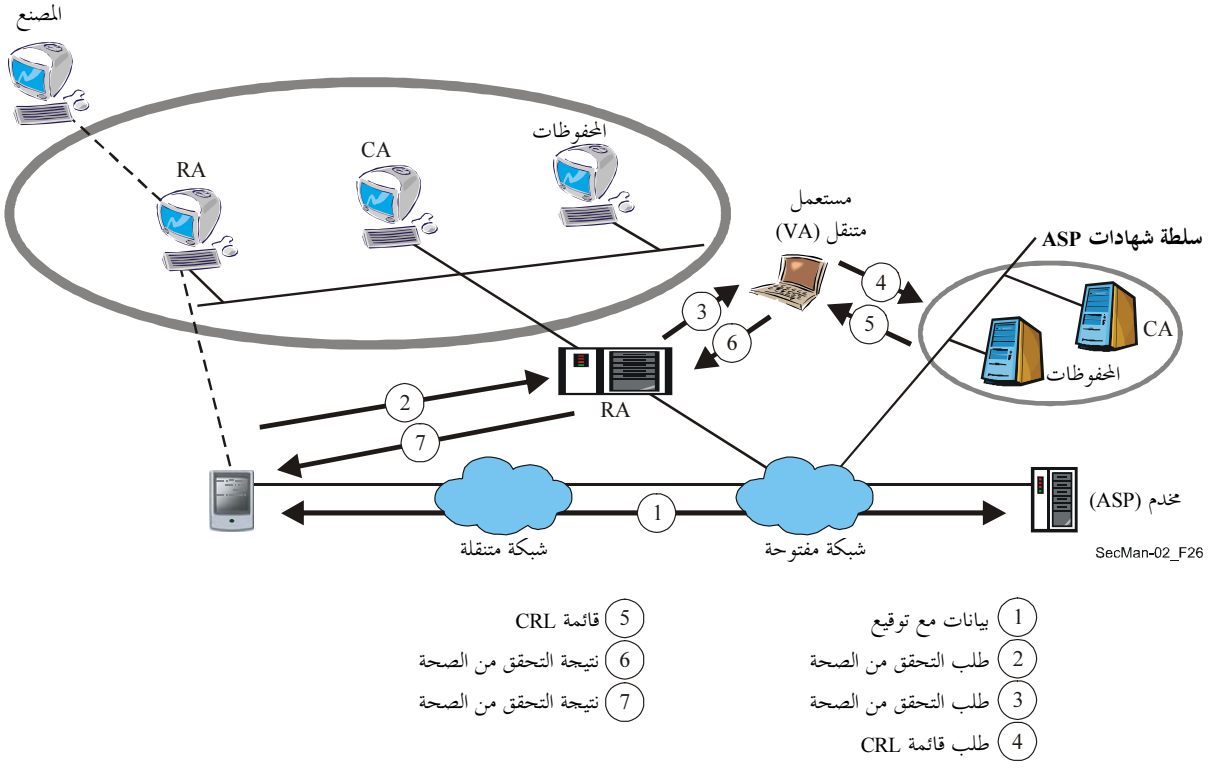
الشكل 6-20 – نموذج PKI عام لاتصالات بيانات متنقلة من طرف إلى طرف

هنالك طريقتان لإصدار الشهادات تبعاً لموقع توليد المفتاح العمومي/الخاص. في الطريقة الأولى يتولد زوج المفاتيح المجفرة ويستحدث في مصنع المطراف المتنقل، أما في الطريقة الثانية فيتولد زوج المفاتيح المجفرة في المطراف المتنقل أو في العلامة المصونة من التلاعب كالبطاقة الذكية المتصلة بالمطراف المتنقل. ويصور الشكل 6-21 الإجراءات التي يتّبعها المطراف المتنقل للحصول على الشهادة باستعمال إجراءات إدارة الشهادات حيث يتولد زوج المفاتيح المجفرة في المطراف المتنقل.



الشكل 6-21 – إجراءات إصدار الشهادات للمطراف المتنقل

يتمتع المطراف المتنقل بقدرة حوسبة محدودة وذاكرة محدودة. ونتيجة لذلك يُفضل مخطط إثبات صحة الشهادات على الخط على مخطط إثبات صحة الشهادات خارج الخط الذي يقوم على أساس قائمة إبطال الشهادات (CRL). وعندما يتلقى المطراف المتنقل زوج توقيع الرسالة مع سلسلة الشهادة ويريد التحقق من صلاحية التوقيع ينبغي استعمال الشهادة بعد التحقق من صلاحيتها باستعمال مخطط إثبات صحة الشهادات. ويصور الشكل 6-22 إجراءات إثبات صحة الشهادات خارج الخط بالنسبة إلى المطراف المتنقل.



الشكل 6-22 – إجراءات التحقق من الشهادات من أجل اتصالات البيانات المتنقلة من طرف إلى طرف

يمكن استعمال نظام البنية التحتية للمفاتيح العمومية PKI لاتصال متنقل من طرف إلى طرف من أجل توفير نموذجين من نماذج الاستعمال: يمكن استعمال أحدهما من أجل طبقة الجلسات ويمكن استعمال الآخر من أجل طبقة التطبيقات. ويوفر نموذج استعمال طبقة الجلسات خدمات أمن من قبيل الاستيقان من الزبون والاستيقان من المخدم وخدمة السرّية وخدمة السلامة. ويوفر نموذج استعمال طبقة التطبيقات خدمة عدم التنصل وخدمة السريّة لاتصال بيانات متنقلة من طرف إلى طرف.

وختاماً فإن التوصية ITU-T X.1122 تصف اعتبارات من أجل بناء أنظمة متنقلة آمنة تقوم على أساس البنية التحتية للمفاتيح العمومية PKI من وجهة النظر التالية: إمكانية التشغيل البيني مع نظام قائم على أساس البنية التحتية PKI في شبكة مفتوحة، واستعمال البنية التحتية PKI في البيئة المتنقلة (بما في ذلك مسائل توليد المفاتيح ومسائل طلب الشهادات وإصدارها ومسائل استعمال الشهادات ومسائل سلطات الشهادات) والبنية التحتية PKI عموماً (بما في ذلك مسائل إدارة دورة حياة الشهادة). ويمكن أن تستعمل بمثابة مبادئ توجيهية لدى بناء أنظمة متنقلة آمنة تقوم على أساس تكنولوجيا PKI.

7 بُعد التيسر وطبقة البنية التحتية

تشير التوصية ITU-T X.805 التي تناولها القسم 2 إلى:

- أبعاد الأمن كمجموعة من تدابير الأمن المصممة لكي تتناول جانباً محدداً من جوانب أمن الشبكة؛
- طبقات الأمن. تطبق أبعاد الأمن على هيكلية متراتبة من تجهيزات الشبكة وتجميعات مرافقها، والتي يشار إليها باسم طبقات الأمن.

ويضمن بُعد أمن التيسر أن ليس هناك من رفض للنفاذ المرخص له إلى عناصر الشبكة والمعلومات المختزنة وتدفقات المعلومات والخدمات والتطبيقات بسبب أحداث تؤثر على الشبكة. وتندرج في هذه الفئة حلول إعادة الأمور إلى نصابها بعد كارثة ما.

وتتألف طبقة أمن البنية التحتية من مرافق الإرسال في الشبكة وكذلك من عناصر إفرادية في الشبكة تحميها أبعاد الأمن. وتمثل طبقة البنية التحتية لَبنات البناء الأساسية في الشبكات وخدماتها وتطبيقاتها. ومن أمثلة المكونات التي تنتمي إلى طبقة البنية التحتية المسيّرات وَالبدالات والمخدمات الإفرادية وكذلك وصلات الاتصال بين هذه المسيّرات والبدالات والمخدمات الإفرادية.

والمتطلبات الوظيفية أو التنفيذية أو التشغيلية التي يحددها القطاع ITU-T كجزء من المفاهيم الوارد ذكرها أعلاه متعددة ومتنوعة. وقد تتصل بالأداء من حيث الخطأ وبالتحكم في الازدحام وبالإبلاغ عن الأعطال وباتخاذ الإجراءات التصحيحية، والعديد غيرها. ويتناول الجزء المتبقي من هذا القسم بعض وجهات النظر المختلفة بشأن المتطلبات المتصلة بشبكات الاتصالات والتي ترمي إلى الحد من محاذير عدم التيسر وعواقبها على موارد الإرسال.

ولكي يتمكن مشغل شبكة اتصالات ما من انتقاء طوبولوجيا شبكة ملائمة من حيث أهداف التيسر يُقترح الرجوع إلى الملحق ألف بالتوصية ITU-T G.827، *أمثلة لطوبولوجيات المسير وحسابات تيسر المسير من طرف إلى طرف*.

1.7 طوبولوجيات المسير وحسابات تيسر المسير من طرف إلى طرف

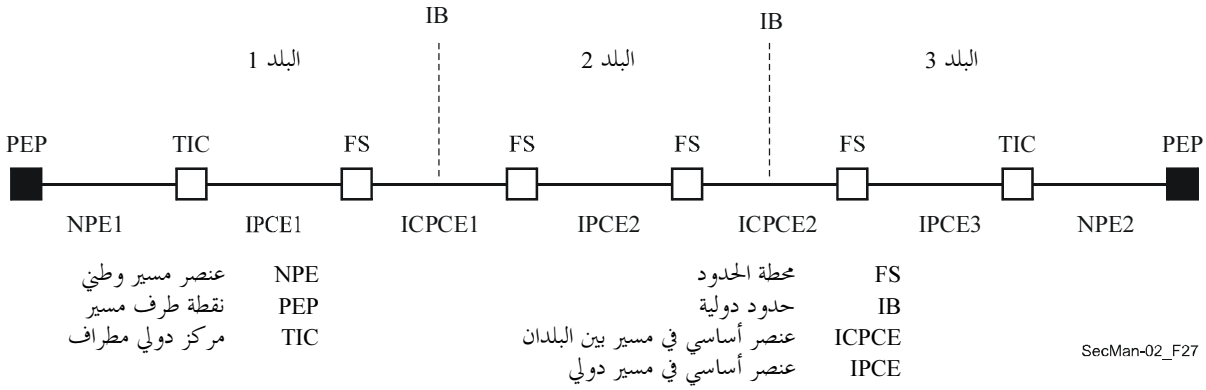
يبيّن الشكلان 7-1 و7-2 طوبولوجيات المسير الرئيسية التي يمكن بناؤها باستعمال عناصر مسير مسبقة التحديد.

ويبين الشكل 7-1 مسيراً أساسياً بسيطاً دون حماية ويبيّن الشكل 7-2 إضافة مسير حماية من طرف إلى طرف ينبغي أن يكون لها تسييراً منفصلاً لتحقيق حماية قصوى.

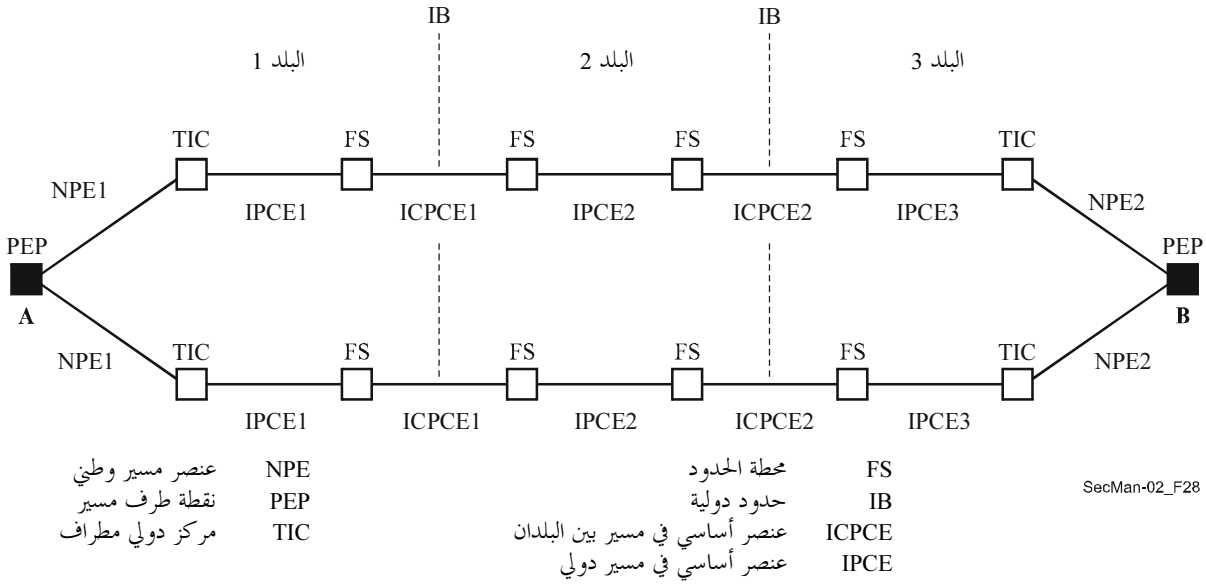
ويُدعى هذا الشكل من أشكال الحماية 1+1. وكل مسير عبارة عن توصيل ثنائي الاتجاه حيث تكون إشارة الإرسال من كل طرف موصولة دائماً بكلا المسيرين وهنالك جهاز تبديل في كل مستقبِل لانتقاء أفضل إشارة.

وثمة ترتيب أكثر اقتصاداً يكمن في استعمال مسير حماية واحد لحماية عدة مسيرات أخرى. ويُعرف هذا الترتيب باسم ترتيب n:1 ويتطلب وجود بدالة انتقاء في المرسلات والمستقبلات على السواء.

ولأغراض حسابات التيسر من طرف إلى طرف من الأسهل استعمال نسبة عدم التيسر. وتقدم التوصية ITU-T G.827 في الملحق ألف بعض المبادئ الأساسية لتقييم التيسر بالنسبة لأي من مسير أساسي بسيط (الشكل 7-1) أو الحماية من طرف إلى طرف 1+1 (الشكل 7-2) أو طوبولوجيات نسبة الحماية n:1.



الشكل 7-1 – مثال لمسير أساسي بسيط دون حماية



الشكل 7-2 – مثال لمسير يتمتع بحماية من طرف إلى طرف

ويتناول القسم 3.7 طوبولوجيات أكثر تعقيداً، ومنها مثلاً الطوبولوجيا الحلقية للتراتب الرقمي المتزامن (SDH) التي تبيّن إمكانية إعادة تسيير الحركة حول وصلة معطّلة ولكن مسير الحماية يتوقف على مقدرات التبديل في مختلف عقد الحلقة وقد لا يكون أقصر مسافة بين عقدتين. وفي الطوبولوجيات الأكثر تعقيداً تكون مشكلة تقييم التيسر صعبة إلى حد ما. وهنالك عدد من البحوث مدرجة في التذييل طاء في التوصية G.827 تتناول هذه المسألة.

2.7 تعزيز التيسر في شبكة نقل – لمحة عامة

تصف الأقسام من 2.7 إلى 4.7 الملامح المعمارية للنهج الأكثر شيوعاً المتّبعة لتعزيز تيسر شبكة نقل ما. ويتحقق التعزيز بالاستعاضة عن كيانات النقل المعطلة أو المتدهورة بكيانات موارد مكرسة أو متقاسمة. وتجري عملية الاستعاضة عادة لدى اكتشاف عيب أو تدهور في الأداء أو طلب خارجي (إدارة الشبكة مثلاً).

الحماية – تستخدم الحماية قدرة مخصصة مسبقاً بين العقد. وتشتمل أبسط معمارية على كيان حماية مكرس واحد لكل كيان عامل (1+1). وتشتمل أكثر المعماريات تعقيداً على عدد "m" من كيانات الحماية المتقاسمة بين عدد "n" من الكيانات العاملة (n:m). ويكون التبديل لغرض الحماية إما وحيد الاتجاه أو ثنائي الاتجاه. ويتخذ التبديل لغرض الحماية ثنائي الاتجاه إجراءات تبديل للحركة في كلا الاتجاهين حتى لو كان العطل وحيد الاتجاه. أما التبديل لغرض الحماية وحيد الاتجاه فلا يتخذ إجراءات التبديل إلا بالنسبة إلى اتجاه الحركة المتأثرة في حالة عطل وحيد الاتجاه.

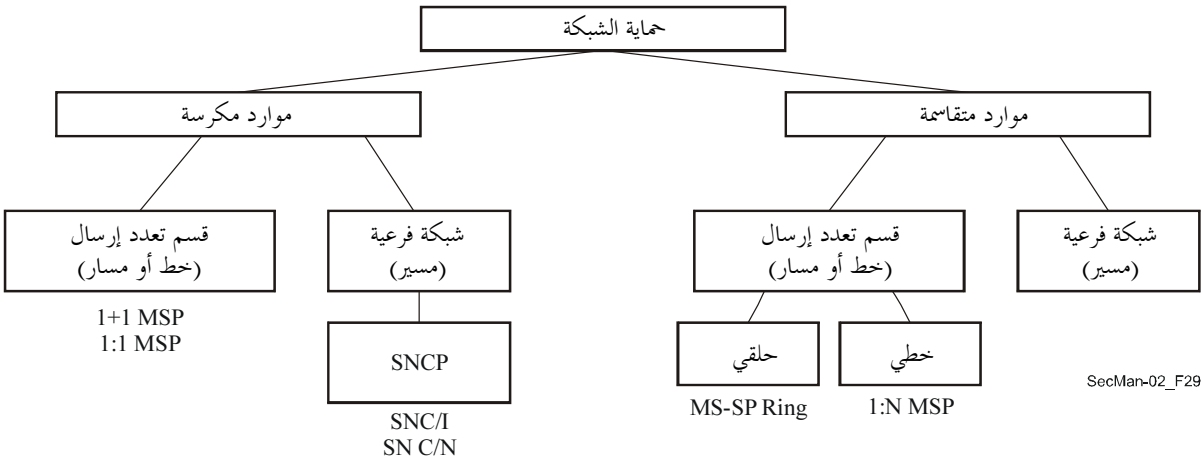
الترميم – يستخدم الترميم أي قدرة متاحة بين العقد. وتنطوي خوارزميات الترميم عموماً على إعادة تسيير. وعند استخدام الترميم تُحجز نسبة مئوية معينة من قدرة شبكة النقل من أجل إعادة تسيير الحركة العاملة.

وتتضمن التوصية ITU-T G.805 معلومات رئيسية عن هذه الجوانب.

3.7 الحماية

لا يمكن تحقيق تيسر الخدمة عالي السوية إلا باستخدام بنية تحتية للشبكة على درجة عالية من الموثوقية والديمومة. فإذا حدث عطل في تجهيز عالي الموثوقية ينبغي أن تتوفر إمكانية التحول إلى مورد بديل للإشارة (قناة حماية).

هنالك نوعان من الحماية. أولاً *حماية التجهيزات* حيث تتوفر رزم دارات احتياطية. فإذا حدث عطل قوي في رزمة دارة عندئذ يجري التبديل إلى رزمة دارة أخرى أوتوماتياً. ثانياً هنالك *حماية الشبكة* من عمليات قطع الألياف بتوفير مسيرات بديلة تسلكها الإشارة. وقد تكون هذه المسيرات البديلة إما مكرسة أو متقاسمة. وهذه الآليات مبينة في الشكل 7-3.



الشكل 7-3 – أشكال التبديل الوقائي

تكون آليات الحماية وحيدة الاتجاه أو ثنائية الاتجاه. كما قد تكون معاودة أو غير معاودة. وهذه المصطلحات معرّفة في التوصية ITU-T G.780/Y.1351.

الحماية وحيدة الاتجاه تعرّف كما يلي: "في حالة عطل وحيد الاتجاه (أي عطل يؤثر فقط على اتجاه إرسال واحد) يجري تبديل الاتجاه المتأثر فقط (من المسار، توصيل الشبكة الفرعية، وغير ذلك). وهذا يعني أن الأمر يقتصر على قرار محلي من جانب المستقبل (عقدة محلية) دون اعتبار حالة العقدة النائية عند إجراء التبديل الوقائي. وهذا في حالة عطل وحيد الاتجاه (أي عطل يؤثر فقط على اتجاه إرسال واحد) حيث يجري تبديل الاتجاه المتأثر فقط من أجل الحماية.

الحماية ثنائية الاتجاه تعرّف كما يلي: "في حالة عطل وحيد الاتجاه، يجري تبديل كلا الاتجاهين (من المسار، توصيل الشبكة الفرعية، وغير ذلك)، بما في ذلك الاتجاه المتأثر وغير المتأثر". وهذا يعني أن كلتا الحالتين المحلية والنائية تؤخذ في الاعتبار عند إجراء تبديل وقائي. وهذا في حالة عطل وحيد الاتجاه (أي عطل يؤثر فقط على اتجاه إرسال واحد) حيث يجري تبديل كلا الاتجاهين، الاتجاه المتأثر والاتجاه غير المتأثر، من أجل الحماية.

عملية (الحماية) المعاودة تعرّف كما يلي: "في عملية المعاودة، تعود إشارة (خدمة) الحركة دائماً إلى مسار/توصيل الشبكة الفرعية العامل (أو تبقى عنده) إذا انتهت طلبات التبديل، أي عندما يكون المسار/توصيل الشبكة الفرعية العامل قد خرج من حالة الخلل أو أن الطلب الخارجي قد تحرر". وهذا يعني في أسلوب عملية المعاودة أن الإشارة في قناة الحماية تعود ثانية إلى القناة العاملة عندما تكون هذه القناة العاملة قد خرجت من حالة الخلل.

عملية (الحماية) غير المعاودة تعرّف كما يلي: "في العملية غير المعاودة، لا تعود إشارة (خدمة) الحركة إلى مسار/توصيل الشبكة الفرعية العامل إذا انتهت طلبات التبديل". وهذا يعني في أسلوب العملية غير المعاودة (التي تنطبق فقط على معماريات 1+1)، عندما تخرج القناة العاملة من حالة الخلل، الحفاظ على اختيار إشارة الحركة الاعتيادية أو المحمية في قناة الحماية.

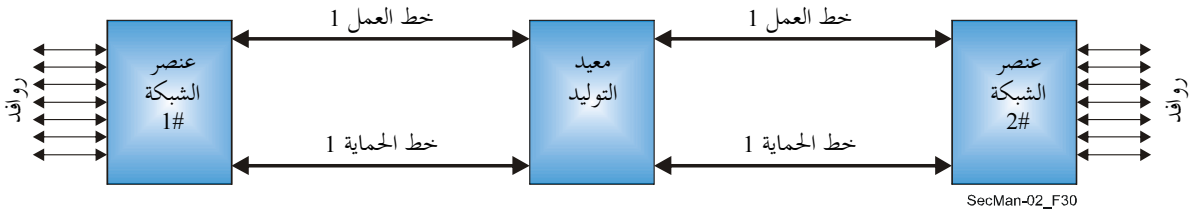
وأكثر أشكال الحماية شيوعاً هي:

- 1:1 MSP (جزء تعدد الإرسال، التبديل الوقائي 1:1، انظر الفقرة 1.3.7)
- 1+1 MSP (جزء تعدد الإرسال، التبديل الوقائي 1+1، انظر الفقرة 2.3.7)
- MS-SPRing (جزء تعدد الإرسال، حلقة الحماية المتقاسمة، انظر الفقرة 3.3.7)
- SNCP (حماية توصيل شبكة فرعية، انظر الفقرة 4.3.7)

تناقش آليات الحماية هذه بمزيد من التفصيل أدناه. وعلى أي حال تنطبق في هذه الأحوال مجموعة مشتركة من التوصيات المرجعية، وهي G.841 (الخصائص) وG.842 (التشغيل البيني) وG.783 (النماذج الوظيفية) وG.806 (العيوب) وG.808.1 (التبديل الوقائي النوعي).

1.3.7 جزء تعدد الإرسال، التبديل الوقائي 1:1

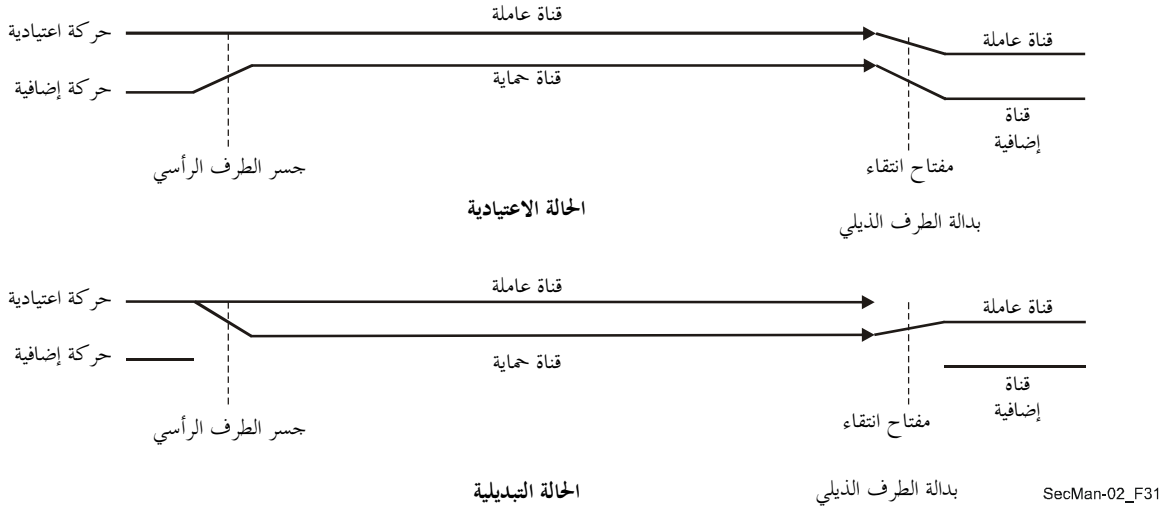
يبدو في الشكل 7-4 المخطط البياني للشبكة:



الشكل 7-4 – المخطط البياني للشبكة للتبديل الوقائي 1:1

هنالك في التبديل الوقائي 1:1 قناة حماية واحدة لكل قناة عاملة. وقد تحمل قناة الحماية حركة أخرى يمكن تعليقها.

ويبين الشكل 7-5 مخططاً بيانياً يصور داخل عنصر الشبكة.



الشكل 7-5 – جزء تعدد الإرسال، الحماية الخطية 1:1

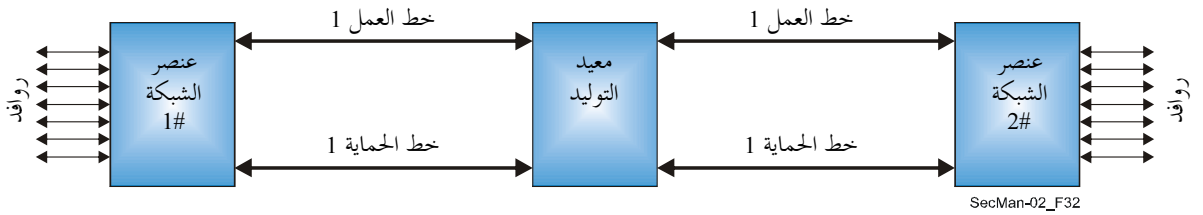
يمكن في الظروف الاعتيادية حمل "الحركة الإضافية" عبر قناة الحماية. ولكن عندما تأتي النسبة الصحيحة K1/K2 من البايتات (التي تفعّل وظيفة الحماية) عندئذ يجري تمرير "الحركة الاعتيادية" عبر جسر إلى قناة الحماية عند "الطرف الرأسي" ثم تبدل عند "الطرف الذيلي". ويكون التحكم من خلال البايتات K1 وK2 في قناة الحماية.

وهذا يقابل حماية الخط في الوحدة النموذجية للنقل المتزامن، السوية N (السوية STM-N (N ≤ 1)).

والأحوال التي من شأنها تفعيل التبديل هي التبديل القسري وعدد من أحوال الخلل أو التعطيل (مثال ذلك فشل الإشارة وفقدان الإشارة وفقدان الرتل والأخطاء المفرطة وتدهور الإشارة). وثمة تفاصيل واردة في التوصية ITU-T G.806.

2.3.7 جزء تعدد الإرسال، التبديل الوقائي 1+1

يبدو في الشكل 7-6 المخطط البياني للشبكة.



الشكل 7-6 – المخطط البياني للشبكة للتبديل الوقائي 1+1

هنالك في التبديل الوقائي 1+1 قناة حماية واحدة لكل قناة عاملة. وتحمل شبكة الحماية نسخة من إشارة القناة العاملة.

ويبين الشكل 7-7 مخططاً بيانياً يصور داخل عنصر الشبكة.

الشكل 7-7 – قسم تعدد الإرسال، الحماية الخطية 1+1

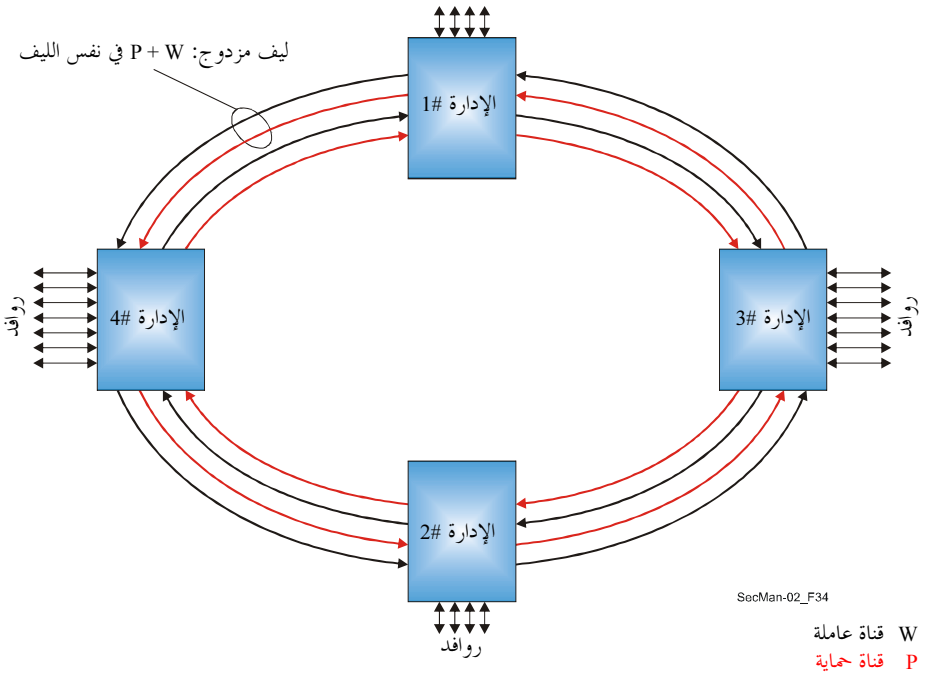
تكون إشارة الإرسال موصولة بجسر دائم إلى خط الحماية. وينتقي المستقبِل أفضل الإشارتين.

ليس هنالك من مقدرة لتحميل "حركة إضافية" في مخطط الحماية 1+1. فهو يقوم بوظيفة حماية خطية. ولذا فهو يعمل فقط على أساس أسلوب النقل المتزامن STM-n، مهما كان معدل الخط. ويمكن اعتباره بمثابة مجموعة فرعية من التبديل الوقائي 1:1. ولا يتطلب آلية تحكم (البايتات K1 وK2 في التبديل الوقائي الأوتوماتي (APS) في رأسية قسم تعدد الإرسال (MSOH)) لتشغيله. ويكون التبديل على أساس نفس أحوال الخلل المشار إليه في الفقرة 1.3.7.

وهنالك صيغة من آلية الحماية هذه تُدعى 1+1 ثنائية الاتجاه، حيث تتبدل مفاتيح الانتقاء في الطرفين. وهذا يتطلب التحكم من خلال البايتات K1/K2 التي يتعين إرسالها.

3.3.7 التبديل الوقائي في قسم تعدد الإرسال – حلقة الحماية المتقاسمة (MS-SPRing)

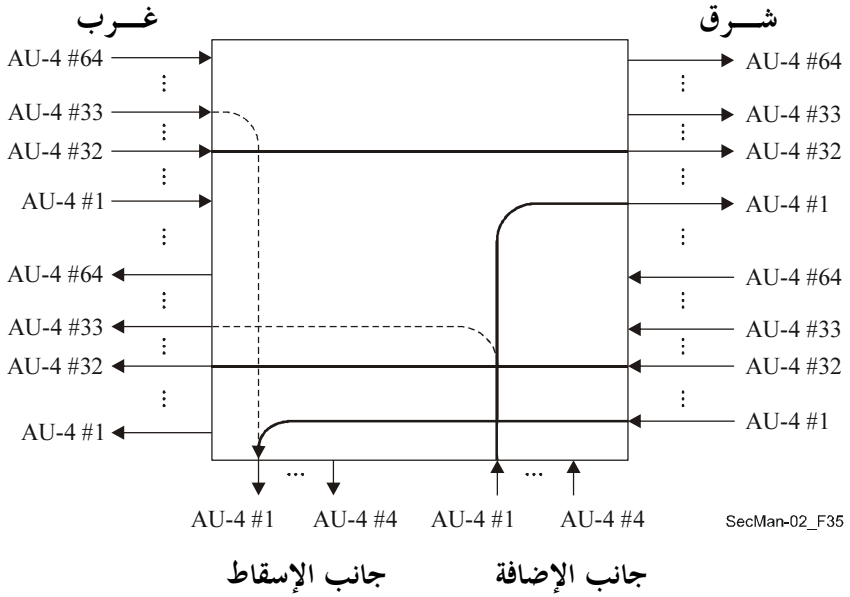
يبدو في الشكل 7-8 المخطط البياني للشبكة.



الشكل 7-8 – مخطط الشبكة للتبديل الوقائي في قسم تعدد الإرسال – حلقة الحماية المتقاسمة

إن تشكيل حلقة الحماية المتقاسمة في تعدد الإرسال (MS-SPRing) مزدوج الليف هو التشكيل الغالب في شبكات التراتب الرقمي المتزامن. وهنالك زوج من الألياف لكل باع في الحلقة يحمل كل منهما نصف عرض النطاق للقنوات العاملة وقنوات الحماية (مثال ذلك خط أسلوب STM-64 مع الوحدات الإدارية وAU-4 من 1 إلى 32 قناة عاملة وAU-4 من 33 إلى 64 من أجل الحماية). والحركة الاعتيادية المحمولة في القنوات العاملة في أحد الألياف تحميها قنوات الحماية في الاتجاه المعاكس.

ويبدو في الشكل 7-9 وظيفة حلقة الحماية المتقاسمة في تعدد الإرسال مزدوج الليف.



الشكل 7-9 – حلقة حماية متقاسمة في تعدد الإرسال STM-64 مصحوبة بنظام STM-4 إضافة–إسقاط

في الشكل 7-9 تحوّل الإشارة المكونة "AU-4 #1 إضافة" إلى إشارة "إرسال AU-4 #1 شرق". وتسقط من "استقبال AU-4 #1 شرق" إلى "AU-4 #1 إسقاط". وهنالك أيضاً توصيل عابر في AU-4 #32 يبدو في الشكل 7-9.

فإذا حصل انقطاع في الليف شرقاً عندئذ ينبغي إرسال "AU-4 #1 إضافة" خارج جانب الحماية غرباً ("إرسال AU-4 #33 غرب") وإسقاط إشارة الاستقبال من جانب الحماية غرباً ("استقبال AU-4 #33 غرب") إلى "AU-4 #1 إسقاط". وينبغي تحليق AU-4 #32 من الغرب إلى AU-4 #64. وتكون AU-4 #32 من الشرق قد حَلّقت عائدة إلى قناة الحماية (AU-4 #64) على الجانب الآخر من مكان الانقطاع، ومن ثم ينبغي عند هذه العقدة تحليق الحماية ("استقبال AU-4 #64 غرب") إلى القناة العاملة (AU-4 #32).

ويحدث التبديل الوقائي على أساس خشونة AU-4 أو AU-3 عبر جميع الإشارات في الليف. وترسل الطلبات وإشعارات الاستقبال باستعمال البايتات K1 وK2 في التبديل الوقائي الأوتوماتي (APS) في رأسية قسم تعدد الإرسال (MSOH). وترسل البايتات K1 وK2 على الخط الذي يحمل قنوات الحماية. وهي ترسل في الاتجاهين (شرقاً وغرباً)، أحدهما المسير القصير والآخر المسير الطويل.

ويحصل الإسكات لتجنب توصيل الحركة إلى غير الزبون في حالة انعزال العقدة أو فشل العقدة مع حركة الإضافة/الإسقاط (خدمات من نفس الفتحة الزمنية ولكن على أبواع مختلفة). وللاطلاع على وصف لعملية الإسكات يرجى الرجوع إلى التذييل II في التوصية G.841.

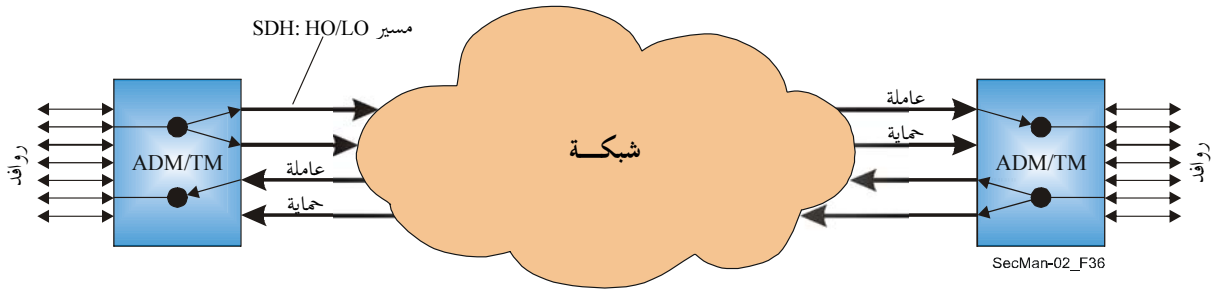
وأحوال العُطل بالنسبة إلى فشل الإشارة وانحطاط الإشارة هي نفس الأحوال كما في التبديل الوقائي الخطي (انظر الفقرة 1.3.7).

هناك ثلاث تشكيلات تبديل تؤخذ بعين الاعتبار:

- عادي (دون أعطال)
- عطل في جانب الشرق (ضرورة التحليق غرباً والاقتصار على الإضافة/الإسقاط من الغرب)
- عطل في جانب الغرب (ضرورة التحليق شرقاً والاقتصار على الإضافة/الإسقاط من الشرق)
- تبديل باعي من أجل ليف رباعي في حلقة حماية متقاسمة في تعدد الإرسال MS-SPRing (تبديل من أجل الحماية، دون تحليق)

4.3.7 التبديل الوقائي لحماية توصيل الشبكة الفرعية (SNCP)

يبدو في الشكل 7-10 المخطط البياني للشبكة.



الشكل 7-10 – التبديل الوقائي SNCP

تقوم حماية توصيل الشبكة الفرعية (SNCP) على أساس المسير. وعليه لا تبدل سوى إشارة واحدة (AU-3، AU-4، وهكذا) في أي وقت. ويمكن اعتبارها أيضاً بمثابة حماية وحيدة الاتجاه 1+1 بالنسبة إلى فرادى المسيرات. ويجري التبديل الوقائي على سوية المسير:

- تراتب رقمي متزامن (SDH): حاوية افتراضية عالية الدرجة HO – VC-4/3، وحدة رافدة منخفضة الدرجة LO – TU-3/2/11/12

لا يستخدم أي بروتوكول (سوى لمفتاح التبديل الإجباري). ويتوقف قرار التبديل بين نسخة عاملة ونسخة حماية على الأحوال المحلية، حيث ترصد النسختان.

- اشتراط زمن التبديل الوقائي أقل من 50 ms. وهكذا، وفي حالة انقطاع ليف عالي عرض النطاق، 10 Gbit/s أو 40 Gbit/s مثلاً، وعندما تكون جميع المسيرات محمية في إطار SNCP، لا يمكن عادة تلبية هذا الاشتراط الزمني إذا جرى التبديل الوقائي في برمجية تحتوي على معالجة الأعطال في جملة أحوال وتبادل الرسائل بين لوحة ومراقب مركزي.

4.7 الترميم

تصف التوصية ITU-T G.805 أساليب تعزيز تيسر شبكة النقل. ويستخدم كل من عبارة "حماية" (الاستعاضة عن مورد معطل بمورد احتياطي مخصص مسبقاً) و"ترميم" (الاستعاضة عن مورد معطل بإعادة التسيير باستعمال قدرة احتياطية) لتصنيف هذه الأساليب. وتستكمل إجراءات الحماية عموماً في مدى عشرات ميلي ثانية بينما تستكمل إجراءات الترميم عادة في فترات تتراوح من مئات ميلي ثانية إلى بضع ثوان.

ومن شأن مستوى التحكم في الشبكة البصرية أوتوماتية التبديل (ASON) أن يزود مشغل شبكة ما بالقدرة على تزويد مستعمل ما بصنف خدمة (CoS) قابل للانتقاء (من ذلك مثلاً التيسر ومدة الانقطاعات والثواني المحتوية على أخطاء، وما إلى ذلك). والحماية والترميم آليتان (تُستخدمان في الشبكة) لتوفير صنف الخدمة الذي يطلبه المستعمل. ويتوقف انتقاء آلية قابلية البقاء (الحماية أو الترميم أو لا شيء) بالنسبة إلى توصيل معين يحمل نداء ما على ما يلي: سياسة مشغل

الشبكة، وطوبولوجيا الشبكة، ومقدرة التجهيزات المنشورة. ويمكن استعمال آليات قابلية بقاء مختلفة في التوصيلات المقامة سلسلياً لتوفير النداء. وإذا كان للنداء أن يعبر شبكة أكثر من مشغل واحد عندئذ ينبغي أن تكون كل شبكة مسؤولة عن قابلية بقاء توصيلات العبور. ولن تحتوي طلبات التوصيل عند السطح بين المستعمل والشبكة (UNI) أو عند السطح البيني الخارجي بين عقدتين (E-NNI) سوى صنف الخدمة المطلوب وليس نمط حماية أو ترميم محدد صراحة.

ويمكن تفعيل الحماية أو الترميم في توصيل ما أو تبطيلهما مؤقتاً بأمر من مستوي الإدارة. ويمكن استخدام هذه الأوامر لتمكين أداء أنشطة صيانة مبرمجة زمنياً. كما يمكن استعمالها لتجاوز العمليات الأوتوماتية في بعض أحوال العطل الاستثنائية.

يرجى الرجوع إلى التوصية ITU/T G.8080/Y.1304.

5.7 التجهيزات الخارجية

ثمة جوانب عديدة في ظل مسألة الأمن في أنظمة الاتصالات. والقطاع ITU-T ينظر أيضاً في الجوانب المتصلة بالأمن المادي للتجهيزات الخارجية. وهو يتناول في هذا الصدد المشكلات التي تواجه مقدرة عتاد النظام على مقاومة تهديد الحريق والكوارث الطبيعية والاقتحام المقصود أو العرضي من جانب الناس. ومن أهم مسائل الأمن المشمولة مسألة جعل مكونات الأنظمة والكبلات والأغلفة والخزائن، وما إلى ذلك، قادرة مادياً على مقاومة التلف وكذلك مسألة مراقبة الأنظمة لمنع أي تلف حيثما أمكن أو الاستجابة إلى المشكلات واستعادة وظيفة النظام بأسرع وسيلة ممكنة.

وعموماً فإن أهم العوامل التي يتعين النظر فيها بشأن هذه الجوانب من جوانب الأمن:

- سبب تلف/فقدان البيانات:
  - صيانة الشبكة؛
  - الحوادث والنكبات (غير مقصودة)؛
  - عمليات التخريب (مقصودة؛ عشوائية)؛
  - نفاذ من قبل أفراد غير مرخص لهم (مدنيون، تقنيون لدى مشغلين آخرين مثلاً)؛
  - أعمال إجرامية (مثل إتلاف مطراف أو التوصيل بقصد السرقة؛ سرقة الكبلات؛ التنصت غير المشروع في كبل ما)؛
  - قوة مركزة أو عنف (مقصودة)؛
- أوضاع بيئة التجهيزات:
  - مواقع داخل المبنى (مكتب مركزي، موقع الزبون)؛
  - هوائي خارجي (تعرض لفعل الإنسان/الطبيعة)؛
  - خارج المبنى في الشارع (احتمال تلف بسبب أشغال)؛
  - خارج المبنى في باطن الأرض (ضمن أنابيب أو دفن مباشر).

وعموماً يمكن التوصية بالإجراءات التالية من باب الاحتياط فيما يتعلق بالطبقة المادية. ومعظم هذه الإجراءات تمليها الممارسات المحلية والقواعد لدى كل من المشغلين:

- تجنب استعمال العقد في مستوى الشارع (مثل الخزائن والمنصات والصناديق المثبتة على الجدران) لأنها حساسة للحوادث وأعمال التخريب والعنف والحريق والفضول عامة، والأسلم استعمال عقد أو كبلات في باطن الأرض؛
- ينبغي أن تكون خزائن الشارع (أو صناديق أخرى في مستوى الشارع) صلبة "منيعة إزاء العبث"؛
- جميع الأماكن المغلقة ينبغي أن يكون في الإمكان إقفالها أو ختمها لتجنب النفاذ غير المطلوب إليها؛
- الكبلات المغلفة في أنابيب أقل تأثراً من تلك المدفونة مباشرة، والتي قد تتعرض للتلف عرضاً بسبب عمليات الحفر؛
- قد يكون لنقاط الانتهاء أو نقاط الحدود فاصل (قابل للقفل) ما بين جانب الشبكة وجانب الزبون؛ أو بين الدارات التي يستخدمها مشغلون مختلفون؛
- مطاريف الزبائن داخل المباني أقل تأثراً من تلك المركّبة (داخل الجدران) خارج المباني (في حالة السرقة مثلاً)؛

- قد يكون من المفيد تخزين مقدار إضافي من الكبل في مواقع منتظمة في الشبكة، وذلك لتيسير الإصلاح في حالة تلف عرضي (سواء فوق الأرض أو تحت الأرض)؛
- بالنسبة لتجهيزات الألياف البصرية يوصى بمراعاة سوية ملائمة من فصل الدارات فضلاً عن استقرار بصري دينامي، وذلك لتجنب فقدان البيانات/اضطراب الحركة أثناء صيانة الشبكات؛
- بالنسبة للخطوط الحيوية قد يوصى بالتكرار (خطوط احتياط) من خلال كبلات وشبكات منفصلة مادياً (مثال ذلك هيكليات حلقية للمصارف والمستشفيات).

ومن الإجراءات الأخرى التي يمكن تنفيذها:

- وضع إجراءات أمن من أجل التجهيزات خارج المباني؛
- تركيب أجهزة لكشف الحريق ولمراقبة التجهيزات الخارجية والتحكم فيها؛
- وضع معايير لتقييم التعايش الآمن في نفس الموقع من الشبكة لأكثر من مشغل واحد يقدمون خدمات متعددة، مثل أنظمة الهاتف التقليدية (POTS) والشبكات الرقمية متكاملة الخدمات (ISDN) وخطوط المشترك الرقمية (xDSL)، وما إلى ذلك، دون أي شكل من أشكال التفاعلات الضارة؛
- استخدام حلول تقنية من شأنها تيسير تفكيك رزم الخدمات والحفاظ في الوقت ذاته على السلامة والمعوّلية وإمكانية التشغيل البيني ضمن طوبولوجيات الشبكات شائعة الاستعمال في كل العالم؛
- تركيب أجهزة تشوير على امتداد الكبلات تحت الأرض؛
- توفير المراقبة والصيانة وأنظمة الاختبار للتجهيزات الخارجية؛
- النظر في تصميم الكبل الذي تكون وظيفته الأولى حماية السلامة المادية لوسط الإرسال – الألياف البصرية؛
- النظر في جوانب بناء الكبلات، وتلحيم الألياف، وعملية التنظيم والأغلفة، ووحدات التفريع، وعملية المسح وتخطيط المسير، وخصائص السفن الكبلية، وأنشطة التحميل والمد، وطرائق الإصلاح، وطرائق الحماية والاختبار بالنسبة إلى كبلات الألياف البصرية الممدودة في قاع البحار.

8 تنظيم الحوادث ومعاملة حوادث الأمن (مبادئ توجيهية) لمنظمات الاتصالات

تشمل إدارة الأمن والوعي بأهميته عدداً من العمليات. ومنها تعريف الهياكل والإجراءات من أجل معاملة المعلومات التي تتناول الأحداث المتصلة بالأمن وتعميم هذه المعلومات. وهذا أيضاً مجال استجاب فيه خبراء القطاع ITU-T إلى حاجة معلنة ومن ثم وضعوا التوصية ITU-T E.409. والغرض من هذه التوصية، وهي بعنوان *"تنظيم الأحداث ومعاملة أحداث الأمن: مبادئ توجيهية لمنظمات الاتصالات"*، هو تحليل عملية إدارة الحدث ووضع بنية لها واقتراح طريقة لإنشاء منظمة تهتم بإدارة الأحداث ضمن منظمة اتصالات ما تهتم بتوفير الاتصالات الدولية، حيث يكون التركيز على كيفية تدفق الحدث وبنيته. وعملية التدفق والمناولة عملية مفيدة في تحديد ما إذا كان يتعين تصنيف حدث ما على أنه حدث أو حادث أو حادث أمن أو أزمة. كما يشمل التدفق القرارات الحرجة الأولى التي يتعين اتخاذها.

وتقدم هذه التوصية لمحة عامة وإطاراً يوفر الإرشاد لتخطيط تنظيم الحادث والتعامل مع حادث الأمن.

والتوصية عمومية في طابعها ولا تحدد ولا تتناول المتطلبات اللازمة لشبكات معينة.

وبينما ترمي هذه التوصية إلى تيسير التطورات الدولية فيما يتعلق بأمن شبكات الاتصالات فإن هذه التطورات يمكن تيسيرها لو أمكن أيضاً تطبيق المتطلبات على شبكات المعلومات والاتصالات (ICN) الوطنية.

والجريمة السيبرانية تأتي في أعقاب الاستعمال المكثف المتزايد للحواسيب في الاتصالات الدولية. وطوال السنوات القليلة الماضية ازدادت الجرائم السيبرانية أضعافاً مضاعفة، كما يشهد بذلك العديد من الدراسات الاستقصائية الدولية والوطنية. وفي غالبية البلدان ليس هنالك من إحصاءات دقيقة عن عدد حالات الاقتحام السيبراني أو حوادث الأمن، ولا سيما تلك المتصلة بالاتصالات الدولية.

ومعظم منظمات أو شركات الاتصالات ليس لديها هيئة متخصصة للتعامل مع حوادث الأمن في شبكات المعلومات والاتصالات (ICN) (ومع ذلك قد يكون لديها فريق لمواجهة أي نوع من الأزمات عموماً). وعندما يقع حادث أمن

في شبكة من هذه الشبكات فإنه يعامَل في حينه، أي أن الأشخاص الذين يكتشفون حادث أمن ما يأخذون على عاتقهم مسؤولية التصدي للحادث قدر استطاعتهم. وفي بعض المنظمات قد يحاولون تجاهل حوادث الأمن في الشبكة أو التستر عليها خشية أن تؤثر على الإنتاج أو التيسر أو العائدات.

وكثيراً ما يحدث عندما يكتشف حادث أمن في شبكة ICN أن الشخص الذي اكتشفه لا يدري إلى أي جهة يبلغ عنه. وقد يؤدي ذلك إلى قيام مدير النظام أو الشبكة بالالتفاف حول الحادث أو حله مؤقتاً لمجرد التخلص من المشكلة. وليس لدى هؤلاء السلطة المفوضة أو الوقت أو الدراية لتقويم النظام لئلا يقع حادث أمن الشبكة ICN ثانية. ولهذه الأسباب الوجيهة من الأفضل أن تكون هنالك وحدة أو مجموعة مدرّبة قادرة على تناول حوادث الأمن فوراً وكما ينبغي. وعلاوة على ذلك، قد يخضع العديد من المسائل في مجالات متنوعة شتى من علاقات الوسائط إلى الشؤون القانونية أو إنفاذ القوانين أو حصة السوق أو الشؤون المالية.

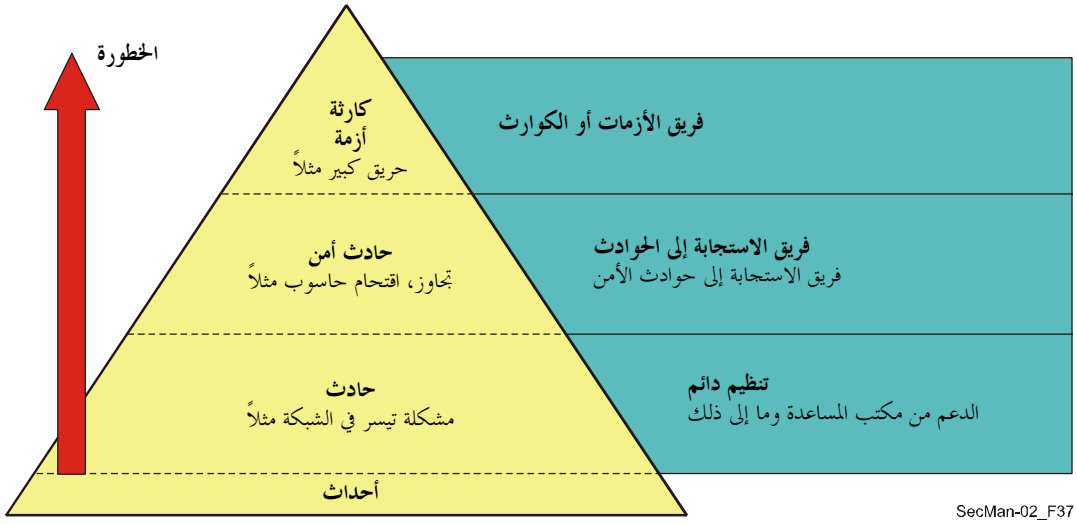
ولدى الإبلاغ عن حادث أو التصدي له فإن استخدام تصنيفات مختلفة قد يؤدي إلى سوء الفهم. وهذا قد يؤدي بدوره إما إلى حرمان حادث أمن الشبكة من الاهتمام الملائم أو من التصدي له حالاً الأمر الذي لا بد منه لمنع الحادث من الوقوع ثانية أو لاحتوائه أو لإعاقته. وقد يفضي ذلك إلى عواقب خطيرة بالنسبة إلى المنظمات المتأثرة (الضحية).

ولكي نتمكن من تناول الحوادث والإبلاغ عنها علينا أن نلمّ بكيفية الكشف عنها والتصدي لها والتغلب عليها. ومن شأن إنشاء بنية عامة للحوادث (أي الحوادث المادية والإدارية أو التنظيمية، والمنطقية) أن تمكننا من الحصول على صورة عامة لبنية الحادث وتدفقه. والمصطلحات الموحدة أساس الفهم المشترك للكلمات والعبارات.

1.8 تعاريف

يمكن تعريف حادث الأمن بأنه "ثغرة أمن وتهديد وضعف وخلل قد يكون لها أثر على أمن أصول المنظمة". وفي هذه التوصية يفترض أن حادثاً ما أقل حدّة من حادث أمن وأن حادث أمن معلومات نمط معين من حوادث الأمن.

ويبيّن الشكل 8-1 هرم الأحداث. ففي قاعدة الهرم نجد الحدث ثم الحادث ثم حادث الأمن وفي القمة نجد الأزمة والكارثة. وكلما اقترب الحدث من القمة ازداد خطورة. وحرصاً على استعمال مصطلحات موحدة ومستقرة بشأن التعامل مع الحوادث ضمن منطقة الشبكة ICN، يوصى باستعمال التعاريف التالية أدناه.



الشكل 8-1 – هرم الأحداث في التوصية ITU-T E.409

1.1.8 حدث: واقعة قابلة للملاحظة ومن غير الممكن التنبؤ بها (كلياً) أو التحكم بها (كلياً).

2.1.8 حادث: حدث ربما أدى إلى واقعة أو سلسلة وقائع ليست خطيرة.

3.1.8 حادث أمن: أي حدث معاكس قد يتهدد جانباً ما من جوانب الأمن.

4.1.8 حادث أمن في شبكات المعلومات والاتصالات (ICN): أي حدث معاكس حقيقي أو مشتبه به فيما يتعلق بأمن الشبكات ICN. ومن ذلك:

- اقتحام أنظمة حاسوبية في شبكة ICN من خلال الشبكة؛
- انتشار فيروسات حاسوبية؛
- عمليات لسبر مواطن الضعف من خلال الشبكة في طائفة من الأنظمة الحاسوبية؛
- تسرب نداء في بدالة خاصة أوتوماتية (PABX)؛
- أي أحداث أخرى غير مرغوب فيها ناشئة عن أي إجراءات داخلية أو خارجية غير مرخص بها، بما في ذلك هجمات رفض الخدمة والكوارث وغيرها من حالات الطوارئ، وما إلى ذلك.

1.5.8 أزمة: حالة نجمت عن حدث – أو معرفة حدث وشيك الوقوع – قد تسفر عن عواقب وخيمة. وقد يكون من الممكن، في أفضل الأحوال، اتخاذ تدابير أثناء أزمة ما لمنع الأزمة من أن تصبح كارثة. وعندما تقع *كارثة* يكون هنالك عادة خطة لاستمرار الأعمال (BCP) وفريق لإدارة الأزمات لمعالجة الحالة.

2.8 المسوّغات

توصى منظمات الاتصالات التي هي بصدد إنشاء أفرقة استجابة لحوادث أمن الحاسوب (CSIRT) بأن تعلن، منذ الخطوة الأولى، استعمالها للتصنيف وذلك لتجنب أي حالات سوء فهم. إذ يكون العمل المشترك أيسر جداً عندما تُستعمل نفس "المصطلحات".

توصى المنظمات باستعمال مصطلح "حادث" و"حادث أمن ICN"، وبأن تعرّف تقسيماتها الفرعية الخاصة بها تبعاً لخطورة حادث الأمن. ومن حيث الجوهر فإن حادث أمن ICN هو أي حدث غير مرغوب فيه وغير مرخص له – أي أن حادث أمن ICN يشمل اقتحام الحاسوب أو هجمة رفض الخدمة أو انتشار فيروس، وذلك يتوقف على البواعث والخبرات والموارد المطّلعة المتاحة في المنظمة. وفي المنظمات التي أنشأت فريقاً فعالاً لمكافحة الفيروسات قد لا يُعتبر انتشار الفيروس بمثابة حادث أمن ICN وإنما بمثابة حادث.

وقد يتخذ التقسيم الفرعي المثال أو النموذج التالي:

- حوادث
  - انتهاك قواعد سلوك الإنترنت (رسائل اقتحامية، محتوى مسيء، وما إلى ذلك)
  - انتهاك سياسات الأمن
  - فيروسات بمفردها
- حوادث أمن الشبكات ICN
  - عمليات المسح والسبر
  - عمليات اقتحام الحاسوب
  - تخريب الحاسوب وإتلافه (هجمات التيسر مثل القصف وهجمات رفض الخدمة)
  - برمجيات مؤذية (فيروسات، خدع (طروادة)، ديدان، وما إلى ذلك)
  - سرقة المعلومات والتجسس
  - انتحال الهوية

ومن الممكن، باستخدام نفس درجة الخشونة والدقة في المصطلحات، اكتساب الخبرة في المجالات التالية:

- الاسترشاد فيما يتعلق بالحدة والنطاق؛
- مؤشر عن درجة الإلحاح (لاستعادة السوية المطلوبة من الأمن مثلاً)؛
- تأثيرات التدابير المضادة المحتملة؛
- التكاليف المترتبة الممكنة.

9 الخلاصة

عكف قطاع تقييس الاتصالات (ITU-T) طوال مدة طويلة على وضع مجموعة من التوصيات الأساسية بشأن الأمن، منها: التوصية X.800 وهي وثيقة مرجعية بشأن معمارية الأمن للتوصيل البيني للأنظمة المفتوحة، وتتضمن سلسلة التوصيات X.810-X.816 تعريف إطار عام للأمن للأنظمة المفتوحة يشمل الإشراف والاستيقان، والتحكم في النفاذ، وعدم التنصل، والسرية، والسلامة والأمن وإنذارات التدقيق على التوالي. وقد وضعت حديثاً التوصية ITU-T X.805 لوصف معمارية الأمن للأنظمة التي توفر الاتصالات من طرف إلى طرف. والتوصية X.805 عبارة عن تنقيح لمعمارية الأمن يأخذ في الاعتبار التهديدات المتزايدة ومواطن الضعف الناتجة عن ظهور بيئة مقدمي شبكات متعددة وخدمات متعددة. ومن المؤكد أن التوصية ITU-T X.509 بشأن المفاتيح العمومية وأطر شهادات النعوت هي أكثر النصوص التي ترجع إليها الجهات المعنية في تطبيقات الأمن، سواء بشكل مباشر أو ضمني، في إطار المعايير الأخرى التي وُضِعت على أساس مبادئ التوصية X.509.

وبالإضافة إلى هذه التوصيات الإطارية، قام القطاع ITU-T بوضع أحكام للأمن في العديد من الأنظمة والخدمات التي عرّفها في توصياته. وفي هذا الكتيب بعضها موصوف في القسم 6: نقل الصوت بواسطة بروتوكول الإنترنت باستعمال التوصية H.323 أو الاتصالات الكبلية بواسطة بروتوكول الإنترنت (IPCablecom)، وتأمين إرسال الفاكس، وإدارة الشبكات. ويتضمن الكتيب أيضاً مثالاً لتطبيق المفاتيح العمومية وتطبيقات البنية التحتية لإدارة الامتيازات في مجال الصحة الإلكترونية. وفي *إطار التحفظ الواجب* هنالك *العديد* من المجالات الأخرى حيث تتناول توصيات القطاع ITU-T احتياجات الأمن في الاتصالات وتكنولوجيا المعلومات. ويعكف عدد من لجان الدراسات التابعة للقطاع على دراسة هذه الجوانب وغيرها، مثل منع الاحتيال وإعادة الأوضاع إلى ما كانت عليه قبل حدوث الكوارث، وسوف تتناولها الطبعات المقبلة من هذا الكتيب. ومن الأمور التي تساعد على تعزيز أعمال القطاع في مجال الأمن تنظيم الحلقات الدراسية أو ورش العمل الدولية بشأن الأمن أو المشاركة فيها، ووضع مشروع للأمن وذلك بتعيين لجنة دراسات رائدة تتولى مسائل الأمن في قطاع تقييس الاتصالات، والمشاركة في أعمال المنظمات الأخرى المعنية بوضع المعايير (ISO/IEC JTC 1/SC 27 مثلاً).

المراجع

بالإضافة إلـــى توصيات قطاع تقييس الاتصالات المشار إليها فـــي هذا الكتيب، (والتي يمكن الاطلاع عليها في الموقع http://www.itu.int/ITU-T/publications/recs.html) اعتمد إعداد هذا الكتيب أيضاً على المواد التالية:

[ApplCryp] SCHNEIER (B.), "*Applied Cryptography – Protocols, Algorithms and Source Code in C*" 2nd edition, Wiley, 1996; ISBN 0-471-12845-7

[Chadwick] CHADWICK (D.W.), "*The Use of X.509 in E-Healthcare*", Workshop on Standardization in E-health; Geneva, 23-25 May 2003; PowerPoint at www.itu.int/itudoc/itu-t/workshop/e-health/s5-02.html and audio presentation at www.itu.int/ibs/ITU-T/e-health/Links/B-20030524-1100.ram

[Euchner] EUCHNER (M.), PROBST (P.-A.), "*Multimedia Security within Study Group 16: Past, Presence and Future*", ITU-T Security Workshop; 13-14 May 2002, Seoul, Korea; www.itu.int/itudoc/itu-t/workshop/security/present/s2p3r1.html

[FreePresc] Free prescriptions statistics in the UK; www.doh.gov.uk/public/sb0119.htm

[Packetizer] "*A Primer on the H.323 Series Standard*" www.packetizer.com/iptel/h323/papers/primer/

[Policy] CHADWICK (D.W.), MUNDY (D.), "*Policy Based Electronic Transmission of Prescriptions*"; IEEE POLICY 2003, 4-6 June, Lake Como, Italy. sec.isi.salford.ac.uk/download/PolicyBasedETP.pdf

[SG17] ITU-T Study Group 17; "Lead Study Group on Telecommunication Security" www.itu.int/ITU-T/studygroups/com17/tel-security.html (Catalogue of Approved Recommendations related to Telecommunication Security; Approved ITU-T Security Definitions)

[Shannon] SHANNON (G.), "*Security Vulnerabilities in Protocols*"; ITU-T Security Workshop; 13-14 May 2002, Seoul, Korea; www.itu.int/itudoc/itu-t/ workshop/security/present/s1p2.html

[Wisekey] MANDIL (S.), DARBELLAY (J.), "*Public Key Infrastructures in e-health*"; written contribution to Workshop on Standardization in E-health; Geneva, 23-25 May 2003; www.itu.int/itudoc/itu-t/workshop/e-health/wcon/s5con002_ww9.doc

ISO/IEC 18033-1:2005, *Information technology – Security techniques – Encryption algorithms – Part 1: General*

ISO/IEC 18033-2:2006, *Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers*

ISO/IEC 18033-3:2005, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*

ISO/IEC 18033-4:2005, *Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers*

الملحق ألف

قائمة بتوصيات قطاع تقييس الاتصالات المتعلقة بالأمن

قامت بتجميعها لجنة الدراسات 17 التابعة للقطاع ITU-T، وهي لجنة الدراسات الرائدة بشأن أمن الاتصالات.

الرقم	العنوان	الأغراض الرئيسية والجوانب المتعلقة بالأمن	لجنة الدراسات
E.408	متطلبات أمن شبكات الاتصالات	توفر نظرة شاملة لمتطلبات الأمن وإطاراً يحدّد التهديدات المحدقة بأمن شبكات الاتصالات بوجه عام (الثابتة والمتنقلة على السواء؛ وكذلك الصوتية وشبكات المعطيات) وتقدّم إرشادات من أجل تخطيط التدابير المضادة التي يمكن اتخاذها للتخفيف من المخاطر الناشئة عن التهديدات.	2
E.409	تنظيم إدارة الحوادث ومناولة حوادث الأمن: خطوط توجيهية لمنظمات الاتصالات	تحلل وتنظم وتقترح نهجاً لإنشاء تنظيم لإدارة الحوادث داخل منظمة الاتصالات المعنية بتوفير خدمات الاتصالات الدولية حيث يتركز تدفق وبنية حادث ما. والتدفق والمناولة مفيدان في تحديد ما إذا كان يمكن تصنيف حدث باعتباره حدثاً أو حادثاً أو حادثة أمن أو أزمة. ويغطي التدفق أيضاً القرارات الأولى بالغة الأهمية التي يتعين اتخاذها. وللتمكن من النجاح في مناولة حادث وفي الإبلاغ عن حادث ينبغي أن يتوافر للمرء فهم لكيفية كشف الحوادث ومناولتها وحل مشكلتها. ومن خلال إقامة هيكل عام بشأن الحوادث (أي الحوادث المادية أو الإدارية أو التنظيمية أو المنطقية) من الممكن الحصول على صورة عامة للبنية والتدفق الخاصين بحادث ما. وتشكل المصطلحات المتجانسة الأساس اللازم لتوفير فهم مشترك للكلمات والمصطلحات.	17
F.400	نظام مناولة الرسائل ونظرة عامة على الخدمة	توفر هذه التوصية نظرة عامة على تعريف النظام الشامل وخدمة نظام مناولة الرسائل MHS وتقدم نظرةً عامة للنظام MHS. وهذه النظرة هي واحدة من مجموعة توصيات تصف نموذج النظام وعناصر خدمة النظام ونظام خدمات مناولة الرسائل (MHS). وتستعرض هذه التوصية قدرات نظام مناولة الرسائل الذي تستخدمه وكالات توفير الخدمة من أجل توفير خدمات عمومية لمناولة الرسائل (MH) تمكن المستعملين من تبادل الرسائل على أساس التخزين وإعادة الإرسال. ويُصمم نظام مناولة الرسائل طبقاً لمبادئ نموذج مرجعي لتوصيل بيني لأنظمة مفتوحة (OSI نموذج مرجعي) للتطبيقات في قطاع تقييس الاتصالات (X.200) ويستعمل خدمات طبقة العرض والخدمات التي تقدمها عناصر خدمة تطبيقات أخرى أكثر عمومية. ويمكن إنشاء نظام مناولة الرسائل باستخدام أي شبكة تناسب نطاق التوصيل البيني للأنظمة المفتوحة OSI. وتكون خدمة نقل الرسائل التي توفرها خدمة نقل الرسائل مستقلة التطبيق. ومن أمثلة التطبيقات المقيسة خدمة المراسلة فيما بين الأشخاص (X.420 + F.420)، وخدمة مراسلة تبادل البيانات الإلكترونية (X.435 + F.435) وخدمة المراسلة الصوتية (X.440 + F.440). ويمكن للأنظمة الطرفية أن تستخدم خدمة نقل الرسائل (MT) لتطبيقات محددة معروف أنها ثنائية. وتخص خدمات مناولة الرسائل التي يوفرها مزودو الخدمة زمرة الخدمات التليماتية. ويرد تعريف الخدمات العمومية المبنية على نظام مناولة الرسائل وكذلك النفاذ إلى نظام مناولة الرسائل للخدمات العمومية ومنه في سلسلة توصيات F.400. ويرد تعريف معمارية النظام الشامل لنظام مناولة الرسائل في التوصية ITU-T X.402. وعناصر الخدمة هي خصائص الخدمة الموفرة من خلال عمليات التطبيق. وتعتبر عناصر الخدمة مكونات الخدمة الموفرة للمستعملين وهي إما عناصر خدمة أساسية أو أنها تسهيلات اختيارية للمستعملين وهي مصنفة على أنها تسهيلات ضرورية اختيارية للمستعملين أو تسهيلات إضافية اختيارية للمستعملين. ويرد وصف قدرات الأمن لنظام مناولة الرسائل في الفقرة 15 من التوصية F.400 بما في ذلك تهديدات أمن نظام مناولة الرسائل. ونموذج الأمن وعناصر الخدمة التي تصف خصائص الأمن (معرّفة في الملحق B) وإدارة الأمن ومكونات أمن نظام مناولة الرسائل، وأمن المراسلة فيما بين الأشخاص.	17

F.440	خدمة مناولة الرسائل: خدمة المراسلة الصوتية	تحدد هذه التوصية جوانب الخدمة العامة والاختيارية ونوعياتها لخدمة المراسلة الصوتية العمومية الدولية (VM)، وهو نوع محدد من خدمة مناولة الرسائل (MH)، وهي خدمة اتصالات دولية تقدمها إدارات تمكّن المشتركين من إرسال رسالة لمستقبل أو أكثر وتسلّم رسائل عبر شبكات الاتصالات باستخدام الجمع بين التخزين وإعادة الإرسال وتقنيات التخزين والاسترداد. وتمكن خدمة المراسلة الصوتية المشتركين من طلب خصائص متنوعة لأدائها خلال مناولة وتبادل الرسائل الصوتية المشفرة. وبعض الخصائص ملازمة في خدمة المراسلة الصوتية الأساسية، ويمكن للمشترك اختيار خصائص غير أساسية سواء على أساس كل إرسال على حدة أو لفترة من الوقت تعاقدية متفق عليها، إذا كانت توفرها الإدارة. ويمكن توفير مراسلة اتصال بيني مع خدمة مراسلة فيما بين الأشخاص (IPM) كخيار في خدمة المراسلة الصوتية. ويتعين أن تتيح الإدارات دولياً خصائص أساسية. وتصنّف الخصائص غير الأساسية الواضحة للمشترك، إما على أنها أساسية أو إضافية. وينبغي للإدارات أن تتيح دولياً الخصائص الأساسية الاختيارية ويمكن أن تتيح بعض الإدارات الخصائص الإضافية الاختيارية للاستخدام الوطني والدولي على أساس اتفاق ثنائي. وتُسمى الخصائص غير الأساسية تسهيلات اختيارية للمستعمل (VM) باستخدام أي شبكة اتصالات. ويمكن عرض خدمة المراسلة الصوتية على نحو منفصل أو الجمع بين خدمات التليماتية المختلفة أو اتصالات البيانات وترد في سلسلة التوصيات X.400 المواصفات والبروتوكولات المستخدمة في خدمة المراسلة الصوتية. الملحق زاي: تأمين عناصر خدمة المراسلة الصوتية؛ الملحق حاء: نظرة عامة لأمن المراسلة الصوتية.	17
F.851	خدمة الاتصالات الشخصية العالمية (UPT) – وصف الخدمة (مجموعة الخدمات 1)	ترمي هذه التوصية إلى وصف خدمة الاتصالات الشخصية العالمية (UPT) والأحكام المتعلقة بتشغيلها. وتقدم هذه التوصية وصفاً عاماً للخدمة من وجهة نظر المشترك الفردي في الاتصالات الشخصية العالمية أو مستعملها. وتسمح هذه الاتصالات أيضاً لمستخدمها بالمشاركة في مجموعة من الخدمات المشمولة في الاشتراك والتي يحددها المستعمل بنفسه لتشكل مظهراً جانبياً للخدمة. ويمكن لمستعمل هذه الاتصالات أن يستخدم خدمة الاتصالات الشخصية العالمية مع حد أدنى من مخاطر انتهاك الخصوصية أو الترسيم الخاطئ الذي يرجع إلى الاستخدام الاحتيالي. ومن ناحية المبدأ، يمكن استخدام خدمات الاتصالات الأساسية مع خدمة الاتصالات الشخصية العالمية. وتقتصر الخدمات المقدمة لمستعمل على الاتصالات فقط على الشبكات والمطاريف المستخدمة. ويكون من بين الخصائص الضرورية للمستعمل "*الاستيقان من هوية مستعمل الاتصالات الشخصية العالمية*"، وكخيار لخاصية المستعمل هنالك *الاستيقان* من وكالة *تقديم* خدمة الاتصالات الشخصية العالمية. ويرد في القسم 4.4 تفاصيل متطلبات الأمن.	2
G.808.1	تبديل الحماية النمطية – حماية خطية لمسلك الشبكة الفرعية	توفر هذه التوصية نظرة عامة على تبديل الحماية الخطية. وهي تغطي شبكات النقل البصرية (OTN)، وشبكات التراتب الرقمي المتزامن (SDH)، وشبكات النقل بأسلوب النقل غير المتزامن (ATM) المستندة إلى مخططات الحماية. وستوفر في توصيات أخرى نظرات عامة لحلقة الحماية والشبكة الفرعية مزدوجة العقد (على سبيل المثال الحلقة).	15
G.827	معلمات وأهداف التيسر للمسيرات الدولية الرقمية من طرف إلى طرف بمعدّل بتات ثابت	تعرّف هذه التوصية معلمات وأهداف أداء الشبكات بالنسبة لعناصر المسير وتيسر المسيرات الدولية الرقمية من طرف إلى طرف بمعدّل بتات ثابت. وهذه المعلمات مستقلة عن نمط الشبكة المادية الداعمة للمسير من طرف إلى طرف، على سبيل المثال، الألياف البصرية، المرحِّلة الراديوية أو الساتل. وثمة إرشادات مدرجة بشأن طرق تحسين التيسر وحساب التيسر من طرف إلى طرف بخليط من عناصر الشبكة.	12
G.841	أنماط وخصائص معماريات حماية شبكات التراتب الرقمي المتزامن (SDH)	تصف هذه التوصية مختلف آليات حماية شبكات التراتب الرقمي المتزامن (SDH) وأهدافها وتطبيقاتها. وتصنّف مخططات الحماية باعتبارها حماية تسجيل التراتب الرقمي المتزامن (في طبقة القسم أو المسير) وحماية لتوصيل شبكة فرعية لتراتب رقمي متزامن (مع رصد داخلي ورصد غير مقحم ورصد طبقة فرعية).	15

G.842	التشغيل البيني لمعماريات حماية شبكة التراتب الرقمي المتزامن	تصف هذه التوصية آليات التشغيل البيني لمعمارية حماية الشبكة. ويجري وصف التشغيل البيني للتوصيل البيني لعقدة واحدة ومزدوجة لحركة التبادل بين الحلقات. ويمكن تشكيل كل حلقة لحماية خدمة صيانة متقاسمة أو حماية توصيل الشبكة الفرعية SNCP.	15
G.873.1	شبكة النقل البصرية (OTN)–الحماية الخطية	تعرّف هذه التوصية بروتوكول تبديل الحماية الأوتوماتية وعملية تبديل الحماية لمخططات الحماية الخطية لشبكة النقل البصرية عند مستوى وحدة بيانات القناة البصرية (ODUK). ومخططات الحماية التي تُبحث في هذه التوصية هي حماية تسجيل وحدة بيانات القناة البصرية؛ حماية توصيل الشبكة الفرعية لوحدة بيانات القناة البصرية مع الرصد الداخلي؛ وحماية توصيل الشبكة الفرعية لوحدة بيانات القناة البصرية مع رصد غير مقحم؛ وحماية توصيل الشبكة الفرعية لوحدة بيانات القناة البصرية مع رصد الطبقة الفرعية.	15
G.911	معلمات الاعتمادية والتيسر وطرق حسابها في أنظمة الألياف البصرية	تعرّف هذه التوصية الحد الأدنى لمجموعة معلمات ضرورية لتمييز الاعتمادية وتيسر أنظمة الألياف البصرية. وترد معلمات مختلفة للاعتمادية وصيانة النظام من أجل اعتمادية جهاز بصري نشط ومن أجل اعتمادية جهاز بصري منفعل، ومن أجل اعتمادية الألياف البصرية والكبلات. وتوفر هذه التوصية أيضاً خطوطاً توجيهية وطرقاً لحساب الاعتمادية المتوقعة للأجهزة والوحدات والأنظمة. وتتضمن التوصيات أمثلة.	15
H.233	نظام السرية في الخدمات السمعية المرئية	يتألف نظام *الخصوصية* من جزأين، *آلية السرية* أو *عملية تجفير* المعطيات، ونظام فرعي *لإدارة المفاتيح*. وتصف هذه التوصية الجزء الخاص بالسرية من نظام حماية سرية مناسب لاستخدامه في الخدمات السمعية المرئية ذات النطاق الضيق. ومع أن هذا النظام يستلزم *خوارزمية تجفير*، فإن مواصفات هذه الخوارزمية غير واردة هنا، إذ إن النظام يتقبل عدة خوارزميات محددة. ويمكن تطبيق *نظام السرية* على الوصلات من نقطة إلى نقطة بين المطاريف أو بين مطراف ووحدة تحكم متعددة النقاط؛ ويمكن توسيع نطاق تطبيقه ليشمل التشغيل متعدد النقاط دون فك الشفرة في الوحدة.	16
H.234	إدارة مفاتيح التجفير ونظام الاستيقان من الخدمات السمعية المرئية	يتألف *نظام الخصوصية* من جزأين، *آلية السرية* أو *عملية تجفير* البيانات، ونظام فرعي *لإدارة المفاتيح*. وتصف هذه التوصية طرق *الاستيقان وإدارة المفاتيح* لنظام خصوصية مناسب لاستخدامه في الخدمات السمعية المرئية ذات النطاق الضيق. وتتحقق الخصوصية بواسطة استخدام *مفاتيح سرية*. ويجري تحميل المفاتيح في *جزء السرية* من نظام الخصوصية ومراقبة الطريقة التي يجري بها التجفير وفك تجفير البيانات المرسلة. وإذا تمكن طرف ثالث من النفاذ إلى المفاتيح المستخدمة، يصبح نظام الخصوصية غير آمن. ومن ثم، يصبح حفاظ المستعملين على المفاتيح جزءاً مهماً من نظام الخصوصية. وترد في هذه التوصية ثلاثة طرق عملية بديلة *لإدارة المفاتيح*.	16
H.235	أمن وتجفير المطاريف متعددة الوسائط للسلسلة H (المطاريف H.323 وغيرها من نمط H.245)	تصف هذه التوصية التعزيزات في إطار سلسلة التوصيات H.3xx لتتضمن *خدمات الأمن مثل الاستيقان والخصوصية (تجفير البيانات)*. وينطبق المخطط المقترح على كل من مؤتمرات بسيطة من نقطة إلى نقطة ومتعددة النقاط لأي مطاريف تستخدم التوصية ITU-T H.245. وعلى سبيل المثال تعمل أنظمة H.323 على شبكات قائمة على رزم لا توفر نوعية خدمة مضمونة. ولنفس الأسباب التقنية التي تجعل الشبكة الأساسية لا توفر نوعية الخدمة، لا توفر الشبكة *خدمة آمنة*. وتتضمن الاتصالات الآمنة في الوقت الفعلي عبر شبكات غير آمنة بوجه عام مجالين رئيسيين من مجالات الاهتمام هما *الاستيقان والخصوصية*. وتصف هذه التوصية البنية التحتية للأمن *والتقنيات* المحددة *للخصوصية* التي يتعين استعمالها من قبل السلسلة H.3xx الخاصة بالمطاريف متعددة الوسائط. وستتناول هذه التوصية المجالات المثيرة للاهتمام الخاصة بالمؤتمرات التفاعلية. وتشمل هذه المجالات على سبيل المثال لا الحصر *الاستيقان والخصوصية* بالنسبة لجميع تدفقات الوسائط في الوقت الفعلي التي يتم تبادلها في المؤتمر. وتوفر التوصية البروتوكول والخوارزمية اللازمة بين كيانات H.323. وتستخدم هذه التوصية التسهيلات العامة المدعمة في التوصية ITU-T H.245 وبهذه الصفة يمكن لأي معيار يعمل بالتضافر مع بروتوكول التحكم هذا أن يستخدم هذا الإطار للأمن. ومن المتوقع حيثما أمكن أن تستطيع مطاريف أخرى للسلسلة H العمل بينياً وأن تستخدم مباشرة الأساليب الوارد وصفها في هذه التوصية. ولن توفر هذه التوصية بصورة أولية تنفيذاً كاملاً في جميع المجالات، كما أنها ستبرز على وجه التحديد *استيقان النقطة الطرفية وخصوصية الوسائط*.	16

		وتتضمن القدرة على التفاوض بشأن الخدمات والعناصر الوظيفية عموماً وعلى الانتقائية فيما يتعلق بتقنيات وقدرات التجفير المستخدمة. وتتعلق الطريقة المحددة التي تستخدم بها بقدرات الأنظمة، ومتطلبات التطبيق وتقييدات السياسة الأمنية المحددة. وهي تدعم خوارزميات تجفيرية متنوعة مع خيارات متنوعة ملائمة لمختلف الأغراض: على سبيل المثال أطوال المفاتيح. ويمكن أن توزع بعض *الخوارزميات التجفيرية* على خدمات أمنية محددة (على سبيل المثال واحدة بالنسبة لتجفير تدفق الوسائط والآخر بالنسبة لتجفير التشوير). وينبغي الإشارة أيضاً إلى أن بعض خوارزميات أو آليات التجفير المتيسرة يمكن حجزها للتصدير أو لأية مسائل وطنية أخرى (على سبيل المثال مع أطوال مفاتيح مقيّدة). وتدعم هذه التوصية تشوير الخوارزميات المعروفة جيداً بالإضافة إلى تشوير خوارزميات التجفير غير المقيسة أو المسجلة الملكية. ولا توجد خوارزميات ملزمة على وجه التحديد: إلاّ أنه يُقترح بشدّة أن تدِّعم النقاط الطرفية أكبر عدد ممكن من الخوارزميات المطبقة من أجل تحقيق التشغيل البيني. ويوازي هذا المفهوم الذي مؤداه أن دعم التوصية ITU-T H.245 لا يضمن التشغيل البيني بين كودكي كيانين. وتحل الطبعة 2 من التوصية ITU-T H.235 محل الطبعة 1 من التوصية H.235 التي تعرض عدة تحسينات من مثل تجفير المنحنى الإهليلجي، والمظاهر الجانبية للأمن (توقيعات قائمة على كلمة سر بسيطة ورقمية متطورة)، وتدابير مضادة جديدة لتوفير الأمن (مكافحة الرسائل الاقتحامية للوسائط)، ودعم خوارزمية التجفير المتقدمة (AES)، ودعم الخدمة الطرفية الخلفية، ومُعرّفات الأغراض المحددة والتغييرات المتضمنة من دليل المنفذين H.323. وتحل الطبعة 3 من H.235 محل الطبعة 2 من H.235 وتصف سمات إجراء الإشارات متعددة الترددات بنغمة مزدوجة DTMF، ومعرّفات الأغراض بالنسبة لخوارزمية التجفير المتقدمة لتجفير الحمولة النافعة للوسائط، أسلوب (OFB أسلوب الخرج بالتغذية الراجعة) المحسّن (EOFB) لتجفير التدفق من الوسائط، كما تصف خياراً للاستيقان فقط في الملحق دال من أجل اجتياز سلس لترجمة عنوان الشبكة NAT/جدار الحماية، وإجراء توزيع مفتاح على قناة RAS، وإجراءات لنقل مفتاح الدورة بطريقة أكثر أمناً، وتوزيع وتحديث أقوى لمفاتيح الدورات، وإجراءات لتأمين تدفقات متعددة للحمولة النافعة، ودعم أفضل للأمن من أجل النداءات المسيرة مباشرة في ملحق طاء جديد، وتشوير وسائل للإبلاغ عن الأخطاء بطريقة أكثر مرونة وإجراء توضيحات وتحسينات في الكفاءة لأمن الانطلاق السريع ولتشوير ديفي هيلمان إلى جانب معلمات ديفي هيلمان الأطول والتغييرات المتضمنة من دليل منفذي H.323. الملحق واو/H.235: *الملامح العامة المهجنة للأمن*. يصف هذا الملحق *مظهراً جانبياً مهجناً للأمن قائماً على بنية تحتية للمفاتيح العمومية*، فعالاً وقابلاً للاتساع، ينتشر *بتواقيع رقمية* من التوصية H.235 الملحق هاء وينتشر *بمظهر جانبي لخط أساس أمن* من التوصية H.235 الملحق دال. ويعتبر هذا الملحق خياراً. وقد تنفذ *كيانات الأمن* التوصية H.323 (مطاريف وبوابون وبوابات ووحدات مراقبة متعددة النقاط، وما إلى ذلك) هذا *المظهر الجانبي المهجن للأمن* لتحسين الأمن أو عندما يكون مطلوباً. وتعني فكرة "مهجن" في هذا النص تطبيق إجراءات أمن فعلية من المظهر الجانبي للتوقيع في التوصية H.235 الملحق هاء على نحو سريع؛ وما تزال التواقيع الرقمية تتطابق مع إجراءات خوارزمية ريفست وشامير وأدلمان (RSA) بالمفتاح العمومي. ومع ذلك، تنتشر *التواقيع الرقمية* عندما تكون ضرورية فقط وإلا تستخدم *تقنيات أمن متناظرة* فعالة من المظهر الجانبي لأمن خط الأساس في التوصية H.235 الملحق دال. وينطبق المظهر الجانبي المهجن للأمن على المهاتفة التي يمكن قياسها "عالمياً" باستخدام بروتوكول الإنترنت. ويتغلب المظهر الجانبي للأمن على حدود مظهر جانبي للأمن بسيط وخط أساس التوصية H.235 الملحق دال عند تطبيقه بصرامة. وفضلاً عن ذلك، يتغلب المظهر الجانبي للأمن على بعض قيود التوصية H.235 الملحق هاء مثل الحاجة إلى عرض نطاق أعلى وحاجات أداء متزايد للمعالجة عند تطبيقه بصرامة. فمثلاً، لا يعتمد المظهر الجانبي المهجن للأمن على إدارة (سكونية) لأسرار متبادلة متقاسمة لقفزات في ميادين مختلفة. ومن ثم، يمكن للمستعملين اختيار مزود خدمة نقل الصوت باستعمال بروتوكول الإنترنت بشكل أسهل. ولهذا، يدعم المظهر الجانبي للأمن هذا نوعاً من التنقلية كذلك. ويطبق التجفير اللاتناظري مع تواقيع وشهادات عند الضرورة فقط وإلا يستخدم تقنيات تناظرية أكثر بساطة وأكثر كفاءة. ويتم توفير مرور رسائل التوصية H.245 عبر نفق لسلامة رسائل التوصية H.245 وتوفير عدم رفض الرسائل. ويفوض المظهر الجانبي المهجن للأمن نموذجاً يسيّره بواب ويقوم على أساس تقنيات أنفاق التوصية H.245؛ أما النماذج غير المسيّرة من بواب فتحتاج لمزيد من الدراسة.

		الملحق زاي/H.235: *استعمال بروتوكول إدارة المفاتيح MIKEY مع بروتوكول النقل المؤمَّن SRTP في أنظمة H.235*. يمكّن هذا الملحق من نشر أمن وسائط بروتوكول النقل المؤمَّن في الوقت الفعلي (SRTP) بحسب IETF حيث يوفّر بروتوكول إدارة المفاتيح MIKEY المفاتيح ومعلمات الأمن اللازمة فيما بين النقاط الطرفية من طرف إلى طرف المعينة. ويمكن نشر الملحق زاي في ميدان H.323 بين أنظمة H.235 وأنظمة الملحق زاي الممكّنة H.323. ويحدد الملحق تمديدات بروتوكول الأمن إلى RAS H.225.0 وتشوير النداء فضلاً عن H.245 مع الإجراءات المناسبة. وبالإضافة إلى ذلك، يوفّر هذا الملحق القدرات اللازمة لدعم التشغيل البيني مع الكيانات IETF SIP التي نفّذت بروتوكول إدارة المفاتيح MIKEY والبروتوكول SRTP. وينبغي الإشارة إلى أن هذا الملحق مكتوب كملمح عام لأمن H.235 الذي يُعرض كخيار، ويمكن أن يستكمل السمات الأمنية الأخرى للوسائط الخاصة بالتوصية H.235 (انظر الملحقين باء ودال.7). **ملاحظة** – أعيد تشكيل هيكل H.235 على النحو التالي: • H.235.0، H.323 الأمن: إطار للأمن في السلسلة H (H.323 وغيرها القائمة على H.245) الأنظمة متعددة الوسائط • H.235.1، H.323 الأمن: مواصفة الأمن الأساسي • H.235.2، H.323 الأمن: مواصفة الأمن بالتواقيع • H.235.3، H.323 الأمن: مواصفة الأمن الهجينة • H.235.4، H.323 الأمن: الأمن المباشر والانتقائي للنداء المسيّر • H.235.5، H.323 الأمن: إطار للاستيقان المأمون خلال تبادل رسائل التسجيل والقبول والوضع (RAS) بواسطة أسرار متقاسمة ضعيفة • H.235.6، H.323 الأمن: مواصفة التجفير الصوتي بإدارة مفاتيح أصلية H.245/H.235 • H.235.7، H.323 الأمن: استعمال بروتوكول إدارة المفاتيح MIKEY من أجل بروتوكول النقل المؤمن في الوقت الفعلي في إطار H.235 • H.235.8، H.323 الأمن: تبادل المفاتيح من أجل البروتوكول SRTP باستعمال قنوات تشوير مؤمنة • H.235.9، H.323 الأمن: دعم بوابة الأمن من أجل H.323	
H.323	نظام اتصالات لوسائط متعددة قائم على الرزم	تصف هذه التوصية مطاريف وكيانات أخرى توفر خدمات اتصالات سمعية وفيديوية وبيانات و/أو وسائط متعددة في الوقت الفعلي عبر شبكات قائمة على رزم قد لا تضمن نوعية الخدمة. إن الدعم السمعي إلزامي، أما البيانات والفيديو فهما اختياريان، أما إذا تم دعمهما، فتكون قدرة استخدام أسلوب التشغيل المشترك إلزامية بحيث يمكن لجميع المطاريف الداعمة لنوع الوسائط ربطها بينياً. وقد تشمل الشبكة القائمة على الرزم شبكات مناطق محلية أو شبكات مناطق مؤسسات أو شبكات مناطق حضرية أو شبكات داخلية أو شبكات توصيلية (بما في ذلك الإنترنت) أو توصيلات من نقطة إلى نقطة أو جزء واحد من شبكة أو شبكة توصيل ذات أجزاء متعددة مع طوبولوجيات معقدة، وبالتالي يمكن للكيانات أن تستخدم تشكيلات من نقطة إلى نقطة أو نقاط متعددة أو إذاعية. ويمكن لهذه الكيانات أن تشتغل بينياً مع مطاريف على شبكة رقمية متكاملة الخدمات ذات نطاق عريض وشبكة رقمية متكاملة الخدمات ذات نطاق ضيق وضمان نوعية خدمة شبكات المناطق المحلية والشبكة الهاتفية العمومية التبديلية و/أو الشبكات اللاسلكية، ويمكن دمجها في الحواسيب الشخصية أو تنفيذها في أجهزة قائمة بذاتها مثل الهواتف المرئية. الملحق ياء: الأمن لأنماط النقاط الطرفية البسيطة.	16
H.350.2	معمارية خدمات الدليل للتوصية H.235	تصف هذه التوصية مخطط بروتوكول سريع النفاذ إلى الدليل (LDAP) لتمثيل عناصر H.235. وهي من صنف مساعد يتعلق بالتوصية H.350 كما تشتق كثيراً من عناصرها الوظيفية من المعمارية. وينبغي للمنفذين أن يستعرضوا H.350 بالتفصيل قبل الشروع في تنفيذ هذه التوصية. إذ تتضمن نعوتها عناصر هوية وكلمة سر وشهادة H.235. ويمكن تحميل هذه العناصر إلى نقطة طرفية من أجل تشكيل أوتوماتي أو لكي ينفذ إليها حارس بوابة من أجل تشوير واستيقان النداء. ولا يشمل مجال تطبيق هذه التوصية النهج المعيارية لاستعمال دليل البروتوكول سريع النفاذ إلى الدليل LDAP ذاته أو استعمال البيانات التي يتضمنها. والغرض من هذا المخطط ليس تمثيل جميع عناصر البيانات الممكنة في البروتوكول H.235 وإنما تمثيل المجموعة الدنيا اللازمة لتحقيق أهداف التصميم التي سُردت في H.350.	16

H.530	إجراءات الأمن التناظرية للتوصية H.510 في البيئات المتنقلة للتوصية H.323	توفر هذه التوصية إجراءات الأمن في بيئات متنقلة للتوصية H.323 مثلاً بناء على منظور التوصية H.510 الذي يصف تنقلية الأنظمة والخدمات للوسائط المتعددة للتوصية H.323. وتوفر هذه التوصية تفاصيل حول إجراءات أمن التوصية H.510. وحتى الآن، تصمم مقدرات تشوير التوصية H.235 في صيغة 1 و2 لمناولة الأمن في بيئات معظمها سكوني للتوصية H.323. ويمكن أن تحقق تلك البيئات وأنظمة الوسائط المتعددة بعض التنقلية المحدودة في مناطق بوابين؛ ولا توفر التوصية H.323 بشكل عام والتوصية H.235 بشكل خاص إلا الدعم القليل لتجول آمن للمستعملين المتنقلين والمطاريف عبر ميادين مختلفة مع كيانات كثيرة متضمنة في بيئة تنقل موزعة مثلاً. وتعرض سيناريوهات تنقلية التوصية H.323 الموصوفة في التوصية H.510 فيما يتعلق بالتنقلية الطرفية حالة جديدة مع سمة مرنة وديناميةٍ من وجهة نظر الأمن أيضاً. ويتعين الاستيقان من المستعملين الجوالين للتوصية H.323 والمطاريف المتنقلة من قبل ميدان أجنبي مزار. وبالمثل، يود المستعمل المتنقل أن يحصل على إثبات الهوية الحقيقية للميدان المزار. وبالإضافة إلى ذلك، قد يكون من المفيد الحصول على إثبات هوية مطاريف تستكمل الاستيقان من المستعمل. ومن ثم، تطلب هذه المتطلبات من أجل الاستيقان المتبادل للمستعمل والميدان المزار واختيارياً أيضاً لهوية المطراف. وبما أن المستعمل المتنقل معروف فقط للميدان المحلي حيث يكون مشتركاً له كلمة سر، لا يعرف الميدان المزار المستعمل المتنقل في البداية. وفي هذه الحالة، لا يتقاسم الميدان المزار أي علاقة أمن قائمة مع المستعمل المتنقل والمطراف المتنقل. ومن أجل أن يحقق الميدان المزار الاستيقان وضمان تخويل المستعمل المتنقل والمطراف المتنقل، يفوض الميدان المزار بعض مهمات الأمن مثل التحقق من الترخيص أو إدارة المفاتيح لميدان محلي من خلال الشبكة الوسيطة وكيانات الخدمة. ويتطلب هذا تأمين الاتصالات وإدارة المفاتيح فيما بين الميدان المزار والميدان المحلي أيضاً. وبينما تكون البيئات المتنقلة للتوصية H.323 من حيث المبدأ مفتوحة أكثر من الشبكات المغلقة للتوصية H.323، هناك بالطبع حاجة أيضاً لتأمين مهمات إدارة المفاتيح على نحو صحيح. وصحيح أيضاً أن الاتصالات في الميادين المتنقلة وعبرها تستحق الحماية من العبث المؤذي.	16
J.93	متطلبات النفاذ المشروط في التوزيع الثانوي لتلفزيون رقمي أو أنظمة تلفزيون كبلي	تعرّف هذه التوصية خصوصية البيانات ومتطلبات النفاذ لحماية شفرات تلفزيون رقمي لفريق خبراء الصور المتحركة (MPEG) تمر عبر شبكات التلفزيون الكبلية بين طرف رأسية الكبل والمشترك النهائي. ولا توجد خوارزميات مجفرة دقيقة مستخدمة في هذه العملية في التوصية J.93 لأنها تحدد إقليمياً و/أو تحددها الصناعة.	9
J.96	الطريقة التقنية لضمان خصوصية إرسال تلفزيوني دولي لمسافة بعيدة لفريق خبراء الصور المتحركة MPEG-2 بموجب التوصية ITU-T J.89	تحتوي هذه التوصية على معيار مشترك لنظام نفاذ مشروط لإرسال دولي لمسافة بعيدة لتلفزيون رقمي طبقاً للمواصفة المهنية لفريق خبراء الصور المتحركة MPEG-2 (4:2:2). وتصف نظاماً أساسياً لتخليط التشغيل البيني (BISS) القائم على مواصفة إذاعة فيديوية رقمية – خوارزمية تخليط مشتركة باستخدام المفاتيح الواضحة الثابتة تسمى كلمات الجلسة. ويقدم أسلوب متلائم خلفي آخر آلية إضافية لإدراج كلمات الجلسة المجفرة، بينما يحتفظ في نفس الوقت بقابلية التشغيل البيني.	9
J.112	أنظمة إرسال الخدمات التفاعلية للتلفزيون الكبلي	أُنشئت خدمات التلفزيون الرقمي في بلدان كثيرة، كما أن فوائد تمديد هذه الخدمات لتوفر خدمات تفاعلية أمر مُسلَّم به على نطاق واسع. وأنظمة توزيع التلفزيون الكبلي مناسبة بوجه خاص لتنفيذ خدمات البيانات ثنائية الاتجاه. وهذه التوصية تستكمل وتوسع نطاق J.83 "الأنظمة الرقمية متعددة البرامج للخدمات التلفزيونية والصوتية وخدمات البيانات من أجل التوزيع الكبلي" لتتيح توفير بيانات ثنائية الاتجاه عبر كوابل متحدة المحور وكوابل الألياف الهجينة متحدة المحور من أجل الخدمات التفاعلية. كما تتضمن التوصية عِدَّة ملحقات اعترافاً ببيئات الوسائط القائمة المختلفة. ويوصى من أجل إدخال النفاذ السريع إلى الإنترنت و/أو الخدمات التفاعلية للتلفزيون الكبلي، بأن تُستخدم الأنظمة لتحقيق فوائد وفورات الحجم الكبير، وتسهيل التشغيل البيني. وهي تُحدِّد متطلبات الأمن واستعمال بيانات نظام تخزين الوثائق SP-DOCSS عبر مواصفة نظام (DOCSS) لنظام الأمن الكبلي؛ ومواصفة وحدات الأمن النمطية القابلة للإزالة (SP-RSM) ومواصفة أمن البيانات الأساسية عبر الكبل (SP-BDS).	9

J.160	الإطار المعماري لتقديم خدمات في الوقت الحرج على شبكات تلفزيون كبلية تستعمل مودمات كبلية	توفر هذه التوصية الإطار المعماري الذي يمكن مشغلي التلفزيون الكبلي من توفير خدمات في الوقت الحرج عبر شبكاتهم التي عُزِّزت لتدعِّم مودمات كبلية. وتتمثل خدمات الأمن المتيسرة من خلال طبقة الخدمة الرئيسية للاتصالات الكبلية باستخدام بروتوكول الإنترنت في الاستيقان، ومراقبة النفاذ، والسلامة، والسرية، وعدم الإنكار. ويمكن لسطح بيني في بروتوكول الاتصالات الكبلية بواسطة IPCablecom أن يستخدم واحداً أو أكثر أو لا يستخدم أياً من هذه الخدمات لتلبية متطلباته الأمنية الخاصة. ويتناول أمن IPCablecom المتطلبات الأمنية لكل سطح بيني لمكونات البروتوكول من خلال ما يلي: • تحديد نموذج التهديد الخاص بكل سطح بيني لمكونات البروتوكول؛ • تحديد الخدمات الأمنية (الاستيقان، الترخيص، السرية، السلامة، عدم الإنكار) اللازمة لمواجهة التهديدات المحدّدة؛ • تحديد آلية الأمن الخاصة التي توفر خدمات الأمن اللازمة. وتشمل آليات الأمن كلاً من بروتوكول الأمن (على سبيل المثال IPsec وأمن طبقة RTP وأمن SNMPv3) وبروتوكول إدارة المفاتيح الداعم (على سبيل المثال IKE، PKINIT/Kerberos).	9
J.170	مواصفات أمن الاتصالات الكبلية باستخدام بروتوكول الإنترنت IPCablecom	تعرّف هذه التوصية معمارية الأمن والبروتوكولات والخوارزميات والمتطلبات الوظيفية المصاحبة وأي متطلبات تقنية يمكنها توفير الأمن لنظام شبكة الاتصالات الكبلية باستخدام بروتوكول الإنترنت. وينبغي توفير *خدمات أمن الاستيقان والتحكم في النفاذ وسلامة محتوى الرسالة والحمالة والسرية وعدم التنصل*، كما عرّفت لكل السطوح البينية لعناصر الشبكة.	9
J.191	رزمة خواص بروتوكول الإنترنت لتعزيز المودمات الكبلية	توفر هذه التوصية مجموعة من الخواص القائمة على بروتوكول الإنترنت التي يمكن إضافتها إلى المودم الكبلي بحيث تمكن مشغلي الكبل من توفير مجموعة إضافية من الخدمات المعزّزة إلى زبائنهم بما في ذلك تقديم الدعم لنوعية خدمات (QoS) الاتصالات الكبلية بواسطة بروتوكول الإنترنت، والأمن المعزز، وخواص إضافية للتنظيم الإداري وتوفير الخدمات، ومناولة محسّنة لتوجيه العناوين والرزم. وتكمن هذه الخواص القائمة على بروتوكول الإنترنت في العنصر المنطقي لخدمة بوابة (PS أو مجرّد البوابة). والمودم الكبلي الذي يحتوي على هذه الخواص المعزّزة هو مودم كبلي معزّز لبروتوكول الإنترنت (IPCM) وهو تنفيذ لصنف جهاز J.190 HA. ويشمل صنف الجهاز HA حسبما وصف في التوصية ITU-T J.190 العنصر الوظيفي للمودم الكبلي بالإضافة إلى العنصر الوظيفي لخدمات البوابة على السواء. والفصل 11 الأمن: يعرف السطوح البينية للأمن وبروتوكولاته ومتطلباته الوظيفية اللازمة لتقديم خدمات موثوقة قائمة على بروتوكول الإنترنت في بيئة مؤمَّنة لخدمة البوابة. والغرض من أي تكنولوجيا للأمن هو حماية قيمة، سواء تدفق لدخل أو نمط من أصول المعلومات القابلة للشراء. وتحدث التهديدات لتدفق الدخل هذا عندما يدرك مستعمل للشبكة القيمة وينفق الجهد والمال ويبتكر تقنية من أجل تجنّب المدفوعات اللازمة. الملحق جيم: تهديدات الأمن والتدابير الوقائية.	9
M.3010	مبادئ شبكة إدارة الاتصالات	تعرّف هذه التوصية مفاهيم معمارية شبكة إدارة الاتصالات (معمارية وظيفية لشبكة إدارة الاتصالات ومعمارية معلومات شبكة إدارة الاتصالات والمعماريات المادية لشبكة إدارة الاتصالات) وعناصرها الأساسية. وتصف هذه التوصية العلاقة فيما بين ثلاث معماريات وتوفر إطاراً لاشتقاق متطلبات مواصفات لمعماريات مادية لشبكة إدارة الاتصالات من معماريات وظيفية ومعلومات شبكة إدارة الاتصالات. ويتوفر نموذج مرجعي منطقي لتقسيم وظيفة الإدارة وهو معمارية منطقة الطبقات (LLA). وتعرّف هذه التوصية أيضاً كيفية بيان تطابق وامتثال شبكة إدارة الاتصالات لغرض تحقيق قابلية التشغيل البيني. وتشمل متطلبات شبكة إدارة الاتصالات القدرة على ضمان النفاذ الآمن للمستعملين المخولين إلى معلومات الإدارة. وتشمل شبكة إدارة الاتصالات قدرات وظيفية يجري فيها أداء عنصر وظيفي للأمن بواسطة تقنيات أمن لحماية بيئة شبكة إدارة الاتصالات لضمان سلامة المعلومات المتبادلة عبر السطوح البينية والموجودة في تطبيق الإدارة. وتتعلق أيضاً مبادئ وآليات الأمن بمراقبة حقوق نفاذ مستعملي شبكة إدارة الاتصالات إلى معلومات مرتبطة بتطبيقات شبكة إدارة الاتصالات.	4

M.3016	الأمن في مستوى الإدارة	توفر هذه التوصية نظرة عامة وإطاراً يعرِّف تهديدات الأمن لشبكة إدارة الاتصالات وتوجز كيفية تطبيق خدمات الأمن المتاحة في سياق معمارية وظيفية لشبكة إدارة الاتصالات، كما وصفت في التوصية ITU-T M.3010. وهذه التوصية عمومية في طابعها ولا تعرف أو تتناول متطلبات لسطح بيني محدد لشبكة إدارة الاتصالات. **ملاحظة** – أُعيد تشكيل هيكل التوصية ITU-T M.3016 كما يلي: • M.3016.0 – الأمن في مستوي الإدارة: نظرة شاملة • M.3016.1 – الأمن في مستوي الإدارة: متطلبات الأمن • M.3016.2 – الأمن في مستوي الإدارة: خدمات الأمن • M.3016.3 – الأمن في مستوي الإدارة: آلية الأمن • M.3016.4 – الأمن في مستوي الإدارة: نموذج مواصفات	4
M.3210.1	خدمات إدارة شبكة إدارة الاتصالات TMN لإدارة أمن الاتصالات المتنقلة الدولية–2000	هذه التوصية واحدة من سلسلة توصيات خدمة إدارة شبكة إدارة الاتصالات التي توفر وصفاً لخدمات الإدارة وأهدافها وسياقها فيما يتعلق بجوانب إدارة شبكات الاتصالات المتنقلة الدولية 2000. وتصف هذه التوصية مجموعة فرعية لخدمات إدارة الأمن لتوفير متطلبات وتحليل إدارة الأمن والمظهر الجانبي *لإدارة الاحتيال* في الشبكة المتنقلة للاتصالات المتنقلة الدولية 2000. والتأكيد هو على السطح البيني X بين مزودين للخدمة وخدمات الإدارة المطلوبة بين الاثنين لكشف ومنع الاحتيال بواسطة تشغيل نظام جمع المعلومات عن الاحتيال (FIGS) كوسيلة لرصد مجموعة محددة من أنشطة المشتركين تحد من تعرضهم المالي لفواتير كبيرة غير مسددة وجدت في حسابات المشترك بينما يقوم هذا المشترك بالتجول. وتبنى هذه التوصية على مجموعة الوظائف المعرفة في التوصية ITU-T M.3400 بواسطة تحديد مجموعات وظائف جديدة ووظائف ومعلمات وإضافة المزيد من الدلالات والتقييدات.	4
M.3320	إطار متطلبات الإدارة للسطح البيني لشبكة إدارة الاتصالات TMN X	هذه التوصية جزء من سلسلة توصيات تتناول نقل المعلومات لإدارة شبكات وخدمات الاتصالات، وتتناول بعض الأجزاء فقط جوانب الأمن. والغرض من هذه التوصية تعريف إطار متطلبات لجميع المتطلبات الوظيفية والخدمة ومستوى الشبكة لتبادل معلومات شبكة إدارة الاتصالات بين الإدارات. وتوفر هذه التوصية أيضاً الإطار العام لاستخدام السطح البيني X لشبكة إدارة الاتصالات لتبادل المعلومات بين الإدارات ووكالات التشغيل المعترف بها ومشغلي شبكات آخرين وزبائن وكيانات أخرى. وتتضمن مواصفات متطلبات الأمن للسطح البيني X لشبكة إدارة الاتصالات.	4
M.3400	وظائف إدارة شبكة إدارة الاتصالات	هذه التوصية جزء من سلسلة توصيات شبكة إدارة الاتصالات حيث توفر مواصفات وظائف إدارة شبكة إدارة الاتصالات ومجموعة وظائف إدارة شبكة إدارة الاتصالات. وقد وضع المحتوى لدعم قاعدة معلومات مهمات B (أدوار وموارد ووظائف) مرتبطة بالمهام 2 (وصف سياق إدارة شبكة إدارة الاتصالات) في منهجية مواصفات السطح البيني لشبكة إدارة الاتصالات المحددة في التوصية ITU-T M.3020. وعند أداء تحليل سياق إدارة شبكة إدارة الاتصالات، من المستصوب النظر في الاستخدام الأمثل لمجموعات وظائف إدارة شبكة إدارة الاتصالات المتاحة في هذه التوصية. وتشمل التوصية وصفاً لوظيفة إدارة الأمن التي تدعمها شبكة إدارة الاتصالات.	4
Q.293	الفترات التي يتعين فيها اتخاذ تدابير الأمن	هذا مقتطف من الكتاب الأزرق ويحتوي فقط على الأقسام من 5.8 (الفترات التي يتعين فيها اتخاذ تدابير الأمن) إلى 9.8 (طريقة تقاسم الحمولة) من التوصية Q.293.	4
Q.813	عناصر خدمة تطبيق تحويلات الأمن من أجل عناصر خدمة العمليات عن بعد (STASE-ROSE)	توفر هذه التوصية مواصفات لدعم تحويلات الأمن مثل *التجفير والفرم والختم والتوقيع* مع التركيز على عناصر خدمة العمليات عن بُعد (ROSE) لوحدات بيانات البروتوكول (PDUs). وتستخدم تحويلات الأمن لتوفير خدمات أمن مختلفة مثل *الاستيقان والسرية والسلامة وعدم التنصل*. وتصف هذه التوصية منهجاً لتوفير تحويلات أمن تنفذ في طبقة التطبيق ولا تتطلب وجود عنصر وظيفي محدد للأمن في أي من طبقات التوصيل البيني للأنظمة المفتوحة. وتعزز هذه التوصية أمن شبكات إدارة الاتصالات من خلال دعم تحويلات الأمن ROSE PDUs وتبادل معلومات الأمن ذات الصلة.	4

Q.815	مواصفات وحدة الأمن لحماية رسالة بأكملها	تحدد هذه التوصية وحدة أمن نمطية اختيارية تستخدم مع التوصية ITU-T Q.814، *مواصفات لوكيل بيانات إلكترونية متبادلة تفاعلية*، التي توفر خدمات الأمن لوحدات بيانات بروتوكول (PDUs) بأكملها. وتدعم وحدة الأمن النمطية، بصورة خاصة، *عدم إنكار الإرسال والاستلام* وكذلك *سلامة الرسالة* بأكملها.	4
Q.817	بنية تحتية للمفاتيح العمومية لشبكة إدارة الاتصالات – شهادات رقمية وملامح عامة لقوائم إبطال الشهادات	تشرح هذه التوصية كيفية استخدام الشهادات الرقمية وقوائم إبطال الشهادات في شبكة إدارة الاتصالات وتتضمن متطلبات عن عمليات تمديد الشهادات وقوائم إبطال الشهادات. والقصد من هذه التوصية الترويج لقابلية التشغيل البيني فيما بين عناصر شبكة إدارة الاتصالات التي تستخدم بنية تحتية للمفاتيح العمومية لدعم وظائف متعلقة بالأمن. والغرض هو توفير آلية تشغيل بيني قابلة للاتساع *لتوزيع المفاتيح وإدارتها* في شبكة إدارة الاتصالات عبر جميع السطوح البينية وكذلك لدعم خدمة *عدم التنصل* عبر السطح البيني X. وتنطبق على جميع السطوح البينية وتطبيقات شبكة إدارة الاتصالات. وهي مستقلة عن أي مجموعة بروتوكولات الاتصالات أو بروتوكولات إدارة الشبكة المستخدمة. ويمكن استخدام تسهيلات البنية التحتية للمفاتيح العمومية لمدى واسع من وظائف الأمن مثل *الاستيقان والسلامة وعدم التنصل وتبديل المفاتيح* (M.3016). ومع ذلك، لا تحدد هذه التوصية كم عدد الوظائف التي ينبغي تنفيذها مع بنية تحتية للمفاتيح العمومية أو بدونها.	4
Q.1531	متطلبات أمن الاتصالات الشخصية العالمية لخدمة من المجموعة 1	تحدد هذه التوصية متطلبات أمن الاتصالات الشخصية العالمية لكل من المستعمل إلى الشبكة واتصالات شبكة التوصيل البيني المطبقة على خدمة الاتصالات الشخصية العالمية من المجموعة 1 كما عرفت في التوصية ITU-T F.851. وتشمل هذه التوصية جميع جوانب الاتصالات الشخصية العالمية المستخدمة لنفاذ تردد متعدد بنغمة مزدوجة ونفاذ مستعمل قائم على معيار توقيع رقمي لنطاق خارجي 1.	11
Q.1741.1	مراجع الاتصالات المتنقلة الدولية–2000 لإصدار 1999 من النظام العمومي للاتصالات المتنقلة المتطورة للشبكة الأساسية للنظام العالمي للاتصالات المتنقلة مع شبكة نفاذ إلى شبكة نفاذ عالمية راديوية للأرض	تشمل هذه التوصية مراجع لمواصفات أمن 3GPP التالية، أي *TS 21.133: تمديدات الأمن ومتطلباته، TS 33.102: معمارية الأمن، TS 33.103: مبادئ توجيهية لإدماج الأمن، TS 33.105: متطلبات الخوارزمية المجفرة، TS 33.106: متطلبات الاعتراض المشروع، TS 33.107: معمارية الاعتراض المشروع ووظائفها، TS 33.120: أهداف ومبادئ الأمن.*	19
Q.1741.2	مراجع الاتصالات المتنقلة الدولية–2000 للإصدار 4 من النظام العمومي للاتصالات المتنقلة المتطورة للشبكة الأساسية للنظام العالمي للاتصالات المتنقلة مع شبكة نفاذ إلى شبكة نفاذ عالمية راديوية للأرض	تشمل هذه التوصية مراجع لمواصفات أمن 3GPP أي *TS 21.133: تمديدات الأمن ومتطلباته، TS 22.048: آليات الأمن لمجموعة أدوات تطبيق SIM (U) و TS 22.101: ملامح الخدمة؛ مبادئ الخدمة، TS 33.102: معمارية الأمن، TS 33.103: مبادئ توجيهية لإدماج الأمن، TS 33.105: متطلبات الخوارزمية المجفرة، TS 33.106: متطلبات الاعتراض المشروع، TS 33.107: معمارية الاعتراض المشروع ووظائفها، TS 33.120: أهداف ومبادئ الأمن، TS 33.200: أمن ميدان الشبكة–MAP، TS 35.205, .206, .207, .208: مواصفات مجموعة خوارزميات MILENAGE.*	19

Q.1741.3	مراجع الاتصالات المتنقلة الدولية–2000 للإصدار 5 من النظام العمومي للاتصالات المتنقلة المتطورة للشبكة الأساسية للنظام العالمي للاتصالات المتنقلة مع شبكة نفاذ إلى شبكة نفاذ عالمية راديوية للأرض	تشمل هذه التوصية مراجع لمواصفات أمن 3GPP مثل *TS 22.101: جوانب الخدمة؛ مبادئ الخدمة، TS 33.102: معمارية الأمن، TS 33.106: متطلبات الاعتراض المشروع، TS 33.107: معمارية الاعتراض المشروع ووظائفها، TS 33.108: سطح بيني لتسليم الاعتراض المشروع، TS 33.200: أمن ميدان الشبكة–نظام فرعي للتطبيق المتنقل MAP، TS 33.203: أمن النفاذ إلى الخدمات القائمة على بروتوكول الإنترنت، TS 33.210 الأمن؛ أمن ميدان الشبكة (NDS)؛ أمن طبقة الشبكة باستخدام بروتوكول الإنترنت، 909. ,208. ,207. ,206. ,TS 35.205؛ مواصفات مجموعة خوارزميات (MILENAGE).*	19
Q.1742.1	مراجع الاتصالات المتنقلة الدولية 2000 للمعهد الأمريكي الوطني للمعايير 41 للشبكة الأساسية المتطورة لشبكة نفاذ متعدد لتقسيم شفري 2000	تربط هذه التوصية معايير الشبكة الأساسية الصادرة عن منظمات وضع المعايير (SDOs) مع مواصفات 3GPP2 التي تمت الموافقة عليها في 17 يوليو 2001 لعضو أسرة الاتصالات المتنقلة الدولية–2000 "المعهد الأمريكي الوطني للمعايير–41 للشبكة الأساسية المتطورة لنفاذ متعدد بتقسيم شفري 2000". وسوف ترتبط مواصفات 3GPP2 التي تمت الموافقة عليها في يوليو 2002 مع معايير الشبكة الأساسية المنشورة في التوصية Q.1742.2 المقبلة لقطاع تقييس الاتصالات. ويرتبط السطح البيني الراديوي وشبكة النفاذ الراديوية والمعايير من منظمات وضع المعايير (SDOs) لعضو أسرة الاتصالات المتنقلة الدولية–2000 في التوصية M.1457 لقطاع تقييس الاتصالات. وروابط الأعضاء الآخرين في أسرة الاتصالات المتنقلة الدولية–2000 محددة في سلسلة التوصية Q.174x. وتجمع هذه التوصية وترتبط بين معايير الشبكة الأساسية ذات الصلة من عدد من منظمات وضع المعايير لهذا العضو في أسرة الاتصالات المتنقلة الدولية–2000 في توصية شاملة.	19
Q.1742.2	مراجع الاتصالات المتنقلة الدولية–2000 (الموافق عليها في 11 يوليو 2002) للمعهد الأمريكي الوطني للمعايير–41 الذي طور الشبكة الأساسية مع نفاذ متعدد بتقسيم شفري 2000 لشبكة النفاذ	تربط هذه التوصية معايير الشبكة الأساسية الصادرة عن منظمات إقليمية لوضع المعايير (SDOs) مع مواصفات 3GPP2 التي تمت الموافقة عليها في 11 يوليو 2002 لعضو أسرة الاتصالات المتنقلة الدولية–2000 "المعهد الأمريكي الوطني للمعايير–41 للشبكة الأساسية المتطورة لنفاذ متعدد بتقسيم شفري 2000". وترتبط مواصفات 3GPP2 التي تمت الموافقة عليها في 17 يوليو 2001 مع معايير الشبكة الأساسية الصادرة عن المنظمات الإقليمية لوضع المعايير في التوصية Q.1742.1 لقطاع تقييس الاتصالات. وسوف ترتبط مواصفات 3GPP2 التي تمت الموافقة عليها في يوليو 2003 مع معايير الشبكة الأساسية الصادرة في التوصية Q.1742.3 لقطاع تقييس الاتصالات. ويرتبط السطح البيني الراديوي وشبكة ومعايير النفاذ الراديوية من منظمات وضع المعايير لعضو أسرة الاتصالات المتنقلة الدولية–2000 في التوصية M.1457 لقطاع الاتصالات الراديوية. وتعرّف الارتباطات للأعضاء الآخرين من أسرة الاتصالات المتنقلة الدولية–2000 في سلسلة التوصية ITU-T Q.174x. وتجمع هذه التوصية وترتبط بين المعايير الإقليمية للشبكة الأساسية لهذا العضو في أسرة الاتصالات المتنقلة الدولية–2000 في توصية شاملة.	19
Q.1742.3	مراجع الاتصالات المتنقلة الدولية–2000 (الموافق عليها حتى 30 يونيو 2003) للمعهد الأمريكي الوطني للمعايير–41 للشبكة الأساسية المتطورة لنفاذ متعدّد بتقسيم شفري 2000	مواصفات تقنية مُحال إليها في التوصية Q.1742.3 فيما يتعلق بجوانب الأمن. *مواصفات فيما بين الأنظمة:* N.S0003-0 وحدة هوية المستعمل (الصيغة 1.0؛ أبريل 2001) N.S0005-0 عمليات فيما بين أنظمة الاتصالات الراديوية الخلوية (الصيغة 1.0؛ دون تاريخ) N.S0009-0 هوية المشترك المتنقل الدولي (الصيغة 1.0؛ دون تاريخ) N.S0010-0 خصائص متطورة لأنظمة تمديد الطيف عريضة النطاق (الصيغة 1.0؛ دون تاريخ) N.S0011-0 توفير خدمة عبر الهواء وإدارة معلمات عبر الهواء (الصيغة 1.0؛ دون تاريخ) N.S0014-0 تعزيزات الاستيقان (الصيغة 1.0؛ دون تاريخ) N.S0018 ترسيم مسبق الدفع لرابطة صناعة الاتصالات/رابطة الصناعات الإلكترونية–41–D (الصيغة 1.0.0؛ 14 يوليو 2000) N.S0028 تشغيل بين الشبكات بين نظام عمومي للاتصالات المتنقلة ونظام فرعي للتطبيق المتنقل والمعهد الأمريكي الوطني للمعايير–41 لنظام فرعي لتطبيق متنقل Rev. B مراجعة: 0 (الصيغة 1.0.0؛ أبريل 2002)	19

		مواصفات بيانات الرزم: P.S0001-A معيار شبكة لا سلكية باستخدام بروتوكول الإنترنت (الصيغة 3.0.0؛ 16 يوليو 2001) P.S0001-B معيار شبكة لا سلكية باستخدام بروتوكول الإنترنت (الصيغة 3.0.0؛ 25 أكتوبر 2002) *مواصفات جوانب الخدمات والأنظمة:* S.R0005-B نموذج مرجعي لشبكة لمراجعة أنظمة تمديد الطيف لنفاذ متعدد لتقسيم شفري 2000: B (الصيغة 1.0؛ 16 أبريل 2001) S.R0006 مراجعة وصف خصائص لا سلكية (الصيغة 1.0.0؛ 13 ديسمبر 1999) S.R0009-0 وحدة هوية المستعمل (الصيغة 1.0؛ مرحلة 1) مراجعة: 0 (13 ديسمبر 1999) S.R0018 ترسيم مسبق الدفع (الصيغة 1.0.0؛ مرحلة 1) مراجعة: 0 (13 ديسمبر 1999) S.R0019 نظام خدمات قائم على تحديد الموقع (الصيغة 1.0.0؛ LBSS) وصف المرحلة 1 (22 سبتمبر 2000) S.R0032 الاستيقان المعزز للمشترك (الصيغة 1.0؛ ESA) والسرية المعززة للمشترك (6 ديسمبر 2000) S.R0037-0 نموذج معمارية شبكة باستخدام بروتوكول الإنترنت لأنظمة تمديد الطيف لنفاذ متعدد لتقسيم شفري 2000 (الصيغة 2.0؛ 14 مايو 2002) S.R0048 معرّف المعدات المتنقلة 3G (الصيغة 1.0؛ MEID) (10 مايو 2001) S.S0053 خوارزميات مجفرة مشتركة (الصيغة 1.0؛ 21 يناير 2002) S.S0054 مواصفات السطح البيني لخوارزميات مجفرة مشتركة (الصيغة 1.0؛ 21 يناير 2002) S.S0055 خوارزميات مجفرة متطورة (الصيغة 1.0؛ 21 يناير 2002) S.R0058 متطلبات نظام الميدان لوسائط متعددة باستخدام بروتوكول الإنترنت (الصيغة 1.0؛ 17 أبريل 2003) S.R0059 ميدان تراث خدمات الإدارة – متطلبات نظام الخطوة 1 (الصيغة 1.0؛ 16 مايو 2002) S.R0066-0 متطلبات المرحلة 1 لخدمات تحديد الموقع على أساس بروتوكول الإنترنت (الصيغة 1.0؛ 17 أبريل 2003) S.R0071 متطلبات المرحلة 1 لمتطلبات رصد تراث بيانات الرزم لخدمات تحديد الموقع (الصيغة 1.0؛ 18 أبريل 2002) S.R0072 متطلبات المرحلة 1 لمتطلبات رصد جميع بيانات الرزم لخدمات تحديد الموقع على أساس بروتوكول الإنترنت (الصيغة 1.0؛ 18 أبريل 2002) S.R0073 إدارة تشكيل سماعات يد على الهواء للإنترنت (الصيغة 1.0؛ IOTA) المرحلة 1 (11 يوليو 2002) S.S0078-0 خوارزميات الأمن المشتركة (الصيغة 1.0؛ 12 ديسمبر 2002)	
T.30	إجراءات لإرسال وثيقة بالفاكس في الشبكة الهاتفية العمومية التبديلية	يوفر الملحق زاي إجراءات لتأمين إرسال وثيقة بالفاكس G3 باستخدام خوارزمية هوثورن لإدارة مفاتيح (HKM) ونظام خوارزمية هوثورن للشفرة فاكس (HFX). ويوفر الملحق حاء الأمن في فاكس G3 القائم على *خوارزمية ريفست وشامير وأدلمان*.	16
T.36	مقدرات الأمن لاستخدام مطاريف الفاكس من الزمرة 3	تعرّف هذه التوصية حلين تقنيين مستقلين يمكن استخدامهما في سياق ضمان إرسال فاكس آمن. ويقوم الحلان التقنيان على أساس خوارزمية هوثورن لإدارة مفاتيح وخوارزمية هوثورن لشفرة فاكس 40 *وخوارزمية ريفست وشامير وأدلمان*.	16
T.123 الملحق باء	توصيلات نقل ممتدة	يتضمن هذا الملحق بالتوصية T.123 المنقحة *لبروتوكول مفاوضة توصيل (CNP)* يوفر مفاوضات مقدرة الأمن. وتشمل آلية الأمن المطبقة وسائل مختلفة لأمن شبكة ونقلها على أساس من عقدة إلى عقدة وتشمل أيضاً أمن مستوى النقل/طبقة مقبس آمن أو الأمن باستخدام بروتوكول الإنترنت أو *إدارة المفاتيح* يدوياً وبروتوكول أمن طبقة النقل X.274/ISO ونظام فرعي أرضي– سطح بيني لبرنامج تطبيق.	16

T.503	مواصفة لتطبيق وثيقة لمبادلة وثائق الفاكس من الزمرة 4	تعرّف هذه التوصية مواصفة لتطبيق وثيقة قد تستخدم بواسطة أي خدمة تلماتية. والغرض منها هو تحديد نسق مبادلة وثائق الفاكس من الزمرة 4 التي تحتوي فقط على رسوم بيانية تنقيطية. ويجري مبادلة الوثائق في شكل منسوق يمكّن المستقبل من عرض أو طبع الوثيقة كما يتوخاها مرسلها.	16
T.563	الخصائص المطرافية لأجهزة الفاكس من الزمرة 4	تعرّف هذه التوصية الجوانب العامة لأجهزة الفاكس من الزمرة 4 والسطح البيني للشبكة المادية.	16
T.611	السطح البيني لبرمجة اتصالات السطح البيني للتطبيق المحلي ولتطبيقات الاتصالات لفاكس من الزمرة 3 وفاكس من الزمرة 4 وتيليتكس وتيلكس وبريد إلكتروني وخدمات نقل الملفات	تعرّف هذه التوصية السطح البيني لبرمجة اتصالات تسمى "السطح البيني للتطبيق المحلي ولتطبيقات الاتصالات" والذي يوفر نفاذاً موحداً لخدمات اتصالات مختلفة مثل فاكس من الزمرة 3 أو خدمات تلماتية أخرى. وتصف هذه التوصية هيكل ومحتويات الرسائل وطريقة تبادلها بين تطبيق محلي (LA) وتطبيق اتصالات (CA). وأي اتصالات تسبقها عملية نفاذ إلى شبكة وإنتهائها بعملية خروج من الشبكة، حيث تيسر كلتا العمليتين تنفيذ مخططات أمن مهمة بصورة خاصة في أنظمة المستعملين المتعددين. وتوفران أيضاً وسائل لتنفيذ آليات الأمن بين التطبيق المحلي وتطبيق الاتصالات. وتشكل هذه التوصية مستوى مرتفعاً من (سطح بيني لبرمجة تطبيق) API يحمي جميع خصائص الاتصالات ويوفر مراقبة قوية ورصداً لنشاط اتصالات مصممي التطبيق.	16
X.217	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – تعريف خدمة لعنصر خدمة مراقبة الترابط	تعرّف هذه التوصية خدمات عنصر خدمة مراقبة الترابط لمراقبة التطبيق – الترابط في بيئة التوصيل البيني للأنظمة المفتوحة. ويدعم عنصر خدمة مراقبة الترابط أساليب التوصيل الموجه وعدم التوصيل للاتصالات. وتعرّف ثلاث وحدات وظيفية في عنصر خدمة مراقبة الترابط. وتستخدم *وحدة النواة الوظيفية* الإلزامية لإنشاء وتحرير التطبيقات – الترابطات. ويشمل عنصر خدمة مراقبة الترابط وحدتين وظيفيتين اختياريتين، إحداهما وحدة وظيفية *للاستيقان* الاختياري توفر تسهيلات إضافية لتبادل المعلومات لدعم الاستيقان خلال إنشاء الترابط دون إضافة خدمات جديدة. ويمكن استخدام *تسهيلات استيقان* عنصر خدمة مراقبة الارتباط لدعم نوع محدود من *طرائق الاستيقان*. ويوفر التعديل 1 دعم آليات الاستيقان لأسلوب عدم التوصيل.	17
X.227	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – بروتوكول موجه نحو توصيل عنصر خدمة مراقبة الترابط: مواصفة البروتوكول	تعرّف مواصفات هذا البروتوكول الإجراءات التي تطبق في حالات اتصالات بين أنظمة تلتمس التوصيل مع بيئة توصيل بيني لأنظمة مفتوحة في أسلوب موجه نحو التوصيل، أي بروتوكول أسلوب موجه نحو توصيل عنصر تطبيق خدمة – من أجل مراقبة الترابط – التطبيق وعنصر خدمة مراقبة الترابط (ACSE). وتشمل مواصفات بروتوكول *وحدة النواة الوظيفية* المستخدمة لإنشاء وتحرير التطبيقات – الترابطات. وتوفر *الوحدة الوظيفية للاستيقان* تسهيلات إضافية لتبادل المعلومات لدعم الاستيقان خلال إنشاء الترابط دون إضافة خدمات جديدة. ويمكن استخدام تسهيلات *الاستيقان* عنصر خدمة مراقبة الترابطات لدعم نوع محدود من *طرائق الاستيقان*. وتوفر الوحدة الوظيفية للتفاوض بشأن سياق التطبيق تسهيلاً إضافياً لاختيار سياق التطبيق خلال إنشاء الترابط. وتشمل مواصفة هذا البروتوكول ملحقاً يصف آلة بروتوكول، مشار إليها باعتبارها آلة بروتوكول مراقبة الترابط (ACPM)، على أساس جدول حالة. وتشمل مواصفات هذا البروتوكول ملحقاً يصف آلية استيقان بسيطة تستخدم كلمة سر مع عنوان كيان التطبيق، والقصد منها الاستخدام العام، وتشمل أيضاً مثالاً *لمواصفة آلية الاستيقان*. ويعين الاسم التالي لآلية الاستيقان هذه (ASN.1 datatype OBJECT IDENTIFIER): {joint-iso-itu-t(2)association-control(2)authentication-mechanism(3) password-1 (1) } وبالنسبة لآلية الاستيقان هذه، تكون كلمة السر هي قيمة الاستيقان. ويكون نوع بيانات قيمة الاستيقان هو "GraphicString".	17

X.237	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – بروتوكول عديم التوصيل لعنصر خدمة مراقبة الترابط: مواصفات البروتوكول	يشمل التعديل 1 على هذه التوصية وسم قابلية تمديد ترميز التركيب المجرد رقم 1 في وحدة تصف البروتوكول. ويعزز أيضاً مواصفة بروتوكول عنصر خدمة مراقبة الارتباط عديم التوصيل لتوفير الدعم لنقل معلمات الاستيقان في A-UNIT-DATA APDU.	17
X.257	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – بروتوكول عديم التوصيل لعنصر خدمة مراقبة الترابط: شكل بيان مطابقة تنفيذ البروتوكول	توفر هذه التوصية شكل بيان مطابقة تنفيذ بروتوكول (PICs) لبروتوكول عديم التوصيل لأنظمة مفتوحة لعنصر خدمة مراقبة الترابط المحدد في التوصية X.237. ويمثل شكل بيان مطابقة تنفيذ البروتوكول، في شكل مجدول، العناصر الإلزامية والاختيارية لبروتوكول عديم التوصيل لأنظمة مفتوحة. ويستخدم شكل البروتوكول هذا لتعريف خصائص واختيارات تنفيذ بروتوكول عديم التوصيل لأنظمة مفتوحة.	17
X.272	انضغاط البيانات والخصوصية عبر شبكات ترحيل الأرتال	تعرّف هذه التوصية خدمة انضغاط البيانات وخدمة الخصوصية لشبكات ترحيل الأرتال بما في ذلك المفاوضات وتغليف انضغاط البيانات *وانضغاط البيانات الآمنة والاستيقان والتجفير* عبر ترحيل الأرتال. ويزيد وجود خدمة انضغاط البيانات الإنتاجية الفعلية للشبكة. ويستدعي الطلب على إرسال بيانات حساسة عبر الشبكات العمومية تسهيلات لضمان *خصوصية* البيانات. ومن أجل تحقيق معدلات انضغاط مثلى، من الضروري ضغط البيانات قبل *تجفيرها*. وبالتالي، من المستصوب توفير تسهيلات في *خدمة انضغاط البيانات* لمفاوضة *بروتوكولات تجفير البيانات* كذلك. ونظراً لأن مهمة الانضغاط ثم التجفير للبيانات مهمة مكثفة حسابياً، فإن الكفاءة تتحقق من خلال *انضغاط وتجفير البيانات* في نفس الوقت (*تأمين انضغاط البيانات*). وتقوم بروتوكولات انضغاط البيانات على أساس بروتوكول مراقبة وصلة من نقطة إلى نقطة (IETF RFC 1661) وبروتوكول مراقبة تجفير من نقطة إلى نقطة (IETF RFC 1968 and 1969). وتنطبق هذه التوصية على أرتال المعلومات (UI) غير المرقمة المغلفة باستخدام التوصية Q.933 الملحق هاء. وهي تتناول انضغاط البيانات والخصوصية في كل من التوصيلات التقديرية الدائمة (PVC) والتوصيلات التقديرية التبديلية (SVC).	17
X.273	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – بروتوكول أمن طبقة الشبكة	تحدد هذه التوصية البروتوكول لدعم خدمات *سلامة البيانات والسرية والاستيقان ومراقبة النفاذ* المعرّفة في نموذج أمن التوصيل البيني للأنظمة المفتوحة في تطبيقه على بروتوكولات طبقة الشبكة بأسلوب التوصيل أو عدم التوصيل. ويدعم البروتوكول هذه الخدمات من خلال استخدام *آليات مجفرة ووسم الأمن ونعوت الأمن المعينة* مثل *المفاتيح المجفرة*.	17
X.274	تكنولوجيا المعلومات – تبادل الاتصالات والمعلومات بين الأنظمة – بروتوكول أمن طبقة النقل	تحدد هذه التوصية البروتوكول الذي يدعم خدمات *سلامة البيانات والسرية والاستيقان ومراقبة النفاذ* المعرّفة في نموذج أمن التوصيل البيني للأنظمة المفتوحة في علاقته بطبقة النقل. ويدعم البروتوكول هذه الخدمات من خلال *استخدام آليات مجفرة ووسم الأمن وخواص الأمن المعينة* مثل *المفاتيح المجفرة*.	17
X.400/ F.400	نظام مناولة الرسائل ونظرة عامة على الخدمة	تحدد هذه التوصية عناصر خدمة نظام مناولة الرسائل (MHS) لخدمات الأمن من وكيل مستعمل إلى وكيل مستعمل ومن وكيل نقل رسائل إلى وكيل نقل رسائل، ومن وكيل مستعمل إلى وكيل نقل رسائل ومن وكيل مستعمل إلى مخزن رسائل والتي تشمل *السرية وسلامة البيانات وعدم التنصل والتحكم في النفاذ* المعرّفة على أنها تتعلق بطبقة التطبيق. (انظر F.400)	17
X.402	تكنولوجيا المعلومات – أنظمة مناولة الرسائل – المعمارية العامة	تحدد هذه التوصية إجراءات الأمن ومعرّفات الأغراض لاستخدامها في بروتوكولات أنظمة مناولة الرسائل (MHS) لتحقيق خدمات *السرية وسلامة البيانات وعدم التنصل والتحكم في النفاذ* المعرّفة على أنها تتعلق بطبقة التطبيق.	17

X.411	تكنولوجيا المعلومات – أنظمة مناولة الرسائل – نظام نقل الرسائل: تعريف وإجراءات الخدمة المجردة	تحدد هذه التوصية آليات وإجراءات تدعم خدمات *السرية وسلامة البيانات والاستيقان وعدم التنصل* المحددة على أنها تتعلق بطبقة التطبيق. ويدعم البروتوكول هذه الخدمات من خلال استخدام *آليات مجفرة ووسم أمن وتوقيعات رقمية* كما عرفت في التوصية ITU-T X.509. وبالرغم من أن هذه التوصية تحدد البروتوكول الذي يستخدم *التقنيات اللاتناظرية المجفرة*، إلا أن *التقنيات التناظرية المجفرة* يجري دعمها أيضاً.	17
X.413	تكنولوجيا المعلومات – أنظمة مناولة الرسائل: مخزن الرسائل: تعريف الخدمة المجردة	تحدد هذه التوصية آليات وبروتوكول وإجراءات تدعم خدمات *سلامة البيانات والتحكم في النفاذ والاستيقان وعدم التنصل* المعرّفة على أنها تتعلق بطبقة التطبيق. ويدعم البروتوكول هذه الخدمات نيابة عن مستعمل مخزن رسائل مباشر.	17
X.419	تكنولوجيا المعلومات – أنظمة مناولة الرسائل: مواصفات البروتوكول	تحدد هذه التوصية إجراءات وسياقات التطبيق لتعريف النفاذ الآمن لكيانات أنظمة مناولة الرسائل والمستعملين عن بُعد من خلال توفير خدمات *الاستيقان والتحكم في النفاذ* المعرّفة في علاقتها بطبقة التطبيق.	17
X.420	تكنولوجيا المعلومات – أنظمة مناولة الرسائل: نظام المراسلة فيما بين الأشخاص	تحدد هذه التوصية الآليات والبروتوكول والإجراءات لتبادل الأغراض بين مستعملي المراسلة فيما بين الأشخاص أو وكلاء مستعملين نيابة عن مستعملها المباشر المعرف على أنه يتعلق بطبقة التطبيق. وخدمات الأمن الداعمة هي *سلامة البيانات والسرية والاستيقان والتحكم في النفاذ* المعرّفة على أنها تتعلق بطبقة التطبيق.	17
X.435	تكنولوجيا المعلومات – أنظمة مناولة الرسائل: نظام المراسلة المتبادلة لبيانات إلكترونية	تحدد هذه التوصية الآليات والبروتوكول والإجراءات لتبادل الأغراض بين الوكلاء المستعملين لمبادلة البيانات الإلكترونية (EDI) نيابة عن مستعملها المباشر. وخدمات الأمن التي تدعمها هي *سلامة البيانات والسرية والاستيقان والتحكم في النفاذ* المعرّفة على أنها تتعلق بطبقة التطبيق.	17
X.440	تكنولوجيا المعلومات – أنظمة مناولة الرسائل: نظام المراسلة الصوتية	تحدد هذه التوصية الآليات والبروتوكول والإجراءات لتبادل الأغراض بين وكلاء مستعملي الصوت نيابة عن مستعملها المباشر. وخدمات الأمن التي تدعمها هي *سلامة البيانات والسرية والاستيقان والتحكم في النفاذ* المعرّفة على أنها تتعلق بطبقة التطبيق.	17
X.500	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – الدليل: نظرة عامة على المفاهيم والنماذج والخدمات	وُضعت هذه التوصية مع توصيات أخرى لتسهيل التوصيل البيني لأنظمة معالجة المعلومات من أجل توفير خدمات الدليل. ويمكن اعتبار مجموعة هذه الأنظمة مع معلومات الدليل التي تحتويها بمثابة كل متكامل يسمى الدليل. وتستخدم المعلومات التي يتضمنها الدليل والمعروفة إجمالاً على أنها قاعدة معلومات الدليل (DIB) عادة لتسهيل الاتصال بين الأغراض أو معها أو عنها من مثل كيانات التطبيق والأشخاص والمطاريف وقوائم التوزيع. ويؤدي الدليل دوراً هاماً في التوصيل البيني للأنظمة المفتوحة يهدف إلى إتاحة التوصيل البيني لأنظمة معالجة المعلومات بأدنى حد من الاتفاق التقني خارج معايير التوصيل البيني ذاتها. وتعرض هذه التوصية وتشكل مفاهيم الدليل وقاعدة معلومات الدليل والاستعراضات العامة للخدمات والمقدرات التي توفرها. وتستخدم توصيات أخرى هذه النماذج في تعريف الخدمة المجرّدة التي يوفّرها الدليل، وفي تحديد البروتوكولات التي يمكن من خلالها الحصول على هذه الخدمة أو نشرها. وتحدد هذه التوصية خصائص الدليل وخصائص أمنه.	17
X.501	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – الدليل: نماذج	توفر هذه التوصية عدداً من النماذج المختلفة للدليل كإطار للتوصيات الأخرى للقطاع ITU-T في السلسلة X.500. والنماذج هي النموذج (الوظيفي) الإجمالي والنماذج النمطية لمعلومات الدليل التي توفر رأي مستعمل الدليل والمستعمل الإداري بشأن معلومات الدليل ووكيل نظام الدليل (DSA) النمطي، ونماذج معلومات الوكيل والإطار التشغيلي ونموذج أمن. وهي تُحدد استعمال الدليل لأطر شهادات المفاتيح العمومية والنعوت في إطار التوصية X.509.	17

X.509	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – الدليل: --- إطار الاستيقان (طبعة 1993 – *الطبعة/الصيغة الثانية*) --- إطار الاستيقان (طبعة 1997 – *الطبعة/الصيغة الثالثة*) --- أطر شهادات المفاتيح العمومية والنعوت (طبعة 2000 – *الطبعة/الصيغة الرابعة*) --- أطر شهادات المفاتيح العمومية والنعوت (طبعة 2005 – *الطبعة/الصيغة الخامسة*)	تعرّف هذه التوصية إطار شهادات المفاتيح العمومية وشهادات النعوت وتعرّف إطار توفير خدمات الاستيقان من قبل دليل إلى مستعمليه. وتصف مستويين من الاستيقان: *الاستيقان البسيط*، باستخدام كلمة سر للتحقق من الهوية المزعومة؛ *والاستيقان القوي* الذي يتضمن تفويضات مشكلة باستخدام تقنيات مجفرة. وبينما يوفر الاستيقان البسيط بعض الحماية المحدودة من النفاذ غير المخول، فإنه ينبغي استخدام الاستيقان القوي فقط كأساس لتوفير الخدمات الآمنة. ويمكن أن تستخدم الأطر المعرّفة لتحديد الملامح العامة للتطبيق على البنى *التحتية للمفاتيح العمومية (PKI) والبنى التحتية لإدارة الامتيازات (PMI)*. ويشمل إطار شهادات المفاتيح العمومية مواصفات أغراض البيانات المستخدمة لتمثل الشهادات نفسها وكذلك إشعارات إبطال للشهادات الصادرة التي ينبغي ألا يوثق فيها. وبينما تعرف بعض المكونات الحرجة لبنى تحتية للمفاتيح العمومية، فهي لا تعرفها بالكامل. ومع ذلك، فهي توفر أساساً يمكن أن تبنى عليه بنية تحتية للمفاتيح العمومية ومواصفاتها. ويشمل إطار شهادات النعوت مواصفات *أغراض البيانات* التي تستخدم لتمثل الشهادات نفسها وكذلك *إشعارات إبطال* للشهادات الصادرة التي ينبغي ألاّ يوثق فيها. وبينما تعرّف بعض مكونات حرجة لبنية تحتية لإدارة متميزة، فإنها لا تعرفها بالكامل. ومع ذلك فهي، توفر أساساً يمكن أن تبنى عليه بنى تحتية لإدارة امتيازات ومواصفاتها. وتعرف أيضاً *أغراض المعلومات* للاحتفاظ بأغراض البنية التحتية لمفاتيح عمومية والبنية التحتية لإدارة الامتيازات في الدليل ومن أجل مقارنة القيم المقدمة مع القيم المخزونة.	17
X.519	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – الدليل: مواصفة البروتوكول	تحدد هذه التوصية الإجراءات وسياقات التطبيق لتعريف النفاذ الآمن أثناء توثيق كيانات الدليل.	17
X.680	تكنولوجيا المعلومات – التوصيل الشبكي في التوصيل البيني للأنظمة المفتوحة OSI وجوانب النظام – ترميز التركيب المجرد رقم 1 (ASN.1): مواصفة الترميز الأساسي	توفّر هذه التوصية ترميزاً معيارياً يسمى ترميز التركيب المجرد رقم 1 (ASN.1) لتحديد تركيب بيانات المعلومات. وهي تُعرِّف عدداً من أنماط البيانات البسيطة، وتُحدد ترميزاً للإحالة المرجعية لهذه الأنماط وتحديد قيمها. ويمكن تطبيق الترميز ASN.1 حيثما يكون ذلك ضرورياً لتحديد التركيب المجرّد للمعلومات بدون التقيد على أي نحو بالكيفية التي شُفرت بها المعلومات من أجل إرسالها. ويُستعمل الترميز ASN.1 لتحديد أنماط البيانات وقيمها والتقييدات على هذه الأنماط، أي يحدد عدد الأنماط البسيطة مع وسماتها، ويُحدد ترميزاً للإحالة المرجعية إلى هذه الأنماط ولتحديد قيم هذه الأنماط؛ ويُعرّف آليات لإنشاء أنماط جديدة من أنماط أكثر أساسية، كما يُحدد ترميزاً لتعريف هذه الأنماط ويخصص وسْمات لها، ولتحديد قيم لهذه الأنماط؛ ويُعرّف مجموعات من السمات (بالإحالة إلى توصيات أخرى لاستعمالها ضمن الترميز ASN.1). ونمط البيانات (أو النمط توخياً للاختصار) هو فئة من المعلومات (على سبيل المثال العددية أو النصية أو معلومات الصورة الثابتة أو المعلومات الفيديوية). وقيمة البيانات (أو القيمة توخياً للاختصار) هي حالة لهذا النمط. وتُعرّف هذه التوصية عدة أنماط أساسية والقيم المطابقة لها، وقواعد الجمع بينها في أنماط وقيم أكثر تعقيدا. وفي بعض معماريات البروتوكول، تحدد كل رسالة على أنها القيمة الاثنينية لتتابع أثمونات. إلاّ أن واضعي المعايير يتعين عليهم تعريف أنماط بيانات معقدة تماماً لحمل رسائلهم دون الاكتراث لتمثيلها الاثنيني. وبغية تحديد أنماط البيانات هذه فإنهم يحتاجون إلى ترميز لا يُحدد بالضرورة تمثيل كل قيمة. والترميز ASN.1 هو مجرّد ترميز. وهو يستكمل بمواصفة خوارزمية أو أكثر تُسمى قواعد التجفير التي تُحدد قيمة الأثمونات التي تحمل دلالات التطبيق (التي تُسمى تركيب النقل). **ملاحظة** – استخدمت سلسلة التوصيات ASN.1 (وبوجه خاص قواعد التجفير المميزة والقانونية لASN.1) على نطاق واسع في كثير من المعايير والتوصيات المتعلقة بالأمن. وبوجه خاص، تعتمد التوصية H.323 والسلسلة X.400 وX.500 اعتمادا كبيرا على الترميز ASN.1. وقد شكلت هذه التوصيات وما فتئت تُشكل لبنات هامة في بناء العمل المتعلق بالأمن.	17

X.681	تكنولوجيا المعلومات – التوصيل البيني لشبكات الأنظمة المفتوحة وجوانب النظام – ترميز التركيب المجرّد رقم 1 (ASN.1): مواصفات أغراض المعلومات	توفر هذه التوصية الترميز ASN.1 الذي يُتيح تعريف أصناف أغراض المعلومات وكذلك فرادى أغراض المعلومات والمجموعات الخاصة بها وإعطائها أسماء مرجعية، أي أنها توفّر ترميزاً لتحديد أصناف أغراض المعلومات ومجموعات أغراض المعلومات. ويُعرّف صنف غرض المعلومات شكل جدول مفاهيمي (مجموعة أغراض معلومات) بعمود واحد لكل ميدان في صنف غرض المعلومات، ومع كل صف كامل يُعرّف غرض معلومات. ويحتاج مصمم التطبيق في أكثر الأحيان إلى تصميم بروتوكول يعمل مع أي عدد من حالات بعض أصناف أغراض المعلومات حيث تُعرف حالات الصنف بحكم طائفة متنوعة من الأجسام الأخرى ويمكن أن يضاف إليها بمضي الوقت. والأمثلة على أصناف أغراض المعلومات هذه هي "عمليات" خدمة العمليات عن بعد (ROS) و"نعوت" دليل التوصيل البيني للأنظمة المفتوحة (OSI). وتوفر هذه التوصية ترميزاً يتيح تعريف أصناف أغراض المعلومات وفرادى أغراض المعلومات ومجموعات أغراض المعلومات الخاصة بها وإعطائها أسماء مرجعية. انظر الملاحظة أعلاه (X.680).	17
X.682	تكنولوجيا المعلومات – التوصيل البيني لشبكات الأنظمة المفتوحة وجوانب النظام – ترميز التركيب المجرد رقم 1 (ASN.1): مواصفات التقييدات	هذه التوصية جزء من ترميز التركيب المجرد رقم 1 (ASN.1) كما توفر ترميزاً لتحديد التقييدات التي يحددها المستعمل، وتقييدات الجداول، وتقييدات المحتويات. وتوفر ترميز ASN.1 للحالة العامة لمواصفة التقييد والاستثناءات التي يمكن بواسطتها الحد من قيم البيانات الخاصة بنمط بيانات منظم. ويوفر الترميز أيضاً التشوير في حالة انتهاك قيد ما. ويحتاج مصممو التطبيق إلى ترميز لتعريف نمط بيانات منظم لنقل دلالاته كما يلزم الترميز من أجل مواصلة تقييد القيم التي قد تظهر. ومن أمثلة هذه التقييدات تقييد مدى مكون ما أو مكونات ما، أو استعمال مجموعة أغراض معلومات محددة لتقييد مكون "ObjectClassFieldType"، أو استعمال "AtNotation" لتحديد علاقة بين المكونات. انظر الملاحظة أعلاه (X.680).	17
X.683	تكنولوجيا المعلومات – التوصيل البيني لشبكات الأنظمة المفتوحة وجوانب النظام – ترميز التركيب المجرد رقم 1 (ASN.1): وضع معلمات مواصفات الترميز ASN.1	هذه التوصية جزء من ترميز التركيب المجرد رقم 1 (ASN.1) وتحدّد ترميزاً لوضع معلمات مواصفات الترميز ASN.1، أي تعرف الأحكام الخاصة بالأسماء المرجعية التي وضعت معلماتها والتخصيصات التي وضعت معلماتها لأنماط البيانات المفيدة للمصممين عندما يدونون مواصفات تُركت بعض جوانبها دون تحديد في مراحل معينة من التطور لتُملأ في مرحلة لاحقة من أجل إنتاج تعريف كامل لتركيب مجرد. ويحتاج مصممو التطبيقات إلى كتابة مواصفات تترك بعض الجوانب فيها دون تحديد. وتُحدد تلك الجوانب لاحقاً من قبل مجموعة أو أكثر (كل منها بطريقتها الخاصة) من أجل إنتاج مواصفة معرّفة تعريفاً كاملاً لاستخدامها في تعريف تركيب مجرّد (واحد لكل مجموعة). وفي بعض الحالات، يمكن ترك جوانب من المواصفة (حدود مثلاً) دون تحديد حتى في وقت تعريف التركيب المجرد لتستكمل بواسطة مواصفات دولية مقيسة أو مواصفات وظيفية من قبل هيئة ما أخرى. انظر الملاحظة أعلاه (X.680).	17
X.690	تكنولوجيا المعلومات – قواعد تجفير الترميز ASN.1؛ مواصفات قواعد التجفير الأساسية BER، وقواعد التجفير القانونية (CER) وقواعد التجفير المميزة (DER)	تحدد هذه التوصية مجموعة من قواعد التجفير الأساسية (BER) التي يمكن تطبيقها على قيم أنماط معرّفة باستخدام الترميز ASN.1، أي تستخدم لاشتقاق مواصفات تركيب نقل لقيم أنماط معرّفة باستعمال الترميز المحدد في سلسلة توصيات القطاع X.680، المشار إليها باعتبارها ترميز التركيب المجرد رقم واحد أو ASN.1. ويؤدي تطبيق قواعد التجفير هذه إلى تركيب نقل لهذه القيم. وتنطوي مواصفة قواعد التجفير هذه ضمناً على أنها تستخدم أيضاً في فك التجفير، أي أن قواعد التجفير الأساسية هذه تطبق أيضاً في فك تجفير تركيب نقل من هذا القبيل من أجل تحديد قيم البيانات التي يجري نقلها. وتُحدد هذه المواصفة أيضاً مجموعة من قواعد التجفير القانونية والمميزة التي تقيّد تجفير القيم في مجرّد أحد البدائل التي توفرها قواعد التجفير الأساسية أي أنها تحدد أيضاً مجموعة من قواعد التجفير المميزة (DER) ومجموعة من قواعد التجفير القانونية (CER) وكلتاهما توفر قيوداً على قواعد التجفير الأساسية (BER). والفارق الرئيسي بينهما هو أن قواعد التجفير المميزة تستخدم نسق طول محدّد للتجفير بينما تستخدم قواعد التجفير القانونية نسق طول غير محدّد. وقواعد التجفير المميزة (DER) أنسب لقيم التجفير الصغيرة في حين أن قواعد التجفير القانونية CER أنسب لقيم التجفير الكبيرة. وتنطوي مواصفة قيم التجفير هذه ضمناً على أنها تستخدم أيضاً من أجل فك التجفير. انظر الملاحظة أعلاه (X.680).	17

X.691	تكنولوجيا المعلومات – قواعد تجفير الترميز ASN.1: مواصفات قواعد التجفير بالرزم (PER)	تصف سلسلة التوصيات X.680 ترميز التركيب المجرد رقم 1 (ASN.1)، وهو ترميز لتعريف الرسائل المتبادلة بين التطبيقات الند. وتصف هذه التوصية مجموعة من قواعد التجفير التي يمكن تطبيقها على قيم جميع أنماط الترميز (ASN.1) لتحقيق تمثيل أكثر تكثيفاً بكثير من الذي تحققه قواعد التجفير الأساسية ومشتقاتها (الموصوفة في التوصية X.690)، أي أنها تحدد مجموعة من قواعد التجفير بالرزم التي يمكن استخدامها لاشتقاق تركيب نقل لقيم الأنماط المعرّفة في التوصية ITU-T X.680. وتُطبَّق قواعد التجفير بالرزم أيضاً على فك تجفير تركيب نقل من هذا القبيل من أجل تحديد قيم البيانات التي يجري نقلها. وهناك أكثر من مجموعة واحدة من قواعد التجفير التي يمكن تطبيقها على قيم أنماط الترميز ASN.1. وقواعد التجفير بالرزم هذه (PER) مسماة هكذا لأنها تحقق تمثيلاً أكثر تكثّفاً بكثير من ذلك الذي تحققه قواعد التجفير الأساسية (BER) ومشتقاتها الموصوفة في التوصية ITU-T X.690. انظر الملاحظة أعلاه (X.680).	17
X.692	تكنولوجيا المعلومات – قواعد تجفير الترميز ASN.1: مواصفات ترميز ضبط التجفير (ECN) + الملحق هاء: دعم تجفيرات هوفمان Huffman	تعرّف هذه التوصية ترميز ضبط التجفير (ECN) المستخدم في تحديد تجفيرات الأنماط ASN.1 أو أجزاء من أنماط تختلف عن الأنماط التي توفرها قواعد التجفير المقيَّسة من مثل قواعد التجفير الأساسية (BER) وقواعد التجفير بالرزم (PER). وتوفر التوصية عدّة آليات لهذه المواصفات. كما توفر وسائل ربط مواصفة التجفيرات بتعريف الأنماط التي يتعين تطبيقها عليها. ويمكن استخدام ترميز ضبط التجفير لتجفير جميع أنماط مواصفة ASN.1 لكن يمكن استخدامه أيضاً مع قواعد التجفير المقيَّسة من مثل قواعد التجفير الأساسية (BER) أو قواعد التجفير بالرزم (PER) من أجل أن يُحدّد فقط تجفير الأنماط ذات المتطلبات الخاصة. ويُحدد أي نمط ASN.1 مجموعة من القيم المجرّدة. وتُحدد قواعد التجفير تمثيل هذه القيم المجرّدة باعتبارها سلسلة من البتات. انظر الملاحظة أعلاه (X.680).	17
X.693	تكنولوجيا المعلومات – قواعد تجفير ASN.1: قواعد تجفير لغة التوسيم القابلة للتوسيع XML	أصبح نشر ترميز التركيب المجرد رقم 1 (ASN.1) الترميز المستخدم بوجه عام في تعريف الرسائل المتبادلة بين التطبيقات الند. وتُحدد هذه التوصية قواعد التجفير التي يمكن تطبيقها لتجفير قيم أنماط ASN.1 باستخدام لغة التوسيم القابلة للتوسيع (XML) أي أنها تُحدد مجموعة من قواعد تجفير XML الأساسية (XER) التي يمكن استخدامها في اشتقاق تركيب نقل لقيم الأنماط المعرّفة في سلسلة التوصيات X.680. وتُحدد هذه التوصية أيضاً مجموعة من قواعد التجفير XML القانونية التي توفّر قيوداً على قواعد تجفير XML الأساسية، وتُنتج تجفيراً وحيداً لأي قيمة ASN.1 ما. وتنطوي مواصفة قواعد التجفير هذه ضمناً على أنه يمكن استخدامها أيضاً من أجل فكّ التجفير. ويؤدي تطبيق قواعد التجفير هذه إلى تركيب نقل لهذه القيم. وتنطوي مواصفة قواعد التجفير هذه ضمناً على أنها تُستخدم أيضاً في فك التجفير. وهناك أكثر من مجموعة قواعد تجفير واحدة يمكن تطبيقها على قيم أنماط ASN.1. وتعرّف هذه التوصية مجموعتين من قواعد التجفير التي تستخدم لغة التوسيم القابلة للتوسيع XML. وتُسمى هذه قواعد تجفير XML (XER) بالنسبة للترميز ASN.1، وتُنتج كلتاهما وثيقة XML تمتثل للغة W3C XML 1.0. وتُسمى المجموعة الأولى قواعد تجفير XML الأساسية وتُسمى المجموعة الثانية قواعد تجفير XML القانونية لأن هناك وسيلة واحدة لتجفير قيمة ASN.1 باستخدام قواعد التجفير هذه. (وتُستخدم قواعد التجفير القانونية بوجه عام في تطبيقات تستخدم الخصائص المتعلقة بالأمن من مثل التواقيع الرقمية.)	17
X.733	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – إدارة الأنظمة: وظيفة الإبلاغ عن الإنذار	تعرّف هذه التوصية وظيفة إدارة الأنظمة التي يمكن أن تستخدم بواسطة عملية تطبيق في بيئة إدارة مركزية أو لا مركزية للتفاعل من أجل إدارة الأنظمة. وتعرّف هذه التوصية وظيفة تتألف من تعاريف عمومية وخدمات ووحدات وظيفية موجودة في طبقة التطبيق. وتوفر التبليغات عن الإنذار التي تعرفها هذه الوظيفة معلومات قد يحتاجها المدير للعمل بشأن الحالة التشغيلية ونوعية الخدمة في نظام ما.	4
X.735	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – إدارة الأنظمة: وظيفة التحكم في التسجيل	تعرّف هذه التوصية وظيفة إدارة الأنظمة التي يمكن أن تستخدم بواسطة عملية تطبيق في بيئة إدارة مركزية أو لا مركزية للتفاعل من أجل إدارة الأنظمة. وتعرّف هذه التوصية وظيفة تحكم في التسجيل وتتألف من خدمات ووحدتين وظيفيتين. وتوجد هذه الوظيفة في طبقة التطبيق.	4

X.736	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – إدارة الأنظمة: الوظيفة الأمنية المتعلقة بالإبلاغ عن الإنذار	تعرّف هذه التوصية الوظيفة الأمنية المتعلقة بالإبلاغ عن الإنذار، وهي وظيفة إدارة الأنظمة التي يمكن أن تستخدمها عملية التطبيق في بيئة إدارة مركزية أو لا مركزية لتبادل المعلومات لغرض إدارة الأنظمة. وتوجد هذه التوصية في طبقة التطبيق. ويرد وصف دور وظائف إدارة الأنظمة في CCITT X.701 | ISO/IEC 10040. وتوفر التبليغات عن إنذارات الأمن التي تعرّفها وظيفة إدارة الأنظمة معلومات تتعلق بالحالة التشغيلية ونوعية الخدمة المتعلقة بالأمن.	4
X.740	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – إدارة الأنظمة: وظيفة تسجيل تدقيق الأمن	تعرّف هذه التوصية وظيفة تسجيل تدقيق الأمن. وهذه الوظيفة هي وظيفة إدارة الأنظمة التي يمكن أن تستخدمها عملية التطبيق في بيئة إدارة مركزية أو لا مركزية لتبادل المعلومات والأوامر لغرض إدارة الأنظمة. وتوجد هذه التوصية في طبقة التطبيق.	4
X.741	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – إدارة الأنظمة: أغراض ونعوت التحكم في النفاذ	تعرّف هذه التوصية المواصفات المطبقة على توفير التحكم في النفاذ للتطبيقات التي تستخدم خدمات وبروتوكولات إدارة التوصيل البيني للأنظمة المفتوحة (OSI). ويمكن استخدام معلومات التحكم في النفاذ المحدّدة في هذه التوصية دعماً لمخططات التحكم في النفاذ المستندة إلى قوائم ومقدرات التحكم في النفاذ ووسمات الأمن، والتقييدات السياقية.	4
X.790	وظيفة إدارة الخلل بالنسبة لتطبيقات قطاع تقييس الاتصالات في الاتحاد ITU-T	تُعنى هذه التوصية بإدارة الخلل في تشغيل أنظمة وشبكات الاتصالات من منظور مورّد الخدمة ومستعمل تلك الخدمة. فالخلل في التشغيل هو مشكلة ذات تأثير ضار على نوعية الخدمة التي يتوقعها مستعملو الشبكة. وعندما يُكتشف خلل ما، رُبما نتيجة لإبلاغ إنذار فإنه يمكن لمستعمل أن يُدخل تقريراً عن الخلل أو يمكن للنظام أن يرفع تقريراً عنه بشكل تلقائي. وإدارة التقرير المتعلق بالخلل ضرورية لضمان أن يلقى الاهتمام وأن يتم توضيح الخلل لإعادة الخدمة إلى مستوى مقدرتها السابق. ويُعرّف نسق تقرير ليتيح للمستعمل الإبلاغ عن خلل ثم يتدرج بعدئذٍ إلى الحل من قبل مورّد الخدمة. وأثناء الحل من قبل هذا المورد، يمكن لمستعمل الخدمة أن يُحدد الحالة الراهنة للحل من خلال إصدار طلب لهذه المعلومات. وعند إزالة الخلل يمكن للمورّد أن يبلغ المستعمل. وتتضمن هذه التوصية أنماطاً خاصة من الخلل: إلاّ أن استخدام تطبيق معيّن لهذه التوصية يمكن أن يتطلب استخدام أنماط خلل خاصة بذلك التطبيق – وهو أمر يتم الاستجابة إليه. ووقت حدوث الخلل قد تكون شبكة ما تشتغل بينياً مع شبكة أخرى من أجل توفير الخدمة ويمكن أن تكون المشكلة أو الخلل في التشغيل عائداً إلى الشبكة الأخرى. ولذلك قد يكون من الضروري تبادل المعلومات المتعلقة بإدارة الخلل بين أنظمة الإدارة عبر سطوح بينية قد تكون زبائن لمورّد الخدمة أو سطوح بينية لمورّد خدمة إلى مورّد خدمة، كما قد تمثل حدوداً بين اختصاصات وحدود داخل الاختصاصات. وبالإضافة إلى تبادل المعلومات المتعلّقة بالخلل الذي اكتشف فعلياً، قد يتعيّن أيضاً تبادل معلومات مسبّقة عن عدم قابلية النفاذ إلى الخدمة. وبالتالي قد يحتاج مورّد خدمة إلى إبلاغ زبون بعدم إمكانية النفاذ إلى خدمة ما (بسبب صيانة من المزمع القيام بها، على سبيل المثال). ويشمل مجال تطبيق هذه التوصية جميع العمليات المذكورة أعلاه لتبادل معلومات الإدارة.	4
X.800	معمارية الأمن للتوصيل البيني للأنظمة المفتوحة لتطبيقات اللجنة الاستشارية الدولية للبرق والهاتف CCITT	تعرّف هذه التوصية العناصر المعمارية العامة المتعلقة بالأمن التي يمكن تطبيقها على نحو ملائم في الظروف التي تتطلب حماية الاتصالات بين الأنظمة المفتوحة. وتضع، في إطار نموذج مرجعي، خطوطاً توجيهية وتقييدات لتحسين التوصيات الحالية أو وضع توصيات جديدة في سياق التوصيل البيني للأنظمة المفتوحة من أجل السماح بتأمين الاتصالات، ومن ثم توفير منهج متسق للأمن في التوصيل البيني للأنظمة المفتوحة. وتمدد هذه التوصية النموذج المرجعي ليشمل جوانب الأمن التي هي عناصر معمارية عامة لبروتوكولات الاتصالات، ولكن لم تناقش في النموذج المرجعي. وتوفر هذه التوصية وصفاً عاماً لخدمات الأمن والآليات ذات الصلة التي يمكن أن يوفرها النموذج المرجعي؛ وتعرّف الحالات في النموذج المرجعي حيث يمكن توفير الخدمات والآليات.	17
X.802	تكنولوجيا المعلومات – نموذج الأمن في الطبقات السفلى	تصف هذه التوصية جوانب الطبقة المستعرضة لتنقيح خدمات الأمن في الطبقات السفلى لنموذج مرجعي للتوصيل البيني للأنظمة المفتوحة (النقل والشبكة ووصلة البيانات والوصلة المادية). وتصف المفاهيم المعمارية المشتركة لهذه الطبقات وأساس التفاعلات المتعلقة بالأمن بين الطبقات ووضع بروتوكولات الأمن في الطبقات السفلى.	17

X.803	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – نموذج الأمن في الطبقات العليا	تصف هذه التوصية انتقاء ووضع واستخدام خدمات الأمن وآلياته في الطبقات العليا (طبقات التطبيقات والتقديم والجلسة) للنموذج المرجعي للتوصيل البيني للأنظمة المفتوحة.	17
X.805	معمارية أمن لأنظمة توفر الاتصالات من طرف إلى طرف	تعرّف هذه التوصية العناصر المعمارية العامة المتعلقة بالأمن التي يمكنها عند تطبيقها على نحو ملائم، ولا سيما في بيئة بائعين متعددين، أن تضمن حماية الشبكة بشكل ملائم من الهجمات المؤذية أو غير المتعمدة وتعمل على توفير معلمات الأداء مثل التيسر العالي ووقت الاستجابة الملائم وسلامة البيانات وقابلية الاتساع ووظيفة الفوترة الدقيقة.	17
X.810	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: نظرة عامة	تعرّف هذه التوصية الإطار الذي تحدد فيه خدمات أمن الأنظمة المفتوحة. ويصف هذا الجزء من أطر الأمن تنظيم *إطار الأمن* ويعرّف *مفاهيم الأمن* المطلوبة في أكثر من جزء واحد لإطار الأمن وتصف ترابط علاقات الخدمات والآليات المعرّفة في الأجزاء الأخرى للإطار. ويصف هذا الإطار جميع جوانب *الاستيقان* نظراً لأنها تطبق على الأنظمة المفتوحة وعلاقة الاستيقان مع وظائف الأمن الأخرى مثل *التحكم في النفاذ* ومتطلبات إدارة الاستيقان.	17
X.811	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: إطار الاستيقان	تعرّف هذه التوصية إطاراً عاماً لتوفير الاستيقان. والهدف الأولي للاستيقان هو *مواجهة تهديدات التنكر والتلاعب*.	17
X.812	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: إطار التحكم في النفاذ	تعرّف هذه التوصية إطاراً عاماً لتوفير التحكم في النفاذ. والهدف الأولي للتحكم في النفاذ هو *مواجهة التهديدات من عمليات غير مرخص بها* تتضمن حاسوباً أو نظام اتصالات؛ وغالباً ما تنقسم هذه التهديدات إلى أنواع تعرف *بالاستخدام غير المرخص به والكشف والتعديل والتدمير ورفض الخدمة*.	17
X.813	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: إطار عدم التنصل	تعرّف هذه التوصية إطاراً عاماً لخدمات عدم التنصل. وهدف خدمة عدم التنصل هو *الجمع والاحتفاظ والتيسير وإقرار صلاحية الدليل الذي لا يدحض فيما يتعلق بتحديد مرسلين ومستقبلين ضالعين في نقل المعطيات*.	17
X.814	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: إطار السرية	تعرّف هذه التوصية إطاراً عاماً لتوفير خدمات السرية. والسرية هي خاصية *أن المعلومات لا تتاح أو يكشف عنها* لأفراد أو كيانات أو عمليات غير مرخص لها بذلك.	17

X.815	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: إطار سلامة البيانات	تعرّف هذه التوصية إطاراً عاماً لتوفير خدمات سلامة البيانات. وتسمى خاصية *عدم تعرض البيانات للتعديل أو التدمير* بطريقة غير مرخص بها، خاصية السلامة.	17
X.816	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أطر الأمن للأنظمة المفتوحة: إطار تدقيق الأمن والإنذارات	تصف هذه التوصية نموذجاً أساسياً لمناولة إنذارات الأمن والقيام بتدقيق الأمن للأنظمة المفتوحة. وتدقيق الأمن هو *استعراض مستقل وفحص لسجلات وأنشطة النظام*. وتوفر خدمة تدقيق الأمن سلطة تدقيق لها مقدرة على تحديد واختيار وإدارة أحداث تحتاج إلى أن تسجل في تسجيل تدقيق الأمن.	17
X.830	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أمن الطبقات العليا العمومية: نظرة عامة ونماذج وترميز	تنتمي هذه التوصية إلى سلسلة من التوصيات التي تقدم مجموعة من التسهيلات للمساعدة على بناء بروتوكولات الطبقة العليا للتوصيل البيني للأنظمة المفتوحة (OSI) التي تدعم توفير خدمات الأمن. وتحدد هذه التوصية ما يلي: أ) *نماذج عامة لوظائف بروتوكول تبادل الأمن وتحولات الأمن*؛ ب) مجموعة من *الأدوات الترميزية* لدعم مواصفة متطلبات الحماية الانتقائية للمجالات في مواصفة قواعد التركيب المجرد ولدعم مواصفة تبادلات وتحولات الأمن؛ ج) مجموعة من *المبادئ التوجيهية الإعلامية* فيما يتعلق بتطبيق تسهيلات أمن الطبقة العليا العمومية التي تغطيها هذه السلسلة من التوصيات.	17
X.831	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أمن الطبقات العليا العمومية: تعريف خدمة عنصر خدمة تبادل الأمن	تنتمي هذه التوصية إلى سلسلة من التوصيات التي تقدم مجموعة من التسهيلات للمساعدة على بناء بروتوكولات الطبقة العليا للتوصيل البيني للأنظمة المفتوحة (OSI) التي تدعم توفير خدمات الأمن. وتحدد هذه التوصية الخدمة التي يوفرها عنصر خدمة تبادل الأمن (SESE). وهذا العنصر هو عنصر– خدمة– تطبيق (ASE) ييسر اتصال *معلومات الأمن* لدعم توفير *خدمات الأمن* في طبقة التطبيق العليا للتوصيل البيني للأنظمة المفتوحة.	17
X.832	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أمن الطبقات العليا العمومية: مواصفة بروتوكول عنصر خدمة تبادل الأمن	تنتمي هذه التوصية إلى سلسلة من التوصيات التي تقدم مجموعة من التسهيلات للمساعدة على بناء بروتوكولات الطبقة العليا التي تدعم توفير خدمات الأمن. *وتحدد* هذه التوصية *البروتوكول* الذي يوفره عنصر خدمة تبادل الأمن. وهذا العنصر هو عنصر– خدمة– تطبيق (ASE) ييسر توصيل *معلومات الأمن* لدعم توفير *خدمات الأمن* في طبقة التطبيق للتوصيل البيني للأنظمة المفتوحة.	17
X.833	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أمن الطبقات العليا العمومية: مواصفة حماية قواعد تركيب النقل	تنتمي هذه التوصية إلى سلسلة من التوصيات التي تقدم مجموعة من التسهيلات للمساعدة على بناء بروتوكولات الطبقة العليا للتوصيل البيني للأنظمة المفتوحة (OSI) التي تدعم توفير خدمات الأمن. تعرّف هذه التوصية قواعد تركيب النقل المقترنة بدعم طبقة التقديم *لخدمات الأمن* في طبقة التطبيق.	17

X.834	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أمن الطبقات العليا العمومية: شكل الإعلان عن تطابق تنفيذ بروتوكول عنصر خدمة تبادل الأمن	تنتمي هذه التوصية إلى سلسلة توصيات بشأن أمن الطبقات العليا العمومية، وهي شكل الإعلان عن الامتثال لتنفيذ البروتوكول بالنسبة إلى عنصر خدمة تبادل الأمن المحدد في التوصية X.832 لقطاع تقييس الاتصالات وتبادل الأمن الوارد في التوصية X.830 لقطاع تقييس الاتصالات. الملحق جيم يوفر وصفاً لمقدرات وخيارات مقيسة في شكل يدعم تقييم الامتثال لتنفيذ معين.	17
X.835	تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – أمن الطبقات العليا العمومية: شكل الإعلان عن تطابق تنفيذ بروتوكول حماية قواعد تركيب النقل	تنتمي هذه التوصية إلى سلسلة توصيات بشأن أمن الطبقات العليا العمومية، وهي شكل الإعلان عن الامتثال لتنفيذ بروتوكول حماية قواعد تركيب النقل المحدد في التوصية X.833 لقطاع تقييس الاتصالات. وتوفر هذه التوصية وصفاً لمقدرات وخيارات مقيسة في شكل يدعم تقييم الامتثال لتنفيذ معين.	17
X.841	تكنولوجيا المعلومات – تقنيات الأمن – أغراض معلومات أمن لمراقبة النفاذ	توفر هذه التوصية تعاريف أغراض لازمة بوجه عام في *معايير الأمن* لتجنب تعاريف متعددة ومختلفة لنفس العنصر الوظيفي. وتتحقق الدقة في هذه التعاريف باستخدام ترميز تركيب مجرد رقم واحد (ASN.1). وتشمل هذه التوصية الجوانب السكونية فقط لأغراض معلومات الأمن.	17
X.842	تكنولوجيا المعلومات – تقنيات الأمن – خطوط توجيهية لاستخدام وإدارة خدمات الطرف الثالث الموثوق به	توفر هذه التوصية توجيهاً لاستخدام خدمات طرف ثالث موثوق به وتعريف واضح للواجبات والخدمات الأساسية المقدمة ووصفها وأغراضها وأدوارها ومسؤوليات أطراف ثالثة موثوق بها وكيانات تستخدم خدماتها. وتعرّف هذه التوصية الفئات الرئيسية المختلفة لخدمات الطرف الثالث الموثوق به بما في ذلك *دلالة الوقت وعدم التنصل وإدارة المفاتيح وإدارة الشهادات والتصديق الإلكتروني*.	17
X.843	تكنولوجيا المعلومات – تقنيات الأمن – مواصفة خدمات الطرف الثالث الموثوق به لدعم تطبيق التواقيع الرقمية	تعرّف هذه التوصية الخدمات المطلوبة لدعم تطبيق التواقيع الرقمية *لعدم التنصل* عند استحداث وثيقة ما. ونظراً لأن هذا يتضمن *سلامة* الوثيقة *والاستيقان* من صاحبها فإنه يمكن جمع الخدمات الموصوفة لتنفيذ *خدمات سلامة البيانات وصحتها*.	17

X.901	تكنولوجيا المعلومات – معالجة موزعة مفتوحة – نموذج مرجعي: نظرة عامة	أدى النمو السريع للمعالجة الموزعة إلى الحاجة إلى إطار تنسيقي لتقييس المعالجة الموزعة المفتوحة (ODP). ويوفر النموذج المرجعي هذا مثل هذا الإطار ويقوم بإنشاء معمارية لدعم التوزيع والتشغيل البيني وتضمين قابليةٍ الحمل. وتحتوي هذه التوصية على نظرة عامة تتناول المعالجة الموزعة المفتوحة وتوضح نطاقها وأسبابها وتشرح مفاهيمها الرئيسية وتشمل موجزاً لمعماريتها. وتحتوي على مواد تفسيرية عن كيفيةٍ تفسير النموذج المرجعي هذا واستخدامه من قبل مستعمليه وواضعي المعايير ومهندسي أنظمة المعالجة الموزعة المفتوحة. كما أن التوصية تحتوي أيضاً على تصنيف مجالات التقييس المطلوبة المعبر عنها بالنقاط المرجعية حول الامتثال المعرّف في التوصية X.903. ويتعين تأمين أنظمة المعالجة الموزعة المفتوحة، أي ينبغي بناؤها وصيانتها بطريقة تضمن حماية تسهيلات وبيانات النظام من *النفاذ غير المرخص به والاستخدام غير المشروع وأي تهديدات أو هجمات أخرى*. وتصبح متطلبات الأمن صعبة التحقيق بحكم بعد التفاعلات وتنقلية النظام ومستعملي النظام. وقد تحدد قواعد الأمن لأنظمة المعالجة الموزعة المفتوحة اكتشاف تهديدات الأمن؛ *والحماية من تهديدات الأمن؛ والحد من أي ضرر يتسبب فيه أي انتهاكات للأمن.*	17
X.902	تكنولوجيا المعلومات – معالجة موزعة مفتوحة – نموذج مرجعي: الأسس	تحتوي هذه التوصية على تعريف المفاهيم والإطار التحليلي لوصف مقيّس لأنظمة المعالجة الموزعة (الاعتباطية). وتقدم مبادئ الامتثال لمعايير المعالجة الموزعة المفتوحة والطريقة التي تطبق بها. وذلك حتى سوية معينة من التفصيل تكفي *لوضع متطلبات لتقنيات مواصفة جديدة.*	17
X.903	تكنولوجيا المعلومات – معالجة موزعة مفتوحة – نموذج مرجعي: المعمارية	تحتوي هذه التوصية على مواصفة الخصائص المطلوبة التي تجعل المعالجة الموزعة مفتوحة. وهذه هي التقييدات التي ينبغي أن تمتثل لها معايير المعالجة الموزعة المفتوحة. وتستخدم التقنيات الوصفية من التوصية ITU-T X.902.	17
X.904	تكنولوجيا المعلومات — معالجة موزعة مفتوحة — نموذج مرجعي: الدلالات المعمارية	تحتوي هذه التوصية على تقييس مفاهيم نمذجة المعالجة الموزعة المفتوحة المعرّفة في التوصية X.902، الفقرتان 8 و9. ويتحقق التقييس من خلال تفسير كل مفهوم على أساس تركيبات مختلف تقنيات الوصف الشكلي المقيسة.	17
X.1051	نظام إدارة أمن المعلومات – المتطلبات الخاصة بالاتصالات (ISMS-T)	بالنسبة لمنظمات الاتصالات، تمثل المعلومات وعمليات الدعم، وتسهيلات الاتصالات وشبكاتها وخطوطها أصولاً تجارية هامة. ولكي تدير منظمات الاتصالات هذه الأصول التجارية إدارة ملائمة، ولكي تواصل على نحو سليم وبصورة ناجحة أنشطتها التجارية، تعتبر إدارة أمن المعلومات مسألة ضرورية للغاية. وتوفر هذه التوصية المتطلبات الخاصة بإدارة أمن المعلومات اللازمة لمنظمات الاتصالات. وتُحدد هذه التوصية المتطلبات اللازمة لإنشاء وتنفيذ نظام موثّق لإدارة أمن المعلومات وتشغيل هذا النظام ومراقبته واستعراضه وصيانته وتحسينه في سياق المخاطر التجارية الإجمالية للاتصالات. وتُحدد التوصية المتطلبات اللازمة لعمليات المراقبة الأمنية المناسبة لاحتياجات فرادى شبكات الاتصالات أو أجزاء منها.	17
X.1081	نموذج القياسات الحيوية عن بعد متعدد الأساليب – إطار لمواصفة جوانب الأمن والسلامة الخاصة بالقياسات الحيوية عن بعد	تعرّف هذه التوصية نموذجاً للقياسات الحيوية عن بعد متعدد الأساليب يوفر إطاراً عاماً لمواصفة أربع مسائل أمنية مترابطة فيما بينها: الخصوصية والاستيقان والسلامة والأمن. ويُغطي نموذج القياسات الحيوية عن بعد متعدد الأساليب جميع الإمكانيات الخاصة بتوفير تفاعلات سالمة وآمنة متعددة الأساليب بين الإنسان والآلة، وهو مشتق جزئياً من معيار ISO 31 والمعيار IEC 60027-1. فالطرائق الإدراكية والمفاهيمية والسلوكية لكائن بشري هي أمور ذات صلة أيضاً بميدان الاتصالات، ومن المحتمل أن تُستخدم من قبل محساس أو مؤشر للقياس الحيوي في المستقبل لأغراض الاستيقان. وهي مشمولة في نموذج القياسات الحيوية عن بعد متعدد الأساليب. وتُقدم هذه التوصية تصنيف التفاعلات التي تحدث في الطبقة متعددة الوسائل حيث يتفاعل جسم الإنسان مع الأجهزة الإلكترونية أو الفوتونية أو الكيميائية أو المادية ملتقطاً معلمات قياسات حيوية أو مؤثراً على ذلك الجسم. واستيقان كائن بشري مع المحافظة على خصوصيته وسلامته يمكن تحديده من حيث التفاعلات بين الأجهزة ومجال الخصوصية الشخصية الذي يقوم بنمذجة وكبسلة تفاعلات كائن بشري مع بيئته جاعلاً مناقشة هذه التفاعلات أمراً واضحاً وقابلاً للهندسة. وتشمل هذه التوصية مواصفة مجال الخصوصية الشخصية وتصنيفاً لطرائق التفاعل عبر ذلك المجال والوحدات الأساسية والمشتقة اللازمة لقياس وتحديد هذه التفاعلات (بطريقة كمية) وتراتباً من حيث المقياس للقرابة النسبية.	17

X.1121	إطار تكنولوجيات الأمن لاتصالات البيانات المتنقلة من طرف إلى طرف	تصف هذه التوصية تهديدات الأمن في اتصالات البيانات المتنقلة من طرف إلى طرف، ومتطلبات الأمن بالنسبة للمستعمل المتنقل ومورّد خدمة التطبيق (ASP) في الطبقة العليا من النموذج المرجعي للتوصيل البيني للأنظمة المفتوحة OSI لنموذج اتصالات البيانات المتنقلة من طرف إلى طرف بين مطراف متنقل في شبكة متنقلة ومخدّم تطبيق في شبكة مفتوحة. وبالإضافة إلى ذلك، تبين التوصية أين تظهر تكنولوجيات الأمن التي تحقق وظيفة أمن معيّنة في نموذج اتصالات البيانات المتنقلة من طرف إلى طرف. وتوفر التوصية إطاراً لتكنولوجيات الأمن اللازمة لاتصالات البيانات المتنقلة من طرف إلى طرف.	17
X.1122	منهج لتنفيذ أنظمة آمنة متنقلة تستند إلى البنى التحتية للمفاتيح العمومية (PKI)	تكنولوجيا البنى التحتية للمفاتيح العمومية هي تكنولوجيا أمنية تُطبق على العلاقة بين المطراف المتنقل ومُخدّم التطبيق في النموذج العام لاتصالات البيانات المتنقلة من طرف إلى طرف بين مستعمل متنقل ومورّد خدمة التطبيق ASP أو تطبق على العلاقة بين مطراف متنقل وبوابة أمن متنقلة أو بين بوابة أمن متنقلة ومُخدّم في نموذج بوابة لاتصالات بيانات متنقلة من طرف إلى طرف بين مستعمل متنقل ومورّد خدمة التطبيق ASP. ولئن كانت تكنولوجيا البنى التحتية للمفاتيح العمومية تكنولوجيا مفيدة للغاية في حماية اتصالات البيانات المتنقلة من طرف إلى طرف، فإن هناك خصائص محددة لاتصالات البيانات المتنقلة تتطلب مواءمة تكنولوجيا PKI عند بناء أنظمة متنقلة آمنة (التجفير، والتوقيع الرقمي، وسلامة البيانات وما إلى ذلك). ونظراً لأنه لم توضع طرائق لبناء وإدارة الأنظمة المتنقلة الآمنة المستندة إلى تكنولوجيا البنى التحتية للمفاتيح العمومية فإن هذه التوصية ترسم منهجا لبناء الأنظمة المتنقلة الآمنة المستندة إلى تكنولوجيا PKI.	17

الملحق باء

مصطلحات الأمن

استخلصت التعاريف والمختصرات التالية المتصلة بمجال الأمن في إطار قطاع تقييس الاتصالات من التوصيات ذات الصلة الصادرة عن القطاع.

توفر قاعدة بيانات القطاع ITU-T على الخط المعروفة باسم SANCHO (*مختصرات وتعاريف القطاع في مجال الاتصالات على غرار قاموس المترادفات*) إمكانية النفاذ إلى "المصطلحات والتعاريف" أو "المختصرات والتسميات المختصرة" المعرّفة في منشورات القطاع ITU-T، بالإنكليزية والفرنسية والإسبانية. وهذا المورد المتيسر على الخط مجاناً يمكن النفاذ إليه في العنوان التالي: www.itu.int/sancho. وتنشر بانتظام أيضاً نسخة مسجلة على قرص CD-ROM. ويمكن الاطلاع على جميع المصطلحات والتعاريف الواردة أدناه في "SANCHO" مع قائمة بالتوصيات التي استخدم فيها المصطلح أو التعريف.

وقد أعدت لجنة الدراسات 17 التابعة لقطاع تقييس الاتصالات خلاصة وافية للتعاريف المتعلقة بالأمن المستعملة في توصيات القطاع ITU-T والتي يمكن الاطلاع عليها في العنوان التالي:
http://www.itu.int/ITU-T/studygroups/com17/tel-security.html.

باء.1 قائمة بالمصطلحات والتعاريف المتصلة بمجال الأمن

تضم القائمة التالية مصطلحات الأمن شائعة الاستخدام المعرّفة في التوصيات الراهنة للقطاع ITU-T. وهنالك قائمة أشمل بتعاريف الأمن في الخلاصة الوافية التي تحتفظ بها لجنة الدراسات 17 (انظر الموقع المشار إليه أعلاه).

المصطلح	التعريف	المرجع
التحكم في النفاذ **access control**	1. منع استخدام غير مرخص به لمورد ما، بما في ذلك منع استخدام مورد بطريقة غير مرخص بها. 2. قصر تدفق المعلومات من موارد نظام ما إلى أشخاص مرخص لهم أو برامج أو عمليات أو موارد نظام أخرى على الشبكة مرخص لها بذلك.	X.800 J.170
قائمة التحكم في النفاذ **access control list**	قائمة بالكيانات المرخص لها بالنفاذ إلى مورد ما، مشفوعة بحقوق هذه الكيانات في النفاذ.	X.800
سياسة التحكم في النفاذ **access control policy**	مجموعة القواعد التي تحدد الشروط التي يمكن أن يتم بموجبها أي نفاذ.	X.812
خدمة التحكم في النفاذ **access control service**	توفر خدمة التحكم في النفاذ وسيلة لضمان نفاذ صاحب الشأن إلى الموارد فقط بطريقة مرخص بها. ويمكن أن تكون الموارد المعنية النظام المادي، أو برمجية النظام، أو التطبيقات والبيانات. ويمكن أن تُعرّف وتنفّذ خدمة التحكم في النفاذ على مستويات مختلفة من الدقة في شبكة إدارة الاتصالات TMN: على مستوى الوكيل أو مستوى الغرض أو مستوى النعت. والتقييدات على النفاذ مبينة في معلومات التحكم في النفاذ: أي وسائل تحديد أي الكيانات مرخص لها بالنفاذ؛ وأي نوع من النفاذ مسموح به (القراءة، الكتابة، التعديل، الإنشاء، الحذف).	M.3016.2
التهديدات العرضية **accidental threats**	التهديدات التي تنشأ دون سابق قصد. ومن الأمثلة على التهديدات التي تتحقق عرضاً أعطال النظام وهفوات التشغيل وعيوب البرمجية.	X.800
المساءلة accountability	الخاصية التي تضمن أن أعمال كيان ما يمكن تتبعها إلى ذلك الكيان فقط.	X.800
التهديد النشط active threat	التهديد بتغيير متعمد غير مرخص له في المعلومات المتضمنة في النظام، أو تغيير لحالة النظام. *ملاحظة* – من أمثلة التهديدات النشطة المتعلقة بالأمن: إدخال تعديل على الرسائل، وتكرار الرسائل، وإدراج رسائل مزيفة والتنكر ككيان مرخص له ورفض الخدمة والتغيير المؤذي في جداول التسيير لنظام ما من قِبَل مستعمل غير مرخص له بذلك.	X.800
المحكّم adjudicator	كيان يحكم في المنازعات التي قد تنشأ نتيجة أحداث أو أعمال مرفوضة، أي الكيان الذي يقيّم الأدلة ويحدد ما إذا كان الإجراء أو الحدث موضع النـــزاع قد وقع أم لم يقع. ولا يمكن توفير *التحكيم* على نحو فعّال إلاّ إذا قبل أطراف النـــزاع *سلطة* المحكم.	X.813
خوارزمية algorithm	عملية رياضية يمكن استخدامها لتخليط تدفق البيانات وإزالة تخليطها.	J.93
طريقة استيقان لا تناظرية **asymmetric authentication method**	طريقة استيقان لا يتقاسم فيها كلا الكيانين جميع معلومات الاستيقان.	X.811

المصطلح	التعريف	المرجع
خوارزمية تجفير لا تناظرية asymmetric cryptographic algorithm	خوارزمية لأداء تجفير أو فك تجفير مقابل تكون فيه المفاتيح المستخدمة للتجفير وفك التجفير مختلفة. *ملاحظة* – في بعض الخوارزميات المجفرة اللاتناظرية، يتطلب فك تجفير نص مجفر أو توليد توقيع رقمي استخدام أكثر من مفتاح خاص.	X.810
الهجوم attack	الأنشطة المضطلع بها لتجاوز أو استغلال جوانب القصور في آليات أمن النظام. وبالهجوم مباشرة على نظام ما، تستغل الأنشطة جوانب القصور في الخوارزميات أو المبادئ أو خصائص آلية الأمن في النظام. ويحدث الهجوم غير المباشر عندما تتجاوز الآلية أو عندما تجعل النظام يستخدم الآلية بطريقة غير صحيحة.	H.235
النعت attribute	في سياق مناولة الرسائل، يكون النعت بند معلومات أو مكوّناً في قائمة نعوت يصف قائمة مستعمل أو قائمة توزيع كما يمكنه أيضاً أن يحدد موقعها بالنسبة إلى البنية المادية أو التنظيمية لنظام مناولة رسائل (أو الشبكة التي يستند إليها).	X.400
سلطة تحديد النعت Attribute Authority	1. سلطة تعين امتيازات من خلال إصدار شهادات النعوت. 2. كيان موثوق به من كيان أو أكثر لاستحداث وتوقيع شهادات النعوت. *ملاحظة* – يمكن أن تقوم سلطة إصدار الشهادات بمهمة سلطة تحديد النعوت.	X.509 X.842
شهادة النعت attribute certificate	هيكل بيانات وقعته رقمياً سلطة تحديد النعت ويربط بعض قيم النعوت بمعلومات تُعرِّف هوية حامليها.	X.509
نمط النعت attribute type	مُعرّف يدل على صنف معلومات (أسماء شخصية مثلاً). وهو جزء من النعت.	X.400
قيمة النعت attribute value	حالة صنف المعلومات الذي يدل عليه نمط النعت (اسم شخصي معين مثلاً). وهو جزء من النعت.	X.400
التدقيق audit	انظر تدقيق الأمن.	X.800
تسجيل التدقيق audit trail	انظر تسجيل تدقيق الأمن.	X.800
الهوية المستيقنة authenticated identity	معرّف مميز لكيان تم التأكد منه من خلال الاستيقان.	X.811
الاستيقان authentication	1. عملية تأييد صحة هوية. *ملاحظة* – انظر الكيان الأصلي والمحقق وشكلي الاستيقان المميزين (استيقان أصل البيانات + استيقان الكيان). ويمكن أن يكون الاستيقان منفرداً أو متبادلاً. ويوفّر الاستيقان *المنفرد* تأكيد هوية كيان أصلي واحد فقط. ويوفّر الاستيقان *المتبادل* تأكيد هويتي كلا الكيانين الأصليين. 2. توفير تأكيد للهوية المدعاة لكيان ما. 3. انظر استيقان أصل البيانات، واستيقان الكيان الند. ولا يُستخدم مصطلح "الاستيقان" فيما يتعلق بسلامة البيانات؛ إذ يُستخدم مصطلح "سلامة البيانات" بدلاً منه. 4. تأييد صحة هوية الأغراض ذات الصلة بإنشاء علاقة ترابط. وقد تشمل مثلاً استيقان الكيانات، واستيقان التطبيقات واستيقان الناس مستعملي التطبيقات. *ملاحظة* – عُرّف هذا المصطلح لتوضيح أن الأمر يتناول نطاق استيقان أوسع مما يشمله استيقان الكيان الند الوارد في التوصية X.800 للجنة الاستشارية الدولية للبرق والهاتف CCITT. 5. عملية التحقق من الهوية المدّعاة من كيان لدى كيان آخر. 6. العملية التي تهدف إلى تمكين النظام من التحقق يقيناً من هوية طرف ما.	X.811 X.811 X.800 X.217 J.170 J.93

المصطلح	التعريف	المرجع
شهادة الاستيقان **authentication certificate**	شهادة أمن تضمنها سلطة استيقان ويمكن أن تستخدم لتأكيد هوية كيان ما.	X.811
تبادل الاستيقان **authentication exchange**	1. آلية القصد منها التأكد من هوية كيان بواسطة تبادل المعلومات. 2. تتابع لعملية نقل واحدة أو أكثر لتبادل معلومات الاستيقان لأغراض القيام بعملية استيقان.	X.800 X.811
خدمة الاستيقان **authentication service**	توفر الدليل على أن هوية غرض أو موضوع هي حقاً الهوية المزعومة. وتبعاً لنمط الجهة الفاعلة وغرض تعرف الهوية قد يستدعي الأمر الأنواع التالية من الاستيقان: استيقان المستعمل، استيقان الكيان الند، استيقان أصل البيانات. ومن أمثلة الآلية المستخدمة في تنفيذ خدمة الاستيقان كلمات السر وأرقام التعرف الشخصية (PINs) (والاستيقان البسيط) والطرائق المستندة إلى التجفير (الاستيقان القوي).	M.3016.2
علامة الاستيقان (علامة) **authentication token (token)**	معلومات تنقل خلال تبادل الاستيقان القوي، ويمكن أن تستخدم للاستيقان من هوية مرسلها.	X.509
الموثوقية authenticity	1. القدرة على ضمان أن المعلومات المقدمة خالية من أي تعديل أو تزييف وأن الذي أنتجها في الواقع هو الكيان الذي يدعي أنه قدم المعلومات. 2. خاصية إمكانية التحقق من مصدر البيانات المدّعى على نحو يرضاه المتلقي.	J.170 T.411
السلطة authority	كيان مسؤول عن إصدار الشهادات. وهنالك نوعان من السلطة؛ سلطة إصدار الشهادات التي تُصدر شهادات المفاتيح العمومية، وسلطة النعوت التي تصدر شهادات النعوت.	X.509
شهادة السلطة **authority certificate**	شهادة تصدر لسلطة (لسلطة إصدار شهادات أو سلطة نعوت مثلاً).	X.509
الترخيص authorization	1. منح حقوق تشمل منح النفاذ استناداً إلى حقوق النفاذ. *ملاحظة* – ينطوي هذا التعريف ضمناً على حقوق أداء نشاط ما (مثل النفاذ إلى البيانات)؛ وعلى أن الحقوق مُنحت لعملية أو كيان أو فرد ما. 2. منح الإذن على أساس هوية مستيقنة. 3. عملية تمكين النفاذ إلى خدمة أو جهاز ما إذا كان لدى المرء تصريح بالنفاذ.	X.800 H.235 J.170
التيسر availability	خاصية قابلية النفاذ والاستخدام عند الطلب من قبل كيان مرخص له بذلك.	X.800
بوابة أمن الكبل **cable security portal (CSP)**	عنصر وظيفي يوفّر إدارة الأمن والترجمة بين شبكة الألياف الهجينة متحدة المحور HFC والشبكة الأصل.	J.191
مخدم إدارة النداء **call management server (CMS)**	الاتصال الكبلي بواسطة بروتوكول الإنترنت IPCablecom. يتحكم في التوصيلات السمعية. ويسمى أيضاً وكيل النداء في مصطلحات بروتوكول التحكم في بوابة الوسائط وبروتوكول مراقبة التشفير MGCP/SGCP.	J.191
المقدرة capability	علامة تستخدم كمعرّف لمورد بحيث تضفي حيازة العلامة حقوق نفاذ إلى المورد.	X.800

المصطلح	التعريف	المرجع
الشهادة certificate	مجموعة من البيانات المتعلقة بالأمن تصدرها سلطة الأمن أو طرف ثالث موثوق به مع معلومات أمن تستخدم لتوفير سلامة البيانات وخدمات الاستيقان من أصل البيانات (شهادة الأمن – X.810). وفي هذه التوصية يشير المصطلح إلى شهادات "المفاتيح العمومية" وهي قيم تمثل مالكي المفاتيح العمومية (ومعلومات اختيارية أخرى) كما تم الاستيقان منها ووقعتها سلطة موثوق بها في نسق لا يمكن تزويره.	H.235
سياسة الشهادة certificate policy	مجموعة معينة من القواعد تشير إلى قابلية تطبيق الشهادة على مجموعة و/أو صنف معين من التطبيقات له متطلبات أمن مشتركة. فقد تشير سياسة شهادة معينة مثلاً إلى مدى قابلية تطبيق نمط شهادة ما على الاستيقان من معاملات تبادل البيانات الإلكترونية لتبادل البضائع في نطاق سعر معين.	X.509
قائمة إبطال الشهادات Certificate Revocation List (CRL)	1. قائمة موقعة تضم مجموعة من الشهادات لم يعد يعتبرها مُصدر الشهادة صالحة. وبالإضافة إلى المصطلح العمومي لهذه القائمة، تعرف بعض أنواع محددة من هذه القائمة لتشمل مجالات معينة. 2. قائمة تشمل الأرقام المسلسلة للشهادات التي أُبطلت (لأن المفتاح أصبح مكشوفاً مثلاً أو لأن الشخص المعني لم يَعُد يعمل مع الشركة) والتي لم تنته فترة صلاحيتها بعد.	X.509 Q.817
سلطة إصدار الشهادات Certification Authority (CA)	1. سلطة موثوق بها من قبل مستعمل أو أكثر لاستحداث وتخصيص شهادات مفاتيح عمومية. ويمكن لسلطة إصدار الشهادات، اختيارياً، أن تستحدث مفاتيح المستعملين. 2. كيان يوثق به (في سياق سياسة أمن) لإصدار شهادات أمن تحتوي على صنف أو أكثر من أصناف البيانات المتعلقة بالأمن.	X.509 X.810
مسير إصدار الشهادات certification path	تتابع منتظم لشهادات أغراض في شجرة معلومات الدليل يمكن معالجته، مع المفتاح العمومي للغرض الأولي في المسير، للحصول على تتابع الغرض النهائي في المسير.	X.509
التحدي challenge	معلمة متغيرة الزمن يولدها متحقق.	X.811
التجفير cipher	1. خوارزمية مجفرة، تحويل رياضي. 2. خوارزمية تحول بيانات بين نص عادي ونص مُجفر.	H.235 J.170
نص التجفير ciphertext	بيانات منتجة من خلال استخدام التجفير. ولا يتاح المحتوى الدلالي للبيانات الناتجة. *ملاحظة* – قد يخضع النص المُجفر نفسه للتجفير، بحيث يكون الناتج نصاً مضاعف التجفير.	X.800
المطالب claimant	كيان يكون أو يمثل العنصر *الرئيسي* لأغراض الاستيقان. ويشمل المطالب الوظائف اللازمة للشروع في تبادلات للاستيقان بالنيابة عن العنصر الرئيسي.	X.811
نص واضح cleartext	بيانات مفهومة يكون محتوى دلالاتها متاحاً.	X.800
إثبات غير قاطع compromised evidence	إثبات كان مرضياً في وقت ما لكنه لم يعد يحظى بثقة الطرف الثالث الموثوق به أو المُحكم.	X.813
السرية confidentiality	ضمان عدم كشف المعلومات أو إتاحتها لأفراد أو كيانات أو عمليات غير مرخص لها بذلك.	X.800
خدمة السرية confidentiality service	توفر خدمة السرية حماية من الكشف غير المرخص به للبيانات المتبادلة. ويميز بين الأنواع التالية من الخدمات السرية: سرية بحسب المجال؛ سرية التوصيل؛ سرية تدفق البيانات.	M.3016.2

المصطلح	التعريف	المرجع
سلامة المحتوى content integrity	1. تمكن المتلقي من التحقق من أن المحتوى الأصلي للرسالة لم يُعدّل.	X.400
	2. يمكّن عنصر الخدمة هذا مرسل الرسالة من أن يزوّد متلقي الرسالة بوسيلة تمكّنه من التحقق من أن محتوى الرسالة لم يُعدّل. وتُحدد سلامة المحتوى على أساس كل متلق على حدة، ويمكن أن تستخدم تقنية تجفير لا تناظري أو تقنية تجفير تناظري.	X.400
توقيع التصديق counter-signature	توقيع رقمي يذيل وحدة بيانات قد وقعها كيان آخر (طرف ثالث موثوق به مثلاً).	X.813
بيانات التصديق credentials	بيانات تنقل لإثبات هوية الكيان المدّعاة.	X.800
تحليل التجفير cryptanalysis	1. تحليل نظام مجفر و/أو مدخلاته ومخرجاته لاستخراج متغيرات سرية و/أو بيانات حساسة بما في ذلك نص واضح.	X.800
	2. عملية استرجاع نص عادي لرسالة أو مفتاح تجفير دون النفاذ إلى المفتاح.	J.170
	3. علم استرجاع نص عادي للرسالة دون النفاذ إلى المفتاح (إلى المفتاح الإلكتروني في أنظمة التجفير الإلكترونية).	J.93
خوارزمية تجفير cryptographic algorithm	وظيفة رياضية تحسب النتيجة من قيمة أو قيم عديدة مدخلة.	H.235
تجفير مسلسل cryptographic chaining	أسلوب استخدام خوارزمية تجفير حيث يتوقف التحويل الذي تقوم به على قيم مدخلات أو مخرجات سابقة.	X.810
قيمة التجفير cryptographic checkvalue	معلومات مشتقة من أداء تحويل التجفير (انظر التجفير) في وحدة بيانات. *ملاحظة* – يمكن اشتقاق قيمة التجفير في خطوة أو أكثر وهو نتيجة لدالة رياضية بين المفتاح ووحدة بيانات. وتستخدم عادة للتحقق من سلامة وحدة بيانات.	X.800
نظام التجفير cryptographic system, cryptosystem	1. مجموعة تحويلات من نص عادي إلى نص مجفر والعكس بالعكس، وتقوم المفاتيح بانتقاء التحويل (التحويلات) اللازمة. وتُعرّف التحويلات عادة بواسطة خوارزمية رياضية.	X.509
	2. خوارزمية تحول بيانات مدخلة إلى شيء لا يمكن تمييزه (تجفير)، كما تُحول البيانات التي لا يمكن تمييزها إلى نسقها الأصلي (فك التجفير). ويرد وصف تقنيات التجفير RSA (ريفست وشامير وأدلمان) في X.509	Q.815
علم التجفير cryptography	التخصص الذي يجسد مبادئ ووسائل وطرائق تحويل البيانات من أجل إخفاء محتواها من المعلومات ومنع تعديلها خلسة و/أو منع استخدامها غير المرخص به. (*ملاحظة* – يحدد علم التجفير الطرائق المستخدمة في التجفير وفك التجفير. ويعتبر الهجوم على أي مبدأ أو وسيلة أو طريقة للتجفير بمثابة تحليل للتجفير).	X.800
سرية البيانات data confidentiality	تستخدم لتوفير حماية البيانات من إفشاء غير مرخص به. وتعتمد خدمة سرية البيانات على إطار الاستيقان. ويمكن أن تستخدم للحماية من اعتراض البيانات.	X.509
سلامة البيانات data integrity	ضمان عدم تغيير البيانات أو إتلافها بطريقة غير مرخص بها.	X.800
الاستيقان من أصل البيانات data origin authentication	1. التأكد من أن مصدر البيانات المتلقاة هو المصدر المزعوم.	X.800
	2. التأكد من هوية العنصر الرئيسي المسؤول عن وحدة بيانات محددة.	X.811

المصطلح	التعريف	المرجع
فك التشفير decipherment	عكس عملية تشفير قابلة لذلك.	X.800
فك التجفير decryption	انظر فك التشفير.	X.800
التفويض delegation	نقل امتياز من كيان يتمتع به إلى كيان آخر.	X.509
رفض الخدمة denial of service	منع نفاذ مرخص له إلى الموارد أو تأخير عمليات حرجة التوقيت.	X.800
إزالة التخليط descrambling	1. استعادة خصائص إشارة مرئية/صوتية/بيانات لإتاحة استقبال في نسق واضح. وهذا الاسترجاع عملية محددة تحت مراقبة نظام النفاذ المشروط (الطرف المستقبل). 2. عملية عكس وظيفة التخليط (انظر "التخليط") للتوصل إلى صور وخدمات صوتية وبيانات صالحة للاستعمال.	J.96 J.93
بصمة رقمية digital fingerprint	خاصية بند بيانات، مثل قيمة التجفير أو نتيجة أداء وظيفة فرم في اتجاه واحد على بيانات، يختص بها لدرجة كافية بحيث لا يمكن حسابياً العثور على بند بيانات آخر له نفس الخصائص.	X.810
التوقيع الرقمي digital signature	1. بيانات ملحقة أو تحويل مجفرٍ (انظر تجفير) لوحدة بيانات تسمح لمتلقي وحدة بيانات أن يبرهن على مصدر وسلامة وحدة البيانات وتحميها من التزوير، من جانب المتلقي مثلاً. 2. تحويل مجفّر لوحدة بيانات يسمح لمتلقي وحدة بيانات أن يبرهن على مصدر وسلامة وحدة البيانات ويحمي مرسل ومتلقي وحدة البيانات من التزوير من قبل أطراف ثالثة، ويحمي المرسل من التزوير من جانب المتلقي.	X.800 X.843
الهجوم المباشر direct attack	هجوم على نظام يستغل أوجه القصور في الخوارزميات أو المبادئ أو الخصائص التي تنطوي عليها آلية الأمن.	X.814
خدمة الدليل directory service	خدمة البحث عن معلومات واسترجاعها من كتالوج أغراض محددة جيداً يمكن أن يتضمن معلومات عن الشهادات وأرقام الهواتف وظروف النفاذ والعناوين وغيرها. مثال ذلك خدمة الدليل التي تمتثل للتوصية X.500.	X.843
تقنية التغليف المزدوج double enveloping technique	حماية إضافية يمكن توفيرها لرسالة كاملة، بما في ذلك معلمات الغلاف، من خلال القدرة على اعتبار محتوى الرسالة في حد ذاته رسالة كاملة، أي أن تقنية تغليف مزدوج متيسرة من خلال استعمال منطق نمط المحتوى الذي يجعل في الإمكان اعتبار محتوى رسالة بمثابة غلاف داخلي.	X.402
التنصت eavesdropping	انتهاك السرية بمراقبة الاتصال.	M.3016.0
المفتاح الإلكتروني electronic key	كناية عن إشارات البيانات التي تستخدم في التحكم في عملية إزالة التخليط في مفككات تشفير المشترك. *ملاحظة* – هناك على الأقل ثلاثة أنماط للمفاتيح الإلكترونية: المفاتيح المستخدمة لتدفقات إشارات التلفزيون، والمفاتيح المستخدمة لحماية عمليات نظام التحكم، والمفاتيح المستخدمة لتوزيع المفاتيح الإلكترونية على نظام الكبل.	J.93
التشفير encipherment	1. التحويل المجفر للبيانات (انظر علم التجفير) لإنتاج نص مجفر. *ملاحظة* – قد يكون التشفير غير قابل للعكس، وفي هذه الحالة لا يمكن إجراء عملية فك التشفير المقابلة. 2. التشفير (التجفير) عملية تجعل البيانات غير قابلة للقراءة من قبل كيانات غير مرخص لها بذلك، بواسطة تطبيق خوارزمية مجفرة. وفك التشفير (التجفير) عملية عكسية يتحول فيها نص مجفر إلى نص عادي.	X.800 H.235

المصطلح	التعريف	المرجع
التجفير encryption	1. طريقة لترجمة معلومات في نص عادي إلى نص مجفر. 2. عملية تخليط إشارات لمنع النفاذ غير المصرح له. (انظر أيضاً التشفير)	J.170 J.93
كيان طرف end entity	صاحب شهادة يستخدم مفتاحه الخاص لأغراض غير توقيع الشهادات أو كيان بمثابة طرف ترحيل.	X.509
تشفير من طرف إلى طرف end-to-end encipherment	تشفير البيانات ضمن نظام أو في طرف مصدره يقابله فك تشفير لا يحدث إلا ضمن نظام أو في طرف مقصده. (انظر أيضاً التشفير من وصلة إلى وصلة).	X.800
كيان entity	1. إنسان أو منظمة أو مكوّن حاسوب أو جزء من برمجية. 2. أي شيء ملموس أو مجرّد ذو أهمية. وإذا كانت كلمة كيان تستخدم بوجه عام للإشارة إلى أي شيء فإنها في سياق النمذجة تقتصر على الإشارة إلى أشياء في نطاق الموضوع الذي يجري نمذجته.	X.842 X.902
استيقان الكيان entity authentication	التأكد من هوية عنصر رئيسي في سياق علاقة اتصال. *ملاحظة* – لا يمكن استيقان هوية العنصر الرئيسي إلا عند تفعيل هذه الخدمة. ويمكن ضمان مواصلة الاستيقان بالطرائق الموصوفة في البند 7.2.5 في التوصية X.811.	X.811
مميز الحدث event discriminator	وظيفة توفّر تحليلاً أوليّاً لحدث متعلق بالأمن وتولّد، إذا كان ذلك ملائماً، تدقيقاً للأمن و/أو إنذاراً.	X.816
الإثبات evidence	معلومات يمكن أن تستخدم، إمّا في حد ذاتها أو بالاقتران مع معلومات أخرى، لتسوية نزاع. *ملاحظة* – من أشكال الإثبات التوقيعات الرقمية والأغلفة الآمنة وعلامات الأمن. وتستخدم التوقيعات الرقمية في تقنيات المفاتيح العمومية في حين تستخدم الأغلفة الآمنة وعلامات الأمن مع تقنيات المفاتيح السرية.	X.813
مولّد إثبات evidence generator	كيان يولّد إثبات عدم التنصل. *ملاحظة* – قد يكون هذا الكيان طالب خدمة عدم التنصل أو المرسل أو المتلقي أو أطراف متعددة تعمل معاً (موقّع ومشارك في التوقيع مثلاً).	X.813
التزوير forgery	كيان يصطنع معلومات ويدَّعي أن هذه المعلومات متلقاة من كيان آخر أو أرسلت إلى كيان آخر.	M.3016.0
وظيفة الفرم hash function	وظيفة (رياضية) تختصر مجموعة كبيرة (ربما كبيرة جداً) من القيم إلى مقدار صغير منها.	X.810
الإخفاء hide	عملية تطبق حماية السريّة على بيانات غير محمية أو توفّر حماية إضافية للسرية لبيانات محمية أصلاً.	X.814
سياسة أمن قائمة على الهوية identity-based security policy	سياسة أمن قائمة على الهويات و/أو نعوت المستعملين أو زمرة من المستعملين أو كيانات تعمل نيابة عن المستعملين والموارد/الأغراض التي يجري النفاذ إليهم أو إليها.	X.800
هجوم غير مباشر indirect attack	هجوم على نظام لا يقوم على أساس أوجه القصور في آلية أمن معينة (مثال ذلك هجمات تتجاوز الآلية أو هجمات تعتمد على النظام الذي يستخدم الآلية بطريقة غير صحيحة).	X.814
السلامة integrity	ضمان عدم تعديل البيانات بطريقة غير مرخص بها. (انظر أيضاً سلامة البيانات)	H.235

المصطلح	التعريف	المرجع
خدمة السلامة integrity service	توفّر وسيلة لضمان صحة البيانات المتبادلة وحمايتها من التعديل أو الحذف أو الإنشاء (الإدراج) أو التكرار. ويميز بين الأنواع التالية من خدمات السلامة: سلامة بحسب المجال، سلامة التوصيل دون استرجاع؛ سلامة التوصيل مع الاسترجاع.	M.3016.2
قناة محمية السلامة integrity-protected channel	قناة اتصالات طُبقت عليها خدمة السلامة. (انظر سلامة التوصيل والسلامة عديمة التوصيل).	X.815
بيانات محمية السلامة integrity-protected data	البيانات وجميع النعوت ذات الصلة بها في بيئة محمية السلامة.	X.815
بيئة محمية السلامة integrity-protected environment	بيئة تمنع فيها تغييرات البيانات غير المرخص بها (بما في ذلك الإنشاء والحذف) أو يمكن كشف هذه التغييرات.	X.815
تهديدات مقصودة intentional threats	تهديدات تتراوح بين الفحص العابر باستعمال أدوات رصد متيسرة والهجمات المتطورة باستخدام المعارف الخاصة بالنظام. ويمكن اعتبار التهديد المقصود، إذا تحقّق، بمثابة "هجوم".	X.800
مقاومة الاقتحام intrusion resistance	قدرة مكونة حاسوب على رفض النفاذ المادي أو الكهربائي أو الإشعاعي لأطراف غير مرخص لها بذلك إلى عنصر وظيفي داخلي.	J.93
الاتصالات باستخدام بروتوكول الإنترنت IPCablecom	مشروع لقطاع تقييس الاتصالات في الاتحاد يتضمن معمارية وسلسلة توصيات تمكّن من تقديم الخدمات في الوقت الفعلي على شبكات التلفزيون الكبلي باستخدام مودمات كبلية.	J.160
Kerberos	بروتوكول استيقان شبكة مفاتيح سرية يستخدم طائفة من الخوارزميات للتجفير وقاعدة بيانات مركزية للاستيقان.	J.170
مفتاح key	1. متوالية رموز تتحكم في عمليات التجفير وفك التجفير. 2. قيمة رياضية مدخلة في خوارزمية تجفير مختارة.	X.800 J.170
خدمة توزيع المفاتيح key distribution service	خدمة توزيع المفاتيح بصورة آمنة على كيانات مرخص لها يقوم بها مركز لتوزيع المفاتيح وهي موصوفة في المعيار ISO/IEC 11770-1.	X.843
بدالة مفاتيح key exchange	تبادل مفاتيح عمومية بين كيانات لكي تُستخدم لتجفير الاتصال بين الكيانات.	J.170
إدارة مفاتيح key management	توليد المفاتيح وتخزينها وتوزيعها وإلغائها وأرشفتها وتطبيقها طبقاً لسياسة الأمن.	X.800
تسرب المعلومات leakage of information	عندما يحصل على المعلومات طرف غير مرخص له بذلك من خلال مراقبة عمليات الإرسال أو عن طريق نفاذ غير مرخص به إلى المعلومات المخزونة في أي كيان لنظام مناولة الرسائل (MHS)، أو عن طريق التنكر الذي قد ينجم عن انتحال شخصية أخرى أو إساءة استخدام خدمة نقل الرسائل (MTS) أو من خلال التسبب في تشغيل مكيّف مطراف وسائط (MTA) تشغيلاً خاطئاً. وتشمل تهديدات تسرب المعلومات ما يلي: فقدان السرية؛ فقدان غفل الهوية، اختلاس الرسائل، تحليل الحركة.	X.402
التشفير وصلة وصلة link-by-link encipherment	تطبيق التشفير على البيانات إفرادياً في كل وصلة في نظام الاتصالات. (انظر أيضاً التشفير من طرف إلى طرف). *ملاحظة* – يعني التشفير وصلة وصلة أن البيانات ستكون في شكل نص واضح في كيانات ترحيل.	X.800

المصطلح	التعريف	المرجع
ضياع أو إتلاف المعلومات **loss or corruption of information**	تعرّض سلامة البيانات المنقولة للخطر بفعل الحذف أو الإدراج أو التعديل أو إعادة التركيب أو التكرار أو التأخير غير المرخص بها.	M.3016.0
كشف التلاعب **manipulation detection**	آلية لكشف ما إذا كانت البيانات قد تم تعديلها (سواء عرضاً أو عمداً).	X.800
التنكر masquerade	إدعاء كيان بأنه كيان آخر.	X.800
شفرة استيقان الرسالة **message authentication code (MAC)**	قيمة تحقق تجفيري تستخدم في توفير استيقان مصدر البيانات وسلامة البيانات.	X.813
استيقان أصل الرسالة **message origin authentication**	تمكّن المتلقي، أو أي مكيف مطراف وسائط تمر فيه الرسالة، من استيقان هوية مرسل الرسالة.	X.400
سلامة تتابع الرسائل **message sequence integrity**	1. تتيح للمرسل أن يقدّم للمرسل إليه الدليل على المحافظة على تتابع الرسائل. 2. يتيح عنصر الخدمة هذا لمرسل الرسالة أن يزود متلقي الرسالة بوسيلة تمكّنه من التحقق من المحافظة على تتابع الرسائل من المرسل إلى المرسل إليه (دون فقدان الرسائل أو إعادة ترتيبها أو تكرارها). وتكون سلامة التتابع على أساس كل مرسل إليه كما يمكن أن تستخدم تقنية تجفير لا تناظري أو تقنية تجفير تناظري.	X.400
تتابع الرسائل **message sequencing**	عندما يكرر جزء من رسالة أو تكرر الرسالة بأكملها، أو تُزحزح زمنياً أو يُعاد ترتيبها، مثلاً للاستفادة من معلومات الاستيقان في رسالة صحيحة وإعادة تتابع رسائل صحيحة أو زحزحتها زمنياً. وإذا كان من المستحيل منع التكرار في خدمات أمن نظام مناولة الرسائل، فإنه يمكن كشف آثار التهديد واستبعادها. ويشمل تتابع الرسائل: تكرار الرسائل؛ إعادة ترتيب الرسائل؛ الاستعراض المسبّق للرسائل؛ تأخير الرسائل.	X.402
دور المراقبة monitoring role	الدور الذي يؤديه طرف ثالث موثوق به في مراقبة الإجراء أو الحدث وفي تقديم دليل عمّا تمت مراقبته.	X.813
الاستيقان المتبادل **mutual authentication**	التأكد من هويتي العنصرين الرئيسيين.	X.811
عدم التنصل non-repudiation	1. المقدرة على منع المرسل من أن ينكر فيما بعد أنه أرسل رسالة أو قام بإجراء ما. 2. الحماية من إنكار أحد الكيانات المشاركة في اتصال أنه شارك في الاتصال بأكمله أو في جزء منه. 3. عملية لا يستطيع بموجبها مرسل رسالة (طلب رؤية على أساس الدفع مثلاً) أن ينكر أنه أرسل رسالة.	J.170 H.235 J.93
التوثيق notarization	تسجيل البيانات لدى طرف ثالث موثوق به يسمح لاحقاً بتأكيد دقة خصائص البيانات من حيث المحتوى والأصل والوقت والتسليم مثلاً.	X.800
الموثق notary	طرف ثالث موثوق به تُسجَّل لديه البيانات بحيث يمكن لاحقاً تأكيد دقّة خصائص البيانات.	X.813
تهديد سلبي passive threat	تهديد بإفشاء غير مرخص به لمعلومات دون تغيير في حالة النظام.	X.800

المصطلح	التعريف	المرجع
كلمة السر password	1. معلومات الاستيقان السرية وتتألف عادة من سلسلة سمات. 2. سلسلة سمات يدخلها المستعمل: هي بمثابة مفتاح الأمن المخصص الذي يتقاسمه المستعمل المتنقل مع الميدان الأصل. وينبغي استخدام كلمة سر المستعمل هذه والسر المشتق الذي يتقاسمه المستعمل لغرض استيقان المستعمل.	X.800 H.530
استيقان الكيان الند peer-entity authentication	1. التأكيد بأن الكيان الند في رابطة ما هو الكيان المزعوم. 2. إقامة الدليل على هوية الكيان الند أثناء علاقة اتصال.	X.800 M.3016.0
بيئة الأمن الشخصي personal security environment (PSE)	تخزين محلي آمن لمفتاح خاص لكيان ما ومفتاح سلطة إصدار الشهادات الموثوق بها مباشرة وربما بيانات أخرى. وتبعاً لسياسة أمن الكيان أو متطلبات النظام يمكن أن يكون مثلاً: ملف محمي تجفيرياً أو علامة في حاسوب مقاومة للتلاعب.	X.843
أمن مادي physical security	تدابير مستخدمة لتوفير حماية مادية لموارد من تهديدات متعمدة أو عارضة.	X.800
العنصر، الطرف، الجهة principal	كيان يمكن استيقان هويته.	X.811
الخصوصية privacy	1. حق الأفراد في التحكم أو التأثير فيما يتناول المعلومات التي تتعلق بهم من حيث جمعها وتخزينها ومن يقوم بذلك ولمن يجوز إفشاء هذه المعلومات. *ملاحظة* – بما أن هذا المصطلح يتعلق بحق الأفراد فإنه لا يمكن أن يكون دقيقاً جداً وينبغي تجنب استخدامه إلا كدافع لاشتراط الأمن. 2. أسلوب اتصالات حيث لا يمكن تفسير الاتصال إلا من جانب الأطراف المخولة ذلك صراحة. ويتحقق هذا عموماً من خلال التجفير وتقاسم مفتاح (مفاتيح) التجفير.	X.800 H.235
مفتاح خاص؛ مفتاح سري (لا ينصح باستعماله) private key; secret key (deprecated)	1. (في نظام تجفير مفتاح عمومي) هو ذلك المفتاح من زوج المفاتيح لدى مستعمل ما معروف لديه فقط. 2. مفتاح يستخدم مع خوارزمية تجفير لا تناظرية وحيازته مقيدة (تقتصر عادة على كيان واحد فقط). 3. المفتاح المستخدم في تجفير المفتاح العمومي الذي يخص كياناً منفرداً وينبغي أن يظل سرّاً.	X.509 X.810 J.170
امتياز privilege	نعت أو خاصية منسوبة إلى كيان من قبل سلطة.	X.509
بنية تحتية لإدارة الامتيازات Privilege Management Infrastructure (PMI)	البنية التحتية القادرة على دعم إدارة الامتيازات لدعم خدمة ترخيص شاملة ذات علاقة مع بنية تحتية لمفاتيح عمومية.	X.509
مفتاح عمومي public key	1. (في نظام تجفير مفتاح عمومي) هو ذلك المفتاح من زوج المفاتيح لدى مستعمل ما معروف عموماً. 2. مفتاح يستخدم مع خوارزمية تجفير لا تناظرية ويمكن إتاحته عموماً 3. المفتاح المستخدم في تجفير المفتاح العمومي الذي يخص كياناً فردياً ويوزع عموماً. وتستخدم كيانات أخرى هذا المفتاح لتجفير بيانات ترسل إلى صاحب المفتاح.	X.509 X.810 J.170

المصطلح	التعريف	المرجع
شهادة مفتاح عمومي **public key certificate**	1. المفتاح العمومي للمستعمل، مع بعض المعلومات الأخرى، جُعل منيعاً للتزوير بواسطة التجفير مع المفتاح الخاص لدى سلطة إصدار الشهادات التي أصدرته. 2. قيم تمثل مفتاحاً عمومياً لدى صاحبه (ومعلومات اختيارية أخرى) تحققت منه ووقعته سلطة موثوق بها في نسق لا يمكن تزويره. 3. ارتباط بين مفتاح عمومي لكيان ما ونعت أو أكثر يتعلق بهويته، ويعرف أيضاً بالشهادة الرقمية.	X.509 H.235 J.170
تجفير مفتاح عمومي **Public Key Cryptography**	تقنية تجفير قائمة على خوارزمية ذات مفتاحين، خاص وعمومي، حيث تجفّر الرسالة بالمفتاح العمومي ولكن لا يمكن فك تجفيرها إلا بالمفتاح الخاص. ويُعرف أيضاً باسم نظام المفتاح الخاص-العمومي. *ملاحظة* – معرفة المفتاح العمومي لا تؤدي إلى معرفة المفتاح الخاص. مثال: يستنبط الطرف A زوجاً من المفاتيح ويرسل المفتاح العمومي علناً إلى جميع من يرغبون في الاتصال بالطرف A، لكنه يحتفظ بالمفتاح الخاص سرّاً. وبينما يمكن لأي شخص يحوز المفتاح العمومي أن يُجفّر رسالة للطرف A فإن الطرف A فقط هو الذي يمكنه فك تجفير الرسائل بالمفتاح الخاص.	J.93
البنية التحتية للمفاتيح العمومية **Public Key Infrastructure (PKI)**	البنية التحتية القادرة على دعم إدارة مفاتيح عمومية قادرة على دعم خدمات الاستيقان والتجفير وسلامة البيانات وعدم التنصل.	X.509
سلطة التسجيل **Registration Authority (RA)**	1. كيان مسؤول عن تعرّف هوية مواضيع الشهادات واستيقانها، لكنه ليس سلطة إصدار شهادات أو سلطة نعوت ومن ثم فإنه لا يوقّع أو يصدر شهادات. *ملاحظة* – يمكن لسلطة التسجيل أن تساعد في عملية إصدار الشهادة أو عملية إبطالها أو كلتيهما. 2. سلطة مخوّلة وموثوق بها لأداء خدمة التسجيل.	X.842 X.843
الهجوم بالترحيل relay attack	هجوم على الاستيقان يتم فيه اعتراض تبادل معلومات التوثيق ثم إحالتها فوراً.	X.811
الطرف المعتمِد relying party	مستعمل أو وكيل يعتمد على البيانات الواردة في شهادة عند اتخاذ قراراته.	X.509
التكرار replay	تكرار رسالة أو جزء من رسالة لإنتاج أثر غير مرخص به. على سبيل المثال يمكن تكرار رسالة صحيحة تتضمن معلومات الاستيقان من قبل كيان آخر بغية استيقان ذاته (باعتباره غير ما هو حقا).	X.800
الإنكار repudiation	1. إنكار أحد الكيانات المشاركة في اتصال ما أنها شاركت في الاتصال بأكمله أو في جزء منه. 2. كيان مشارك في تبادل اتصال ما ثم ينكر ذلك فيما بعد. 3. (في حالة نظام مناولة الرسائل) عندما ينكر مستعمل خدمة نقل الرسائل أو خدمة نقل الرسائل بالذات لاحقاً تقديم أو تلقي أو إرسال رسالة ويشمل ذلك: إنكار المصدر، إنكار التقديم، إنكار التسليم.	X.800 M.3016.0 X.402
الإفشاء reveal	عملية تُزيل بعض وسائل حماية السرية المطبقة سابقاً أو كلها.	X.814
شهادة الإبطال **revocation certificate**	شهادة أمن تصدرها سلطة الأمن لبيان أن شهادة أمن معينة قد أبطلت.	X.810
شهادة قائمة الإبطال **revocation list certificate**	شهادة أمن بقائمة شهادات أمن قد أبطلت.	X.810

المصطلح	التعريف	المرجع
التحكم في التسيير **routing control**	تطبيق القواعد أثناء عملية التسيير بحيث يمكن انتقاء أو تجنب شبكات أو وصلات أو مرحّلات معينة.	X 800
سياسة أمن قائمة على القواعد **rule-based security policy**	سياسة أمن قائمة على قواعد شاملة تفرض على جميع المستعملين. وتعتمد هذه القواعد عادة على مقارنة حساسية الموارد التي يجري النفاذ إليها وتوفر النعوت المقابلة لدى مستعملين أو مجموعة مستعملين أو كيانات تعمل نيابة عن مستعملين.	X.800
الختم seal	قيمة تحقق تجفيري تدعم سلامة البيانات ولكنها لا تحمي من التزوير من جانب المتلقي (أي لا توفر عدم التنصل). وعندما يقترن الختم مع عنصر بيانات يقال عن الأخير إنه *مختوم*. *ملاحظة* – بالرغم من أن الختم في حد ذاته لا يوفر عدم التنصل، فإن بعض آليات عدم التنصل تستفيد من خدمة سلامة البيانات التي توفرها الأختام، لحماية الاتصالات مع أطراف ثالثة موثوق بها مثلاً.	X.810
مفتاح سري secret key	مفتاح يستخدم في خوارزمية تجفير لا تناظرية. وامتلاك مفتاح سري مقصور (على كيانين عادة).	X.810
الأمن security	يستخدم مصطلح *"الأمن"* بمعنى التقليل إلى أدنى حد من مواطن ضعف الأصول والموارد. والأصل هو أي شيء له قيمة. *وموطن الضعف* هو أي نقطة يمكن أن تُستغل لانتهاك نظام ما أو المعلومات التي يتضمنها. *والتهديد* انتهاك محتمل للأمن.	X.800
مدير الأمن **security administrator**	شخص مسؤول عن تعريف أو إنفاذ جزء أو أكثر من سياسة الأمن.	X.810
إنذار الأمن security alarm	رسالة تتولد عندما يكشف عن حدث متصل بالأمن معرّف في سياسة الأمن على أنه حالة إنذار. والقصد من إنذار الأمن أن يحظى باهتمام كيانات معينة في الوقت المناسب.	X.816
رابطة الأمن **security association**	علاقة بين كيانين أو أكثر لها نعوت (معلومات حالة وقواعد) لتنظيم توفير خدمات الأمن المتعلقة بهذه الكيانات. العلاقة بين كيانات اتصال الطبقة السفلى التي لها نعوت ترابط أمن مقابلة.	X.803 X.802
تدقيق الأمن security audit	استعراض وفحص مستقلين لسجلات وأنشطة نظام ما من أجل اختبار كفاءة ضوابط النظام لضمان الامتثال للسياسة القائمة والإجراءات التشغيلية ولكشف انتهاكات الأمن والتوصية بأي تغييرات يشار بها في مجالات التحكم والسياسة والإجراءات.	X.800
سجل تدقيق الأمن **security audit trail**	بيانات مجمعة قد تُستخدم لتيسير تدقيق الأمن.	X.800
مدقق الأمن security auditor	فرد أو عملية يمكنها النفاذ إلى سجلات تدقيق الأمن وإعداد تقارير عن التدقيق.	X.816
سلطة الأمن security authority	1. كيان مسؤول عن تعريف أو تنفيذ أو إنفاذ سياسة الأمن. 2. الكيان المسؤول عن إدارة سياسة الأمن ضمن ميدان أمني. 3. المدير المسؤول عن تنفيذ سياسة الأمن.	X.810 X.841 X.903
شهادة الأمن **security certificate**	مجموعة بيانات متعلقة بالأمن تصدرها سلطة أمنية أو طرف ثالث موثوق به مع معلومات أمن تستخدم لتوفير سلامة البيانات وخدمات الاستيقان من أصل البيانات. *ملاحظة* – تعتبر جميع الشهادات شهادات أمن. واعتمد مصطلح شهادة الأمن في السلسلة X.800 لتجنب تضارب المصطلحات مع التوصية X.509.	X.810

المصطلح	التعريف	المرجع
ميدان الأمن security domain	1. مجموعة من المستعملين والأنظمة تخضع لسياسة أمن مشتركة. 2. مجموعة الموارد التي تخضع لسياسة أمنية واحدة.	X.841 X.411
تبادل الأمن security exchange	تحويل أو سلسلة تحويلات لمعلومات التحكم في بروتوكول التطبيق بين أنظمة مفتوحة كجزء من تشغيل آلية أمن أو أكثر.	X.803
معلومات الأمن security information (SI)	المعلومات اللازمة لتنفيذ خدمات الأمن.	X.810
وسم الأمن security label	توسيم مرتبط بمورد (قد يكون وحدة بيانات) يسمي أو يحدد نعوت الأمن لذلك المورد.	X.800
إدارة الأمن security management	تتألف إدارة الأمن من جميع الأنشطة اللازمة لإنشاء جوانب أمن نظام ما والمحافظة عليها وإنهائها. ومن المواضيع التي تشملها: إدارة خدمات الأمن؛ إنشاء آليات الأمن؛ إدارة المفاتيح (جزء الإدارة)؛ تحديد الهويات، والمفاتيح، ومعلومات التحكم في النفاذ وغيرها؛ إدارة سجل تدقيق الأمن وإنذارات الأمن.	M.3016.0
نموذج الأمن security model	إطارٌ لوصف خدمات الأمن التي تصد التهديدات المحتملة في خدمة نقل الرسائل وكذلك عناصر الأمن التي تدعم تلك الخدمات.	X.402
سياسة الأمن security policy	1. مجموعة القواعد التي تضعها سلطة الأمن والتي تحكم استخدام وتوفير خدمات وتسهيلات الأمن. 2. مجموعة معايير لتوفير خدمات الأمن. *ملاحظة* – انظر سياسة الأمن القائمة على الهوية والقائمة على القواعد. تتناول سياسة الأمن الكاملة بالضرورة شواغل كثيرة تقع خارج نطاق التوصيل البيني للأنظمة المفتوحة.	X.509 X.800
قواعد الأمن security rules	معلومات محلية تُحدِّد، في ضوء الخدمات الأمنية المختارة، آليات الأمن الأساسية التي يتعين استخدامها، بما في ذلك جميع المعلمات اللازمة لتشغيل الآلية. *ملاحظة* – قواعد الأمن هي شكل من قواعد التفاعل الآمن على النحو المحدد في نموذج أمن الطبقات العليا.	X.802
خدمة الأمن security service	خدمة توفرها طبقة في أنظمة الاتصالات المفتوحة تضمن الأمن الكافي للأنظمة أو لنقل البيانات.	X.800
حالة الأمن security state	معلومات عن الحالة في نظام ما مفتوح تكون مطلوبة لتوفير خدمات الأمن.	X.803
علامة الأمن security token	مجموعة بيانات تحميها خدمة أمن أو أكثر، مع معلومات أمن تستخدم في توفير خدمات الأمن، تُنقل بين كيانات الاتصالات.	X.810
تحويل الأمن security transformation	مجموعة من الوظائف (وظائف أمن الأنظمة ووظائف اتصالات الأمن) تتناول مجتمعة بنود بيانات للمستعمل لحماية هذه البنود بطريقة معينة أثناء اتصال أو تخزين.	X.803
حماية مجالات انتقائية selective field protection	حماية مجالات محددة في رسالة يتعين إرسالها.	X.800
الحساسية sensitivity	خاصية مورد تدل على قيمته أو أهميته.	X.509
سر متقاسم shared secret	مفتاح الأمن لخوارزميات تجفير؛ قد يكون مشتقاً من كلمة السر.	H.530
التدريع shield	تحويل البيانات إلى بيانات محمية السلامة.	X.815
التوقيع signature	انظر التوقيع الرقمي.	X.800

المصطلح	التعريف	المرجع
الاستيقان البسيط simple authentication	الاستيقان بواسطة ترتيبات كلمة سر بسيطة.	X.509
مصدر السلطة Source of Authority (SOA)	سلطة نعوت يثق بها متحقق الامتياز لمورد معين باعتبارها السلطة النهائية لتخصيص مجموعة من الامتيازات.	X.509
الرسائل الاقتحامية spamming	هجوم يسفر عن رفض الخدمة عند إرسال فيض من البيانات غير المرخص بها إلى نظام ما. والوسائط الاقتحامية حالة خاصة حيث ترسل رزم بروتوكول الوقت الفعلي على بوابات بروتوكول بيانات المستعمل. وما يحدث هو أن النظام يُغمر بالرزم التي تستهلك معالجتها موارد ثمينة في النظام.	H.235
الاستيقان القوي strong authentication	الاستيقان بواسطة شهادات مشتقة بالتجفير.	X.509
طريقة الاستيقان التناظرية symmetric authentication method	طريقة للاستيقان يتقاسم فيها كلا الكيانين معلومات استيقان مشتركة.	X.811
خوارزمية تجفير تناظرية symmetric cryptographic algorithm	خوارزمية للتجفير أو خوارزمية مقابلة لفك التجفير تتطلب نفس المفتاح لكل من التجفير وفك التجفير.	X.810
التهديد threat	احتمال انتهاك الأمن.	X.800
خدمة تسجيل الوقت time stamping service	خدمة تشهد على وجود بيانات إلكترونية في لحظة محددة من الوقت. *ملاحظة* – خدمات تسجيل الوقت مفيدة وربما لا غنى عنها لدعم التثبت من صلاحية التوقيعات لفترة طويلة.	X.842
تحليل الحركة traffic analysis	استدلال المعلومات من ملاحظة تدفقات الحركة (وجودها وغيابها وكميتها واتجاهها وتواترها).	X.800
سرية تدفق الحركة traffic flow confidentiality	خدمة سرية لحماية الحركة من التحليل، أي خدمة أمنية لحماية المعلومات التي يمكن أن تُستنتج من مراقبة تدفقات الحركة.	X.800
تبطين الحركة traffic padding	توليد حالات مزيفة من الاتصالات ووحدات بيانات مزيفة و/أو بيانات مزيفة في وحدات البيانات.	X.800
باب التسلل trapdoor	نتيجة عملٍ يُغير فيه أحد كيانات نظام ما للسماح لمهاجم بإحداث تأثير غير مرخص به في إصدار أمر أو في حدث أو سلسلة أحداث محدّدة مسبقاً. إذ يمكن مثلاً تعديل عملية إثبات صلاحية كلمة سر بحيث يمكن، بالإضافة إلى أثرها العادي، أن تُقر أيضاً صلاحية كلمة سر مهاجم.	X.800
"حصان طروادة" Trojan horse	عندما يدخل "حصان طروادة" إلى النظام يكون له وظيفة غير مرخص بها بالإضافة إلى وظيفته المرخص بها. والترحيل الذي ينسخ أيضاً رسائل إلى قناة غير مرخص لها يقوم بدور "حصان طروادة".	X.800
الثقة trust	يقال إن الكيان X يثق في الكيان Y للقيام بمجموعة أنشطة فقط في حالة ما إذا اطمأن الكيان X إلى أن الكيان Y سوف يتصرف بأسلوب معين فيما يتعلق بالأنشطة.	X.810
كيان موثوق به trusted entity	كيان يمكنه أن ينتهك سياسة الأمن، إما بالقيام بأعمال لا يفترض أن يقوم بها أو بعدم القيام بأعمال من المفترض أن يقوم بها.	X.810

المصطلح	التعريف	المرجع
عنصر وظيفي موثوق به **trusted functionality**	عنصر وظيفي يبدو صحيحاً فيما يتعلق ببعض المعايير، كما وردت في سياسة الأمن مثلاً.	X.800
طرف ثالث موثوق به **trusted third party (TTP)**	سلطة أمن أو وكيلها الموثوق به (من كيانات أخرى) فيما يتعلق ببعض الأنشطة المتعلقة بالأمن (في سياق سياسة الأمن).	X.810
النفاذ غير المرخص به **unauthorized access**	كيان يحاول النفاذ إلى بيانات منتهكاً سياسة الأمن النافذة.	M.3016.0
إزالة التدريع unshield	تحويل البيانات محمية السلامة إلى البيانات التي كانت أصلاً قبل تدريعها.	X.815
استيقان المستعمل **user authentication**	إقامة الدليل على هوية المستعمل أو عملية التطبيق.	M.3016.0
التثبت من الصلاحية validate	فحص البيانات محمية السلامة لتحرّي أي فقدان في السلامة.	X.815
المتحقق verifier	الكيان الذي يتطلب هوية مستيقنة أو يمثّل هذا الكيان. ويشمل المتحقق الوظائف اللازمة للشروع في عمليات تبادل الاستيقان.	X.811
موطن الضعف vulnerability	أي نقطة يمكن استغلالها لانتهاك نظام ما أو المعلومات التي يحتوي عليها.	X.800
شهادة X.509 **X.509 certificate**	مواصفة شهادة مفتاح عمومي أُعدت كجزء من دليل معايير التوصية ITU-T X.500.	J.170

باء.2 المختصرات المتعلقة بالأمن

المختصر	التعريف
AA	[X.509] سلطة نعوت
ACI	[SANCHO] معلومات التحكم في النفاذ
AE	[M.3010] كيان تطبيق
AES	[H.235] [J.170] خوارزمية معيارية للتجفير المتطور
APS	[SANCHO] تبديل وقائي أوتوماتي
ASN.1	[H.680] ترميز تركيب مجرد رقم واحد
ASON	[SANCHO] شبكة بصرية تبديلية أوتوماتية
ASP	[X.805] [X.1121] مزود خدمة التطبيق
CA	[H.234] [H.235] [J.170] [X.509] سلطة إصدار شهادات. منظمة موثوق بها تقبل طلبات لإصدار الشهادات من كيانات وتقوم بالاستيقان من الطلبات وإصدار الشهادات وتحتفظ بحالة المعلومات عن الشهادات. [J.170] وكيل نداء. جزء من تركيب رسالة مجفرة يحتفظ بحالة الاتصالات ويتحكم في جانب الخط من الاتصالات.
CME	[X.790] كيان إدارة مطابق
CMIP	[M.3010] بروتوكول معلومات إدارة مشتركة
CMS	[J.170] تركيب رسالة مجفرة. [J.170] مخدم إدارة نداء يتحكم في التوصيلات السمعية. ويسمى أيضاً وكيل نداء في مصطلحات بروتوكول التحكم في بوابة الوسائط وبرتوكول التحكم في بوابة التشفير (وهذا مثال على مخدم التطبيقات).
CORBA	[SANCHO] معمارية وسيط لطلب غرض مشترك
COS	[SANCHO] صنف الخدمة
CP	سياسة الشهادة
CPS	[SANCHO: X.842] بيان ممارسة إصدار الشهادات [SANCHO: Q.817] بيان سياسة الشهادات
CRL	[H.235] [X.509] قائمة إبطال الشهادات
DCN	[SANCHO] شبكة اتصالات البيانات
DES	[SANCHO] معيار تجفير البيانات، معيار تجفير رقمي
DHCP	[SANCHO] بروتوكول تشكيل مضيف دينامي
DOCSIS	[SANCHO] مواصفات سطح بيني لخدمة البيانات عبر الكبل
DSA	[X.509] وكيل نظام الدليل [SANCHO] خوارزمية توقيع رقمي
DSL	[SANCHO] عروة مشترك رقمية
DSP	[SANCHO] معالج إشارة رقمية [SANCHO] بروتوكول خدمة الدليل
FDS	[SANCHO] نظام اكتشاف الاحتيال
FEAL	[T.36] خوارزمية تجفير البيانات السريعة أسرة من الخوارزميات التي تقابل 64 نصاً عادياً إزاء قدرات نص مجفر له 64 بتة بموجب مفتاح سري له 64 بتة. وهي تشبه معيار تجفير البيانات ولكنها أسهل جداً من حيث وظيفة f. وصممت من أجل السرعة والبساطة مما يجعلها مناسبة لمعالجات صغرية أقل تعقيداً (كالبطاقات الذكية مثلاً). في (A. Menezes et al., Handbook of Applied Cryptography, CRC Press, 1997)
FIGS	[M.3210.1] نظام جمع معلومات عن الاحتيال

المختصر	التعريف
GK	[H.235] [H.510] [H.530] حارس بوابة
GW	[H.235] بوابة
HFC	[SANCHO] كبل هجين ليفي متحد المحور
HFX	[T.30] [T.36] تجفير فاكس هوثورن
HKM	[T.30] [T.36] خوارزمية إدارة مفاتيح هوثورن
ICN	شبكة معلومات واتصالات
ICT	تكنولوجيا المعلومات والاتصالات
ID	[H.235] معرّف
IDEA	[T.36] الخوارزمية الدولية لتجفير البيانات هي خوارزمية تجفير وضعها Xuejia Lai وJames Massey في عام 1992 وتستخدم تجفير فدرة بواسطة مفتاح من 128 بتة (فدرات من 64 بتة بمفتاح من 128 بتة) وتُعتبر عموماً آمنة جداً. كما تُعتبر من بين أفضل الخوارزميات المعروفة. وطوال السنوات العديدة التي استخدمت فيها لم تنشر أي هجمات عملية عليها بالرغم من محاولة العثور على بعض هذه الهجمات (http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci213675,00.html)
IKE	[J.170] بدالة مفاتيح الإنترنت هي آلية إدارة مفاتيح تستخدم للتفاوض واشتقاق المفاتيح المرتبطة بالأمن في أمن بروتوكول الإنترنت
IKE–	[J.170] ترميز محدد للإشارة إلى استخدام بدالة مفاتيح الإنترنت على أساس مفاتيح مسبقة التقاسم من أجل الاستيقان
IKE+	[J.170] ترميز محدد للإشارة إلى بدالة مفاتيح الإنترنت التي تحتاج إلى شهادات مفاتيح عمومية
IMT-2000	[M.3210.1] الاتصالات المتنقلة الدولية 2000
IP	[X.805] بروتوكول الإنترنت
IPSec	[H.235] [H.530] [J.170] [X.805] أمن بروتوكول الإنترنت
IVR	[J.170] نظام تفاعلي لاستجابة صوتية
LAN	[M.3010] شبكة منطقة محلية
LDAP	[H.235] بروتوكول نفاذ سريع إلى الدليل
LLA	[M.3010] معمارية منطقية الطبقات
MAC	[H.235] [J.170] شفرة الاستيقان من الرسائل. بند بيانات ثابت الطول يرسل مع رسالة لضمان سلامة البيانات، وتعرف أيضاً باسم شفرة سلامة الرسالة. [J.170] التحكم في نفاذ الوسائط. وهو طبقة فرعية في طبقة وصلة بيانات. ويجري عادة فوق الطبقة المادية مباشرة
MCU	[H.235] وحدة توزيع متعدد [H.323] وحدة تحكم متعددة النقاط
MD5	[H.235] [J.170] ملخص الرسالة رقم 5
MG	[J.170] بوابة وسائط
MGC	[J.170] مراقب بوابة وسائط
MGCP	[J.170] بروتوكول التحكم في بوابة الوسائط
MIB	[J.170] [M.3010] قاعدة معلومات الإدارة
MIS	[M.3010] نظام معلومات الإدارة
MS	[M.3210.1] نظام إدارة مخزن رسائل قسم تعدد الإرسال
MSP	[SANCHO] حماية قسم تعدد الإرسال

المختصر	التعريف
MS-SPRing	حلقة الحماية المتقاسمة لقسم تعدد الإرسال
MTA	[J.170] مكيف مطراف الوسائط مكيف مطراف متعدد الوسائط وكيل نقل الرسائل
NAT	[H.235] ترجمة عناوين الشبكة
OAM&P	[SANCHO] العمليات والإدارة والصيانة وتوفير الخدمات
OS	[M.3010] [X.790] نظام العمليات
OSF	[M.3010] وظيفة أنظمة العمليات
OSI	[SANCHO] توصيل بيني للأنظمة المفتوحة
OSS	[J.170] نظام دعم العمليات. برمجيات المكتب الخلفي المستخدمة للتشكيل والأداء والأعطال والمحاسبة وإدارة الأمن.
PDA	مساعد بيانات شخصي
PKI	[H.235] [H.530] [X.509] [J.170] بنية تحتية للمفاتيح العمومية. وهي عملية إصدار شهادات المفاتيح العمومية تشمل المعايير وسلطات إصدار الشهادات والاتصالات بين السلطات والبروتوكولات لإدارة عمليات إصدار الشهادات.
PKINIT	[J.160] استيقان أولي من تجفير المفاتيح العمومية [J.191] تجفير المفاتيح العمومية من أجل الاستيقان الأولي
PMI	[X.509] البنية التحتية لإدارة الامتيازات
QoS	[SANCHO] نوعية الخدمة
RA	سلطة التسجيل
RADIUS	[J.170] خدمة الاستيقان عن بعد لمستعمل المراقمة
RAS	[SANCHO] التسجيل والقبول والحالة [SANCHO] بروتوكول التسجيل والقبول والحالة
RBAC	[X.509] التحكم في النفاذ على أساس الأدوار
RKS	[J.170] مخدم حفظ السجلات. جهاز يجمع مختلف رسائل الأحداث ويربط بينها.
RSA	[H.235] [T.30] [T.36] ريفست وشامير وأدلمان (خوارزمية المفاتيح العمومية)
RTP	[H.225.0] [H.235] [J.170] بروتوكول الوقت الفعلي
SHA1	[H.235] خوارزمية الفرم الآمن رقم 1
SG	بوابة التشوير
SIP	[J.170] [X.805] بروتوكول استهلال الجلسة. بروتوكول (تشوير) تحكم في طبقة التطبيق من أجل استهلال وتعديل وإنهاء جلسة مع مشارك أو أكثر.
SNC	[SANCHO] توصيل شبكة فرعية
SNMP	[J.170] [X.805] بروتوكول بسيط لإدارة الشبكة
SoA	[X.509] مصدر السلطة
SRTP	[H.235] بروتوكول النقل الآمن في الوقت الفعلي
SS7	[J.170] [X.805] نظام التشوير رقم 7 هو معمارية ومجموعة من البروتوكولات لأداء تشوير نداء خارج النطاق في شبكة هاتف
SSL	[H.235] [X.805] طبقة مقبس آمن
TFTP	[SANCHO] بروتوكول نقل الملفات المبسّط

المختصر	التعريف
TGS	[J.160] مخدم إصدار البطاقات
TLS	[H.235] أمن مستوى النقل
TMN	[M.3010] [M.3210.1] [X.790] شبكة إدارة الاتصالات
TTP	[X.810] طرف ثالث موثوق به
UDP	[J.170] بروتوكول كتلة بيانات المستعمل
VA	سلطة إقرار الصلاحية
VoIP	[X.805] نقل الصوت باستعمال بروتوكول الإنترنت
VPN	[X.805] شبكة تقديرية خاصة

الملحق جيم

قائمة بلجان الدراسات والمسائل المتعلقة بالأمن

تقوم لجان الدراسات بأعمال التقييس في قطاع تقييس الاتصالات ويقوم فيها ممثلو أعضاء قطاع تقييس الاتصالات بوضع توصيات (معايير) لمختلف مجالات الاتصالات الدولية. وتقوم لجان الدراسات بعملها في شكل مسائل للدراسة. ويتناول كل من هذه المسائل دراسات تقنية في مجال معين من مجالات تقييس الاتصالات. وفيما يلي قائمة بلجان الدراسات التابعة للقطاع ITU-T في الفترة الدراسية 2005-2008 وعناوينها واختصاصاتها وقائمة بمسائل الدراسة التي تتناول أعمال الأمن.

لجنة الدراسات 2	الجوانب التشغيلية لتوفير الخدمات والشبكات والأداء *لجنة الدراسات الرئيسية المعنية بدراسة تعريف الخدمة والترقيم والتسيير.*
مسؤولة عن الدراسات المتعلقة بمبادئ تقديم الخدمات وتعريفها والمتطلبات التشغيلية لمحاكاة الخدمات؛ ومتطلبات الترقيم والتسمية والعنونة وتخصيص الموارد بما في ذلك معايير وإجراءات الحجز والتخصيص؛ ومتطلبات التسيير والتشغيل البيني؛ والعوامل البشرية؛ والجوانب التشغيلية للشبكات ومتطلبات الأداء المرتبطة بها، بما في ذلك إدارة حركة الشبكات، ونوعية الخدمة (هندسة الحركة، وأداء التشغيل وقياسات الخدمات)؛ والجوانب التشغيلية للتشغيل فيما بين شبكات الاتصالات التقليدية والشبكات المتطورة؛ وتقييم المعلومات المرتدة من جهات التشغيل، وشركات التصنيع والمستعملين بشأن الجوانب المختلفة لتشغيل الشبكات.	
المسائل المتعلقة بالأمن:	
– **المسألة 1/2** – تطبيق خطط الترقيم والتسمية والعنونة على الاتصالات، وجوانب الخدمة والجوانب التشغيلية للترقيم بما في ذلك تعريف الخدمة (F.851)	
– **المسألة 4/2** – الجوانب التشغيلية لنوعية خدمة شبكات الاتصالات (E.408 وE.409 (بالاقتران مع لجنة الدراسات 17))	

لجنة الدراسات 3	مبادئ التعريفات والمحاسبة بما في ذلك القضايا الاقتصادية وقضايا السياسات المتصلة بالاتصالات
مسؤولة عن الدراسات المتصلة بمبادئ التعريفات والمحاسبة الخاصة بخدمات الاتصالات الدولية ودراسة القضايا الاقتصادية وقضايا السياسات المتصلة بالاتصالات. وتحقيقاً لهذه الغاية، تعمل لجنة الدراسات 3 بصفة خاصة على تشجيع التعاون بين أعضائها بغية جعل الأسعار في أدنى المستويات الممكنة بما يتفق مع كفاءة الخدمة ومع مراعاة ضرورة المحافظة على استقلال الإدارة المالية للاتصالات على أساس سليم.	
المسائل المتعلقة بالأمن: لا شيء	

لجنة الدراسات 4	إدارة الاتصالات *لجنة الدراسات الرئيسية المعنية بإدارة الاتصالات.*
مسؤولة عن الدراسات المتصلة بإدارة خدمات الاتصالات، والشبكات، والتجهيزات، بما في ذلك دعم شبكات الجيل التالي (NGN) وتطبيق وتطور هيكل شبكة إدارة الاتصالات (TMN). وهي مسؤولة، بالإضافة إلى ذلك، عن دراسات أخرى لإدارة الاتصالات تتناول التسميات، وإجراءات العمليات المتصلة بالنقل، وتقنيات وأجهزة الاختبار والقياس	
وبوصفها لجنة الدراسات الرئيسية المعنية بأنشطة الإدارة، يتناول عمل لجنة الدراسات 4 بخصوص الأمن المجالات التالية: أ) الاعتبارات المعمارية ومتطلبات السطوح البينية للإدارة، ب) المتطلبات التفصيلية لتأمين شبكة الإدارة (يشار إليها أيضاً بمستوي الإدارة)، ولا سيما أن الشبكات أصبحت متقاربة، ج) بروتوكول ونماذج لدعم تأمين معلومات الإدارة وإدارة معلمات الأمن.	
تعرّف إدارة شبكات الاتصالات على مستويات مختلفة من التجريد، من معلومات مستوى عنصر شبكة الإدارة إلى خدمات الإدارة التي تقدم إلى الزبون. وتتوقف متطلبات الأمن للمعلومات المتبادلة بين أنظمة الإدارة وبين عناصر الشبكة على ما إذا كانت شبكات الإدارة في إدارة واحدة موزعة بين إدارات. وعلى أساس المبادئ المعمارية، تم تعريف متطلبات وآليات وبروتوكول دعم بشكل صريح في التوصيات الحالية وثمة توصيات إضافية أخرى قيد الدراسة. تحل سلسلة التوصيات M.3016 المعتمدة حديثاً محل التوصية الأصلية ITU-T M.3016 (1998). وهي تصف أهمية الأمن وإمكانية تطبيقه في سياق مفهوم شبكة إدارة الاتصالات (TMN). وبدلاً من تخصيص مجموعة من الخدمات للحماية من التهديد فإنها توفر إطاراً لمنظمات معينة لتقوم بالتوصيف الملائم لاستخدام الآليات المتاحة. وتتناول السلسلة M.3016 التهديدات التالية في الشبكة (TMN): التنكر والتنصت والنفاذ غير المرخص به وفقدان المعلومات أو فسادها والتنصل والتزوير ورفض الخدمة. كما تتناول جوانب الأمن التالية: السرية وسلامة البيانات والمساءلة والتيسر.	
المسائل المتعلقة بالأمن:	
– **المسألة 6/4** – مبادئ الإدارة ومعماريتها (M.3010، سلسلة M.3016، M.3400)	
– **المسألة 7/4** – المتطلبات المتعلقة بالسطوح البينية لإدارة الاتصالات من منشأة إلى منشأة ومن عميل إلى منشأة (M.3320)	
– **المسألة 10/4** – نماذج المعلومات الخاصة بالتطبيقات (M.3210.1)	
– **المسألة 11/4** – بروتوكولات للسطوح البينية للإدارة (Q.813، Q.815، Q.817)	

لجنة الدراسات 5	الحماية من التأثيرات البيئية الكهرمغنطيسية

مسؤولة عن الدراسات المتصلة بحماية شبكات وتجهيزات الاتصالات من التداخل والصواعق، وكذلك عن الدراسات المتصلة بالملاءمة الكهرمغنطيسية (EMC)، وجوانب الأمان والصحة المتصلة بالمجالات الكهرمغنطيسية الناتجة عن منشآت وأجهزة الاتصالات، بما في ذلك الهواتف الخلوية.

وقد عكفت اللجنة، لدى تنفيذ المهمة الموكلة إليها، على دراسة مسائل عدة ووضعت عدداً من التوصيات والكتيبات التي تسهم في أمن الشبكة وحمايتها من التهديدات الكهرمغنطيسية. وتشمل هذه التهديدات ظواهر عابرة عالية القدرة ومؤذية من صنع الإنسان، مثل النبضة الكهرمغنطيسية عالية الارتفاع (HEMP) والموجة الصغرية عالية القدرة (HPM). وقد يتضمن الأمن الكهرمغنطيسي أيضاً تسرب معلومات من شبكات الاتصالات من خلال إرسالات راديوية غير متوقعة من المعدات.

ولا يختلف طابع التهديدات المؤذية وتقنيات التخفيف المقابلة عن تلك التي تنطبق على الاضطرابات الكهرمغنطيسية الطبيعية أو غير المتعمدة. وهناك أوجه تشابه بين النبضة الكهرمغنطيسية عالية الارتفاع (HEMP) والنبضة الكهرمغنطيسية التي تولدها صاعقة. كما أن تقنيات الحجب والترشيح التي تخفض إرسالات الطاقة الراديوية غير المطلوبة من المعدات تقلل من إمكانية تسرب الطاقة غير المتعمد. ومن ثم فإن الأنشطة التقليدية للجنة الدراسات 5 المتعلقة بالحماية من الصواعق والتحكم في التداخل الكهرمغنطيسي (EMI) تسهم في أمن الشبكة إزاء التهديدات المؤذية التي هي من صنع الإنسان. وأثناء فترة الدراسة الحالية تُدرَس جوانب الأمن في أعمال لجنة الدراسات في إطار المسألة الجديدة 15/5 بعنوان *أمن أنظمة الاتصالات والمعلومات فيما يتعلق بالبيئة الكهرمغنطيسية*.

وتشمل التهديدات الكهرمغنطيسية ظواهر عابرة عالية القدرة ومؤذية من صنع الإنسان مثل النبضة الكهرمغنطيسية عالية الارتفاع (HEMP) والإرسالات الصادرة عن مولدات كهرمغنطيسية عالية القدرة (HPEM) بما في ذلك الموجات الصغرية عالة القدرة (HPM) والمصادر واسعة النطاق جداً (UWB). وقد يتضمن الأمن الكهرمغنطيسي أيضاً تسرب معلومات من شبكات الاتصالات من خلال إرسالات راديوية غير متوقعة من معدات.

المسائل المتعلقة بالأمن:

- **المسألة 2/5** – الملاءمة الكهرمغنطيسية (EMC) المتعلقة بشبكات النفاذ عريض النطاق (التحكم في الإرسالات غير المطلوبة من أنظمة نفاذ عريض النطاق يسهم في تقليل إمكانية تسرب المعلومات).
- **المسألة 4/5** – قدرة معدات الاتصالات على المقاومة (من شأن مقاومة المعدات للصواعق أن تحسن مقاومة المعدات للتمورات التي تحدثها النبضة الكهرمغنطيسية عالية الارتفاع (HEMP)).
- **المسألة 5/5** – حماية أنظمة الاتصالات من الصواعق (من شأن التقنيات المستخدمة للحماية من الصواعق أن تزود المرفق بدرجة من الصلابة إزاء النبضة الكهرمغنطيسية عالية الارتفاع (HEMP) والموجة الصغرية عالية القدرة (HPE)).
- **المسألة 6/5** – ربط التشكيلات وتأريض أنظمة الاتصالات في البيئة العالمية (من شأن تدابير الربط والتأريض الملائمة أن تساعد في تزويد المرفق بدرجة من الصلابة إزاء النبضة الكهرمغنطيسية عالية الارتفاع (HEMP) والموجة الصغرية عالية القدرة (HPE)).
- **المسألة 12/5** – الحفاظ على توصيات الملاءمة الكهرمغنطيسية (EMC) الحالية وتحسينها (من شأن الملاءمة الكهرمغنطيسية لمعدات الاتصالات أن تحسن من مناعة المعدات إزاء بيئة النبضة الكهرمغنطيسية عالية الارتفاع (HEMP) المنقولة والمشعة وكذلك بيئة الموجة الصغرية عالية القدرة (HPE) المشعة. وتخفض كذلك الملاءمة الكهرمغنطيسية (EMC) لمعدات الاتصالات إمكانية تسرب المعلومات).
- **المسألة 15/5** – أمن أنظمة الاتصالات والمعلومات فيما يتعلق بالبيئة الكهرمغنطيسية (إمكانية مقاومة المعدات للصواعق تحسن من إمكانية مقاومة المعدات للتمورات التي تحدثها النبضة الكهرمغنطيسية عالية الارتفاع (HEMP)).

لجنة الدراسات 6	المنشآت الخارجية والتجهيزات داخل المباني المتصلة بها

مسؤولة عن الدراسات المتصلة بالمنشآت الخارجية والتجهيزات داخل المباني المتصلة بها مثل التشييد والتركيب والتوصيل والنهايات الطرفية والحماية من التآكل، وغير ذلك من أشكال التلف الناجم عن التأثيرات البيئية، باستثناء العمليات الكهرمغنطيسية، وجميع أنواع الكبلات للأرض المستخدمة في الاتصالات العامة والهياكل المرتبطة بها.

المسائل المتعلقة بالأمن:

- **المسألة 1/6** – الإجراءات البيئية والأمنية للمنشآت الخارجية
- **المسألة 6/6** – صيانة شبكات كبلات الألياف البصرية

لجنة الدراسات 9	الشبكات الكبلية المتكاملة عريضة النطاق والإرسال التلفزيوني والصوتي *لجنة الدراسات الرئيسية لدراسة الشبكات الكبلية المتكاملة عريضة النطاق والشبكات التلفزيونية.*

مسؤولة عن الدراسات المتصلة بما يلي:

أ) استعمال الشبكات الكبلية والشبكات الهجينة، المصممة أساساً لتوصيل البرامج التلفزيونية والصوتية إلى المنازل، بمثابة شبكات متكاملة عريضة النطاق لتحمل أيضاً خدمات صوتية أو خدمات أخرى حرجة زمنياً وخدمات فيديو عند الطلب وخدمات تفاعلية، وما إلى ذلك.

ب) استخدام أنظمة الاتصالات للمساهمة والتوزيع الأولي والتوزيع الثانوي لخدمات التلفزيون والبرامج الصوتية وخدمات البيانات المشابهة.

تتولى، بوصفها لجنة الدراسات الرئيسية لدراسة الشبكات الكبلية المتكاملة عريضة النطاق والشبكات التلفزيونية، تقييم التهديدات ومواطن الضعف في الشبكات عريضة النطاق والخدمات وأهداف أمن الوثائق كما تقيم التدابير المضادة وتعرّف معماريات الأمن.

وركزت الأنشطة المتعلقة بالأمن على المجالات التالية:

أ) *خدمات عريضة النطاق آمنة:* توفير خدمات الأمن لشبكات النفاذ عريضة النطاق، أي الاستيقان من المودم الكبلي، وإدارة المفاتيح المجفرة، والخصوصية وسلامة البيانات المرسلة، وتأمين تحميل برمجيات المودم الكبلي.

ب) *خدمات آمنة لنقل الصوت باستعمال بروتوكول الإنترنت:* إن الاتصالات الكبلية بواسطة بروتوكول الإنترنت (IPCablecom) هي مشروع خاص بشأن خدمات تفاعلية حرجة زمنياً عبر شبكة تلفزيون كبلية بواسطة بروتوكول الإنترنت وخاصة الصوتية الفيديوية عبر بروتوكول الإنترنت. وتشمل خدمات الأمن في الاتصالات الكبلية IPCablecom الاستيقان من مكيف المطراف متعدد الوسائط (MTA) من جانب مقدم الخدمة، والاستيقان من مقدم الخدمة من جانب مكيف المطراف متعدد الوسائط، وتأمين وضع الجهاز في الخدمة والتشكيل، وتأمين إدارة الجهاز، وتأمين التشوير، وتأمين الوسائط.

ج) *خدمات آمنة للشبكات المنـــزلية:* يمكن لأجهزة مودم كبلي متطور أن توفر خدمات للشبكات المنـــزلية مثل جدران الحماية وترجمة عناوين الشبكة. وتشمل خدمات الأمن الموفرة لأجهزة المودم الكبلي المتطورة الاستيقان من مكيف المطراف متعدد الوسائط (MTA) من جانب مقدم الخدمة، والاستيقان من مقدم الخدمة من قبل مكيف المطراف متعدد الوسائط، وتأمين وضع الجهاز في الخدمة والتشكيل وتأمين إدارة الجهاز، ووظيفة ترشيح الرزم/جدار الحماية وتأمين وإدارة جدار الحماية، وتأمين تحميل برمجيات المودم الكبلي المتطورة.

د) *بيئات تطبيق آمنة للخدمات التلفزيونية التفاعلية:* تعتمد الخدمات التلفزيونية التفاعلية على خدمات الأمن المعرّفة في برنامج Java ومواصفة المنصة المنـــزلية متعددة الوسائط (MHP).

المسائل المتعلقة بالأمن:

- **المسألة 3/9** – الأساليب والممارسات المطبقة على النفاذ المشروط والحماية من النسخ غير المشروع ومن إعادة التوزيع غير المشروع ("مراقبة إعادة التوزيع" بالنسبة لتوزيع التلفزيون الكبلي الرقمي إلى المنازل) (J.93، J.96)
- **المسألة 8/9** – تقديم الخدمات والتطبيقات الرقمية التي تستعمل بروتوكولات الإنترنت و/أو البيانات القائمة على الرزم بواسطة شبكة التلفزيون الكبلي (J.112)
- **المسألة 9/9** – تطبيقات صوتية وفيديوية على أساس بروتوكول الإنترنت عبر شبكات التلفزيون الكبلي (J.160، J.170، J.191)
- **المسألة 10/9** – توسيع الخدمات الكبلية عبر النطاق العريض في الشبكات المنـــزلية

لجنة الدراسات 11	متطلبات وبروتوكولات التشوير *لجنة الدراسات الرئيسية المعنية بالتشوير والبروتوكولات والشبكات الذكية.*
مسؤولة عن الدراسات المتصلة بمتطلبات وبروتوكولات التشوير اللازمة للوظائف المتصلة ببروتوكول الإنترنت، وبعض الوظائف المتصلة بالتنقلية، ووظائف تعدد الوسائط، وتحسين التوصيات الحالية بشأن بروتوكولات النفاذ والتشوير ما بين الشبكات لأسلوب النقل غير المتزامن (ATM)، والشبكات الرقمية متكاملة الخدمات ضيقة النطاق (N-ISDN) والشبكات الهاتفية العمومية التبديلية (PSTN). وضع معظم توصيات لجنة الدراسات 11 الراهنة من أجل شبكات موثوقة على أساس تعدد الإرسال بتقسيم الزمن (TDM) حيث يمكن استعمال التوصيلات من نقطة إلى نقطة لضمان أمن الاتصالات. وقد أدركت هذه اللجنة أن إدخال تكنولوجيا بروتوكول الإنترنت في الشبكات سوف ينطوي على تحديات أمن جديدة. واعترافاً بإدخال تكنولوجيا IP وبالحاجة إلى القدرة على توفير معلومات التشوير والتحكم على نحو آمن في هذه الشبكة المتطورة، وضعت اللجنة 11 مجموعة من المسائل المتصلة بمتطلبات التشوير والبروتوكول أخذت في الحسبان تحديات الأمن الجديدة هذه في عام 2004.	
المسائل المتعلقة بالأمن:	
– **المسألة 1/11** – المعماريات الوظيفية لتشوير ومراقبة الشبكة في بيئات شبكات الجيل التالي الناشئة	
– **المسألة 7/11** – متطلبات وبروتوكولات التشوير والتحكم لدعم الربط في بيئات شبكات الجيل التالي	

لجنة الدراسات 12	الأداء ونوعية الخدمة *لجنة الدراسات الرئيسية المعنية بدراسة نوعية الخدمة والأداء.*
مسؤولة عن توصيات بخصوص أداء الإرسال من طرف إلى طرف للمطاريف والشبكات فيما يتعلق بالنوعية المدركة والقبول لدى مستعملي النصوص والبيانات والكلام والتطبيقات متعددة الوسائط. ومع أن هذا العمل يشمل الآثار المتصلة بالإرسال فيما يتعلق بجميع الشبكات (كتلك القائمة على أساس التسلسل الرقمي المتقارب المتزامن (PDH) والتسلسل الرقمي المتزامن (SDH) وأسلوب النقل غير المتزامن (ATM) وبروتوكول الإنترنت (IP) وكذلك شبكات الجيل التالي (NGN)) وجميع مطاريف الاتصالات (مثل الأجهزة المحمولة باليد وتلك حرة اليدين وأجهزة الرأس والأجهزة المتنقلة والأجهزة السمعية المرئية والاستجابة الصوتية التفاعلية) فقد تركز الاهتمام بصفة خاصة على نوعية الخدمة في بروتوكول الإنترنت (IP QoS) وإمكانية التشغيل البيني والآثار المترتبة بالنسبة لشبكات NGN، كما يشمل الأنشطة المتصلة بالأداء وإدارة الموارد.	
المسائل المتعلقة بالأمن:	
– **المسألة 10/12** – الاعتبارات المتعلقة بتخطيط وبأداء الإرسال في خدمات النطاق الصوتي وخدمات البيانات والخدمات متعددة الوسائط	
– **المسألة 13/12** – متطلبات أداء وطرائق تقييم نوعية الخدمة وإدراك نوعية الخدمات متعددة الوسائط	
– **المسألة 17/12** – أداء الشبكات القائمة على بروتوكول الإنترنت	

لجنة الدراسات 13	شبكات الجيل التالي *لجنة الدراسات الرئيسية المعنية بشبكات الجيل التالي (NGN) وبالمسائل الساتلية*

مسؤولة عن الدراسات المتصلة بمعمارية شبكات الجيل التالي وتطورها وتقاربها، بما في ذلك الأطر والمعماريات الوظيفية ومتطلبات التشوير لشبكات الجيل التالي، وتنسيق إدارة مشروع شبكات NGN عبر لجان الدراسات وتخطيط الإطلاق وسيناريوهات التنفيذ ونماذج النشر وقدرات الشبكة والخدمة وإمكانية التشغيل البيني وأثر الإصدار السادس من بروتوكول الإنترنت (IPv6) وتنقلية شبكات NGN وتقاربها وجوانب شبكة البيانات العمومية.

وبما أن الأمن واحد من الملامح الرئيسية لشبكات NGN فقد أفردت لجنة الدراسات 13 مسألة مكرسة للأمن: المسألة 15/13، أمن شبكات الجيل التالي (NGN). وترتكز المسألة على دراسات مسائل الأمن الخاصة بالشبكات NGN وعلى تطوير حلول أمنية لها. ومن الأهداف الأساسية لدى اللجنة أن تضع مجموعة من المعايير تضمن، إلى أقصى حد ممكن، أمن البنية التحتية للاتصالات وذلك إبان تطور الشبكات الموروثة نحو شبكات الجيل التالي.

كما قررت لجنة الدراسات 13 أن تدرج في كل توصية جديدة أو مراجعة قسماً عن الأمن يتضمن الإحالات المرجعية إلى تلك الأقسام من التوصية التي تتناول جوانب الأمن.

وتطور لجنة الدراسات 13 جهودها بخصوص المسائل المرتبطة بأمن شبكات الجيل التالي بالتعاون مع لجان الدراسات الأخرى وكذلك مع منظمات أخرى معنية بوضع المعايير. ويندرج فريق مهام هندسة الإنترنت (IETF) (مجالات الإنترنت والأمن والنقل) ومشروع شراكة الجيل الثالث (3GPP) والمشروع الثاني (3GPP2) ومنتدى خط المشترك الرقمي (DSL) بين أكثر المنظمات الخارجية المعنية بوضع المعايير أهمية لدى لجنة الدراسات 13 بالنسبة إلى دراسات الأمن التي تضطلع بها.

المسائل المتعلقة بالأمن:

- **المسألة 2/13** – متطلبات ومخططات التنفيذ للخدمات الناشئة في شبكات الجيل التالي
- **المسألة 3/13** – المبادئ المعمارية الوظيفية لشبكات الجيل التالي
- **المسألة 4/13** – المتطلبات والإطار العام لنوعية الخدمة لشبكات الجيل التالي
- **المسألة 5/13** – العمليات والإدارة والصيانة في شبكات الجيل التالي
- **المسألة 6/13** – تنقلية شبكات الجيل التالي وتقارب الثابت–المتنقل
- **المسألة 7/13** – التشغيل البيني للشبكات والخدمة في بيئة شبكات الجيل التالي
- **المسألة 8/13** – سيناريوهات الخدمات ونماذج نشر شبكات الجيل التالي
- **المسألة 9/13** – تأثير بروتوكول IPv6 على شبكة من شبكات الجيل التالي
- **المسألة 10/13** – قابلية التشغيل البيني للشبكات الساتلية التي تجمع بين شبكات الأرض وشبكات الجيل التالي
- **المسألة 12/13** – ترحيل الأرتال (X.272)
- **المسألة 13/13** – شبكات البيانات العامة
- **المسألة 14/13** – بروتوكولات وآليات الخدمة لشبكات البيانات متعددة الخدمات (MSDN)
- **المسألة 15/13** – أمن شبكات الجيل التالي

وتشمل المهام المتصلة بالأمن ما يلي:

- المبادرة إلى دراسة مسائل الأمن الخاصة بشبكات الجيل التالي في مستوى المشروع ضمن لجنة الدراسات 13 ومع لجان دراسات أخرى. واعترافاً بدور لجنة الدراسات 17 الشامل بوصفها لجنة الدراسات الرئيسية في مجال أمن الاتصالات، تقدم المشورة والمساعدة إلى لجنة الدراسات 17 بشأن مسائل تنسيق أمن شبكات الجيل التالي.
- تقرير كيفية تطبيق التوصية ITU-T X.805، *معمارية الأمن للأنظمة التي توفر الاتصالات من طرف إلى طرف* في سياق بيئة شبكة من شبكات الجيل التالي.
- ضمان اتساق معمارية شبكة الجيل التالي المطورة مع مبادئ الأمن المقبولة.
- ضمان اندماج مبادئ الاستيقان والترخيص والمحاسبة (AAA) حسب الاقتضاء في كل شبكات الجيل التالي.

لجنة الدراسات 15	البنى التحتية للشبكات البصرية وشبكات النقل الأخرى *لجنة الدراسات الرئيسية المعنية بدراسة النقل على شبكات النفاذ* *لجنة الدراسات الرئيسية المعنية بدراسة التكنولوجيا البصرية*

لجنة الدراسات 15 هي البؤرة في قطاع تقييس الاتصالات لوضع المعايير الخاصة بالشبكات البصرية وشبكات النقل الأخرى من حيث البنى التحتية والأنظمة والتجهيزات والألياف البصرية وتكنولوجيات مستوي التحكم المقابلة لتمكين التطور نحو شبكات النقل الذكية. وهذا يشمل وضع المعايير المتصلة بأماكن الزبون والنفاذ، وأقسام المراكز الحضرية الكبرى وأقسام المسافات الطويلة في شبكات الاتصالات.

وتتناول المسألة 14/15 تحديد متطلبات الإدارة والتحكم ودعم نماذج المعلومات لمعدات النقل. وقد اقتدت دراسة المسألة 14/15 بمفهوم وإطار شبكة إدارة الاتصالات الذي وضعه قطاع تقييس الاتصالات في تعريف هذه المتطلبات والنماذج. وتعد إدارة الأمن واحدة من وظائف إدارة شبكة الاتصالات. وتندرج إدارة الأمن في نطاق ودراسة المسألة 14/15:

أ) متطلبات إدارة تجهيزات النقل: تتناول التوصيات G.7710/Y.1701 وG.784 وG.874 وظائف إدارة التجهيزات (EMF) داخل عنصر شبكة نقل تكون مشتركة بين تكنولوجيات متعددة، مخصصة لعنصر شبكة تراتب رقمي متزامن (SDH) ولعنصر شبكة نقل بصرية، على التوالي. وتوصف التطبيقات من أجل التاريخ والوقت، وإدارة الأعطال، وإدارة التشكيل، وإدارة الحساب، وإدارة الأداء، وإدارة الأمن. وتتمخض هذه التطبيقات عن مواصفة للوظائف (EMF) ومتطلباتها. ومتطلبات إدارة الأمن في هذه التوصيات قيد الدراسة حالياً.

ب) معمارية شبكة اتصالات البيانات ومتطلباتها: تعرّف التوصية G.7712/Y.1703 متطلبات المعيارية لشبكة اتصالات البيانات التي تدعم اتصالات إدارة موزعة تتعلق بشبكة إدارة الاتصالات (TMN)، واتصالات التشوير الموزعة التي تتعلق بشبكة بصرية تبديلية أوتوماتية (ASON)، والاتصالات الموزعة الأخرى (مثل اتصالات خدمة الخط أو الاتصالات الصوتية أو تحميل البرمجيات). وتتطلب التطبيقات المختلفة (مثل شبكة إدارة الاتصالات (TMN)، وشبكة النقل التبديلية الأوتوماتية (ASTN)، وما إلى ذلك) شبكة اتصالات قائمة على الرزم لنقل المعلومات بين المكونات المختلفة. فمثلاً، تتطلب شبكة إدارة الاتصالات (TMN) شبكة اتصالات يشار إليها بشبكة اتصالات الإدارة (MCN)، لنقل رسائل الإدارة بين مكونات شبكة إدارة الاتصالات (TMN) (مثل، مكوّن وظيفة عنصر شبكة (NEF)، ومكوّن وظيفة نظام العمليات (OSF)). وتتطلب الشبكة البصرية التبديلية الأوتوماتية (ASON) شبكة اتصالات، يشار إليها بشبكة اتصالات التشوير (SCN)، لنقل رسائل التشوير بين مكونات شبكة النقل التبديلية الأوتوماتية (ASTN) (مثل مكونات التحكم في النداء). وتشير التوصيتان G.7712/Y.1703 إلى سلسلة التوصيات M.3016. فيما يتعلق بمتطلبات أمن شبكة اتصالات الإدارة (MCN). وتعريف متطلبات أمن شبكة اتصالات الأمن (SCN) وارد في التوصية G.7712/Y.1703.

ج) النداء الموزع وإدارة التوصيل: توفر التوصية G.7713/Y.1704 متطلبات النداء الموزع وإدارة التوصيل لكل من السطح البيني لشبكة المستعمل (UNI) والسطح البيني لعقدة الشبكة (NNI). وتحدد المتطلبات في هذه التوصية الاتصالات عبر السطوح البينية للقيام بعمليات نداء أوتوماتية وعمليات توصيل. وتحدَّد نعوت الأمن، إلى جانب غيرها، لتمكين التحقق من عمليات النداء والتوصيل (وقد يشمل ذلك معلومات تمكّن من الاستيقان من طلب النداء وربما فحص طلب النداء للتأكد من سلامته).

لجنة الدراسات 15	البنى التحتية للشبكات البصرية وشبكات النقل الأخرى *لجنة الدراسات الرئيسية المعنية بدراسة النقل على شبكات النفاذ* *لجنة الدراسات الرئيسية المعنية بدراسة التكنولوجيا البصرية*
د) معمارية ومتطلبات التسيير في الشبكات البصرية التبديلية الأوتوماتية (ASON): تحدد التوصية G.7715/Y.1706 متطلبات ومعمارية وظائف التسيير المستخدمة لإقامة توصيلات تبديلية وتوصيلات برمجية دائمة في إطار الشبكة ASON. وتشمل المجالات الرئيسية في هذه التوصية معمارية تسيير الشبكة ASON وبعض المكونات الوظيفية بما في ذلك انتقاء المسير ونعوت التسيير، والرسائل المجردة والرسوم البيانية للحالة. وتشير هذه التوصية إلى توصيات السلسلة M.3016 وإلى X.800 فيما يتعلق باعتبارات الأمن. وتفيد بصورة خاصة، أنه اعتماداً على سياق استخدام بروتوكول التسيير وأهداف الأمن الشاملة المعرفة في توصيات السلسلة ITU-T M.3016 فإن السرية، وسلامة البيانات والمساءلة، والتوافر قد تتخذ سويات مختلفة من الأهمية. وينبغي أن يتناول تحليل التهديد لأي بروتوكول تسيير مقترح البنود التالية القائمة على أساس التوصية ITU-T X.800، وهي التنكر، والتنصت، والنفاذ غير المرخص به، وفقدان المعلومات أو فسادها (بما في ذلك هجمات التكرار) والتنصل، والتزوير ورفض الخدمة.	
هـ) إطار إدارة الشبكة البصرية التبديلية الأوتوماتية (ASON): تتناول التوصية G.7718/Y.1709 جوانب إدارة مستوي التحكم في الشبكة البصرية التبديلية الأوتوماتية أو التفاعلات بين مستوي الإدارة ومستوي التحكم في شبكة ASON وتشمل متطلبات إدارة الأعطال وإدارة التشكيل وإدارة الحسابات وإدارة الأداء وإدارة الأمن من أجل مكونات مستوي التحكم.	
المسائل المتعلقة بالأمن:	
– **المسألة 3/15** – الخصائص العامة لشبكات النقل البصرية (G.911)	
– **المسألة 9/15** – معدات النقل وحماية الشبكة/ترميمها (G.808.1، G.841، G.842، G.873.1)	
– **المسألة 14/15** – إدارة أنظمة ومعدات النقل والتحكم فيها	

لجنة الدراسات 16	المطاريف متعددة الوسائط وأنظمتها وتطبيقاتها *لجنة الدراسات الرئيسية في مجال المطاريف متعددة الوسائط وأنظمتها وتطبيقاتها، وفي مجال التطبيقات الشائعة في كل مكان ("كل شيء إلكترونياً"، كالصحة الإلكترونية والأعمال الإلكترونية).*

لجنة الدراسات 16 هي لجنة الدراسات الرئيسية في مجال المطاريف متعددة الوسائط وأنظمتها وتطبيقاتها، وفي مجال التطبيقات الشائعة في كل مكان ("كل شيء إلكترونياً"، كالصحة الإلكترونية والأعمال الإلكترونية). وتشمل المسألة 25/16 (فرقة العمل 2/16) "أمن الوسائط المتعددة في شبكات الجيل التالي" وتتناول مسائل الأمن التالية.

تطبيقات الوسائط المتعددة المتطورة مثل المهاتفة عبر الشبكات القائمة على الرزم ونقل الصوت بواسطة بروتوكول الإنترنت والمؤتمرات (الفيديوية) التفاعلية والتعاون؛ والمراسلة متعددة الوسائط، والتدفق الصوتي/الفيديوي وغيرها التي تتعرض لمجموعة شتى من تهديدات الأمن الحرجة في بيئات متغايرة. وهجمات سوء الاستخدام والتلاعب المؤذي والتنصت ورفض الخدمة بعض من مخاطر الأمن الحرجة المحتملة، ولا سيما في الشبكات القائمة على بروتوكول الإنترنت.

ومن المسلّم به أن هذه التطبيقات لها احتياجات أمن مشتركة يمكن تلبيتها بواسطة تدابير أمن عمومية، بواسطة أمن الشبكة مثلاً أو الاستيقان على مستوى الشبكة بأكملها. ومع ذلك، تخضع تطبيقات الوسائط المتعددة لاحتياجات أمن خاصة بكل تطبيق من الأفضل الوفاء بها باتخاذ تدابير أمن في طبقة التطبيقات. وتركز المسألة 25/16 على مسائل أمن التطبيقات في تطبيقات الوسائط المتعددة في شبكات الجيل التالي وتأخذ في الاعتبار الأساليب التكميلية لأمن الشبكة، حسب مقتضى الحال. وفريق المسألة 25/16 ملتزم بوضع توصيات أمن تتناول احتياجات السوق في هذا الصدد.

المسائل المتعلقة بالأمن:

- **المسألة 1/16** – الأنظمة متعددة الوسائط والمطاريف والتقاء البيانات (H.233، H.234)
- **المسألة 2/16** – الإرسال الصوتي والفيديوي وإرسال البيانات في الوقت الفعلي عبر شبكات بتبديل الرزم (H.323)
- **المسألة 4/16** – السمات المتقدمة لخدمات الاتصالات متعددة الوسائط الواقعة فوق منصات الأنظمة متعددة الوسائط التي حددها قطاع تقييس الاتصالات (H.350.2)
- **المسألة 25/16** – أمن الوسائط المتعددة في شبكات الجيل التالي (NGN-MM-SEC) (سلسلة H.235.x)
- **المسألة 29/16** – تنقلية أنظمة وخدمات الوسائط المتعددة (H.530)

لجنة الدراسات 17	الأمن واللغات وبرمجيات الاتصالات *لجنة الدراسات الرئيسية في مجال أمن الاتصالات واللغات وتقنيات الوصف.*

لجنة الدراسات 17 مسؤولة عن الدراسات المتصلة بالأمن، وتطبيق اتصالات الأنظمة المفتوحة بما في ذلك التوصيل الشبكي والدليل، وعن اللغات التقنية، وطريقة استعمالها، ومسائل أخرى متصلة بجوانب البرمجيات في أنظمة الاتصالات.

ولجنة الدراسات 17 هي لجنة الدراسات الرئيسية المعنية بمسائل أمن الاتصالات، وتنسق جهود القطاع ITU-T في مجال تقييس الأمن من خلال مشروع جديد للقطاع بشأن الأمن يدار في إطار المسألة 4/17. وكجزء من هذه الجهود وضع كتالوج بتوصيات الاتحاد المتصلة بالأمن وكذلك تجميع لتعاريف الأمن مستخرجة من توصيات القطاع ITU-T المعتمدة. ويجري تحديثهما بانتظام. وعقدت ورشات عمل بشأن الأمن وحلقات دراسية بشأن الأمن السيبراني في مايو 2002 في سيول، كوريا، وفي أكتوبر 2004 في فلوريانوبوليس، البرازيل، وفي مارس 2005 في موسكو، روسيا، وفي أكتوبر 2005 في جنيف، سويسرا. وتنظم ورشات عمل أخرى كلما دعت الحاجة.

وتحت إشراف فرقة العمل 1/17 توفر التوصية ITU-T X.509، *أطر شهادات المفاتيح العمومية والنعوت* القاعدة الأساس للبنى التحتية للمفاتيح العمومية (PKI) والبنى التحتية لإدارة الامتيازات (PMI). ويجري باستمرار تحسين التوصية X.509 لتلبية الاحتياجات المتطورة. وفرقة العمل 2/17 مسؤولة عن وضع التوصيات التي تتناول معمارية الأمن الأساسية وإطارها الهيكلي وبروتوكولها، ولا سيما تلك التوصيات في السلسلة X.800. وأثناء فترة الدراسة الماضية أعدت مجموعة من التوصيات الجديدة المتصلة بالأمن بما فيها التوصية X.805 التي تحدد معمارية أمن لتوفير أمن الشبكة من طرف إلى طرف. ويمكن تطبيق هذه المعمارية على مختلف أشكال الشبكات بصرف النظر عن التكنولوجيا التي تقوم عليها الشبكة. ويمكن استعمالها كأداة لضمان اكتمال اعتبارات الأمن عند وضع التوصيات ومن أجل القيام بعمليات تقييم الأمن في الشبكات. وثمة توصية أساسية أخرى هي التوصية X.1051 تحدد المتطلبات اللازمة لنظام إدارة أمن معلومات (ISMS) في سياق الاتصالات. وهي تحدد المتطلبات اللازمة لإقامة نظام ISMS موثّق وتنفيذه وتشغيله ومراقبته واستعراضه وصيانته وتحسينه ضمن سياق مخاطر الأعمال الإجمالية لدى منظمة الاتصالات. أما التوصية X.1081 فهي توصية إطارية ترسي الأساس لمواصفات القياس الحيوي عن بعد في المستقبل. وتركز التوصيتان X.1121 وX.1122 على اتصالات البيانات المتنقلة من طرف إلى طرف. فالتوصية X.1121 تحلل تهديدات الأمن في بيئة متنقلة ووسائل الحماية من وجهة نظر المستعمل المتنقل ومقدم خدمات التطبيق. والتوصية X.1122 توفر الإرشاد لدى بناء أنظمة متنقلة آمنة تقوم على أساس تكنولوجيا البنية التحتية للمفاتيح العمومية (PKI). والمعلومات الراهنة متاحة في صفحة لجنة الدراسات 17 في موقع الاتحاد على الويب (انظر http://www.itu.int/ITU-T/studygroups/com17/tel-security.html).

المسائل المتعلقة بالأمن:

فرقة العمل 1/17 تكنولوجيا الأنظمة المفتوحة

- **المسألة 1/17** – اتصالات متعددة التوزيع من طرف إلى طرف مع مرفق لإدارة نوعية الخدمة

تنظر هذه المسألة في جوانب المتطلبات والمعمارية وإدارة مجموعة وجلسة وبروتوكول الاتصالات متعددة التوزيع من أجل اتصالات متعددة التوزيع من طرف إلى طرف. ولتحقيق الاتصالات الجماعية الآمنة بين الأعضاء ينظر حالياً في استحداث تمديدات بروتوكول أمن لبروتوكولات الاتصالات متعددة التوزيع من طرف إلى طرف. وتركز الأعمال الجارية على تطبيق آليات الأمن ذات الصلة على بروتوكولات الاتصالات متعددة التوزيع وإجراءات البناء من أجل الاتصال الآمن.

- **المسألة 2/17** – خدمات الدليل وأنظمة الدليل وشهادات المفاتيح العمومية/النعوت

تتناول هذه المسألة وضع التوصية X.509 والحفاظ عليها. وهي تشمل شهادات المفاتيح العمومية وشهادات النعوت وإبطال الشهادات وتوصيف البنى التحتية الداعمة (البنية التحتية للمفاتيح العمومية والبنية التحتية لإدارة الامتيازات). وشهادات المفاتيح العمومية والبنية التحتية الداعمة لها عناصر أساسية للقيام بوظيفة الاستيقان وهي تطبق على وجه الخصوص في مجال التواقيع الرقمية.

- **المسألة 16/17** – أسماء الميادين الدولية

مسائل الأمن جزء من العمل الذي يتناول أسماء الميادين الدولية (IDN). والفريق المعني بهذه المسألة يتعرّف الوثائق التقنية الموجودة التي تبين المبادئ الأساسية للأسماء IDN بما في ذلك الوثائق المتصلة بمخاطر أمن شبكات الاتصالات التي تصاحب تنفيذ الأسماء IDN. ويضطلع بهذه المهمة بالتشاور مع الكيانات المعنية، ومنها ISO/IEC، وكونسورتيوم UNICODE وIETF وICANN وCENTR.

فرقة العمل 2/17 أمن الاتصالات

- **المسألة 4/17** – مشروع أمن أنظمة الاتصالات

هذه المسألة مكرسة لتحديد الرؤية ولتنسيق وتنظيم مجموع أنشطة أمن الاتصالات بأكملها في القطاع ITU-T. ويُتبع نهج من القمة إلى القاعدة إزاء مسألة الأمن وذلك بالتعاون مع لجان دراسات أخرى ومنظمات أخرى تهتم بوضع المعايير. وهذه المسألة موجهة نحو بذل جهود مكثفة في مستوى المشروع وفي المستوى الاستراتيجي.

- **المسألة 5/17** – معمارية الأمن والإطار العام

سعياً إلى إيجاد حلول أمن شاملة وفعالة من حيث التكلفة يمكن تطبيقها على مختلف أنواع الشبكات والخدمات والتطبيقات في بيئة متعددة البائعين، ينبغي تصميم أمن الشبكة انطلاقاً من معماريات الأمن القياسية وتكنولوجيات الأمن القياسية. وإذ تأخذ هذه المسألة في الحسبان تهديدات الأمن في بيئة الاتصالات والتقدم المحرز حتى الآن في تدابير الأمن المضادة لهذه التهديدات، فإنها تنظر في الجديد من متطلبات الأمن والحلول وفي كيفية تطوير معماريات الأمن وهياكله لمواكبة البيئة المتطورة.

- **المسألة 6/17** – الأمن السيبراني

تنظر هذه المسألة في جوانب الأمن السيبراني في سياق عملية التقييس دولياً. وهي تنظر على وجه الخصوص في مجالات الأمن السيبراني التالية:

- عمليات لتوزيع معلومات قابلية التأثر وتقاسمها والكشف عنها؛
- الإجراءات القياسية لعمليات التعامل مع الحوادث في الفضاء السيبراني؛
- استراتيجية لحماية البنية التحتية الحرجة للشبكة.

- **المسألة 7/17** – إدارة الأمن

ترمي هذه المسألة إلى وضع مجموعة من التوصيات تتناول إدارة الأمن للقطاع ITU-T، آخذة في الحسبان الحاجة إلى التعاون مع الفريق ISO/IEC JTC 1. وتركز المسألة خصوصاً على تحديد وإدارة الخطر في أنظمة الاتصالات وعلى اتساق نظام إدارة أمن المعلومات (ISMS) لدى الشركات ناقلة الاتصالات مع معايير نظام ISMS القائمة.

- **المسألة 8/17** – القياس الحيوي عن بعد

تنطلق هذه المسألة من الأعمال القائمة المتصلة بالتعرف الشخصي والاستيقان باستخدام علم القياس الحيوي عن بعد والتي يضطلع بها بالتعاون الوثيق مع أعمال التقييس المتصلة بذلك في منظمات أخرى تهتم بوضع المعايير. وهي تركز خصوصاً على كيفية تحسين تعرّف واستيقان المستعملين وذلك باستخدام طرائق قياس حيوي عن بعد مأمونة وآمنة وكيفية تحديد مسائل تكنولوجيات الاستيقان بالقياس الحيوي في مجال الاتصالات.

- **المسألة 9/17** – خدمات الاتصال الآمنة

نظراً إلى بعض الخصائص المعينة في الاتصالات المتنقلة (مثال ذلك الإرسال عبر الهواء وقدرة الحوسبة المحدودة وحجم الذاكرة في الأجهزة المتنقلة الصغيرة) فإن توفير الأمن مهمة تنطوي على قدر عال من التحديات وتستحق اهتماماً ودراسة خاصة. وتنظر هذه المسألة في كيفية تحديد وتعريف خدمات الاتصال الآمنة في خدمات الاتصال المتنقلة أو في خدمات شبكة الويب، وكيفية تحديد التهديدات التي تتعرض لها خدمات الاتصالات والتعامل معها، والتكنولوجيات لدعم خدمات الاتصال الآمنة، وكيفية الحفاظ على التوصيلية المتبادلة بين خدمات الاتصالات.

- **المسألة 17/17** – صد الرسائل الاقتحامية بالوسائل التقنية

تركز هذه المسألة على المتطلبات التقنية والهياكل العامة والمبادئ التوجيهية والتكنولوجيات الجديدة من أجل صد الرسائل الاقتحامية. وكجزء من هذه الجهود يضع الفريق المهتم بهذه المسألة مجموعة توصيات بشأن صد الرسائل الاقتحامية في البرية الإلكتروني والرسائل الاقتحامية في التطبيقات متعددة الوسائط آخذاً في الحسبان الحاجة إلى التعاون مع لجان الدراسات الأخرى في القطاع ITU-T والتعاون مع المنظمات المعنية بوضع المعايير.

فرقة العمل 3/17 اللغات وبرمجيات الاتصالات

- **المسألة 10/17** – الترميز المجرد لنسق التركيب رقم واحد (ASN.1) ولغات بيانات أخرى

تتناول هذه المسألة الحفاظ على الترميز ASN.1 وتحسينه وكذلك على قواعد التشفير التي يتضمنها، بما في ذلك قواعد التشفير المتميز (DER) المستخدمة في استحداث الشهادات الرقمية أو التواقيع الرقمية بموجب التوصية X.509. ونظام الترميز ASN.1 جزء هام من تمثيل المعلومات بأسلوب يمكن التعويل عليه في تشفير المعلومات وفك تشفيرها وفي توقيعها والتحقق منها. ويواصل فريق هذه المسألة تحسين النظام ASN.1 كيما يلبي الاحتياجات المتغيرة في بيئات الاتصالات اليوم.

لجنة الدراسات 19	شبكات الاتصالات المتنقلة *لجنة الدراسات الرئيسية المعنية بشبكات الاتصال المتنقلة وبمسألة التنقلية*
مسؤولة عن الدراسات المتصلة بجوانب الشبكات في شبكات الاتصالات المتنقلة، بما في ذلك الاتصالات المتنقلة الدولية لعام 2000 وما بعدها، والإنترنت اللاسلكية، وتقارب الشبكات المتنقلة والثابتة، وإدارة التنقلية، ووظائف الوسائط المتعددة المتنقلة، والتشغيل الشبكي البيني، وقابلية التشغيل وإدخال تحسينات على توصيات قطاع تقييس الاتصالات الراهنة الخاصة بالاتصالات المتنقلة الدولية (IMT-2000).	
المسائل المتعلقة بالأمن:	
– **المسألة 1/19** – المتطلبات من حيث مقدرة الخدمات والشبكات ومعمارية الشبكة	
– **المسألة 3/19** – تحديد أنظمة الاتصالات المتنقلة الدولية–2000 القائمة والمتطورة (Q.1741.1، Q.1741.2، Q.1741.3، Q.1742.1، Q.1742.2، Q.1742.3)	
– **المسألة 5/19** – تقارب شبكات الاتصالات المتنقلة الدولية–2000 المتطورة مع الشبكات الثابتة المتطورة	

أعمال قطاع تقييس الاتصالات في مجال الأمن

إطار معمارية الأمن

- X.800 – معمارية الأمن
- X.802 – نموذج الأمن في الطبقات السفلى
- X.803 – نموذج الأمن في الطبقات العليا
- X.810 – أطر الأمن للأنظمة المفتوحة: نظرة شاملة
- X.811 – أطر الأمن للأنظمة المفتوحة: إطار الاستيقان
- X.812 – أطر الأمن للأنظمة المفتوحة: إطار مراقبة النفاذ
- X.813 – أطر الأمن للأنظمة المفتوحة: إطار عدم التنصل
- X.814 – أطر الأمن للأنظمة المفتوحة: إطار السرية
- X.815 – أطر الأمن للأنظمة المفتوحة: إطار سلامة البيانات
- X.816 – أطر الأمن للأنظمة المفتوحة: إطار تدقيق مقتضيات الأمن والإنذار

أمن الاتصالات

- X.805 – معمارية الأمن لأنظمة توفر الاتصالات من طرف إلى طرف
- X.1051 – نظام إدارة أمن المعلومات – المتطلبات الخاصة بالاتصالات (ISMS-T)
- X.1081 – نموذج القياسات الحيوية عن بعد متعدد الأساليب – إطار لمواصفة جوانب الأمن والسلامة الخاصة بالقياسات الحيوية عن بعد
- X.1121 – إطار تكنولوجيات الأمن لاتصالات البيانات المتنقلة من طرف إلى طرف
- X.1122 – منهج لتنفيذ أنظمة آمنة متنقلة تستند إلى البنى التحتية للمفاتيح العمومية (PKI)

البروتوكولات

- X.273 – بروتوكول أمن طبقة الشبكة
- X.274 – بروتوكول أمن طبقة النقل

الأمن في ترحيل الرتل

- X.272 – انضغاط البيانات والخصوصية عبر شبكات ترحيل الرتل

تقنيات الأمن

- X.841 – أغراض معلومات أمن لمراقبة النفاذ
- X.842 – خطوط توجيهية لاستخدام وإدارة خدمات الطرف الثالث الموثوق به
- X.843 – مواصفات خدمات الطرف الثالث الموثوق به لدعم تطبيق التوقيعات الرقمية

خدمات الدليل والاستيقان

- X.500 – نظرة شاملة على المفاهيم والنماذج والخدمات
- X.501 – نماذج
- X.509 – أطر المفاتيح العمومية وشهادات النعوت
- X.519 – مواصفات البروتوكول

أمن إدارة الشبكة

- M.3010 – مبادئ شبكة إدارة الاتصالات
- M.3016.x – أمن شبكة إدارة الاتصالات (توصية متعددة الأجزاء)
- M.3210.1 – خدمات إدارة شبكة إدارة الاتصالات لإدارة أمن الاتصالات المتنقلة الدولية–2000
- M.3320 – إطار متطلبات إدارة للسطح البيني X لشبكة إدارة الاتصالات
- M.3400 – وظائف إدارة شبكة إدارة الاتصالات

إدارة الأنظمة

- X.733 – وظيفة الإخبار عن الإنذار
- X.735 – وظيفة مراقبة لوغاريتمية
- X.736 – وظيفة الأمن للإخبار عن الإنذارات
- X.740 – وظيفة التسجيل الدقيق للأمن
- X.741 – أغراض وخواص لمراقبة النفاذ

أنظمة التلفزيون وأنظمة الكبلات

- J.91 – الطرق التقنية لضمان الخصوصية في الإرسال التلفزيون الدولي لمسافات بعيدة
- J.93 – متطلبات النفاذ المشروط في التسليم الثانوي لتلفزيون رقمي أو أنظمة تلفزيون بكبل
- J.170 – مواصفات أمن الاتصالات الكبلية باستخدام بروتوكول الإنترنت

اتصالات متعددة الوسائط

- H.233 – نظام السرية في الخدمات السمعية المرئية
- H.234 – إدارة مفاتيح التحفير ونظام الاستيقان للخدمات السمعية المرئية
- H.235.x – أمن H.323 (توصية متعددة الأجزاء)
- H.323 الملحق ياء – أنظمة اتصالات متعددة الوسائط قائمة على رزم – أمن الأنظمة H.323 الملحق واو (أمن لأنواع نقطة طرفية بسيطة)
- H.350.2 – معمارية خدمات الدليل للتوصية H.235
- H.530 – تدابير أمن تناظرية لتنقلية H.323 في H.510

الفاكس

- T.30 الملحق زاي – تدابير لإرسال آمن لفاكس من الزمرة 3 باستخدام HKM وHFX
- T.30 الملحق حاء – الأمن في فاكس من الزمرة 3 القائم على خوارزمية ريفست وشامير وأدلمان
- T.36 – مقدرات الأمن لاستخدام مطاريف الفاكس من الزمرة 3
- T.503 – ملامح تطبيق وثيقة لمبادلة وثائق الفاكس من الزمرة 4
- T.563 – الخصائص المطرافية لأجهزة الفاكس من الزمرة 4

أنظمة مناولة الرسائل (MHS)

- X.400/F.400 – نظام مناولة الرسائل ونظرة عامة على الخدمة
- X.402 – المعمارية العامة
- X.411 – نظام نقل الرسائل: تعريف وإجراءات الخدمة المجردة
- X.413 – مخزن الرسائل: تعريف الخدمة المجردة
- X.419 – مواصفات البروتوكول
- X.420 – نظام المراسلة فيما بين الأشخاص
- X.435 – نظام المراسلة المتبادلة لبيانات إلكترونية
- X.440 – نظام المراسلة الصوتية

تتاح توصيات قطاع تقييس الاتصالات من موقع الاتحاد الدولي للاتصالات http://www.itu.int/publications/bookshop/how-to-buy.html (يشمل هذا الموقع معلومات عن نفاذ مجاني محدود لتوصيات قطاع تقييس الاتصالات)

تشمل الأعمال الهامة في مجال الأمن الجارية حالياً في قطاع تقييس الاتصالات

القياسات الحيوية عن بعد وإدارة الأمن وأمن الخدمات المتنقلة والأمن السيبراني وأمن الشبكات المنـــزلية وأمن شبكات الجيل التالي ومكافحة الرسائل الاقتحامية والاتصالات في حالات الطوارئ

لمزيد من المعلومات عن قطاع تقييس الاتصالات ولجان دراساته: http://www.itu.int/ITU-T

طبع في سويسرا
جنيف، 2006