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

ديسمبر 2003

ITU-T قطاع تقييس الاتصالات

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

شـكر

أعد هذا الكتيب بمساهمة من مؤلفين عديدين ممن شاركوا في وضع توصيات قطاع تقييس الاتصالات المتصلة بذا 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 والمصادر التالية: السيدة لاكشيمي رامان، فيما يتعلق بالقسم 4.6 وجزء من الجزء 2. وقد استعرض الجزء 2 كل من السيدين هيرب بيرتين وراو فازيردي. وقد أخِذت المادة الواردة في القسم 3 الذي يتناول التهديدات والمخاطر من الدراسات التي أجراها قطاع تقييس الاتصالات وكذلك من الاستعراض الذي أجراه شانون. ويستند النص في كل من الجزء 5 والقسم 5.6 على مواد عامة مأخوذة من وايزكي والمساهمة الكريمة من الأستاذ ديفيد شادوبك، ولا سيما فيما يتعلق بالوصفات الإلكترونية في القسم 2.5.6 (بالإضافة إلى المادة المأخوذة من نشرة السياسات. ويستند النص الخاص بنقل الصوت باستعمال بروتوكول الإنترنت والأنظمة التي تحددها التوصية H.323 الصادرة عن قطاع تقييس الاتصالات في القسم 1.6 إلى المواد التي أعدها كل من باكتزر وأوشنر بالإضافة إلى المساهمة الكريمة من السيد مارتين أوشنر. ويستند القسم 2.6 إلى التوصية J.169 الصادرة عن قطاع تقييس الاتصالات مع استعراض أجراه السيد إيريك روزنفيلد في القسم 2.1.6. ويستند القسم 3.6 إلى المواد المبينة في التوصية T.30 والتوصية T.36 لقطاع تقييس الاتصالات. كما نود أن نتقدم بالشكر الجزيل للعديد ممن قاموا باستعراضات النصوص دون ذكر أسمائهم. وجاءت المادة الواردة في الملحق جيم من مساهمات خبراء كثيرين في لجان الدراسات التابعة لقطاع تقييس الاتصالات ومن الردود على استبيان لجنة الدراسات 17 بخصوص الأمن، واستندت المادة الواردة في الملحق باء إلى مجموعة التوصيات المتعلقة بالأمن التي وضعها الخبراء المعنيون بالمسألة 10/17 لقطاع تقييس الاتصالات، ولا سيما السيد ساندور مازجون.

المحتويات

شـكر

تمهيد

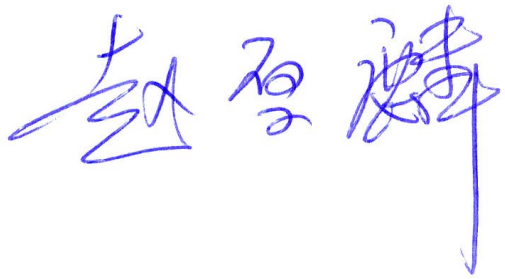
اقتصر الأمن الرقمي في الماضي على مجالات محددة مثل المصارف والتطبيقات الفضائية أو العسكرية إلا أنه أصبح بالتدريج شأن الجميع.

قد تعزى زيادة الاهتمام بالأمن الرقمي إلى عناوين الأخبار الرئيسية التي تتحدث عن انتشار الفيروسات عن طريق البريد الإلكتروني أو عن القراصنة الذين يسرقون تفاصيل بطاقات الائتمان. إلا أن هذا لا يمثل إلا جانباً من القصة. وبما أن استخدام الحواسيب والتواصل عن طريق الشبكات أصبحا جزءاً من الحياة اليومية كالمياه والكهرباء، لم يعد الحديث عن الأمن الرقمي يقتصر على الخبراء فحسب، بل أصبح يتردد أيضاً في أفواه مثلي الحكومات والشركات بل والمستهلكين. وإذا كانت جوانب كثيرة من أعمالنا وحياتنا الخاصة تعتمد على الحواسيب والشبكات، فمن الضروري أن تعمل هذه الأنظمة بأمان.

ومن الضروري أيضاً أن تكون عملية الأمن محل تفكير عميق من بداية وضع النظام وتصميمه مروراً بالتنفيذ إلى السياسات والممارسات ونشر النظام وتشغيله واستخدامه. وينبغي أن يكون عنصر الأمن، لدى وضع المعايير، من عناصر العمل الأساسية، وليس مجرد فكرة يمكن التعامل معها في مرحلة تالية - لأن جوانب الضعف تنشأ في هذه المرحلة. وينحصر دور لجان المعايير في الإستماع إلى ما يتردد في السوق وتوثيق القضايا المعروفة، وتقديم حلول لها كلما كان ممكناً، وإصدار المواصفات أو المبادئ التوجيهية التي تساعد المنفذين والمستعملين على جعل أنظمة وخدمات الاتصالات قوية بما فيه الكفاية.

ولقد كان قطاع تقييس الاتصالات نشطاً في مجال أمن الاتصالات وتكنولوجيا المعلومات طوال سنوات عديدة. ومع ذلك، فلم يكن من اليسير دائماً الوقوف على ما تم إنجازه ومكان وجوده. ويعتبر هذا الكتيب المحاولة الأولى لتجميع كل المعلومات المتاحة. وأود أن أعرب عن تقديري لمهندسي مكتب تقييس الاتصالات في الاتحاد الدولي للاتصالات الذين أنجزوا هذا العمل الشاق، بمساعدة العديد من الخبراء من بين أعضاء الاتحاد. والغرض من هذا الكتيب هو أن يكون بمثابة دليل للعاملين في مجال تكنولوجيا المعلومات والإدارة المتوسطة وكذلك للهيئات التنظيمية، ليساعدهم على التنفيذ العملي لوظائف الأمن. ويتضمن هذا الكتيب أمثلة لتطبيقات عديدة، يستند إليها في شرح وتوضيح قضايا الأمن، مع التركيز على كيفية تناول توصيات قطاع تقييس الاتصالات لها.

وإنني على ثقة من أن هذا الكتيب سيكون دليلاً مفيداً لمن يبحثون في قضايا الأمن وإننا نرحب بأي تعليقات من القراء للاستئناس بها في الطبعات القادمة.



هولين جاو
مدير مكتب تقييس الاتصالات
الاتحاد الدولي للاتصالات
جنيف، ديسمبر 2003

ملخص تنفيذي

ساهمت صناعة الاتصالات، من خلال تلبية الاحتياجات المتزايدة للبيئة التجارية العالمية، في تحسين الإنتاجية وربطت ا تمعات على المستوى العالمي في كل قطاع صناعي تقريباً. ومستوى الكفاءة الذي تتمتع به البنية التحتية للاتصالات، يرجع في جانب كبير منه إلى المعايير التي وضعتها منظمات مثل قطاع تقييس الاتصالات في الاتحاد الدولي للاتصالات. كذلك فإن المعايير التي حافظت على كفاءة الشبكات الحالية هي أيضاً التي تضع أسس شبكات الجيل المقبل. ومع ذلك، بينما واصلت المعايير تلبية احتياجات المستعمل النهائي والصناعة، وزاد استخدام الأسطح البينية المفتوحة والبروتوكولات وتعدد العاملين الجدد، وتنوع التطبيقات والمنابر، وعمليات التنفيذ التي لا تخضع للاختبار بما فيه الكفاية مما زاد من فرص سوء استخدام الشبكات. وقد لوحظ، خلال السنوات الأخيرة، حدوث زيادة كبيرة في انتهاكات الأمن (مثل انتشار الفيروسات وانتهاك سرية البيانات المخزنة) في جميع الشبكات العالمية، مما نتج عنه في أغلب الأحيان آثار ترتبت عليها تكاليف فادحة. والسؤال الذي يطرح نفسه الآن، هو كيف يمكن دعم بنية تحتية لاتصالات مفتوحة دون تعريض المعلومات التي يجري تبادلها على هذه الشبكات للخطر. والإجابة على هذا السؤال نجدها في الجهود التي تبذلها لجان المعايير التي تعمل على مكافحة التهديدات التي يتعرض لها الأمن في جميع مجالات البنى التحتية للاتصالات. وتتناول هذه الأحكام التفاصيل المبينة في مواصفات البروتوكولات وفي التطبيقات وإدارة الشبكات. والغرض من هذا الكتيب هو تقديم عرض مختصر للتوصيات العديدة التي وضعها قطاع تقييس الاتصالات - بالتعاون في بعض الأحيان مع المنظمات الأخرى المعنية بوضع المعايير – لتأمين البنى التحتية للاتصالات والخدمات والتطبيقات ذات الصلة.

ولكي يمكن معالجة الجوانب المتعددة للأمن، فمن الضروري وضع إطار وهيكل عامين لكي تكون لدينا مصطلحات عامة يمكن بناء عليها مناقشة المفاهيم.

والقسم 2 يلخص العناصر المعمارية المبينة في التوصية ITU-T X.805 إلى جانب أبعاد الأمن الثمانية التي تم تحديدها للتعامل مع قضية الأمن من طرف إلى طرف في تطبيقات الشبكات – وهي الخصوصية، وسرية البيانات، والاستيقان، وسلامة البيانات، وعدم التنصل، ومراقبة النفاذ، وأمن الاتصالات والتيسر. وتستخدم هذه المبادئ العامة لتوجيه وفهم التفاصيل التي نوقشت في الأقسام الأخرى. وتشمل العناصر الرئيسية طبقات الأمن ومستويات الأمن والأبعاد المطبقة للجمع بين أي طبقة وأي مستوى.

ويقدم القسم 3 ثلاثة مصطلحات رئيسية عند مناقشة الأمن: هي جوانب الضعف، والتهديد والخطر، مع التمييز بينها وتقديم أمثلة لها. والنقطة الرئيسية في هذا القسم هي ملاحظة كيف أن أي خطر على الأمن يكون نتيجة لوجود جوانب ضعف ولوجود ديد.

ويستند القسم 4 إلى المعلومات الواردة في الأقسام السابقة لتعريف ما وراء المتطلبات اللازمة لوضع إطار الأمن. ومن العناصر الرئيسية لتحقيق الأمن لمكافحة التهديدات هو تعريف الآليات والخوارزميات المرتبطة بتدابير الأمن، مثل الاستيقان ومراقبة النفاذ وتجفير البيانات. ويتضمن القسم 5 تعريف هذه الآليات مع مفهوم المفاتيح العمومية والبنى التحتية للإدارة المتميزة. ويمكن تطبيق هذه الآليات والبنى التحتية على تطبيقات كثيرة للمستعملين النهائيين.

وبالإضافة إلى هذا الإطار والمعمارية والآليات، قام قطاع تقييس الاتصالات بوضع أحكام للأمن في أنظمة وخدمات عديدة حدد ا التوصيات الصادرة عن هذا القطاع. وبالتالي، ينصب التركيز الرئيسي لهذا الكتيب على التطبيقات، كما نرى في القسم 6. وتشمل هذه الطبعة الأولى عينة موعة تطبيقات، من بينها التطبيقات الصوتية والتطبيقات متعددة الوسائط عبر بروتوكول الإنترنت (التوصية H.323 والأنظمة الكبلية باستخدام بروتوكول الإنترنت) والرعاية الصحية والفاكس، مع توصيف هذه التطبيقات على أساس معمارية الاستخدام وكيف تم 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.

وبالإضافة إلى ذلك، يتضمن الكتيب قائمة بالمختصرات والتعاريف المتصلة بالأمن والموضوعات الأخرى التي تعالجها هذه الوثيقة، وهي مقتبسة من توصيات قطاع تقييس الاتصالات ذات الصلة ومصادر أخرى (مثل قاعدة بيانات SANCHO لقطاع تقييس الاتصالات ومجموعات الوثائق التي تتحدث عن أمن أنظمة الاتصالات التي وضعتها لجنة الدراسات 17 التابعة لقطاع تقييس الاتصالات). وهذا ما يأتي بيانه في الملحق ألف. ويتضمن هذا الكتيب أيضاً، القائمة الحالية للتوصيات الصادرة عن قطاع تقييس الاتصالات في شأن جوانب الأمن - والقائمة المستفيضة الواردة في الملحق باء توضح أيضاً مدى اتساع أعمال قطاع التقييس في مجال الأمن. ويلخص الملحق جيم الأعمال المتصلة بالأمن التي تقوم بها لجان الدراسات التابعة لقطاع تقييس الاتصالات. والمواد الواردة في هذه الملحقات يتم تحديثها باستمرار، ويمكن الاطلاع عليها في الموقع التالي على شبكة الويب: www.itu.int/ITU-T.

وفي الختام، ينبغي الإشارة إلى أن قطاع تقييس الاتصالات يطبق منهاجاً استشرافياً - ليس فقط فيما يتعلق بالتكنولوجيات القائمة على بروتوكول الإنترنت، بل أيضاً في تلبية احتياجات قطاعات كثيرة مختلفة في صناعة الاتصالات تتفاوت فيها متطلبات الأمن بشكل كبير. ويبين هذا الكتيب كيف أن توصيات قطاع تقييس الاتصالات تتضمن حلولاً جاهزة يمكن تطبيقها على الأنظمة والمعمارية العامة بل أيضاً على الأنظمة والتطبيقات الخاصة - وهي مطبقة عالمياً من خلال الشبكات ووكالات تقديم الخدمات.

1 نطاق الكتيب

يتضمن هذا الكتيب نظرة عامة على الأمن في الاتصالات وتكنولوجيا المعلومات، ويستعرض القضايا العملية ويوضح كيف يتعامل قطاع تقييس الاتصالات في الاتحاد مع جوانب الأمن المختلفة في التطبيقات المستخدمة في الوقت الحاضر. ويتسم الكتيب بطابع تعليمي: فهو يجمع المواد المتعلقة بالأمن الواردة في توصيات قطاع تقييس الاتصالات في مكان واحد، ويشرح العلاقات فيما بينها. ولا يشمل الكتيب، في طبعته الأولى هذه، جميع جوانب الأمن ولا سيما التي لا تتصل بالتيسر - حيث يتوفر لقطاع تقييس الاتصالات الكثير منها - أو الأضرار البيئية - وهو مجال يعمل فيه القطاع بنشاط. وفضلاً عن ذلك، تستند الجوانب الواردة فيه إلى الأعمال التي أنجزت بالفعل، وليس إلى ما هو جاري تنفيذه - وهي جوانب ستتناولها الطبعات المقبلة من هذا الكتيب.

وهذا الدليل موجه إلى المهندسين ومدراء المنتجات والطلاب والأكاديميين، وكذلك إلى الهيئات التنظيمية التي تحرص على فهم القضايا المتصلة بالأمن على نحو أفضل في التطبيقات العملية.

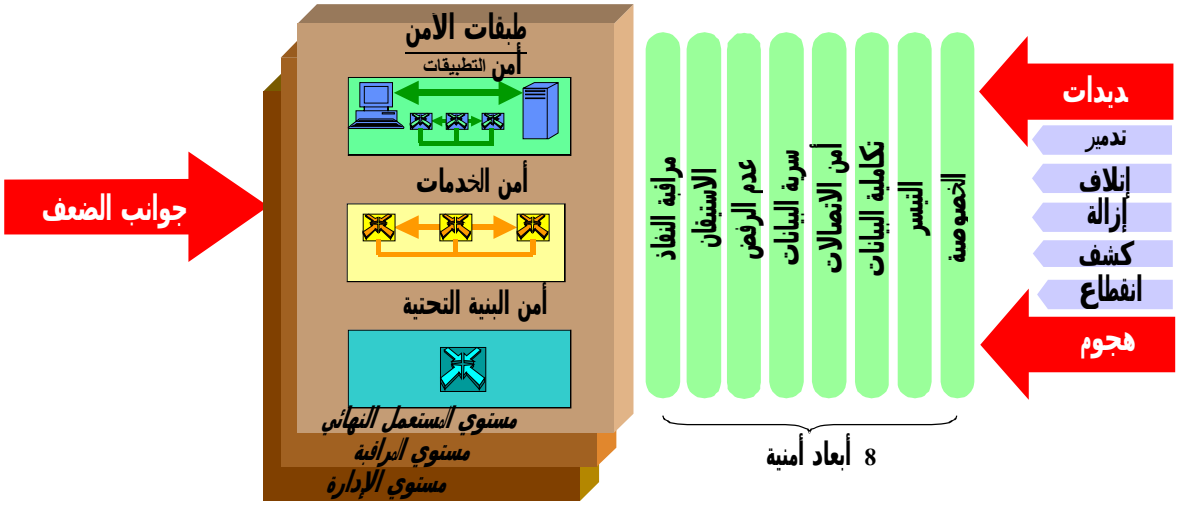
2 معمارية الأمن الأساسية وأبعادها

تتضمن التوصية X.805 تعريف إطار وأبعاد المعمارية اللازمة لتحقيق الأمن من طرف إلى طرف في التطبيقات الموزعة. وتنطبق المبادئ العامة والتعاريف على جميع التطبيقات، على الرغم من أن تفاصيل التهديدات وجوانب الضعف وتدابير التغلب عليها أو منع حدوثها تتفاوت تبعاً لاحتياجات التطبيق.

وتعرف معمارية الأمن على أساس مفهومين رئيسيين، هما الطبقات والمستويات. وتتناول طبقات الأمن الشروط التي تطبق على عناصر الشبكة والأنظمة التي تشكل شبكة الاتصال من طرف إلى طرف. ويعتمد ذلك على منهج تراتبي في تقسيم المتطلبات عبر الطبقات حتى يمكن تحقيق الأمن من طرف إلى طرف بواسطة البناء على كل طبقة. وهذه الطبقات الثلاث هي طبقة البنية التحتية، وطبقة الخدمات، وطبقة التطبيقات. ومن بين مزايا تعريف الطبقات أنه يسمح بإعادة الاستخدام عبر تطبيقات مختلفة عند توفير أمن 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 تحديد طرق التسيير، والبدالات، والمخدمات، وكذلك وصلات التوصيل فيما بينها. وتتناول طبقة الخدمات أمن خدمات الشبكة التي تقدم إلى الزبائن. وتتراوح هذه الخدمات بين مرافق التوصيل الأساسية مثل خدمات الخطوط المؤجرة وخدمات القيمة المضافة مثل التبادل الفوري للرسائل. أما طبقة التطبيق فتوفر متطلبات التطبيقات القائمة على الشبكة التي يستخدمها الزبائن. وقد تكون هذه التطبيقات بسيطة مثل البريد الإلكتروني أو متطورة مثل التطبيقات المرئية المشتركة التي تستخدم فيها تقنيات متطورة للنقل بالفيديو في استكشاف النفط أو تصميم السيارات، وما إلى ذلك.

ويتناول المحور الثاني للإطار العام أمن الأنشطة التي يجري أداؤها داخل الشبكة، ويتضمن تعريف ثلاثة مستويات للأمن تمثل ثلاثة أنواع من الأنشطة المحمية التي تجري على شبكة، وهي: (1) مستوى الإدارة، (2) ومستوى المراقبة، (3) ومستوى المستعمل النهائي. وتتناول مستويات الأمن هذه حاجات الأمن المحددة المرتبطة بأنشطة إدارة الشبكة، أو مراقبة الشبكة أو أنشطة التشوير، وأنشطة المستعمل النهائي المترتبة عليها. ويتعلق مستوى الإدارة، الذي يناقشه القسم 4.6 بمزيد من التفاصيل، بأنشطة العمليات والإدارة والصيانة وتوفير الخدمات، مثل توفير الخدمات اللازمة للمستعمل أو للشبكة، وما إلى ذلك. ويرتبط مستوى المراقبة بجوانب التشوير لإقامة (وتعديل) الاتصالات التي تتم من طرف إلى طرف من خلال الشبكة، بغض النظر عن الوسط والتكنولوجيا المستخدمة في الشبكة. ويتناول مستوى المستعمل النهائي أمن النفاذ واستعمال الزبائن للشبكة، وكذلك حماية تدفق بيانات المستعمل النهائي.

وباعتبار أن طبقات الأمن ومستويات الأمن محوران (3 مستويات أمن و 3 طبقات أمن)، يعرف الإطار أيضاً ثمانية أبعاد مصممة لتناول أمن الشبكة. ويجري تعريف هذه الأبعاد في الأقسام التالية. وتطبق هذه الأبعاد، من منظور معماري، على كل خلية مصفوفة 3 × 3 مشكلة بين الطبقات والمستويات حتى يمكن تحديد التدابير المضادة الملائمة. ويبين الشكل 1 مستويات وطبقات وأبعاد الأمن لمعمارية الأمن. ويبين القسم 4.6 بشأن مستوى إدارة كيفية تناول توصيات قطاع تقييس الاتصالات الخلايا الثلاث لمصفوفة 3 × 3 لمستوى الإدارة.



الشكل 1
عناصر معمارية الأمن في التوصية X.805 الصادرة عن قطاع تقييس الاتصالات

1.2 الخصوصية وسرية البيانات

يعد مفهوم الخصوصية من الدوافع الأساسية للأمن. وتفهم الخصوصية عادة على أ ا حق الأفراد في التحكم في المعلومات التي تتعلق م وتحديد من يجوز لهم جمع هذه المعلومات وتخزينها، ومن لهم الحق في إفشائها ولمن يتم إفشاؤها. وبناء على ذلك، ترتبط الخصوصية أيضاً ببعض الوسائل التقنية (مثل التجفير) لضمان عدم الكشف عن هذه المعلومات لغير الأطراف المقصودين، بحيث يمكن للأطراف المخول لهم فقط تفسير المحتوى المتبادل بينهم.

وبصورة عامة، يستخدم كل من مصطلح الخصوصية (privacy) والسرية (confidentiality) بنفس المعنى، ولكن ينبغي ملاحظة أن التوصية ITU-T X.805 تفرق بين الخصوصية وسرية البيانات، فالأولى تتعلق بحماية الخصوصية فيما يتعلق وية المستعملين والأنشطة التي يقومون ا (مثل الشراء المباشر عبر الإنترنت ومواقع الإنترنت التي يترددون عليها، وما إلى ذلك)، أما الثانية فتتعلق بالحماية من نفاذ غير المخول لهم إلى مضمون البيانات. ويعد التجفير وقوائم مراقبة النفاذ وتصاريح الاطلاع على الملفات من بين الطرق التي تستخدم أحياناً لضمان سرية البيانات.

ويشار إلى مصطلح الخصوصية في العديد من التوصيات الصادرة عن قطاع تقييس الاتصالات، بما في ذلك التوصيات F.115 وH.235 وJ.160 وQ.1531 وX.800 وX.805.

2.2 الاستيفان

الاستيقان هو توفير ما يثبت أن هوية الكيان الطالب حقيقية. ولا تشمل الكيانات هنا المستعملين من البشر فحسب، بل أيضاً الأجهزة والخدمات والتطبيقات. ويوفر الاستيقان أيضاً ضماناً بعدم محاولة التنكر من جانب أي كيان، أو الرد بلا مسوغ على اتصالات سابقة. ويوجد نوعان من الاستيقان: الاستيقان من أن البيانات أصلية (أي الاستيقان المطلوب في حالة طلب التوصيل) والاستيقان من الكيان المناظر (أي الاستيقان في حالة عدم طلب التوصيل). وينبغي للشبكة أن تضمن أن يجري تبادل البيانات مع الكيان المناظر المبين في العنوان (وليس مع كيان يحاول التنكر أو الرد على اتصال سابق) ومن أن مصدر البيانات هو المصدر المطلوب. ويقوم الاستيقان عادة على تعريف الهوية. وينبغي أن تحمي الشبكة المعلومات المستخدمة في التعريف والاستيقان والإذن بالدخول.

ويشار إلى مصطلح الاستيقان في العديد من التوصيات الصادرة عن قطاع تقييس الاتصالات، بما في ذلك التوصيات: F.500 وF.851 وF.852 وH.235 وJ.160 وJ.93 وJ.95 وM.60 وX.217 وX.217-Bis وX.509 وX.800 وX.805 وX.811.

3.2 سلامة البيانات

سلامة البيانات صفة تدل على أن البيانات لم يتم تغييرها بطريقة غير مشروعة. وبناء على ذلك، تعني سلامة البيانات أيضاً أن المعلومات محمية من التعديل أو الحذف أو الإضافة أو الاستنساخ دون تفويض بذلك، وتتضمن ما يدل على حدوث هذه الأنشطة بدون تفويض.

ويشار إلى مصطلح سلامة البيانات في العديد من التوصيات الصادرة عن قطاع تقييس الاتصالات، بما في ذلك التوصيات H.235 وJ.160 وJ.93 وJ.95 وQ.1290 و Q.1531 وX.800 وX.815.

4.2 عدم التنصل

ضمان عدم التنصل هو القدرة على الحيلولة دون إنكار المستعملين فيما بعد أ م قاموا بتصرفات معينة. وتشمل هذه التصرفات ابتكار محتوى والإرسال والاستقبال والتسليم، مثل إرسال أو استقبال رسائل أو إجراء أو استقبال نداءات والمشاركة في مؤتمرات سمعية وفيديوية، وما إلى ذلك.

وتوفر متطلبات عدم التنصل دليلاً لا يمكن تزويره على إرسال و/أو استقبال بيانات، للحيلولة دون تنصل المرسل من رسالة مشروعة أو إنكار المستقبل لاستقبالها. ويمكن للشبكة أن توفر أياً من الشكلين التاليين أو كليهما: تزويد مستقبل البيانات بدليل على أصل البيانات يحميه من محاولة المرسل إنكار إرسال هذه البيانات أو محتويا ا؛ أو تزويد المرسل بما يثبت تسليم البيانات بحيث لا يمكن للمستقبل، فيما بعد، إنكار استقباله للبيانات أو محتويا ا.

ويشار إلى مصطلح عدم التنصل في العديد من التوصيات الصادرة عن قطاع تقييس الاتصالات، بما في ذلك التوصيات F.400 وF.435 وF.440 وJ.160 وJ.93 وJ.95 وM.60 وT.411 وX.400 وX.805 وX.813 وX.843.

5.2 الأبعاد الأخرى المـُعرفة في التوصية X.805

بالإضافة إلى الخصوصية وسرية البيانات والاستيقان وسلامة البيانات وعدم التنصل، تتضمن التوصية ITU-T X.805 تعريف ثلاثة أبعاد أخرى للأمن، هي: مراقبة النفاذ والاتصالات والتيسر.

والبعد الخاص بأمن *مراقبة النفاذ* يحمي من استخدام موارد الشبكة بدون تخويل، ويسمح فقط للأشخاص أو الأجهزة المخولة بالنفاذ إلى عناصر الشبكة، والمعلومات المخزنة، وتدفقات المعلومات والخدمات والتطبيقات. وقد جاء تعريف مراقبة النفاذ في التوصية ITU-T X.810، القسم 3.6 وفي التوصية ITU-T X.812. وهذا الأمر يتعلق بالاستيقان وإن كان خارج نطاقه.

ويعد البعد الخاص بأمن *الاتصالات* من الأبعاد الجديدة التي جاء تعريفها في التوصية ITU-T X.805 وهو يضمن أن المعلومات تتدفق فقط بين نقاط طرفية مخولة. ويتناول هذا البعد تدابير لمراقبة تدفق الحركة في شبكة لمنع تحويل الحركة واعتراضها.

ويضمن البعد الخاص بأمن *التيسر* عدم رفض النفاذ المخول إلى عناصر الشبكة والمعلومات المخزنة وتدفقات المعلومات والخدمات والتطبيقات نتيجة لانقطاع الشبكة. وتشمل هذه الفئة الحلول الخاصة بإعادة الشبكة إلى ما كانت عليه قبل وقوع الكوارث.

3 جوانب الضعف والتهديدات والمخاطر

مع التركيز الهائل على تنفيذ أفضل حلول تكنولوجيا المعلومات أو تحديد أحدث وأفضل تطبيقات الويب والمخدمات وقواعد البيانات التي تناسب أهداف المنظمة، كانت حماية المعلومات التي تحتفظ ا هذه الموجودات تأتي في المرتبة الثانية من الأولوية، في أغلب الأحيان. وقد يساور شركات كثيرة ظن خاطئ بأ ا لم تتعرض لأي هجوم وبالتالي فإن التهديد غير قائم.

وتتمتع الهيئات المعنية بوضع المعايير بقدرة فريدة على معالجة جوانب الضعف في أمن البروتوكولات، كما تقع عليها هذه المسؤولية. وتوجد إجراءات فورية وبسيطة نسبياً يمكن أن تتخذها الهيئات المعنية بوضع المعايير لتحسين أمن جميع البروتوكولات التي يجري تقييمها حالياً.

وترجع *جوانب الضعف في الأمن* إلى وجود خلل أو ضعف في تصميم النظام أو تنفيذه أو تشغيله يمكن استغلاله في انتهاك أمن النظام (RFC 2828). وجوانب الضعف في الأمن ليست خطراً أو تهديداً أو هجوماً.

وتندرج جوانب الضعف تحت أربعة فئات. إذ تنشأ جوانب الضعف في *نموذج التهديد* من صعوبة التنبؤ بالتهديدات في المستقبل (مثل نظام التشوير رقم 7). وتأتي جوانب الضعف في *التصميم والمواصفات* من وقوع أخطاء أو سهو في تصميم بروتوكول ما يجعله ينطوي على جوانب ضعف (مثل WEP in IEEE 802.11b a.k.a. WiFi). أما جوانب الضعف في *التنفيذ* فترجع إلى حدوث أخطاء في تنفيذ بروتوكول. وأخيراً، تنشأ جوانب الضعف في التشغيل والتشكيل من الاستخدام غير السليم للخيارات في التنفيذ أو ضعف في سياسات التنفيذ (مثل عدم استخدام التجفير في شبكة WiFi، أو اختيار مدير الشبكة لتجفير رتل ضعيف).

وطبقاً للتوصية X.800 يتعرض *الأمن للتهديد* عندما يكون هناك انتهاك محتمل للأمن، وقد يكون هذا التهديد نشيطاً (عندما يمكن تغيير حالة النظام) أو سلبياً (كشف غير مخول لمعلومات دون تغيير حالة النظام). ويعد التنكر في شكل كيان مخول ورفض الخدمة من الأمثلة على وجود تهديدات نشيطة، أما التنصت لسرقة كلمة سر واضحة فهو من أمثال التهديدات السلبية. ويمكن أن تأتي التهديدات من هواة العبث أو من الإرهابيين أو المخربين أو من الجريمة المنظمة أو من جانب الدولة، إلا أن عدداً كبيراً من حالات التهديد يكون مصدره أشخاص من داخل المنظمة.

ينشأ *خطر الأمن* عندما تقترن جوانب الضعف في الأمن بوجود تهديد للأمن. فمثلاً، يمكن أن يتطور وجود خطأ خفي في تطبيق نظام التشغيل (أي وجود نقطة ضعف) عندما يقترن بمعرفة أحد هواة العبث وتوافر الأدوات الملائمة والقدرة على النفاذ (أي وجود تهديد) إلى هجوم على مخدم للويب. ويكون من نتائج وجود مخاطر على الأمن ضياع البيانات وإتلافها، وضياع الخصوصية، والتعرض للاحتيال، وتوقف الخدمة وفقدان ثقة الجمهور.

وبينما تتغير التهديدات، توجد جوانب الضعف في الأمن طوال حياة بروتوكول. وفي حالة البروتوكولات الخاضعة لمعايير التقييس، قد تكون مخاطر الأمن التي يتعرض لها البروتوكول كبيرة جداً وعالمية في نطاقها. ولذلك، فمن المهم إدراك جوانب الضعف في البروتوكولات وتعريفها.

4 مقتضيات إطار الأمن

ترجع مقتضيات إطار الأمن في الشبكة العادية لأسباب 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 الأعمال الإرهابية).
- تطالب السلطات الحكومية بتوافر الأمن بموجب توجيهات وتشريعات، لضمان تيسر الخدمات والمنافسة العادلة وحماية الخصوصية.
- تحتاج شركات تشغيل الشبكات وشركات تقديم الخدمات نفسها إلى الأمن لتأمين عمليا ا ومصالحها التجارية، وتلبية التزاما ا تجاه الزبائن والجمهور.

وينبغي أن تقوم مقتضيات الأمن في الشبكات وخدمات الاتصالات على أساس معايير أمن متفق عليها دولياً، لأ ا تزيد من القدرة على التشغيل البيني كما تساعد على تجنب الازدواجية في الجهود. وقد يكون توفير واستخدام خدمات وآليات الأمن باهظة التكاليف مقارنة بقيمة المعاملات المطلوب حمايتها. ولذلك لا بد من الموازنة بين تكاليف تدابير الأمن والآثار المالية المحتملة لانتهاك الأمن. ولهذا فمن المهم توافر القدرة على توفير الأمن قياساً على الخدمات المطلوب حمايتها. وينبغي توفير خدمات وآليات الأمن المستخدمة بطريقة تسمح بذلك. ونتيجة لضخامة عدد العناصر التي يمكن الربط بينها لتوفير خصائص الأمن، فمن المستصوب أن تغطي برامج الأمن مجموعة كبيرة من خدمات شبكات الاتصالات.

ويساعد التقييس على تيسير إعادة استخدام الحلول والمنتجات، وهذا يعني أنه من الممكن توفير الأمن بشكل أسرع وبتكاليف أقل.

ومن الفوائد المهمة للحلول الخاضعة لمعايير التقييس سواء بالنسبة للبائعين أو المستعملين تحقيق وفورات الحجم عند تطوير المنتجات وتوفير إمكانية التشغيل البيني للمكونات في شبكات الاتصالات فيما يتعلق بالأمن.

وتتعلق خدمات وآليات الأمن التي يمكن توفيرها لشبكات الاتصالات وشركات تقديم الخدمات بالحماية من هجوم خبيث مثل إنكار الخدمة، أو التنصت، أو الخداع، أو التلاعب بالرسائل (التعديل، أو التأخير، أو الإلغاء، أو الإضافة، أو إعادة الترحيل، أو إعادة التسيير، أو إعادة ترتيب الرسائل) أو التنصل أو الغش. وتشمل الحماية الوقاية واكتشاف وقوع الهجمات وإعادة الأمور إلى ما كانت عليه، وتدابير الحيلولة دون توقف الخدمة نتيجة للظروف الطبيعية (مثل رداءة الطقس) وكذلك إدارة المعلومات المتعلقة بالأمن. وينبغي وضع الأحكام التي تسمح بالاعتراض القانوني بناء على طلب سلطات قانونية مخولة.

5 البنية التحتية للمفاتيح العمومية والإدارة المتميزة بموجب التوصية X.509

توفر البنية التحتية للمفاتيح العمومية (PKI) بموجب التوصية X.509 معياراً لاستيقان قوي قائم على أساس شهادات المفاتيح العمومية وسلطات إصدار الشهادات. وتوفر البنية التحتية للمفاتيح العمومية طريقة تدريجية للاستيقان من رسائل الأطراف المتراسلة. والتكنولوجيا الأساسية المطبقة في مجال البنية التحتية للمفاتيح العمومية هي تجفير المفاتيح العمومية، ولذلك فسوف نبدأ بشرحها. وبالإضافة إلى البنية التحتية للمفاتيح العمومية، تتناول التوصية X.509 أيضاً البنية التحتية للإدارة المتميزة (PMI)، وتتضمن تعريفاً لمعيار للاستيقان القوي يقوم على أساس شهادات الخواص وسلطات تحديد الخواص. وتستخدم البنية التحتية للإدارة المتميزة للتأكد من حقوق ومزايا المستعملين. ويتضمن الشكل 2 مكونات البنية التحتية للمفاتيح العمومية والبنية التحتية للإدارة المتميزة.

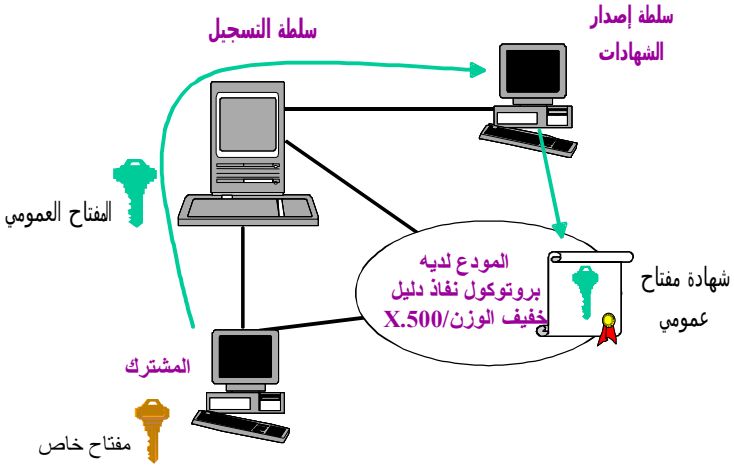
1.5 تجفير المفاتيح السرية والعمومية

يشير *التجفير التناظري* (*أو المفتاح السري*) إلى نظام التجفير الذي تكون فيه مفاتيح التشفير ومفاتيح فك الشفرة هي نفس المفاتيح، كما يوضح الشكل 3 (أ). وتقوم أنظمة التجفير التناظرية على أن تكون الترتيبات الأولية لأفراد يتقاسمون التحكم في مفتاح سري واحد. وينبغي أن يكون المفتاح موزعاً على الأفراد عبر وسائل آمنة لأن معرفة مفتاح التشفير تعني معرفة مفتاح فك الشفرة والعكس بالعكس.

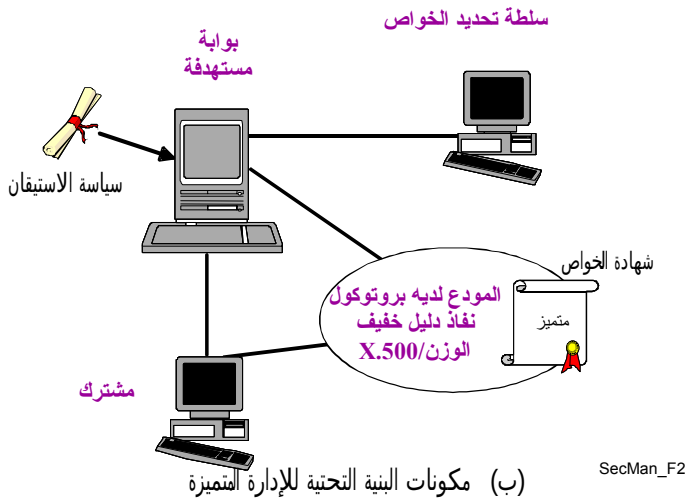
ويقوم نظام التجفير اللاتناظري (أو المفتاح العمومي) على زوج من المفاتيح كما هو مبين في الشكل 3 (ب) - مفتاح عمومي ومفتاح خاص. ويكون أحد المفتاحين عمومياً والإبقاء على المفتاح الآخر سرياً. ويختلف المفتاح العمومي عن المفتاح الخاص، على الرغم من الترابط الرياضي فيما بينهما، وليست هناك طريقة معروفة لاشتقاق المفتاح الخاص من المفتاح العمومي. وتوزع المفاتيح العمومية على نطاق واسع؛ ولكن المفتاح الخاص يبقى سرياً على الدوام (كأن يوضع على بطاقة ذكية أو في شكل رمز مميز، وقد يوضع في المستقبل أيضاً على جهاز رقمي شخصي أو على هاتف متنقل). وعموماً، فلإرسال بيانات سرية مجفّرة إلى شخص آخر، يتم تشفير البيانات بالمفتاح العمومي للمستقبل، ويقوم مستقبل البيانات بفك الشفرة بمفتاحه الخاص المتناظر. ولإرسال بيانات يمكن الاستيقان من صحتها لشخص ما، يقوم المرسل بتشفير البيانات بمفتاحه الخاص، ويقوم المستقبل بالاستيقان من البيانات بالمفتاح العمومي المتناظر الذي استخدمه المرسل. ومع ذلك، يعاني التجفير اللاتناظري المستخدم هذه الطريقة من عيبين. الأول، أن تجفير المفتاح العمومي يعد مكلفاً من حيث الوقت الذي تستغرقه عملية الحوسبة، وبالتالي فمن غير المُجدي تجفير رسائل كاملة باستخدام التجفير اللاتناظري. والثاني، أنه ليس من الممكن تسيير الرسائل إلى مستقبليها إذا كانت الرسالة بأكملها مجفرة، نظراً لأن العقد الوسيطة لن تتمكن من تحديد من هو المستقبل. ولهذا لا يستخدم التجفير اللاتناظري إلا في تجفير أجزاء صغيرة من الرسائل. وعندما تكون السرية مطلوبة، يتم تجفير الرسالة باستخدام التجفير التناظري التقليدي، ويتم تجفير المفتاح التناظري بالطريقة اللاتناظرية باستخدام المفتاح العمومي للمستقبل. وعندما يكون الاستيقان مطلوباً، تفرم الرسالة باستخدام وظيفة فرم آمنة في اتجاه واحد مثل خوارزمية الفرم الآمنة رقم (SHA1) أو

ملخص رسالة رقم 5 (MD5) ويتم تجفير البتات الناتجة وهي 160 أو 128 بتة لا تناظرياً باستخدام المفتاح الخاص للمرسل ويرفق بالرسالة (التي ترسل بوضوح) قبل النقل. وهذا ما يعرف بالتوقيع الرقمي - وهو من الخواص المهمة للتجارة الإلكترونية.

ويعتمد تجفير المفتاح العمومي على الأشخاص الذين تكون في حوز م المفاتيح العمومية الصحيحة التي يستعملها أقرا م حاملي المفاتيح الخاصة. فإذا كان بوب (Bob) يعتقد خطأ أنه يمتلك المفتاح العمومي لأليس (Alice) ، بينما في الحقيقة يرتبط المفتاح العمومي بالمفتاح الخاص الذي تحتفظ به جين (Jane)، فسوف يعتقد بوب أن الرسائل التي وقعتها جين رقمياً جاءت من أليس (الأمر الذي يسمح لجين أن تتنكر في شخصية أليس). وفضلاً عن ذلك، فإذا رغب بوب في إرسال رسالة سرية إلى أليس، فسوف يكون بوسع جين اعتراضها وفك شفرة الرسالة، بينما لن تتمكن أليس من قراء ا. ولذلك فمن المهم جداً أن يجد الأشخاص طريقة للتحقق من المالك القانوني للمفتاح العمومي.

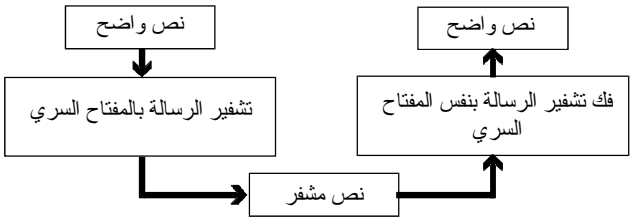


(أ) مكونات البنية التحتية للمفتاح العمومي



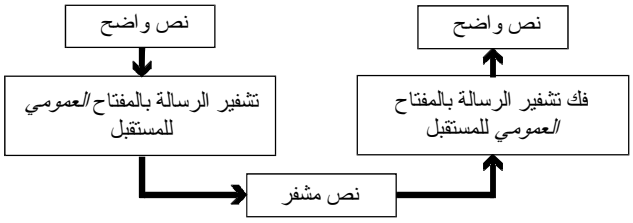
(ب) مكونات البنية التحتية للإدارة المتميزة

الشكل 2
مكونات البنية التحتية للمفاتيح العمومية والبنية التحتية للإدارة المتميزة



- يتقاسم الطرفان مفتاحاً سرياً واحداً
- مشكلة: تبادل المفاتيح بسرية كاملة صعب
- أفضل مثال معروف: معيار تجفير البيانات(DES)

(أ) تجفير المفتاح السري (تناظري)



- يوجد لدى كل مشارك
- مفتاح خاص لا يتقاسمه أحد، زائداً
- مفتاح عمومي معروف للجميع
- المشكلة: أبطأ من تجفير مفتاح سري
- أفضل مثال معروف: خوارزمية ريفست وأدلمان وشامير (RSA)

(ب) تجفير مفتاح عمومي (لا تناظري)

SecMan_F3

الشكل 3
توضيح عمليات تجفير مفتاح تناظري (أو خاص) ولا تناظري (أو عمومي) والتأكيد على الخصائص

2.5 شهادات المفاتيح العمومية

شهادة المفتاح العمومي (التي تسمى أحياناً "الشهادة الرقمية") هي إحدى طرق التحقق من مالك زوج مفاتيح لا تناظرية. وتربط شهادة المفتاح العمومي المفتاح باسم مالكه بقوة، وهو موقّع رقمياً من قبل سلطة موثوق ا تشهد على هذا الربط. وتعرف هذه السلطة بسلطة إصدار الشهادات (CA). وتحدد التوصية X.509 نسق المعيار المعترف به دولياً لشهادات المفاتيح العمومية. وباختصار، تتألف شهادة المفتاح العمومي بموجب التوصية X.509 من مفتاح عمومي ومعرف للخوارزمية اللا تناظرية التي يستخدم معها المفتاح، واسم مالك زوج المفاتيح واسم سلطة إصدار الشهادة التي تشهد ذه الملكية والرقم المسلسل ومدة صلاحية الشهادة ورقم صيغة التوصية X.509 الدال على أن الشهادة مطابقة لسياسة إصدار الشهادات التي تطبقها سلطة إصدار الشهادات، ومجموعة اختيارية الات حفظ المعلومات الدالة على السياسة التي تطبقها سلطة إصدار الشهادات. ثم يتم توقيع الشهادة بأكملها رقمياً باستخدام مفتاح خاص تملكه سلطة إصدار الشهادات. ويمكن الآن نشر الشهادة التي تنص عليها التوصية X.509 على نطاق واسع، كأن تنشر على موقع الويب، وفي دليل بروتوكول نفاذ دليل خفيف الوزن (LDAP) أو في بطاقة V المرفقة برسائل البريد الإلكتروني ويضمن توقيع سلطة إصدار الشهادات أن محتويا ا لا يمكن العبث ا دون معرفة.

ومن الواضح أنه للتحقق من سلامة شهادة المفتاح العمومي لأي مستعمل، يحتاج الشخص إلى النفاذ إلى مفتاح عمومي صالح لسلطة إصدار الشهادات التي أصدرت شهادة المستعمل وذلك للتأكد من التوقيع على شهادة المستعمل. ويجوز لسلطة إصدار الشهادات أن تشهد سلطة أخرى لإصدار الشهادات (تكون عادة أعلى منها) على مفتاحها العمومي بحيث يصبح التحقق من المفاتيح العمومية تكرارياً، ونحن نتحرك على طول سلسلة الشهادات. وينبغي أن تنتهي هذه السلسلة في مكان ما، وذلك عندما نصبح أمام شهادة موقعة ذاتياً من جانب سلطة إصدار الشهادات تكون بمثابة "جذر الثقة". ويتم توزيع جذر المفاتيح العمومية الذي تتحكم فيه سلطة إصدار الشهادات باعتباره شهادة موقعة ذاتياً (يشهد فيها جذر سلطة إصدار الشهادات بأن هذا هو مفتاحها العمومي). ويسمح التوقيع لنا بالتحقق من

أن المفتاح واسم سلطة إصدار الشهادات لم يتم التلاعب فيهما منذ وضِعت الشهادة. ومع ذلك، لا يمكننا أخذ اسم سلطة إصدار الشهادات المتضمنة في شهادة التوقيع الذاتي بالمعنى الظاهري، نظراً لأن سلطة إصدار الشهادات قد أدرجت الاسم في الشهادة بنفسها. وبالتالي، يكون المكون الحرج للبنية التحتية للمفتاح العمومي هو التوزيع الآمن لجذر المفاتيح العمومية الذي وضعته سلطة إصدار الشهادات (باعتبارها شهادات موقعة ذاتياً)، بطريقة تضمن لنا أن المفتاح العمومي ينتمي حقيقةً إلى جذر سلطة إصدار شهادات المبين في الشهادة الموقعة ذاتياً. وبدون ذلك، لا يمكننا ضمان عدم تنكر شخص آخر وانتحال جذر سلطة إصدار الشهادات.

3.5 البنى التحتية للمفاتيح العمومية

الغرض الرئيسي من البنية التحتية للمفاتيح العمومية هو إصدار شهادات المفاتيح العمومية وإدار ا، بما في ذلك الشهادات الموقعة ذاتياً لجذر سلطة إصدار الشهادات. وتشمل إدارة المفاتيح ابتكار زوج مفاتيح، وإنشاء شهادات المفاتيح العمومية، وإبطال شهادات المفاتيح العمومية (مثلما يحدث عندما يتعرض المفتاح الخاص للمستعمل إلى خطر) وتخزين وحفظ المفاتيح والشهادات في الأرشيف، وتدميرها عندما ينقضي أجل استعمالها. وتعمل كل سلطة من سلطات إصدار الشهادات طبقاً موعة من السياسات، ويحدد المعيار المنصوص عليه في التوصية X.509 آليات توزيع ومجالات تمديد الشهادات التي تصدرها سلطة إصدار الشهادات. وتكون قواعد وإجراءات السياسات التي تتبعها سلطة إصدار الشهادات مبينة عادة في سياسة الشهادة (CP) وفي إعلان ممارسة إصدار الشهادات (CPS)، وهما من الوثائق التي تنشرها سلطة إصدار الشهادات. وتساعد هذه الوثائق في ضمان الأساس المشترك لتقييم درجة الثقة التي يمكن أن نضعها في شهادات المفاتيح العمومية التي تصدرها سلطات إصدار الشهادات، على المستوى الدولي وعبر القطاعات. وتوفر لنا هذه الوثائق أيضاً الإطار القانوني الضروري لبناء الثقة فيما بين المنظمات (أو جزء منه) كما أ ا تضع حدوداً لاستخدام الشهادات الصادرة.

وينبغي ملاحظة أنه من أجل الاستيقان من استخدام شهادات المفاتيح العمومية، يشترط أن تقدم النقاط الطرفية توقيعات رقمية باستخدام قيمة المفتاح الخاص المرتبط ا. وتبادل شهادات المفاتيح العمومية لا يوفر بمفرده الحماية من هجمات فرد يكون موقعه بين الطرفين.

4.5 البنية التحتية للإدارة المتميزة

حددت التوصية ITU-T X.509 في صيغتها الأولى العناصر الأساسية للبنى التحتية للمفاتيح العمومية. ويشمل ذلك تعريف شهادات المفاتيح العمومية. ويحتوي التنقيح الذي تمت الموافقة عليه في سنة 2000 تعزيزاً مهماً لشهادات الخواص وإطار البنية التحتية للإدارة المتميزة. وتسمح الآليات المحددة بتحديد امتيازات نفاذ للمستعملين في بيئة بائعين متعددين وتطبيقات متعددة.

وهناك مفاهيم مماثلة بين البنية التحتية للمفاتيح العمومية والبنية التحتية للإدارة المتميزة، إلا أن الأولى تتناول التخويل بينما تركز الثانية على الاستيقان. ويوضح الشكل 2 والجدول 1 التماثل بين البنيتين التحتيتين.

الجدول 1

مقارنة بين خصائص البنية التحتية للإدارة المتميزة والبنية التحتية للمفاتيح العمومية

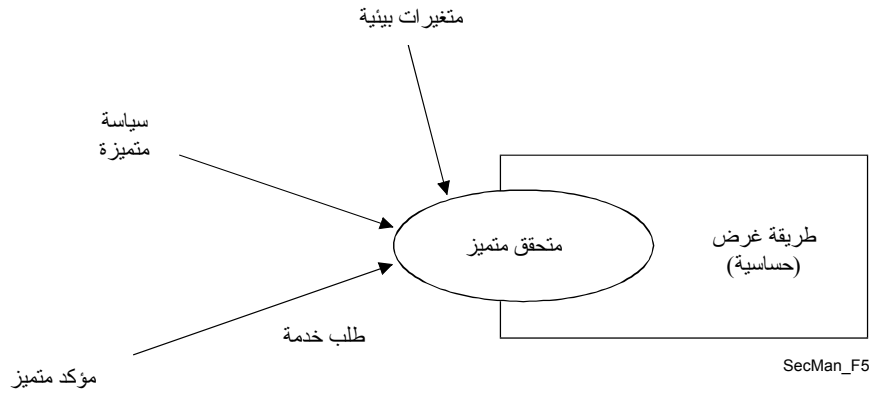
البنية التحتية للإدارة المتميزة	البنية التحتية للمفاتيح العمومية
مصدر السلطة (SoA)	جذر سلطة إصدار الشهادات (مرتكز الثقة)
سلطة تحديد الخواص (AA)	سلطة إصدار شهادات
شهادة الخواص	شهادة المفتاح العمومي
قائمة إبطال شهادات الخواص	قائمة إبطال الشهادات
قائمة إبطال سلطات البنية التحتية للإدارة المتميزة	قائمة إبطال سلطات البنية التحتية للمفاتيح العمومية

والغرض من تعيين امتيازات للمستعملين هو ضمان اتباعهم لسياسة الأمن المقررة التي يضعها مصدر سلطة. وترتبط المعلومات المتعلقة بالسياسة باسم المستعمل في شهادة الخواص، وتتألف من عدد من العناصر المبينة في الشكل 4.

الصيغة
صاحب الشهادة
المُصدر
التوقيع (شفرة تعريف خوارزمية)
الرقم المسلسل للشهادة
مدة الصلاحية
الخواص
شفرة تعريف جهة الإصدار
التمديدات

الشكل 4
هيكل شهادة الخواص بموجب التوصية X.509

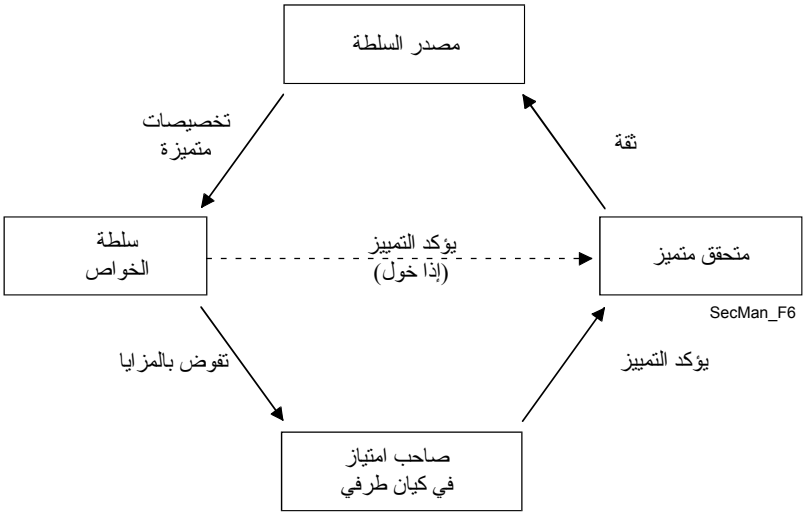
توجد خمسة مكونات لمراقبة البنية التحتية للإدارة المتميزة الواردة في التوصية X.509، مؤكد متميز ومتحقق متميز وطريقة الغرض[1] وسياسة متميزة ومتغيرات بيئية (انظر الشكل 5). وتمكّن التقنيات المتحقق المتميز من مراقبة النفاذ إلى طريقة الغرض بواسطة المؤكد المتميز طبقاً لسياسة متميزة.



الشكل 5
نموذج مراقبة البنية التحتية للإدارة المتميزة بموجب التوصية X.509 الصادرة عن قطاع تقييس الاتصالات

وعندما يكون تفويض التميز ضرورياً من أجل التنفيذ، توجد أربعة مكونات لنموذج التفويض للبنية التحتية للإدارة المتميزة الواردة كما هو مبين في التوصية X.509: متحقق متميز، ومصدر السلطة، وسلطة الخواص، والمؤكد المتميز (انظر الشكل 6).

[1] تعرف طريقة الغرض على أ ا عمل يمكن تنفيذه على مورد (مثلاً يمكن لنظام الملفات أن يقرأ ويكتب وينفذ طرق الأغراض).



الشكل 6

نموذج تفويض البنية التحتية للإدارة المتميزة بموجب التوصية X.509 الصادرة عن قطاع تقييس الاتصالات

وعمليات التنفيذ الحديثة لمخططات التخويل طبقاً لنموذج مراقبة النفاذ القائم على الدور تعتبر أن المستعمل له دور. وسياسة التخويل ترتبط با مجموعة من التصاريح الخاصة بالدور. وعند النفاذ إلى مصدر، يتم التأكد من دور المستعمل طبقاً للسياسة المطبقة قبل القيام بأي عمل. ويوضح تطبيق الوصفات الطبية الإلكترونية الواردة في القسم 2.5.6 استخدام نظام مراقبة النفاذ القائم على الدور (RBAC).

6 التطبيقات

تنتمي التطبيقات التي يتناولها هذا القسم إلى نوعين متميزين. يركز النوع الأول على تطبيقات المستعمل النهائي، مثل نقل الصوت باستعمال بروتوكول الإنترنت حيث تستخدم معمارية الشبكة ومكونا ا لتوفير تطبيق للمستعمل الطرفي كما هو مبين. ويناقش هذا القسم اعتبارات وحلول الأمن للمستويات الثلاثة التي تدعم تطبيقات متعددة الوسائط مع نقل الصوت باستعمال بروتوكول الإنترنت كحالة خاصة. وتطبيقات المستعمل النهائي الأخرى التي يناقشها هذا القسم هي نظام الاتصالات الكبلية باستعمال بروتوكول الإنترنت الذي يوفر الخدمات القائمة على بروتوكول الإنترنت في الوقت الحقيقي على شبكة كبلية، وإرسال الفاكسات. وتشمل التطبيقات غير المقصورة على صناعة الاتصالات الواردة هنا الرعاية الصحية الإلكترونية، ولا سيما نظام الوصفات الطبية الإلكترونية. ويركز النوع الثاني على تطبيقات إدارة الشبكة. ويعد الأمن من الاعتبارات المهمة لضمان جودة وسلامة الخدمات التي تقدمها الجهات المعنية بتقديم الخدمات. ولذلك، فمن الضروري أداء أنشطة الإدارة في وجود المزايا الملائمة والتفويض الملائم.

1.6 نقل الصوت باستعمال بروتوكول الإنترنت طبقاً للأنظمة المبينة في التوصية H.323

إن نقل الصوت باستعمال بروتوكول الإنترنت (VoIP)، المعروف أيضاً بالمهاتفة باستعمال بروتوكول الإنترنت، هو توفير الخدمات التي يتم توفيرها عادة عبر الشبكات الهاتفية العمومية المبدلة عن طريق شبكة تستخدم بروتوكول الإنترنت (وهي التي تقوم على أساسها الإنترنت أيضاً). وتشمل هذه الخدمات في المقام الأول الصوت بالإضافة إلى خدمات تكميلية مثل المؤتمرات الصوتية (التوصيل بين عدة أطراف) وإعادة تسيير النداءات، وخاصية انتظار النداء، وتحويل النداء، وخاصية استبقاء النداء للرد على نداء آخر ثم العودة، وخاصية التتبع، وغير ذلك من الخدمات الكثيرة الأخرى التي توفرها الشبكات الذكية، ومنها أيضاً بيانات النطاق الصوتي لبعض المستعملين. ويعد نقل الصوت باستعمال الإنترنت حالة خاصة لنقل الصوت باستعمال بروتوكول الإنترنت، وفيها يتم ترحيل حركة الصوت عبر الشبكة الأساسية العمومية للإنترنت.

وتعد التوصية H.323 توصية شاملة أصدرها قطاع تقييس الاتصالات لكي توفر أساساً لنقل الصوت والفيديو والبيانات عبر شبكات المناطق المحلية أو عبر الشبكات التي تقوم على بروتوكول الإنترنت، بما في ذلك الإنترنت، وهي لا توفر نوعية خدمة مضمونة. وتسود هذه الشبكات الحواسيب المكتبية للمؤسسات وتشمل نقاط إ اء توصيل الرزم

المبدلة/بروتوكول الإنترنت وتبديل العمل البيني لبروتوكول عبر إثرنت، والإثرنت السريعة وتكنولوجيا شبكة الحلقة الإذنة. ومع الامتثال للتوصية H.323، يمكن تحقيق التشغيل البيني لمنتجات وتطبيقات متعددة الوسائط من بائعين متعددين بما يسمح للمستعملين بالاتصال دون أن يساورهم قلق بشأن التوافق. وكانت التوصية H.323 هي أول بروتوكول لنقل الصوت باستعمال بروتوكول الإنترنت وتعتبر حجر الزاوية للمنتجات القائمة على شبكات المناطق المحلية للمستهلكين والمعاملات 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 ذات علاقة بتنفيذ خدمات تنظيم المؤتمرات متعددة الوسائط والقائمة على الرزم
- H.225.0 - تصف ثلاثة بروتوكولات تشوير (خوارزمية ريفست وأدلمان وشامير وتشوير نداء و"الملحق زاي")
- H.245 - بروتوكول مراقبة الوسائط المتعددة (مشتركة مع H.310 وH.323 وH.324)
- H.235 - الأمن في الأنظمة القائمة على التوصية H.245
- H.246 - التشغيل البيني مع الشبكات الهاتفية العمومية المبدلة
- H.450.x - الخدمات التكميلية
- H.460.x - تمديدات مختلفة للبروتوكول المنصوص عليه في التوصية H.323
- H.501 - بروتوكول للإدارة المتنقلة والاتصالات داخل الميدان وفيما بين الميادين
- H.510 - تنقل المستعملين والمطاريف والخدمات
- H.530 - مواصفات الأمن طبقاً للتوصية H.510

وقد وافق قطاع تقييس الاتصالات على الصيغة الأولى للمواصفات المبينة في التوصية H.323 في سنة 1996. وتمت الموافقة على الصيغة الثانية في يناير 1998، والصيغة الحالية هي الصيغة رقم 5، وقد تمت الموافقة عليها في يوليو 2003. والمعيار واسع في نطاقه ويشمل كلاً من الأجهزة التي تعمل بمفردها والتكنولوجيا المدمجة في الحاسوب الشخصي، وكذلك المؤتمرات التي تتم من نقطة إلى نقطة والمؤتمرات متعددة النقاط. وتتناول التوصية H.323 التحكم في النداءات، وإدارة الوسائط المتعددة، وإدارة عرض النطاق، وكذلك الأسطح البينية بين شبكات المناطق المحلية والشبكات الأخرى.

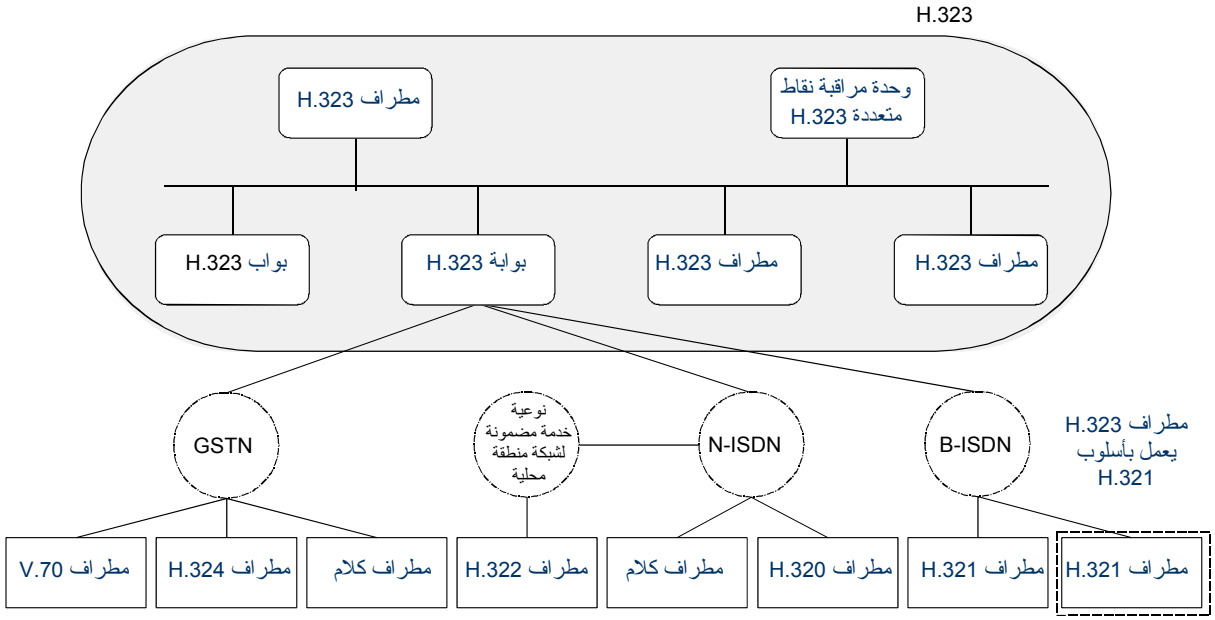
والتوصية H.323 جزء من سلسلة أكبر تشمل معايير الاتصالات التي تمكّن من عقد المؤتمرات المرئية عبر العديد من الشبكات. وهذه التوصية تعرف بالتوصية H.32X، وتشمل هذه السلسلة التوصيتين H.320 وH.324 اللتين تتناولان الاتصالات عبر الشبكات الرقمية متكاملة الخدمات والشبكات الهاتفية العمومية المبدلة، على التوالي. وتتضمن الأولى نظرة شاملة على المعيار المحدد في التوصية H.323، وفوائده ومعماريته وتطبيقاته.

وتتضمن التوصية H.323 تعريف أربعة مكونات رئيسية لنظام الاتصالات القائم على الشبكات، هي: المطاريف، والبوابات، والجهات التي تتحكم في البوابات، ووحدات التحكم متعددة النقاط. وبالإضافة إلى ذلك، يمكن أيضاً وجود عناصر حدودية أو نظيرة. ويتضمن الشكل 7 هذه العناصر.

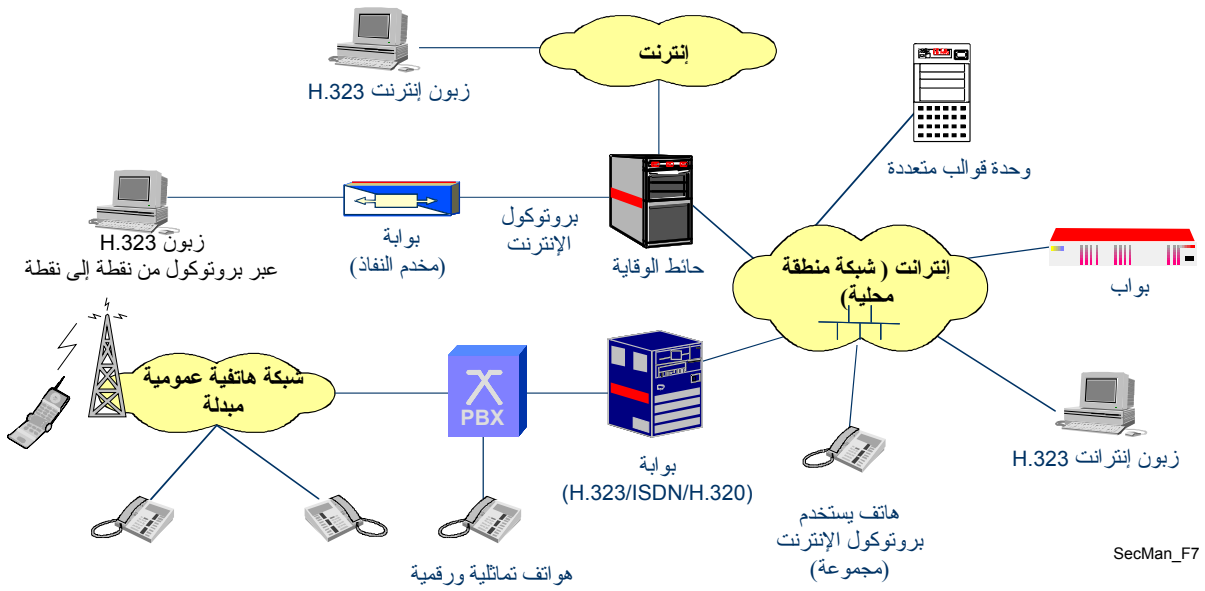
المطاريف (T) هي نقاط طرفية يستخدمها العميل على الشبكة الرئيسية لبروتوكول الإنترنت الذي يوفر اتصالات ثنائية الاتجاه. ويجب أن تدعم المطاريف المشار إليها في التوصية H.323 الاتصالات الهاتفية ويمكن أن تدعم أيضاً شفرات الفيديو وبروتوكولات تنظيم المؤتمرات المشار إليها في التوصية T.120، وقدرات وحدات التحكم متعددة النقاط. ومن أمثلة ذلك: الهواتف التي تستخدم بروتوكول الإنترنت والهواتف المرئية، وأجهزة النظام التفاعلي للاستجابة الصوتية، وأنظمة البريد الصوتي و "الهواتف المبرمجة" (مثل NetMeeting™).

البوابة (GW) هي عنصر اختياري في المؤتمرات المشار إليها في التوصية H.323. وتوفر البوابات خدمات كثيرة أكثرها شيوعاً وظيفة ترجمة بين النقاط الطرفية للمؤتمرات المشار إليها في التوصية H.323 وأنواع المطاريف الأخرى. وتشمل هذه الوظيفة الترجمة بين صيغ الإرسال (أي من H.225.0 إلى H.221) وبين إجراءات الاتصالات (أي من H.245 إلى H.242). وبالإضافة إلى ذلك، تترجم البوابة بين شفرات الصوت والفيديو وتقوم أيضاً بإقامة النداء وتحريره على جانبي شبكة المنطقة المحلية وعلى جانب شبكة الدارة المبدلة.

الجهة التي تتحكم في البوابة (GK) هي أهم مكون في الشبكات التي تعمل طبقاً للتوصية H.323. وتكون بمثابة نقطة مركزية لجميع النداءات في داخل المنطقة التي تتبعها وتوفر خدمات التحكم في النداءات التي تجريها النقاط الطرفية المسجلة. وتعمل جهة التحكم في البوابة طبقاً للتوصية H.323 بطرق كثيرة كبدالة تقديرية لأ ا تتحكم في الإرسال وتستبين العنوان ويمكن أن تسمح بإتمام النداءات بين النقاط الطرفية مباشرة، أو تقوم بتسيير تشوير النداء من خلالها لأداء وظائف مثل التتبع/حاول أن تجدني، وتحويل النداء في حالة الانشغال، وما إلى ذلك. والجهات التي تتحكم في البوابات ترتبط ا عناصر *حدودية* (أو نظيرة) وهي مسؤولة عن تبادل توجيه المعلومات وتشارك في تحويل النداءات بين الميادين الإدارية. كذلك تسمح هذه الوظيفة بالاتصال البيني بين "الجزر" أو الشبكات المختلفة المشار إليها في التوصية H.323. ويتم هذا من خلال تبادل سلسلة من الرسائل كما هو مبين في الشكل 8.



(أ) نظام H.323 ومكوناته [Packetizer]



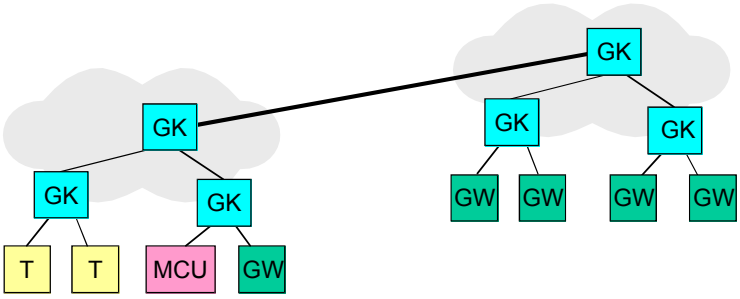
(ب) سيناريوهات التنفيذ H.323 [Euchner]

الشكل 7

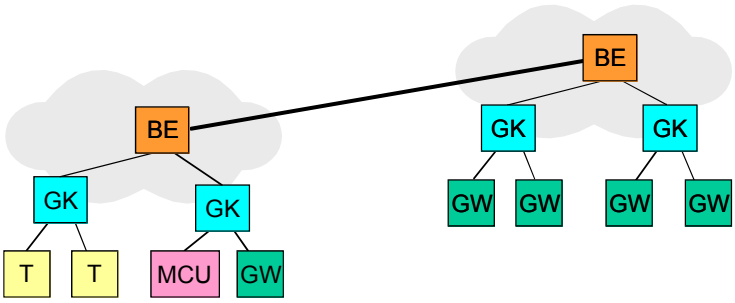
النظام المبين في التوصية H.323: مكونات وسيناريوهات التنفيذ

وحدة التحكم متعددة النقاط (MCU) تدعم تنظيم المؤتمرات بين ثلاث نقاط طرفية أو أكثر. وتنص التوصية H.323 على أن تتألف وحدة التحكم متعددة النقاط من جهاز تحكم، ومعالجات نقاط متعددة قيمتها صفر أو أكثر. وتدير وحدة التحكم في النقاط المتعددة تشوير الرسائل ولكنها لا تتعامل مباشرة مع أي ارتال للوسائط، فهذا متروك لمعالجات النقاط المتعددة، التي تخلط وتبدل وتعالج بتات صوتية وفيديوية و/أو بيانات. ويمكن أن توجد قدرات لوحدة التحكم في النقاط المتعددة ومعالجات النقاط المتعددة في عنصر مخصص أو كجزء من المكونات الأخرى المشار إليها في التوصية H.323.

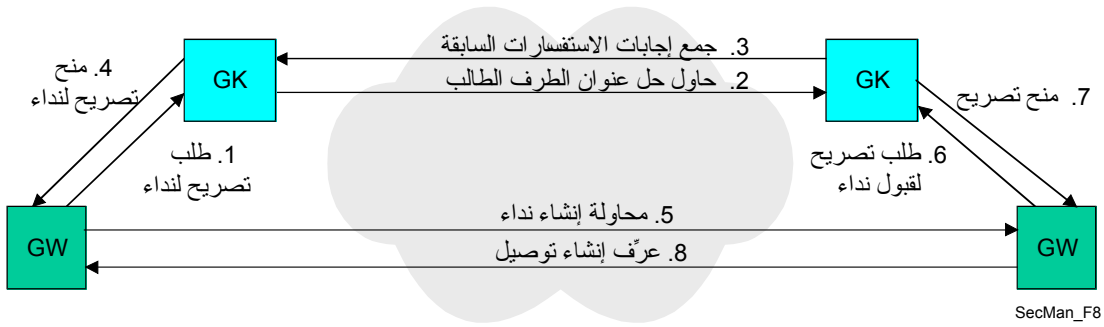
وعلى الرغم من أن التوصية H.323 قد صممت منذ البداية باعتبارها بروتوكول للوسائط المتعددة، تنحصر تطبيقا ا الرئيسية حتى اليوم في سوق نقل الصوت باستعمال بروتوكول الإنترنت. وتحمل الشبكات المشار إليها في التوصية H.323 والتي هي قيد الإنتاج في الوقت الحاضر مليارات من دقائق حركة الصوت والفيديو في الشهر (مع حساب الشبكات العمومية فقط)؛ ويجري نقل معظم حركة المهاتفة باستخدام بروتوكول الإنترنت اليوم طبقاً للتوصية H.323. وتشير التقديرات الحالية إلى أن نقل الصوت باستعمال بروتوكول الإنترنت يمثل أكثر من 10 في المائة من جميع دقائق المسافات الطويلة الدولية. وكذلك تزداد الحركة الفيديوية المشار إليها في التوصية H.323 باستمرار. والسبب الرئيسي لهذا هو نضوج البروتوكول وتنفيذه، وأن التوصية H.323 أثبتت أ ا تمثل حلاً تدريجياً يلبي احتياجات وكالات تقديم الخدمات والشركات، وتتراوح المنتجات المنصوص عليها في التوصية H.323 ما بين بطاريات ورقاقات للهواتف اللاسلكية ومعدات لمؤتمرات مرئية.



(أ) طوبولوجيا مع خوارزمية ريفست وأدلمان وشامير[1]



(ب) طوبولوجيا مع الملحق زاي/H.225.0



(ج) تدفق نداء عالي المستوى

BE: عنصر حدود؛ GK: جهة التحكم في البوابة؛ GW: بوابة؛ MCU: وحدة التحكم في النقاط المتعددة؛ T: مطراف

الشكل 8

اتصالات بين ميادين إدارية

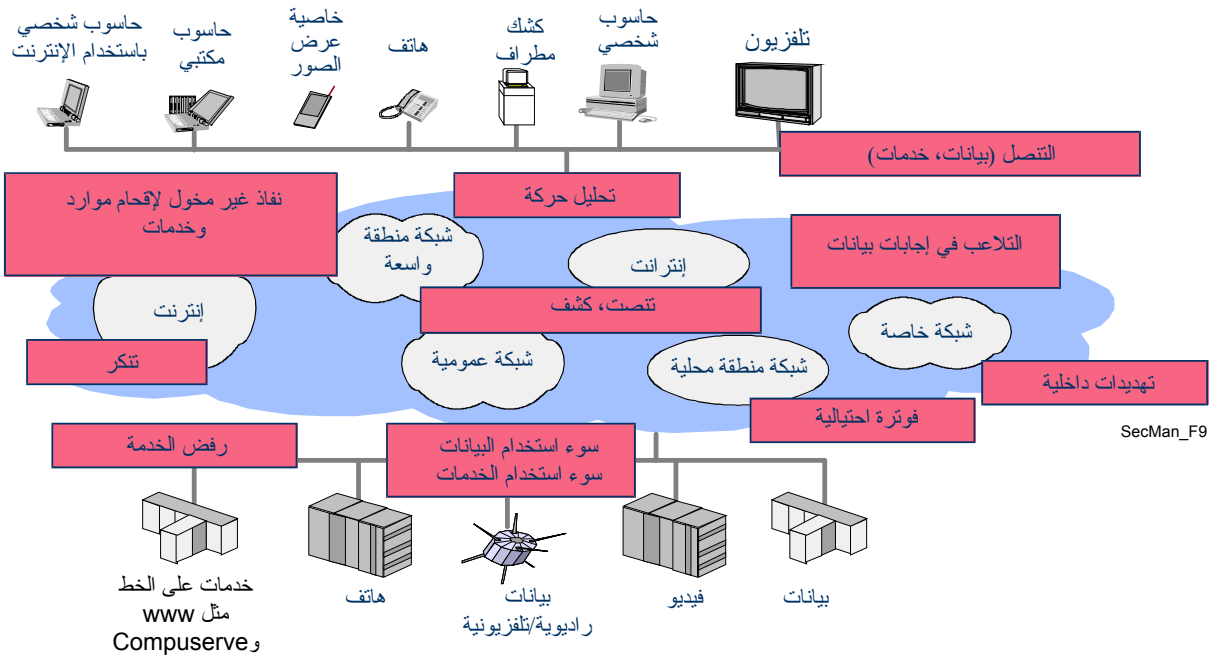
وفيما يلي قائمة بالوظائف التي توفرها الأنظمة المشار إليها في التوصية H.323:

- قدرات لعقد مؤتمرات صوت وفيديو وبيانات
- اتصالات بين أنواع متعددة من المطاريف، بما في ذلك من حاسوب شخصي إلى هاتف ومن فاكس إلى فاكس ومن هاتف إلى هاتف ونداءات ويب
- فاكس T.38 ودعم المودم باستعمال بروتوكول الإنترنت
- خدمات تكميلية كثيرة (إعادة تسيير النداء والتقاط نداء، وما إلى ذلك)
- قابلية التشغيل البيني قوية مع الأنظمة الأخرى المشار إليها في التوصية H.32x، بما في ذلك ما هو منصوص عليه في التوصية H.320 (الشبكات الرقمية متكاملة الخدمات) وH.323M (لاسلكي متنقل 3GPP)
- مواصفة لتجزئة باب وسائط (عبر بروتوكول التحكم في البوابة بموجب التوصية H.248)
- دعم التشوير وأمن الوسائط
- تنقل المستعمل والمطراف والخدمة
- دعم تشوير خدمات الطوارئ

ومن أمثلة استخدام ما هو منصوص عليه في التوصية H.323 عبور بالجملة لوكالات التشغيل، ولا سيما عبر الشبكات الأساسية للمهاتفة باستخدام بروتوكول الإنترنت (بدالات من الفئة 4 لحركة الصوت) وخدمات بطاقات النداء. وفي اتصالات المؤسسات تستخدم التوصية H.323 للبدالات الفرعية الخاصة - بروتوكول الإنترنت وCentrex - بروتوكول الإنترنت والشبكات الخاصة التقديرية الصوتية والأنظمة المتكاملة للصوت والفيديو والبيانات، وهواتف WiFi، وتنفيذ مراكز النداءات والخدمات المتنقلة. وبالنسبة للاتصالات المهنية، تستخدم بشكل واسع في تنظيم مؤتمرات الصوت والفيديو (أو الصوتية) ومؤتمرات الفيديو، والتطبيقات التي تجمع بين الصوت/الفيديو/البيانات، وفي التعلم عن بُعد. وتشمل الاستعمالات في بيئة منـزلية، النفاذ الصوتي البصري عريض النطاق، ومن حاسوب شخصي إلى هاتف، ونقل الأخبار والمعلومات حسب الطلب.

1.1.6 فضايا الأمن في الوسائط المتعددة ونقل الصوت باستعمال بروتوكول الإنترنت

نظراً لإمكانية توزيع جميع عناصر النظام المشار إليه في التوصية H.323 جغرافياً، ونظراً للطابع المفتوح لشبكات بروتوكول الإنترنت، ينشأ العديد من التهديدات للأمن، كما هو مبين في الشكل 9.



الشكل 9
ديدات الأمن في حالة الاتصالات متعددة الوسائط

والقضايا الرئيسية للأمن في اتصالات الوسائط المتعددة والمهاتفة باستعمال بروتوكول الإنترنت بصورة عامة هي [Euchner]:

- الاستيقان من المستعمل والمطراف: تطلب وكالات تقديم خدمة نقل الصوت باستعمال بروتوكول الإنترنت معرفة من يستخدم خدما م للقيام بالحسابات الصحيحة وفوترة استخدام الخدمة. وكشرط أساسي للاستيقان، ينبغي التعرف على المستعمل و/أو المطراف من خلال الهوية. ويتعين على المستعمل/المطراف أن يثبت الهوية الطالبة وأ ا الهوية الحقيقية. ويحدث هذا من خلال إجراءات الاستيقان ا فرة (مثل كلمة سر محمية أو توقيعات رقمية، طبقاً للتوصية X.509). وبالمثل، قد يود المستعملون معرفة من يتهاتفون معهم.
- الاستيقان من الحاسوب الخادم: نظراً لأن مستعملي نقل الصوت باستعمال بروتوكول الإنترنت يتصلون مع بعضهم من خلال بنية تحتية لنقل الصوت باستعمال بروتوكول الإنترنت متصلة بمخدمات (جهات التحكم في البوابات، وأجهزة التسيير متعددة الوظائف، والبوابات)، يهتم المستعملون بمعرفة أ م يتحدثون مع المخدم الصحيح و/أو وكالة الخدمة الصحيحة. ويشمل هذا الجانب مستعملي الخطوط الثابتة والمتنقلة.
- ديدات أمن الاستيقان من المستعمل/المطراف والحاسوب الخادم، مثل التنكر، والتدخل، وخداع عناوين بروتوكول الإنترنت واختطاف التوصيل.
- الاستيقان من النداء هي عملية تحديد ما إذا كان المستعمل/المطراف مسموح له باستخدام موارد الخدمة مثل خاصية خدمة (مثل النداء على الشبكات الهاتفية العمومية المبدلة) أو مصدر شبكة (نوعية الخدمة، وسعة النطاق، والشفرات، وما إلى ذلك). وتأتي معظم وظائف الاستيقان والتخويل معاً لتحقيق قرار التحكم في النفاذ. ويساعد الاستيقان والتخويل في إحباط الهجمات مثل التنكر وإساءة الاستخدام والغش والتلاعب ورفض الخدمة.
- تتناول حماية أمن التشوير حماية بروتوكولات التشوير من التلاعب وإساءة الاستخدام والسرية والخصوصية. وتجري حماية بروتوكولات التشوير بواسطة وسائل محفرة باستخدام التجفير وكذلك سلامة البيانات وإعادة عرضها. وينبغي إيلاء عناية خاصة لتلبية متطلبات الأداء الحرج لإجراء الاتصالات في الوقت الحقيقي بأقل الإجراءات وأقصر الطرق لتجنب الإطالة في إنشاء 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 ومواجهة تنصت البيانات الصوتية المتطفلة. وبصورة عامة، يجري كذلك تجفير رزم الوسائط (مثل الفيديو) لتطبيقات الوسائط المتعددة. كذلك تشمل الحماية المتطورة لرزم الوسائط حماية الاستيقان/وسلامة بيانات الحمولة النافعة.
- لا تشمل إدارة المفاتيح جميع المهام الضرورية لتأمين مواد المفاتيح الموزعة بين الأطراف للمستعملين 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 باستعمال بروتوكول الإنترنت (توفير كلمة سر) أو قد تكون متكاملة مع التشوير عندما يتم التفاوض النشط في شأن أشكال الأمن التي تتوافر لها القدرات اللازمة، ويتم توزيع المفاتيح على أساس الدورة بناء على ذلك.
- يتعامل الأمن فيما بين الميادين مع مشكلة الأنظمة التي تعمل في بيئات غير متجانسة وبالتالي تنفذ خصائص مختلفة للأمن بسبب الحاجات المختلفة والسياسات المختلفة للأمن والقدرات المختلفة للأمن. وفي هذه الحالة، توجد حاجة إلى مفاوضات نشطة لأشكال الأمن وقدرات الأمن، مثل الخوارزميات ا فرة ومعلما ا. ويصبح هذا مهماً بصورة خاصة عند عبور حدود ميدان واشتراك ووجود وكالات مختلفة لتقديم الخدمات وشبكات مختلفة. ومن المقتضيات المهمة لأمن الاتصالات فيما بين الميادين توافر القدرة على عبور الحوائط الواقية بسهولة والتعامل مع المعوقات من أجهزة ترجمة عنوان الشبكة (NAT).

وهذه القائمة ليست شاملة ولكنها تتضمن لب قضايا الأمن المبينة في التوصية H.323. ومع ذلك، يمكن في مجال التطبيق مواجهة قضايا أخرى متعلقة بالأمن تعتبر خارج نطاق التوصية H.323 (مثل 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 كيف يتوفر نقل الصوت باستعمال بروتوكول الإنترنت

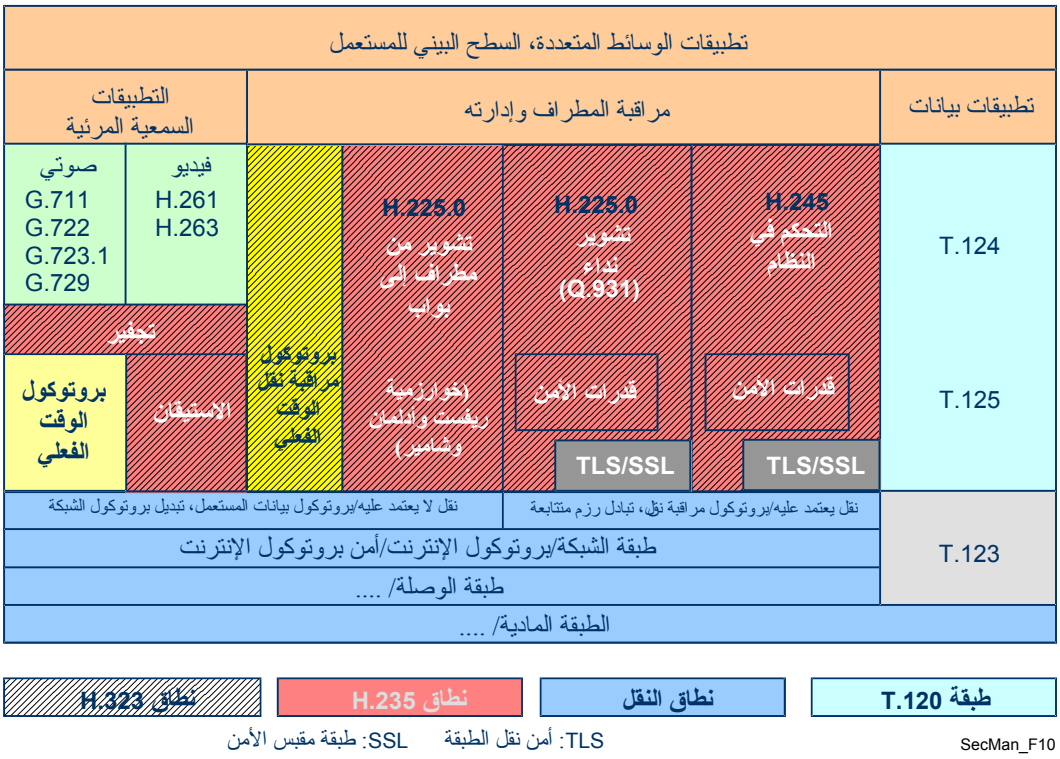
في نظام الوسائط المتعددة المشار إليه في التوصية H.323، تتضمن التوصية H.235 الصادرة عن قطاع تقييس الاتصالات إطار الأمن بما في ذلك مواصفات آليات الأمن وبروتوكولات الأمن المبينة في التوصية H.323. وقدمت التوصية H.235 التي تتناول الأنظمة المبينة في الصيغة 2 للتوصية H.323، لأول مرة في سنة 1998. ومنذ ذلك التاريخ، تطورت التوصية H.235 بمرور الوقت من خلال تجميع آليات الأمن المعروضة وخوارزميات أمن أكثر تطوراً (مثل تجفير معيارية متطورة على درجة عالية من الأمن والسرعة) وبوضع أشكال مفيدة وتتسم بالكفاءة لبعض حالات الاستخدام والبيئات. وتعد الصيغة 3 للتوصية H.235 توصية الأمن التي وضعها قطاع تقييس الاتصالات للأنظمة القائمة على أساس التوصية H.323 التي توفر أمناً متدرجاً موعات صغيرة من المؤسسات والشركات الناقلة التي تعمل على نطاق واسع.

وباختصار، توفر التوصية H.235 حماية مجفرة لبروتوكولات التحكم (خوارزمية ريفست وأدلمان وشامير H.225.0 وتشوير نداء وH.245) وكذلك حماية مجفرة لمعطيات رتل وسائط صوتية/فيديوية. وخلال المراحل المختلفة لتشوير H.323، توفر التوصية H.235 وسائل للتفاوض بشأن خدمات مجفرة مرغوبة ومطلوبة وخوارزميات مجفرة وقدرات الأمن. ويوجد تكامل تام بين وظائف تحديد مفاتيح الدورات النشطة وإجراءات التشوير، مما يساعد على خفض فترة الانتظار في إقامة النداء. وإدارة مفتاح H.235 تدعم الاتصالات "الكلاسيكية" من نقطة إلى نقطة، كما تدعم التشكيلات متعددة النقاط مع أجهزة التسيير متعددة الوظائف عندما تتصل مطاريف متعددة الوسائط داخل مجموعة.

وتشمل التوصية H.235 مجموعة واسعة من تدابير الأمن التي تتناول بيئات مستهدفة مختلفة مثل ما يوجد داخل المؤسسات/وفيما بينها، وفي الشركات الناقلة. واستناداً إلى الافتراضات الخاصة بتوافر البنية التحتية للأمن وتوافر القدرات الطرفية والعتاد (نقاط طرفية بسيطة أو نقاط طرفية ذكية)، تتضمن التوصية H.235 مجموعة من برامج الأمن التي تناسب الأوضاع المختلفة وتصلح للتشغيل البيني. وتوفر برامج الأمن المتاحة تقنيات للأمن تتراوح بين التقنيات البسيطة السرية المشتركة التي تعمل بكلمة سر محمية (الملحق دال بالتوصية H.235 الذي يتناول الاستيقان وسلامة الرسائل) وبرامج متطورة تعمل بتوقيعات رقمية وشهادات البنية التحتية للمفاتيح العمومية طبقاً للتوصية X.509 (الملحق هاء والملحق واو بالتوصية H.235). وهذه التقنيات تسمح بالحماية من مرحلة إلى أخرى باستخدام تقنيات بسيطة ولكنها أقل تدرجاً أو بحماية من طرف إلى طرف باستخدام التقنيات المتدرجة للبنية التحتية للمفاتيح العمومية. ويخفف الملحق طاء بالتوصية H.235 من الاعتماد الصارم على جهة التحكم في بوابة التسيير ومعمارية الجهاز الخادم المركزي وتوفر تدابير الأمن التي تضمن تأمين نموذج من نظير إلى نظير.

وتستفيد التوصية H.235 من تقنيات الأمن الخاصة المثلى كتجفير منحني إهليلجي وتجفير خوارزمية معيارية متطورة لمواجهة قيود الأداء الصارمة. ويتحقق تنفيذ التجفير الصوتي في طبقة التطبيقات بواسطة أحمال نافعة لبروتوكول الوقت الفعلي. وهذا يسمح بتنفيذ مفيد مع حيز صغير في النقاط الطرفية من خلال التفاعل المحكم مع معالج الإشارة الرقمية وجهاز تفكيك انضغاط الصوت دون الاعتماد على عتاد نظام تشغيل. وإذا توافرت أدوات الأمن المناسبة، مثل حزم ومعايير أمن الإنترنت (أمن بروتوكول الإنترنت وطبقة مقبس أمن/أمن مستوى نقل) يمكن استخدامها (إعادة استخدامها) في سياق ما تنص عليه التوصية H.235.

ويبين الشكل 10 نطاق التوصية H.235 التي تحتوي على أحكام لإقامة نداءات (قدرات H.225.0 وH.245) واتصالات في اتجاهين (تجفير أحمال نافعة لبروتوكول الوقت الفعلي الذي يحتوي على صوت و/أو فيديو منضغط). وتشمل العناصر الوظيفية آليات الاستيقان وسلامة البيانات والخصوصية وعدم التنصل. وجهات التحكم في البوابات هي المسؤولة عن الاستيقان عن طريق التحكم في القبول في النقاط الطرفية ولتوفير آليات عدم التنصل. أما الأمن على طبقات النقل والطبقات السفلية، باستخدام بروتوكول الإنترنت، فيعد خارج نطاق كل من التوصيتين H.323 وH.235 ولكنه ينفذ عادة باستخدام فريق مهام الإنترنت الهندسي (أمن بروتوكول الإنترنت) وبروتوكولات أمن طبقة النقل. وبصورة عامة، يمكن استخدام أمن بروتوكول الإنترنت وأمن شفافية الطبقة لتوفير الاستيقان، واختيارياً، لتوفير السرية (أي التجفير) عند طبقة شفافة لبروتوكول الإنترنت لأي (تطبيق) بروتوكول يجري أعلاه. وليس من اللازم تحديث بروتوكول التطبيق للسماح ذا، والاقتصار على تطبيق سياسة الأمن عند كل طرف.



الشكل 10

الأمن في التوصية H.323 كما تنص عليه التوصية H.235 [Euchner]

وبينما تتناول التوصية H.235 معظم البيئات "السكونية" المشار إليها في التوصية H.323 مع أحكام محدودة فيما يتعلق بالقدرة على التنقل، يوجد اعتراف بالحاجة إلى توفير القدرة على التنقل الآمن للمستعملين والمطاريف في البيئات الموزعة المشار إليها في التوصية H.323 خارج التوصيل البيني فيما بين الميادين والقدرة على التنقل في منطقة بوابة محدودة. وتشمل التوصية H.530 لقطاع تقييس الاتصالات حاجات الأمن من خلال تناول جوانب مثل:

- الاستيقان من، وتخويل مطراف/مستعمل متنقل في الميادين الأجنبية التي يقوم بزيار ا.
- الاستيقان من ميدان الزيارة.
- تأمين إدارة المفتاح
- حماية بيانات التشوير بين مطراف متنقل وميدان الزيارة.

وبالإضافة إلى أن التوصيات H.235 وH.350 و H.350.2 تنص على الإدارة المتدرجة للمفاتيح باستخدام بروتوكول نفاذ الدليل خفيف الوزن وطبقة المقبس الآمن 3، تنص التوصية ITU-T H.350.x على قدرات عديدة مهمة تمكن المؤسسات وشركات الاتصالات من إدارة أعداد كبيرة من مستعملي الخدمات الفيديوية والخدمات الصوتية، بأمان، باستعمال بروتوكول الإنترنت. وتوفر H.350 طريقة لتوصيل H.323 وبروتوكول بداية الدورة و H.320 وخدمات المراسلة المعتادة بخدمة الدليل، للتمكن من تطبيق الممارسات الحديثة لإدارة الهوية على الاتصالات متعددة الوسائط. وفضلاً عن ذلك، توفر المعمارية مكاناً يخضع للمعايير لتخزين التفويضات الخاصة بالأمن في استخدام هذه البروتوكولات.

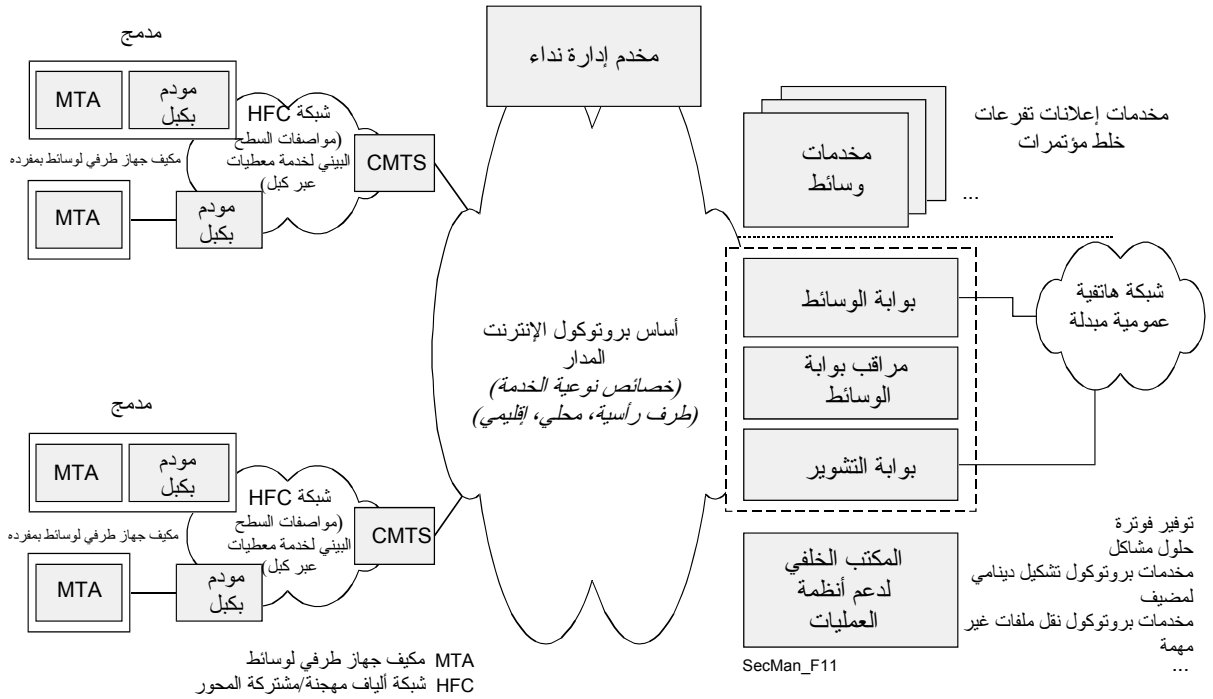
ولا تغير التوصية H.350 معماريات الأمن في أي بروتوكول. ومع ذلك، فإ ا توفر مكاناً خاضعاً للمعايير لتخزين تفويضات الاستيقان حسب مقتضى الحال. وينبغي ملاحظة أن كلاً من التوصية H.323 وبروتوكول بداية الدورة يدعمان الاستيقان من كلمة السر المشتركة (الملحق دال بالتوصية H.235 وموجز بروتوكول نقل نص موسوعي، على التوالي). وتتطلب هذه المناهج أن يكون لمخدم النداء الحق في النفاذ إلى كلمة السر. وبالتالي، ففي حالة تعرض مخدم النداء أو دليل H.350 للخطر، قد تصبح كلمة السر معرضة للخطر أيضاً. وقد تكون جوانب الضعف هذه نتيجة لضعف في الأنظمة (دليل H.350 أو مخدم النداء) وتشغيلها بدلاً من H.350 في حد ذا ا.

ويجري تشجيع وكالات خدمة النداءات والدليل H.350 على أن يستوثق كل منهم من الآخر قبل تقاسم المعلومات. وفضلاً عن ذلك، فمن المستصوب إنشاء الاتصالات بين أدلة H.350 ووكالات خدمة النداءات أو النقاط الطرفية عبر قنوات اتصالات آمنة مثل طبقة مقبس الأمن أو أمن نقل الطبقة.

وينبغي ملاحظة أن قوائم التحكم في النفاذ على مخدمات بروتوكول نفاذ دليل خفيف الوزن تندرج ضمن مسائل السياسات وليست جزءاً من المعيار. ومن المستصوب أن يستخدم مديرو الأنظمة الحصافة عند إقامة مراقبة نفاذ على خواص التوصية H.350. فمثلاً، ينبغي أن يقتصر النفاذ إلى خواص كلمة السر على المستعمل الموثوق به، بينما يمكن أن تكون خواص العناوين متاحة بشكل عام.

2.6 نظام الاتصالات الكبلية باستعمال بروتوكول الإنترنت

يمكّن نظام الاتصالات الكبلية باستعمال بروتوكول الإنترنت شركات تشغيل تلفزيون الكبل من توفير الخدمات في الوقت الفعلي باستعمال بروتوكول الإنترنت (مثل الاتصالات الهاتفية) عبر شبكا ا المهيأة لدعم أجهزة المودم التي تعمل بالكبل. وتتضمن التوصية J.160 الصادرة عن قطاع تقييس الاتصالات تعريف معمارية نظام الاتصالات الكبلية باستعمال بروتوكول الإنترنت. وتتعامل معمارية نظام الاتصالات الكبلية باستعمال بروتوكول الإنترنت مع ثلاث شبكات، على مستوى عال جداً. وهذه الشبكات هي: "شبكة النفاذ بالألياف مهجنة متحدة المحور طبقاً للتوصية J.112" و"شبكة بروتوكول الإنترنت التي تجري إدار ا" والشبكة الهاتفية العمومية المبدلة. وتوفر عقدة النفاذ إمكانية التوصيل بين "شبكة نفاذ بالألياف المهجنةمتحدة المحور طبقاً للتوصية J.112" و"شبكة بروتوكول الإنترنت التي تجري إدار ا". ويوفر كل من بوابة التشوير وبوابة الوسائط إمكانية التوصيل بين "شبكة بروتوكول الإنترنت التي تجري إدار ا" والشبكة الهاتفية العمومية المبدلة. ويوضح الشكل 11 المعمارية المرجعية للاتصالات الكبلية باستعمال بروتوكول الإنترنت.



الشكل 11
معمارية مرجعية للاتصالات الكبلية باستخدام بروتوكول الإنترنت [J.165]

توفر شبكة النفاذ بكبل الألياف المهجنة متحدة المحور طبقاً للتوصية J.112 إمكانية تحقيق النقل الآمن الذي يعتمد عليه بسرعة عالية جداً بين مقار الزبائن وطرف رأسية الكبل. ويمكن لهذه الشبكة أن توفر النفاذ إلى جميع القدرات المشار إليها في التوصية J.112، بما في ذلك نوعية الخدمة والأسطح البينية للطبقة المادية من خلال نظام الإ اء بمودم الكبل.

وتقوم شبكة بروتوكول الإنترنت المدارة بعدة وظائف. أولاً، توفر التوصيل البيني للمكونات الوظيفية للاتصالات الكبلية باستخدام بروتوكول الإنترنت بما في ذلك التشوير، والوسائط، والتهيئة، ونوعية إتمام الخدمة. وبالإضافة إلى ذلك، توفر شبكة بروتوكول الإنترنت المدارة توصيلية بروتوكول الإنترنت طويلة المسافة بين شبكات بروتوكول الإنترنت المدارة وJ.112. وتشمل شبكة بروتوكول الإنترنت المدارة المكونات الوظيفية التالية: مخدم إدارة النداء، ومخدم الإعلان، وبوابة تشوير، وبوابة وسائط، ومراقب بوابة الوسائط، ومخدمات المكتب الخلفي لدعم أنظمة عمليات عديدة.

يوفر *مخدم إدارة النداء* (CMS) مراقبة النداء وخدمات متعلقة بتشوير مكيف جهاز طرفي لوسائط، وعقدة النفاذ، وبوابات الشبكة الهاتفية العمومية المبدلة في شبكة الاتصالات الكبلية باستخدام بروتوكول الإنترنت. ويعتبر مخدم إدارة النداء من عناصر الشبكة التي يمكن الوثوق ا، ويوجد في جزء بروتوكول الإنترنت المدار لشبكة الاتصالات الكبلية باستخدام بروتوكول الإنترنت. *ومخدمات الإعلان* هي مكونات شبكة منطقية تدير وتذيع نغمات وتقدم رسائل معلومات استجابة لأحداث تقع في الشبكة. ووظيفة بوابة التشوير أ ا ترسل وتستقبل تشوير شبكة الدارة المبدلة عند حافة شبكة الاتصالات الكبلية باستخدام بروتوكول الإنترنت. وبالنسبة للأخيرة، فإ ا تدعم فقط وظيفة بوابة التشوير غير المرتبطة بأي مرفق في شكل SS7 (يجري تدعيم التشوير المرتبط بالمرفق في شكل نغمات متعددة التردد مباشرة بواسطة وظيفة بوابة الوسائط). ويستقبل *مراقب بوابة الوسائط* (MGC) معلومات تشوير النداء بين شبكة الاتصالات الكبلية باستخدام بروتوكول الإنترنت وشبكة هاتفية عمومية مبدلة، كما يقوم بدور الوسيط في هذه العملية. ويحتفظ ويراقب حالة النداء في النداءات التي تتطلب توصيلاً بينياً على الشبكة الهاتفية العمومية المبدلة. وتوفر *بوابة الوسائط* (MG) حمالة التوصيلية بين شبكة هاتفية عمومية مبدلة وشبكة بروتوكول الإنترنت للاتصالات الكبلية باستخدام بروتوكول الإنترنت. وتمثل كل حمالة بنقطة طرفية ويوجه مراقب بوابة الوسائط أيضاً بوابة الوسائط لاكتشاف وتوليد أحداث وإشارات متعلقة بحالة النداء المعروفة لمراقب بوابة الوسائط. ويحتوي *المكتب الخلفي لدعم أنظمة العمليات* على أعمال وخدمة ومكونات إدارة شبكة تدعم عمليات الأعمال الرئيسية. وا الات الوظيفية الرئيسية لدعم أنظمة العمليات هي إدارة الأعطال، وإدارة الأداء، وإدارة الأمن، وإدارة الحسابات، وإدارة التشكيل. وتعرف الاتصالات الكبلية باستخدام بروتوكول الإنترنت مجموعة محدودة من المكونات الوظيفية والأسطح البينية لدعم أنظمة عمليات تدعم توفير جهاز مكيف طرفي للوسائط ومراسلة أحداث لحمل معلومات الفوترة.

1.2.6 مسائل الأمن في الاتصالات الكبلية باستخدام بروتوكول الإنترنت

يتعرض كل سطح بيني لبروتوكول الاتصالات الكبلية باستخدام بروتوكول الإنترنت لتهديدات قد تشكل مخاطر على أمن كل من المشترك ووكالة تقديم الخدمة. فمثلاً، قد يعبر مسير رتل الوسائط عدداً كبيراً من أسلاك خدمات الإنترنت غير المعروفة وأسلاك الشبكات الأساسية لوكالات تقديم الخدمة. ونتيجة لذلك، قد يكون رتل الوسائط معرضاً لتنصت خبيث مما ينتج عنه فقدان خصوصية الاتصالات.

2.2.6 آليات الأمن في الاتصالات الكبلية باستخدام بروتوكول الإنترنت

يجري تنفيذ الأمن في الاتصالات الكبلية باستخدام بروتوكول الإنترنت في العناصر السفلية من الرصة، ومن ثم يستخدم الآليات التي عرفها فريق مهام الإنترنت الهندسي. وتتناول معمارية الاتصالات الكبلية باستخدام بروتوكول الإنترنت هذه التهديدات من خلال تحديد كل سطح بيني للبروتوكول المعرف وآليات الأمن المهمة (مثل أمن بروتوكول الإنترنت) التي توفر السطح البيني للبروتوكول مع خدمات الأمن التي يتطلبها. وفي سياق المعمارية المبينة في التوصية X.805، تتناول خدمات الأمن الشاملة للاتصالات الكبلية باستخدام بروتوكول الإنترنت جميع الخلايا التسع الناتجة عن ثلاثة مستويات وطبقات مبينة في الشكل 1. فمثلاً، يدعم أمن بروتوكول الإنترنت خدمات بروتوكولات التشوير لمستوى المراقبة. ويتحقق أمن البنية التحتية للإدارة باستخدام بروتوكول إدارة الشبكة البسيطة v3.

وتكون خدمات الأمن المتاحة من خلال طبقة خدمة لب الاتصالات الكبلية باستخدام بروتوكول الإنترنت هي الاستيقان، ومراقبة النفاذ، وسلامة البيانات، والسرية، وعدم التنصل. وقد لا يستخدم السطح البيني لبروتوكول الاتصالات الكبلية باستخدام بروتوكول الإنترنت أي خدمة أو يستخدم خدمة واحدة أو أكثر من هذه الخدمات لتوفير متطلبات أمن معين.

ويلبي أمن الاتصالات الكبلية باستخدام بروتوكول الإنترنت المتطلبات اللازمة لتحقيق الأمن لكل سطح بيني لمكونات البروتوكول بواسطة:

- تعريف نموذج التهديد الذي يتعرض له كل سطح بيني لمكونات البروتوكول؛
- تعريف خدمات الأمن (الاستيقان، والتخويل، والسرية، وسلامة البيانات، 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، وأمن طبقة بروتوكول الوقت الفعلي، وأمن بروتوكول إدارة الشبكة البسيطة v3) ودعم بروتوكول إدارة المفاتيح (مثل بدالة مفتاح الإنترنت والمفاتيح العمومية لتجفير توثيق أولي/كيربيروس). وتشمل خدمات أمن لب الاتصالات الكبلية باستخدام بروتوكول الإنترنت آلية توفر التجفير من طرف إلى طرف لأرتال وسائط بروتوكول الوقت الفعلي، ومن ثم تقلل بدرجة كبيرة من مديد الخصوصية. ويوضح الشكل 12 موجزاً للأسطح البينية لأمن الاتصالات الكبلية باستخدام بروتوكول الإنترنت. وفي حالة عدم وجود بروتوكول إدارة المفاتيح، فإن ذلك يعني عدم حاجة هذا السطح البيني له. ولا يتضمن الشكل الأسطح البينية للاتصالات الكبلية باستخدام بروتوكول الإنترنت التي لا تتطلب أمناً.

تقسم معمارية أمن الاتصالات الكبلية باستخدام بروتوكول الإنترنت توفير الخدمة إلى ثلاثة أنشطة متميزة، هي: اشتراك مشترك، وتوفير الجهاز، وتخويل الجهاز. وتنشئ عملية *اشتراك المشترك* حساب فوترة دائماً لمشترك ويقوم هذا الحساب بتعريف مكيف الجهاز الطرفي للوسائط لتركيب الرسالة ا فرة عبر الرقم المسلسل للمكيف أو عنوان شفرة توثيق الرسالة. ويستخدم حساب الفوترة أيضاً في تعريف الخدمات التي يشترك فيها المشترك لمكيف الجهاز الطرفي للوسائط. وقد يحدث اشتراك المشترك داخل النطاق أو خارج النطاق. وتقع المواصفات الفعلية لعملية اشتراك المشترك خارج نطاق الاتصالات الكبلية باستخدام بروتوكول الإنترنت، وقد تكون مختلفة لكل وكالة من وكالات تقديم الخدمات. أما بالنسبة *لتوفير الجهاز*، فإن مكيف الجهاز الطرفي للوسائط يتحقق من سلامة ملف التشكيل الذي يقوم بتحميله أولاً بتطبيق إجراءات الأمن التي ينص عليها بروتوكول إدارة الشبكة البسيطة v3 (باستخدام الاستيقان القائم على كيربيروس وإدارة المفاتيح) بين نفسه والمخدم الذي يوفر الخدمة. ثم يقوم المخدم بتعريف مكيف الجهاز الطرفي للوسائط بمكان ملف التشكيل وفرم ملف التشكيل. ويسترد المكيف ملف التشكيل ويؤدي الفرم على ملف التشكيل ويقارن النتيجة مع الفرم الذي أجراه المخدم. ويكون ملف التشكيل قد استوثق مما إذا كان الفرم مطابقاً. وقد يكون ملف التشكيل مجفراً اختيارياً من أجل الخصوصية (ينبغي أن تتمكن سرية بروتوكول إدارة الشبكة البسيطة v3 من تأمين إرسال مفتاح تجفير ملف التشكيل إلى مكيف الجهاز الطرفي للوسائط). يكون *تخويل الجهاز* عندما يوثق مكيف جهاز طرفي لوسائط نفسه لمخدم إدارة النداء ويقيم علاقة أمن مع ذلك المخدم قبل أن يصبح قيد التشغيل بالكامل. ويسمح الاستيقان من الجهاز بتشوير النداء التالي لحمايته بناء على علاقة الأمن القائمة.

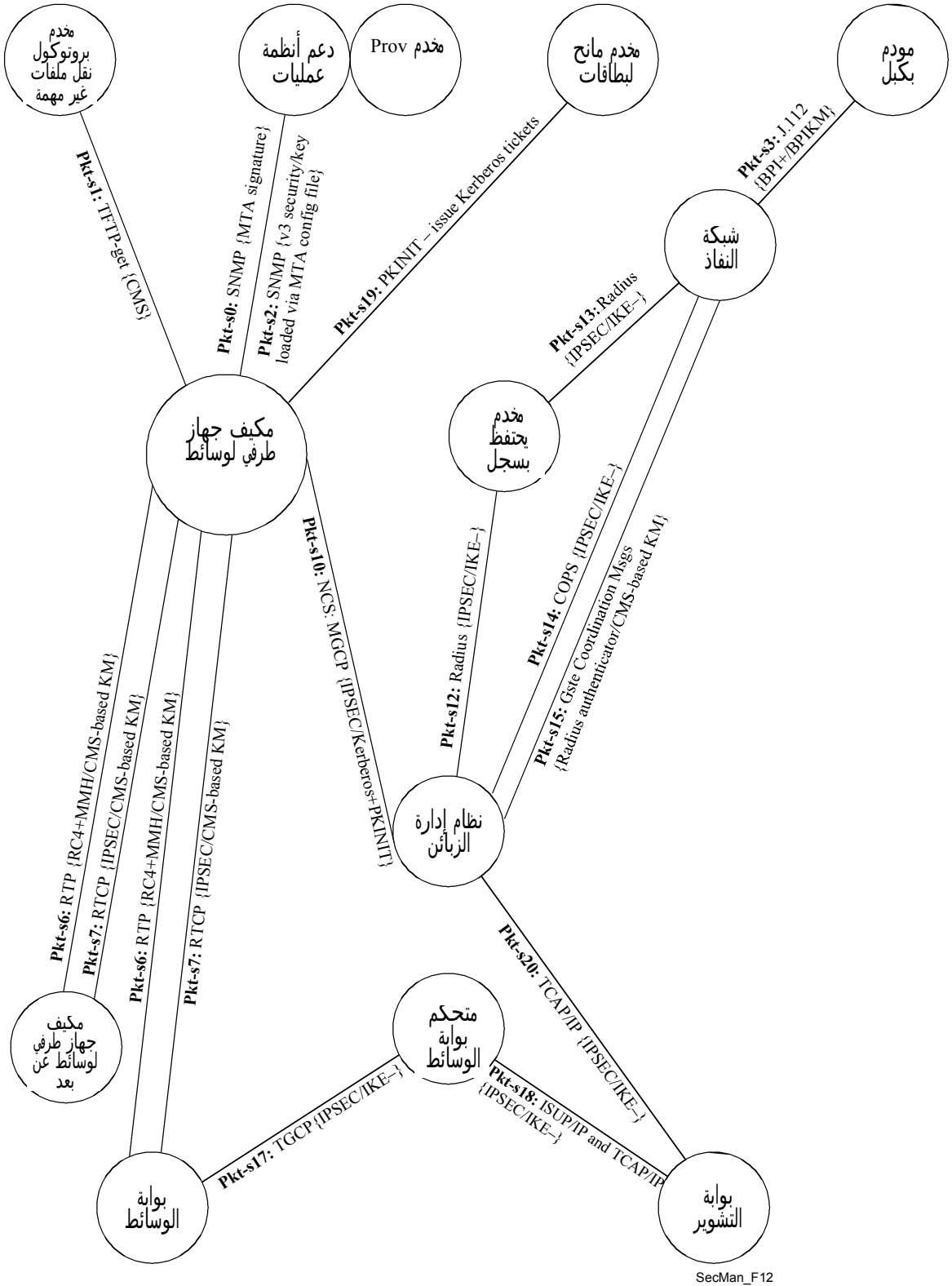
ويمكن حماية حركة التشوير ورتل الوسائط. ويجري تأمين كل حركة التشوير، التي تشمل تشوير نوعية الخدمة وتشوير النداء والتشوير مع السطح البيني لبوابة الشبكة الهاتفية العمومية المبدلة، عبر أمن بروتوكول الإنترنت. وتتم إدارة علاقة أمن بروتوكول الإنترنت من خلال استخدام بروتوكولات إدارة مفتاحين، هما: كيبيروس/المفاتيح العمومية لتجفير الاستيقان الأولي وبدالة مفتاح الإنترنت. وتستخدم كيبيروس/المفاتيح العمومية لتجفير الاستيقان الأولي لتبديل المفاتيح بين زبائن مكيف الجهاز الطرفي للوسائط ومخدم تركيب الرسالة ا فرة؛ وتستخدم بدالة مفتاح الإنترنت لإدارة جميع علاقات أمن تشوير أمن بروتوكول الإنترنت. وفيما يتعلق بأرتال الوسائط، تجفر كل رزمة من وسائط بروتوكول الوقت الفعلي من أجل تحقيق الخصوصية والاستيقان للتحقق من سلامة البيانات وأصل الرزمة. ويتوفر لمكيف الجهاز الطرفي للوسائط المقدرة على التفاوض مع خوارزمية تجفير معينة، بالرغم من أن خوارزمية التجفير المطلوبة الوحيدة هي خوارزمية معيارية متطورة للتجفير. وقد تشمل كل رزمة في بروتوكول الوقت الفعلي شفرة اختيارية للاستيقان من الرسالة. ويمكن أيضاً التفاوض بشأن خوارزمية شفرة توثيق الرسالة، على الرغم من أن الخوارزمية المحددة الوحيدة الحالية هي فرم نظام متعدد الوسائط. وتتوسع حوسبة شفرة الاستيقان من الرسالة إلى رأسية غير مجفرة لرزمة وحمل نافع مجفر.

وتشتق مفاتيح التجفير وحساب شفرة الاستيقان من الرسالة من سر طرف إلى طرف وموهن اختياري يجري تبادلهما بين إرسال مكيف الجهاز الطرفي للوسائط واستقباله كجزء من تشوير النداء. ومن ثم، يتحقق تبادل مفاتيح الأمن لرتل الوسائط الآمنة بواسطة أمن تشوير النداء.

ويتوفر الأمن أيضاً من أجل دعم أنظمة عمليات ونظام الفوترة. وينفذ وكلاء بروتوكول إدارة الشبكة البسيطة لأجهزة الاتصالات الكبلية باستخدام بروتوكول الإنترنت بروتوكول إدارة الشبكة البسيطة v3. ويوفر نموذج أمن مستعمل [طلب تعليقات RFC 2274] لبروتوكول إدارة الشبكة البسيطة v3 خدمات الاستيقان والخصوصية لحركة بروتوكول إدارة الشبكة البسيطة. وقد تستخدم مراقبة النفاذ القائمة على الرؤية لبروتوكول إدارة الشبكة البسيطة v3 من أجل مراقبة النفاذ إلى أغراض قاعدة معلومات الإدارة.

ويستخدم بروتوكول إدارة مفتاح بدالة مفتاح الإنترنت في إنشاء مفاتيح للتجفير والاستيقان بين مخدم يحتفظ بسجل وعنصر شبكة الاتصالات الكبلية باستخدام بروتوكول الإنترنت الذي يولد رسائل أحداث. وعند إقامة علاقات أمن شبكة بروتوكول الإنترنت، ينبغي إنشاء هذه المفاتيح بين كل مخدم يحتفظ بسجل (أولي، أو وثانوي، وغيرهما) وكل نظام من أنظمة إدارة الزبائن وشبكة المنطقة. وقد توجد بدالة مفتاح بين متحكم بوابة الوسائط والمخدم الذي يحتفظ بسجل ويترك لتنفيذ البائع في المرحلة الأولى من الاتصالات الكبلية باستخدام بروتوكول الإنترنت. وترسل رسائل الأحداث من نظام

إدارة الزبائن وشبكة المنطقة إلى المخدم الذي يحتفظ بسجل باستخدام بروتوكول نقل خدمة الاستيقان عن بعد إلى مستعمل المراقمة الداخلية الذي يؤمن بدوره بواسطة أمن بروتوكول الإنترنت.



IKE – ترميز معرف لإشارة مع مفاتيح متقاسمة مسبقاً

IKE + ترميز معرف لإشارة يتطلب شهادات مفاتيح عمومية

CMS-based KM إدارة مفاتيح قائمة على نظام إدارة الزبائن مفاتيح تولد عشوائياً ويوزعها نظام إدارة الزبائن

الشكل 12

الأسطح البينية لأمن الاتصالات الكبلية باستعمال بروتوكول الإنترنت

(labelled as <label>: <protocol> { <security protocol> / <key management protocol> })

3.6 تأمين إرسال الفاكس

الفاكس هو تطبيق شائع جداً. وعرف في البداية للإرسال عبر الشبكات الهاتفية العمومية المبدلة (التوصية ITU-T T.4) ثم للشبكات الرقمية متكاملة الخدمات (التوصية ITU-T T.6)، وتم توسيعه مؤخراً للنقل عبر شبكات بروتوكول الإنترنت (بما في ذلك الإنترنت) للإرسال في غير الوقت الفعلي (ترحيل بريد إلكتروني) باستخدام التوصية ITU-T T.37، وفي الوقت الفعلي (باستخدام بروتوكول الوقت الفعلي) باستخدام التوصية ITU-T T.38. وقضيتا الأمن الشائعتان اللتان تواجهان إرسال الفاكس - بغض النظر عما إذا كان عبر الشبكات الهاتفية العمومية المبدلة أو الشبكات الرقمية متكاملة الخدمات أو بروتوكول الإنترنت - تتعلقان بالاستيقان من الوصول (وفي بعض الأحيان بعدم التنصل) وبسرية البيانات المرسلة. ومع ذلك، فإن التوصيتين T.37 وT.38 زادتا من أهمية هذه القضايا نتيجة للطابع الموزع لشبكة بروتوكول الإنترنت.

وتتضمن التوصية ITU-T T.36 تعريف حلين تقنيين مستقلين يمكن استخدامهما في سياق تأمين إرسال الفاكس لتجفير الوثائق التي يتم تبادلها. ويقوم الحلان التقنيان على أساس خوارزميات هوثورن لإدارة المفاتيح/هوثورن لشفرة الفاكس 40 (HKM/HFX40) (الملحق ألف/T.36) وخوارزمية ريفست وشامير وأدلمان (الملحق باء/T.36). وعلى الرغم من أن مفاتيح الدورة تقتصر على 40 بتة (نتيجة للقواعد الوطنية التي كانت مطبقة في وقت الموافقة على التوصية في سنة 1997)، تم تحديد آلية لتوليد مفتاح لدورة بديلة (من 40 بتة لطول مفتاح دورة) لخوارزميات تتطلب مفاتيح أطول. ويوضح الملحق جيم بالتوصية T.36 استخدام نظام هوثورن لإدارة المفاتيح لتوفير قدرات إدارة المفاتيح الآمنة لمطاريف الفاكس بواسطة طريقة تسجيل بين الكيانين X وY أو تأمين إرسال مفتاح سري بين الكيانين X وY. ويشمل الملحق دال بالتوصية T.36 إجراءات استخدام نظام تجفير الموجة الحاملة لخوارزمية هوثورن لشفرة فاكس 40 لتوفير سرية الرسالة لمطاريف الفاكس. ويوضح الملحق هاء بالتوصية T.36 خوارزمية فرم هوثورن لشفرة فاكس 40، من حيث استخدامها، الحسابات الضرورية والمعلومات الواجب تبادلها بين مطاريف الفاكس لتوفير سلامة رسالة الفاكس المرسلة سواء كان بديلاً مختاراً أو مبرمجاً مسبقاً 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 استقبال رسالة.
- خدمة أمن (اختيارية) تشمل الاستيقان المتبادل وسلامة الرسالة (تجفير) وإقامة مفتاح الدورة.
- خدمة أمن (اختيارية) تشمل الاستيقان المتبادل وسلامة الرسالة وتأكيد استقبال الرسالة وسرية الرسالة (تجفير) وإقامة مفتاح دورة.

ويتم تحديد أربعة خواص للخدمة على أساس خدمات الأمن المعرفة أعلاه، كما هو مبين في الجدول 2 أدناه.

الجدول 2
ملامح الأمن المبينة في الملحق حاء بالتوصية T.30

خدمات الأمن	ملامح الخدمات			
	1	2	3	4
الاستيقان المتبادل	X	X	X	X
• سلامة الرسالة • تأكيد استقبال الرسالة		X		X
• سرية الرسالة (تجفير) • إقامة مفتاح الدورة			X	X

1.3.6 أمن الفاكس باستخدام خوارزمية هوثورن لإدارة المفاتيح وخوارزمية هوثورن لشفرة الفاكس

يوفر الجمع بين خوارزمية هوثورن لإدارة المفاتيح وخوارزمية هوثورن لشفرة فاكس القدرات التالية لتأمين اتصالات الوثائق بين كيانات (مطاريف أو مشغلي المطاريف):

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

يتم توفير إدارة المفاتيح باستخدام نظام هوثورن لإدارة المفاتيح 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 التالية، يوفر نظام هوثورن لإدارة المفاتيح توثيقاً متبادلاً ومفتاح دورة سري لضمان سرية وسلامة الوثائق، وتأكيد الاستقبال، وتأكيد أو رفض سلامة الوثائق.

وتتوفر سرية الوثائق باستخدام شفرة الموجة الحاملة المبينة في الملحق دال بالتوصية T.36. وتستخدم شفرة الموجة الحاملة مفتاحاً رقمياً يقوم على 12 رقماً عشرياً، وهو مساو تقريباً لمفتاح دورة له 40 بتة.

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

وفي أسلوب التسجيل، يتبادل المطرافان المعلومات التي تمكّن الكيانين من التعرف على بعضهما على نحو فريد. ويقوم هذا على أساس اتفاق بين مستعملي المفتاح السري لمرة واحدة. ويقوم كل كيان بتسجيل عدد يتكون من 16 رقماً عشرياً يرتبط بالكيان الذي يقوم بتنفيذ التسجيل دون غيره.

وعندما يكون من المطلوب إرسال وثيقة آمنة، يرسل مطراف الإرسال عدداً سرياً يتكون من 16 رقماً عشرياً يرتبط بالكيان المستقبل مع عدد عشوائي ومفتاح دورة مجفر باعتباره تحدياً للكيان المستقبل. ويجيب المطراف المستقبل بإرسال مفتاح يقوم على 16 رقماً عشرياً يرتبط بالكيان المرسل مع عدد عشوائي وصيغة معاد تجفيرها للتحدي الوارد من الكيان المرسل. ويرسل في نفس الوقت عدداً عشوائياً ومفتاح دورة مجفر كتحد للكيان المرسل. ويجيب المطراف المرسل بعدد عشوائي وصيغة معاد تجفيرها للتحدي الذي جاءه من الكيان المستقبل. ويمكّن هذا الإجراء كلاً منهما من تحقيق الاستيقان المتبادل. وفي نفس الوقت، يرسل مطراف الإرسال عدداً عشوائياً ومفتاح الدورة ا فر الذي يستخدم في التجفير والفرم.

وبعد إرسال الوثيقة، يرسل مطراف الإرسال عدداً عشوائياً ومفتاح دورة مجفر كتحد للكيان المستقبل. وفي نفس الوقت، يرسل عدداً عشوائياً وقيمة الفرم ا فرة التي تمكّن الكيان المستقبل من ضمان سلامة الوثيقة الواردة. ويرسل مطراف الاستقبال عدداً عشوائياً وصيغة التحدي المعاد تجفيرها من الكيان المرسل. وفي نفس الوقت، يرسل عدداً عشوائياً ووثيقة تكاملية مجفرة كتأكيد أو رفض لسلامة الوثيقة الواردة. وتنفذ خوارزمية الفرم المستخدمة في تأكيد سلامة الوثيقة على الوثيقة بأكملها.

ويوجد أسلوب تجاوز، لا يتضمن تبديل أي إشارات أمن بين المطرافين. ويوافق المستعملون على مفتاح دورة سري لمرة واحدة لإدخاله يدوياً. وهذا هو ما يستخدمه المطراف المرسل لتجفير الوثيقة وما يستخدمه المطراف المستقبل لفك تجفير الوثيقة.

2.3.6 أمن الفاكس باستخدام خوارزمية ريفست وشامير وأدلمان

يحدد الملحق حاء بالتوصية T.30 الآليات التي توفر خصائص الأمن القائمة على أساس الآلية ا فرة لخوارزمية ريفست وشامير وأدلمان. وللاطلاع على مزيد من التفاصيل عن خوارزمية ريفست وشامير وأدلمان، يمكن الرجوع إلى [ApplCryp، الصفحات من 466 إلى 474]. وقد يكون مخطط تشفير الوثيقة المرسلة باستخدام خصائص الأمن من أي نوع من الأنواع المشار إليها في التوصيتين T.4 وT.30 (Modified Huffman، MR، MMR وأسلوب السمة كما هو مبين في الملحق دال بالتوصية T.4 ونقل ملف اثنيني BFT وأسلوب نقل ملف آخر معرف في الملحق جيم بالتوصية T.4).

والخوارزمية الأساسية المستخدمة للتوقيع الرقمي (الاستيقان من أنواع الخدمات وسلامتها) هي خوارزمية ريفست وشامير وأدلمان باستخدام زوج "مفاتيح عمومية"/"مفاتيح سرية".

وعند توفير خدمة سرية اختيارية، تجفر الإذنة التي تحتوي على مفتاح الدورة المستخدمة لتجفير الوثيقة أيضاً بواسطة وسائل خوارزمية ريفست وشامير وأدلمان. وزوج المفاتيح المستخدم لهذا الغرض المسمى ("المفتاح العمومي إ فر"/"المفتاح السري ا فر") ليس هو نفسه الذي يستخدم لخدمات أنواع الاستيقان وسلامة البيانات. وهذا من أجل فك الاقتران بين نوعي الاستخدام.

وتنفيذ خوارزمية ريفست وشامير وأدلمان المستخدمة موضح في الملحق حاء في ISO/IEC 9796 (مخطط توقيع رقمي يعطي استرجاع الرسالة).

ولتجفير إذنة تحتوي على مفتاح دورة، تكون القواعد البديلة عند معالجة خوارزمية ريفست وشامير وأدلمان هي نفس الخوارزميات المحددة في ISO/IEC 9796. وينبغي ملاحظة أن بعض الإدارات قد تطلب آلية خوارزمية التوقيع الرقمي [ApplCryp، الصفحات من 483 إلى 502] لتنفيذها بالإضافة إلى خوارزمية ريفست وشامير وأدلمان.

والمعتاد في حالة عدم وجود قواعد أخرى، لا تستخدم *سلطات إصدار الشهادات* المبينة في مخطط الملحق حاء بالتوصية T.30، ومع ذلك فإ ا 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 X.509. ويرد وصف وسائل إرسال شهادة المفتاح العمومي للمرسل في الملحق حاء، ولكن يترك الشكل الدقيق للشهادة للدراسة في المستقبل ويجري التفاوض بشأن الإرسال الفعلي للشهادة في البروتوكول.

وكخاصية إلزامية، يتوفر *أسلوب التسجيل*، 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 (تكون المفاتيح العمومية طويلة بعض الشيء، 64 أثونتاً أو أكثر).

ولأن أسلوب التسجيل يسمح بتبادل المفاتيح العمومية وتخزينها في المطاريف، ليس من الضروري إرسالها عند إجراء اتصالات الفاكس.

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

إن وظائف الفرم التي يمكن استخدامها هي إما (SHA-1، *خوارزمية الفرم الآمنة*) وهي خوارزمية تأتي من المعهد الوطني للمعايير والتكنولوجيا في الولايات المتحدة أو ملخص الرسالة رقم 5 (RFC 1321). وبالنسبة لخوارزمية الفرم الآمنة – 1، يكون طول نتيجة عملية الفرم هو على 160 بتة، وبالنسبة لملخص الرسالة رقم 5، يكون طول نتيجة عملية الفرم هو على 128 بتة. ويمكن لمطراف مطابق للملحق حاء بالتوصية T.30 تنفيذ إما خوارزمية فرم آمنة – 1 أو ملخص الرسالة رقم 5 أو كليهما. ويجري التفاوض بشأن استخدام خوارزمية واحدة أو أخرى في البروتوكول (انظر ما يلي).

ويعد تجفير البيانات من أجل توفير خاصية السرية اختياري. ويجري تسجيل خمسة مخططات تجفير اختيارية في نطاق الملحق حاء بالتوصية T.30: FEAL-32 وSAFER K-64 وRC5 وIDEA وHFX40 (كما ورد في التوصية T.36). وقد يخضع استخدامها، في بعض البلدان، للقواعد الوطنية.

ويمكن استخدام خوارزميات اختيارية أخرى أيضاً، على أن يكون اختيارها مطابقاً للمعيار ISO/IEC 9979 (إجراء لتسجيل خوارزميات مجفرة).

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

4.6 تطبيقات إدارة الشبكة

من الضروري، كما جاء في القسم الخاص بمتطلبات إطار الأمن، تأمين حركة الإدارة المستخدمة لرصد ومراقبة شبكة الاتصالات. وتقسم حركة الإدارة عادة إلى فئات على أساس المعلومات المطلوبة للتعامل مع الأعطال، والتشكيل، والأداء، والمحاسبة، ووظائف إدارة الأمن. ويتناول مجال إدارة الأمن كلاً من إقامة شبكة الإدارة الآمنة وكذلك إدارة أمن المعلومات المتصلة بالمستويات والطبقات الثلاث لأمن المعمارية. ويرد وصف الأخيرة في هذا القسم.

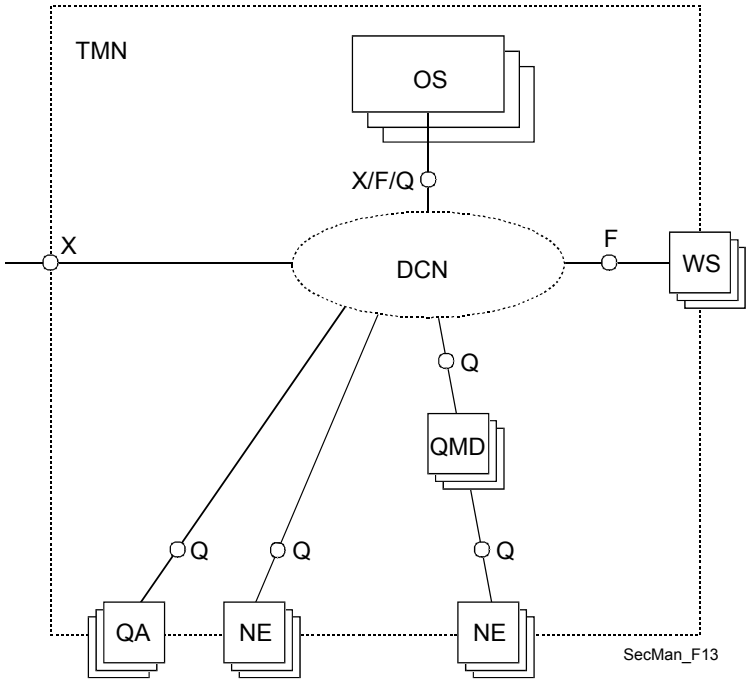
وتقليدياً في شبكة الاتصالات، ترسل حركة الإدارة غالباً على شبكة منفصلة تحمل فقط حركة إدارة الشبكة وليس حركة المستعملين. ويشار غالباً إلى هذه الشبكة بشبكة إدارة الاتصالات الوارد وصفها في التوصية ITU-T T.3010. وتكون شبكة إدارة الاتصالات منفصلة ومعزولة عن البنية التحتية للشبكة العمومية وذلك عند حدوث انقطاع نتيجة لوجود ديد على الأمن في مستوى المستعمل النهائي في الشبكة العمومية لا ينتشر إلى شبكة إدارة اتصالات. ونتيجة هذا الانفصال، من السهل نسبياً تأمين حركة شبكة الإدارة لأن النفاذ إلى هذا المستوى يكون مقصوراً على مديري الشبكة المخولين وتقتصر الحركة على أنشطة الإدارة الصالحة. ومع استخدام شبكات الجيل القادم، قد يتم الجمع بين تطبيق حركة المستعمل النهائي وتطبيق حركة الإدارة، في بعض الأحيان. وعلى الرغم من أن هذا المنهج يساعد على تقليل التكاليف إلى أدنى حد لأنه لا يتطلب فقط وجود بنية تحتية لشبكة متكاملة وحيدة، فإنه يؤدي أيضاً إلى ظهور كثير من تحديات الأمن الجديدة. إذ تصبح التهديدات في مستوى المستعمل النهائي ديدات على مستويات الإدارة والمراقبة، ويصبح مستوى الإدارة مفتوحاً للنفاذ أمام العديد من المستعملين، ويصبح من الممكن حدوث أنواع كثيرة من الأنشطة الخبيثة.

ولتوفير حل كامل من طرف إلى طرف، ينبغي أن تطبق جميع تدابير الأمن (مثل مراقبة النفاذ والتوثيق) على كل نوع من أنواع نشاط الشبكة (أي نشاط مستوى الإدارة ونشاط مستوى المراقبة ونشاط مستوى المستعمل النهائي) للبنية التحتية للشبكة، وخدمات الشبكة، وتطبيقات الشبكة. ويوجد عدد من توصيات قطاع تقييس الاتصالات يركز بشكل محدد على جانب الأمن على مستوى إدارة عناصر الشبكة، وأنظمة الإدارة التي تعد جزءاً 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 تحتاج إليها وكالات تقديم الخدمات المختلفة للتفاعل من أجل تقديم خدمات من طرف إلى طرف، مثل الخطوط المؤجرة للزبائن عبر الحدود الجغرافية أو الهيئات التنظيمية أو الحكومية لدعم العمليات اللازمة في حالات الكوارث.

1.4.6 معمارية إدارة الشبكات

تتضمن التوصية M.3010 تعريف معمارية إدارة شبكات الاتصالات، ويوضح الشكل 13 المعمارية المادية. وتحدد شبكة الإدارة الأسطح البينية التي تحدد البدالات المطلوبة لأداء وظائف العمليات والإدارة والصيانة وتوفير الخدمة على مستويات مختلفة.



سطح بيني
DCN شبكة اتصالات البيانات
NE عنصر الشبكة
OS نظام العمليات
WS محطة العمل

الشكل 13
مثال لمعمارية مادية في M.3010

تتفاوت متطلبات الأسطح البينية المختلفة، من منظور الأمن. ويوجد السطح البيني Q في داخل ميدان إداري واحد، بينما يوجد السطح البيني X بين ميادين إدارية قد تمتلكها وكالات مختلفة من وكالات تقديم الخدمات. وبينما توجد حاجة إلى خدمات الأمن في كل من Q وX، تشتد الحاجة إلى تدابير مطلوبة لمواجهة التهديدات وتصبح أكثر ضرورة في حالة السطح البيني X. وتتضمن التوصية M.3016 الصادرة عن قطاع تقييس الاتصالات بنظرة شاملة على ديدات الأمن، وجوانب الضعف وتدابير الأمن اللازمة مع الإفاضة في بيان تفاصيل جوانب الأمن اللازمة للسطح البيني X في التوصية ITU-T M.3320. وتتضمن التوصيتان ITU-T Q.811 وITU-T Q.812 جوانب البروتوكول الخاص بالطبقات المختلفة للاتصالات.

وعند مناقشة الأمن في سياق الإدارة يبرز جانبان. يتعلق أحدهما بمستوى الإدارة لنشاط من طرف إلى طرف (مثل خدمات نقل الصوت باستعمال بروتوكول الإنترنت). وينبغي أداء نشاط الإدارة الذي يتطلب إدارة المستعملين بطريقة آمنة. وهذا ما يشار إليه *بأمن معلومات الإدارة* المبدل عبر شبكة لتنفيذ التطبيق من طرف إلى طرف. والجانب الآخر هو إدارة معلومات الأمن. وبغض النظر عن التطبيق، مثل نقل الصوت باستعمال بروتوكول الإنترنت أو نشاط الإخبار عن عطل بين وكالتين لتقديم الخدمة، ينبغي إدارة تدابير الأمن مثل استخدام مفاتيح التجفير. ويشار إليها غالباً *بإدارة معلومات الأمن*. وتعتبر البنية التحتية للمفاتيح العمومية المعرفة في القسم السابق مثالاً لهذا الجانب. وتتضمن التوصية ITU-T M.3400 تعريف عدد من الوظائف المتعلقة بكلا الجانبين.

واستناداً إلى الإطار الوارد بالتوصية X.805، وضِعت توصيات عديدة تتناول وظائف إدارة لثلاث خلايا لمستوى الإدارة. وتوضح الأقسام الفرعية الواردة فيما يلي بعض هذه التوصيات وتبين كيف تتناول احتياجات الأمن. وبالإضافة إلى التوصيات للطبقات الثلاث لمستوى الإدارة، توجد توصيات أخرى تتضمن تعريف الخدمات القياسية أو المشتركة مثل إصدار الإنذارات عند حدوث انتهاك مادي للأمن، ووظائف التدقيق، ونماذج معلومات تعريف مستويات حماية الأهداف المختلفة (أي كيانات إدارة).

2.4.6 مستوي الإدارة وتقاطع طبقة 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، ينبغي أن يؤدي المستعمل المخول أنشطة مثل توفير عنصر الشبكة. ويمكن النظر في التوصيلية من طرف إلى طرف على أساس شبكة (أو شبكات) النفاذ ولب الشبكة (أو شبكات). ويمكن استخدام تكنولوجيات مختلفة في هذه الشبكات. وقد تم وضع توصيات تتناول كلاً من شبكات النفاذ والشبكات الأساسية. ومن بين الحالات التي نوقشت هنا الشبكة البصرية المنفعلة ذات النطاق العريض (BPON) المستخدمة في النفاذ. وتتضمن التوصية Q.834.3 إدارة مميزات مستعمل شبكة النفاذ باستخدام منهجية وضع النماذج الموحدة، بينما تتضمن التوصية Q.834.4 تعريف بدالة الإدارة باستخدام معمارية طلب وسيط لغرض مشترك (CORBA). والسطح البيني المشار إليه في هذه التوصيات هو السطح البيني Q المبين في الشكل 13. ويطبق بين نظام إدارة العناصر وأنظمة إدارة الشبكات. ويستخدم الأول لإدارة عناصر الشبكة الفردية، وبالتالي يتضمن التفاصيل الداخلية لمعماريات عتاد وبرمجيات العناصر التي يقوم بتوريدها طرف واحد أو أكثر، بينما يقوم الثاني بأنشطة على مستوى الشبكة من طرف إلى طرف ويتناول أنظمة إدارة العديد من الموردين. ويبين الشكل 14 الأغراض المختلفة المستخدمة لإنشاء، وإلغاء، وتخصيص، واستخدام معلومات مراقبة النفاذ لمستعملي نظام إدارة العناصر. وتحتوي قائمة تصاريح المستعملين على قائمة أنشطة الإدارة المسموح ا لكل مستعمل مخول. ويتحقق مدير مراقبة النفاذ من هوية المستعمل وكلمة سر المستعمل لنشاط الإدارة ويمنحه حق النفاذ إلى العناصر الوظيفية المسموح ا في قائمة التصاريح.

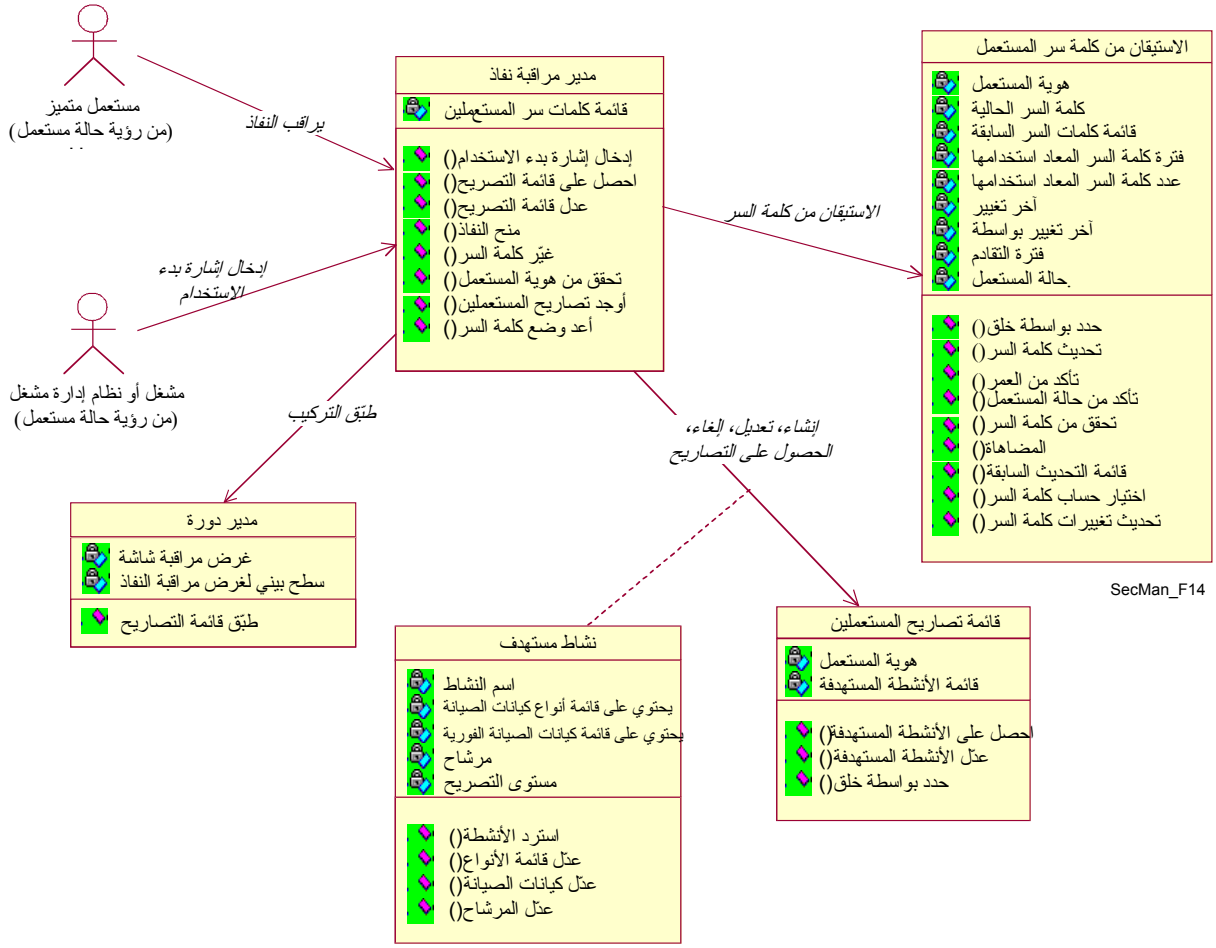
3.4.6 مستوي الإدارة وتقاطع طبقة الخدمات

يتعلق التقاطع بين مستوي الإدارة وطبقة الخدمات بتأمين الأنشطة التي تدخل في رصد ومراقبة موارد الشبكة المخصصة لخدمات التسليم بواسطة وكالة تقديم الخدمات. وتتناول توصيات قطاع تقييس الاتصالات جانبين لهذا التقاطع، يضمن أحدهما توفير تدابير الأمن الملائمة للخدمات المتاحة على الشبكة. ومن أمثلة ذلك ضمان السماح للمستعملين الصالحين بأداء العمليات المرتبطة بتوفير الخدمة، بينما يتناول الجانب الثاني تعريف البدالات الإدارية والإدارة الصالحة. ويساعد مثل هذا التعريف على اكتشاف انتهاكات الأمن. وعندما توجد انتهاكات للأمن، يتم إدار ا غالباً باستخدام أنظمة إدارة محددة.

ومن أمثلة التوصيات التي تتناول الجانب الأول، وهو نشاط إدارة الخدمات، 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/تنشيط، 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 هذه الخدمة هي مجموعة أبعاد الأمن الثمانية الفرعية التي نوقشت في القسم 5.2، وهي الاستيقان من كيان نظير، ومراقبة سلامة البيانات (لمنع التعديل غير المخول للبيانات أثناء العبور)، ومراقبة النفاذ (لضمان عدم حصول مشترك واحد على نفاذ لبيانات مشترك آخر عن قصد أو بشكل عرضي).

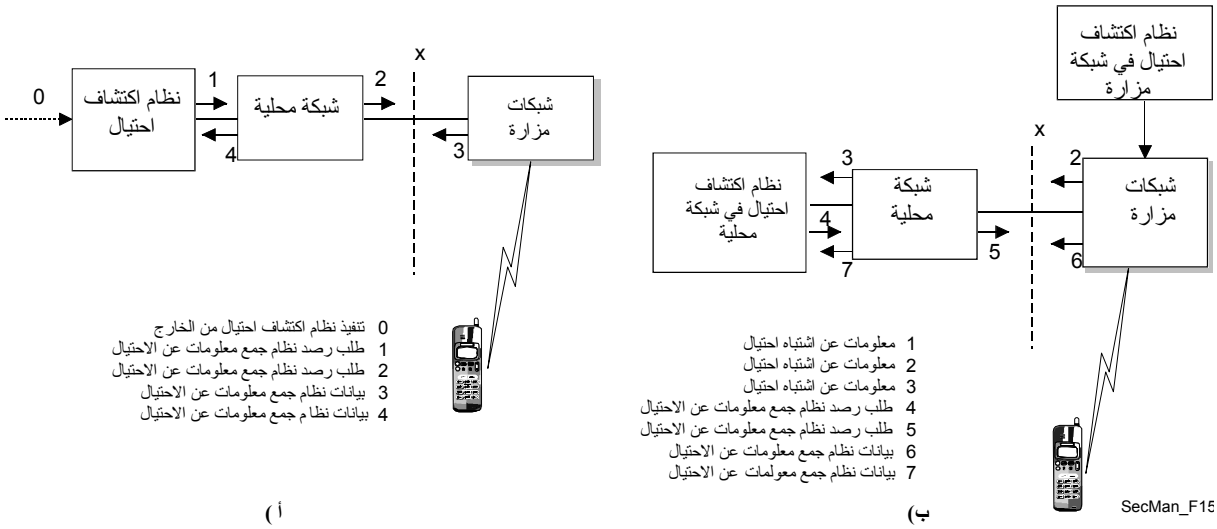
وتعد التوصية ITU-T M.3210.1 مثالاً لتوصية تتضمن تعريف الأنشطة الإدارية المرتبطة بمستوى الإدارة للخدمات اللاسلكية. وينسجم ذلك مع الجانب الثاني الذي سبقت مناقشته.

وفي الشبكة اللاسلكية، قد يعبر المستعملون وهم ينتقلون من الشبكة المحلية إلى شبكة أخرى، ميادين إدارية مختلفة. وتصف الخدمات المعرفة في التوصية ITU-T M.3210.1 كيف أن الميدان الذي تتعرض إدارته للاحتيال في الموقع المحلي يقوم بجمع المعلومات الملائمة حول المشترك بمجرد تسجيله على الشبكة التي يزورها. ويوضح كل من السيناريو (أ) والسيناريو (ب) في الشكل 15 الشروع في رصد نشاط الإدارة سواء بواسطة الشبكة المحلية أو الشبكة التي يزورها المشترك.



الشكل 14

إدارة ميزات المستعمل بموجب التوصية Q.834.3



الشكل 15

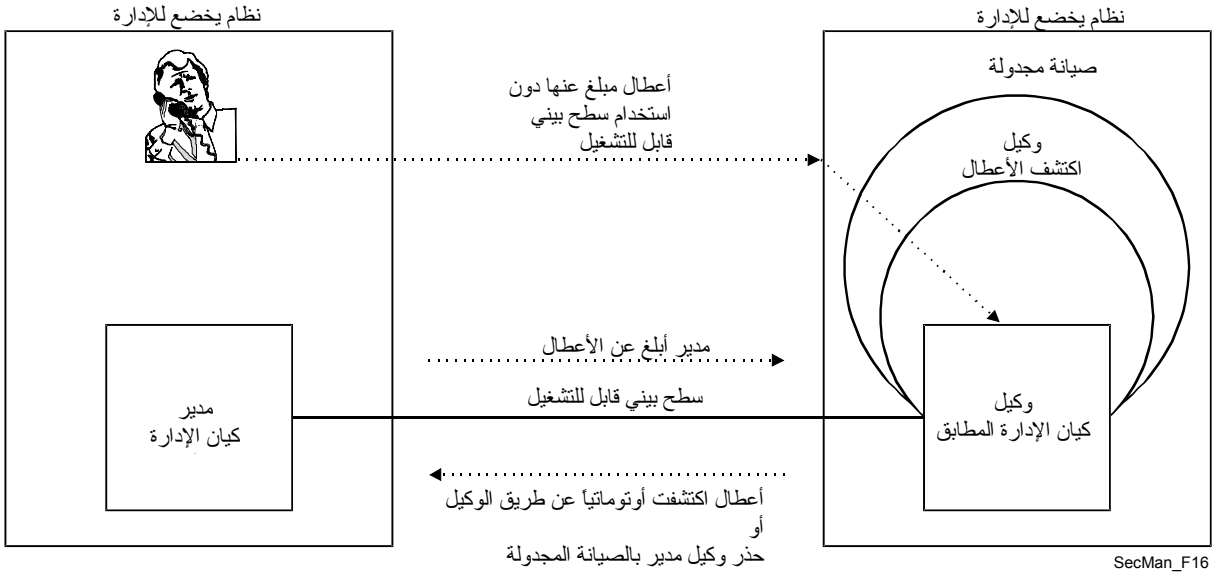
إدارة مقاومة الاحتيال في الخدمات اللاسلكية بموجب التوصية M.3210.1

4.4.6 مستوي الإدارة وتقاطع طبقة التطبيق

الخلية الثالثة المتناظرة مع تقاطع مستوي الإدارة وطبقة التطبيق تتطابق مع تأمين التطبيقات القائمة على شبكة المستعمل النهائي. وتتضمن سلسلة التوصيات X.400 وX.500 تعريف تطبيقات مثل التراسل والدليل.

والنوع الآخر من التطبيقات التي يجري فيها تأمين أنشطة الإدارة هي تطبيقات الإدارة نفسها. وهذا القول ينطوي على نوع من الالتفاف ومن الأفضل شرحه باستخدام الأمثلة. فالمستعملون النهائيون لهذه التطبيقات هم موظفو الإدارة (العمليات) في إدارة الوكالة التي تقدم الخدمة. ولننظر في حالة تقوم فيها إحدى وكالات تقديم الخدمات باستخدام خدمات التوصيل التي توفرها وكالة أخرى من أجل توفير خدمة التوصيل من طرف إلى طرف. واعتماداً على البيئة التنظيمية أو بيئة السوق، قد توفر بعض وكالات تقديم الخدمة خدمات النفاذ، وقد توفر الوكالات الأخرى، التي يشار إليها بالشركات الناقلة فيما بين البدالات، خدمة التوصيل لمسافات بعيدة. وتؤجر الشركات الناقلة فيما بين البدالات خدمات النفاذ من طرف إلى طرف من وكالة محلية عن طريق وصلات موزعة جغرافياً في أماكن متعددة. وعند مواجهة فقدان الخدمة يستخدم تطبيق إدارة يسمى إدارة تقرير الأعطال للتبليغ عن الأعطال التي تحدث بين أنظمة الإدارة. ويتطلب مستعمل هذه الأنظمة وكذلك التطبيق نفسه تخويلاً للإبلاغ عن حدوث أعطال في الخدمة. وينبغي للأنظمة المخولة والمستعملين العمل على إصلاح الأعطال المبلغ عنها. ويوضح الشكل 16 التفاعلات التي ينبغي تنفيذها بطريقة آمنة. ومثل ما يحدث في إدارة صناديق البريد في التطبيق الخاص بالبريد الإلكتروني، تدار امتيازات النفاذ لمنع النفاذ غير المخول إلى تقارير الأعطال. ويسمح لوكالة تقديم الخدمة بالتبليغ فقط عن الأعطال في الخدمات التي تؤجرها وليس في الخدمات التي تؤجرها الوكالات الأخرى.

وتتضمن التوصية X.790 تعريف هذا التطبيق وتستخدم آليات مثل قائمة مراقبة النفاذ والاستيقان المتبادل لتأمين الأنشطة. وقد نفذ هذا التطبيق مع آليات أمن الاستيقان باستخدام هذه التوصيات.



الشكل 16
وضع تقرير عن إدارة الأعطال بموجب التوصية ITU-T X.790

5.4.6 خدمات إدارة الأمن المشتركة

تتضمن التوصيات X.736 وX.740 وX.741 تعريف الخدمات المشتركة التي تطبق على جميع الخلايا الثلاث لمستوى الإدارة لدى استخدام بروتوكول معلومات الإدارة المشتركة عند السطح البيني. وتبلغ أنظمة الإدارة بأنواع الانتهاكات مثل الانتهاك المادي للأمن بموجب التوصية X.736 وكذلك بالتحذيرات المترتبة على مثل هذه الانتهاكات. ويندرج هذا النشاط ضمن مستوى الإدارة الذي يمكن إستخدامه في التبليغ عن انتهاك الأمن عندما يحصل مستعمل غير مخول على نفاذ لأداء أنشطة يوفرها عنصر الشبكة أو اشتراك مستعملين في خدمات أو صناديق بريد. وتوضح وظيفة التدقيق المبينة في التوصية X.740 كيفية تسجيل أحداث انتهاك الأمن، ويمكن أن تطبق على الطبقات الثلاث. وتتضمن التوصية X.741 تعريف نموذج عام وشامل يسمح بتعيين مزايا مراقبة النفاذ المعطاة لأنشطة الإدارة بشكل مستقل عن الأهداف. والنموذج غني بالخواص من خلال تعريف القدرة على تعيين مزايا عند مستوى دقيق من خواص الأهداف.

كذلك اعتمدت التوصية Q.816 الصادرة عن قطاع تقييس الاتصالات خدمات الأمن القياسية التي وضع تعريفها منتدى فريق الإدارة بالأهداف (OMG) لأنشطة الإدارة باستخدام نموذج معيارية طلب وسيط لغرض مشترك (CORBA).

5.6 الوصفات الطبية الإلكترونية

يتطلب توفير الرعاية الصحية، ويولّد مجموعة واسعة من البيانات والمعلومات، وهذا يستدعي جمع هذه البيانات والمعلومات ومعالجتها وتوزيعها والنفاذ إليها واستخدامها – بأمان وباحترام للقواعد الأخلاقية والتشريعية. ويعد هذا حيوياً بصورة خاصة بالنسبة للمعلومات الإكلينيكية والإدارية، فضلاً عن أهميته أيضاً لأنواع أخرى من المعلومات مثل معلومات قواعد البيانات الخاصة بالأوبئة والأدبيات والمعارف الأخرى.

وتوجد مصادر هذه الأنواع من البيانات والمعلومات داخل وخارج البنية التحتية للرعاية الصحية، وتوجد على مسافات متفاوتة من مستعمليها. ومن الناحية العملية، يتطلب المستعملون ويولدون خليطاً من أنواع المعلومات هذه وعلى مستويات مختلفة في وظائفهم، كأن يستشير طبيب قاعدة بيانات بينما يقوم بفحص مريض ويدخل البيانات ذات العلاقة في سجل المريض وقد تستخدم هذه البيانات في أغراض الفوترة.

واللقاءات والمعاملات المرتبطة بالرعاية الصحية متعددة الأوجه. فهي تحدث، مثلاً، بين مريض وطبيب؛ وبين طبيبين؛ وبين طبيب وخبير استشاري؛ وبين مريض ومؤسسة صحية مثل المختبرات أو الصيدليات أو مراكز إعادة التأهيل. ويمكن أن تحدث جميع هذه اللقاءات في مجتمع أي شخص وفي جزء آخر من البلاد أو في الخارج. وجميع هذه التصرفات تتطلب بيانات ومعلومات قبل البدء فيها ويحدث نفس الشيء خلال اللقاء أو بعده مباشرة. وقد تكون هذه البيانات والمعلومات بأحجام مختلفة وفي أوقات مختلفة وفي أشكال مختلفة مثل الصوت والأرقام والنصوص والرسومات البيانية والصور الساكنة أو المتحركة، وقد تكون أحياناً خليطاً من كل ذلك.

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

وفي الماضي، كانت جميع هذه اللقاءات تتم وجهاً لوجه، وكانت الكلمة المنطوقة والمكتوبة هي الأسلوب الرئيسي للاتصالات والاحتفاظ بالسجلات الطبية، وكان نقلها يتم أساساً بواسطة الخدمات العامة والخاصة باستخدام الطرق البرية أو السكك الحديدية أو الطائرات. ومع زيادة شبكات الخدمات الهاتفية، أصبحت شبكات الاتصالات هي وسيلة الاتصال بين المهنيين والمؤسسات الصحية، الوطنية والدولية، إلى أن ظهرت الأدوات التليماتية الحديثة وأصبحت تستخدم في ا لالات الطبية واتسع انتشارها.

وتزداد استخدامات التكنولوجيا بشكل مطرد في الجوانب الإكلينيكية/الطبية لخدمات الرعاية الصحية، بما في ذلك الأجهزة والمعدات، ولا سيما معدات الاستشعار والقياس وخدمات المختبرات والتصوير الدينامي. ومع نمو استخدامات هذه التكنولوجيات وتنوعها وتطورها، لا يمكن تجنب أن تصبح الخدمات التكنولوجية هذه منفصلة عن مؤسسات الرعاية الصحية الأساسية - منفصلة من ناحية المسافة وكذلك من حيث الإدارة، وهذا هو الأهم. ولذلك، أصبحت الاتصالات بين الخدمات القائمة على التكنولوجيا والخدمات الرئيسية للرعاية الصحية من الاعتبارات المهمة في كفاءة مثل هذه الخدمات واقتصادها.

وقد بدأ استخدام تكنولوجيا المعلومات والاتصالات من قِبل قطاع الرعاية الصحية ينتشر منذ أكثر من 25 عاماً عن طريق المراسلات الإلكترونية البسيطة (البريد الإلكتروني) التي تحمل مذكرات هجائية رقمية وتقارير. ومثلما كانت الاتصالات الصوتية هو الدافع الرئيسي لتركيب الهواتف في عيادات الأطباء ومؤسسات الرعاية الصحية، كان البريد الإلكتروني بداية التبرير الرئيسي لتركيب وصلات الاتصالات الحديثة. ومع نمو خدمات البريد الإلكتروني، زادت أيضاً الطلبات على أدائها وتغطيتها الجغرافية: زيادة في عدد الأماكن التي تتاح فيها هذه الخدمة بمزيد من السرعة مع زيادة عرض النطاق لمواجهة الزيادة في مرفقات رسائل البريد الإلكتروني. وشهدت السنوات العشر الأخيرة نمواً مطرداً في استخدام البريد الإلكتروني في قطاع الصحة في داخل البلدان وفيما بينها، حتى في أفقر البلدان، ولا سيما عبر الإنترنت. فمثلاً، حلت المعاملات الإلكترونية محل الوظائف التي لا تتطلب مواجهات وجهاً لوجه مثل إعداد وإرسال الوصفات الطبية، والتقارير، وتحديد المواعيد، وجدولة الخدمات، وتحويل المرضى، وعندما يسمح أداء خدمات الاتصالات، يتم أيضاً إرسال الصور الطبية وقراءات الخبراء المصاحبة لها، سواء كانت مكتوبة أو شفهية.

والمستوى الآخر لتطور استخدامات تكنولوجيا المعلومات والاتصالات هو في مجال الطب عن بعد، وهو "توفير الرعاية الطبية باستخدام الاتصالات الصوتية والمرئية والبيانات"، بما في ذلك التشخيص الفعلي والفحص، وحتى العناية بالمرضى الموجودين في أماكن نائية. والطب عن بعد هو مجال مهم ومتزايد الانتشار، ومن المتوقع أن يؤدي إلى تغيير مناهج تقليدية كثيرة في مجال الرعاية الصحية؛ ويعد في الواقع بداية لنموذج جديد للرعاية الطبية.

وا ال الآخر الذي يجري الحديث عنه منذ فترة قريبة، ولكنه يزداد اتساعاً بشكل مفيد مع انتشار التليماتية، هو النفاذ إلى الأنظمة القائمة على المعرفة واستخدامها. وهذه الأنظمة، المعروفة أيضاً بالأنظمة الخبيرة وأنظمة دعم اتخاذ القرارات، هي أنظمة توفر مشورة الخبراء والتوجيه بشأن المسائل والإجراءات الطبية العلمية. فمثلاً، عند توافر المعلومات الخاصة بمريض والأعراض التي يعاني منها، يمكن تحديد التشخيص واقتراح إجراء اختبارات إضافية أو اقتراح العلاج.

وجميع هذه التطورات لها تأثير أيضاً على أنظمة معلومات الإدارة المطلوبة والمستخدمة في قطاع الصحة، مثل أنظمة معلومات إدارة المستشفيات. وهذه ليست مجرد أنظمة لإدارة رعاية المرضى في المستشفى بدءاً من الدخول إليها إلى الخروج/الترحيل، ولكنها تشمل أسطحاً بينية متعددة للعاملين الطبيين الأذكياء يستخدمو ا، مثلاً، في أنظمة دعم اتخاذ القرارات الإكلينيكية، ووصلات الطب عن بعد، ومواقع الويب، وما إلى ذلك.

وينبغي ذكر حقيقتين أخريين مسلم ما بالنسبة لموظفي الرعاية الصحية والمرضى، وهما: قدر م على التنقل وحاجتهم إلى حرية التصرف، ومن ثم التركيز على الرعاية الطبية نفسها. وتعني القدرة على التنقل إمكانية حصولهم على المعلومات الطبية المطلوبة، مثل السجل الإلكتروني للمريض، أو الحصول على الآلات أو المعدات من مكان بعيد، وتحديد مكان وجودها في المبنى أو المدينة، وأيضاً داخل البلدان وفيما بينها. وتعني حرية التصرف ضرورة إيجاد حلول لتحديد أماكن وجود هذه الآلات والمعدات لا تتضمن قيام المسؤول الطبي بتدخل يدوي، مثل فتح باب أو الدخول إلى الموقع عن طريق لوحة مفاتيح الحاسوب.

وهكذا، تعتبر الرعاية الصحية من القطاعات التي تقوم على المعلومات شديدة التكثيف. ويعتبر 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.

والمطلب الحيوي هنا هو أن جميع هذه التدفقات ينبغي تحقيقها بطريقة آمنة وسرية، مع الالتزام الصارم بالقواعد واللوائح الأخلاقية والقانونية.

1.5.6 اعتبارات البنية التحتية للمفاتيح العمومية والبنية التحتية للإدارة المتميزة في تطبيقات الصحة الإلكترونية

خلال تسلسل سلطات إصدار الشهادات، تخلق البنية التحتية للمفاتيح العمومية هيكلاً تراتبياً للعالم الواقعي، سواء كان تراتباً من الناحية الجغرافية أو السياسية (أقاليم - بلدان - دول - محليات) أو من حيث الموضوع (صحة - طب - جراحة - جراحة متخصصة - جهات توريد المعدات الجراحية). وفضلاً عن ذلك، فلأن قطاع الصحة هو قطاع كلي وهرمي إلى حد بعيد ويتفاعل بشكل متزايد عبر الحدود، تشتد الحاجة إلى تعريف البنية التحتية للمفاتيح العمومية والبنية التحتية للإدارة المتميزة طبقاً للمعايير القياسية في مجال الرعاية الصحية.

ويتعين ضمان قابلية التشغيل البيني التقني للأنظمة الصحية من خلال الاستخدام المكثف لمعايير التكنولوجيا. وقد اعتمد معظم جهات توفير الحلول الخاصة بالأمن معايير مثل المعايير المبينة في التوصية ITU-T X.509. ولما كان الاستيقان من المستعمل من التطبيقات شديدة الأهمية التي تعتمد على المعلومات المحلية، فإن حرية اختيار البنية التحتية للمفاتيح العمومية والبنية التحتية للإدارة المتميزة ينبغي ألا تؤثر على قدرة المستعمل على التشغيل البيني مع الأشخاص الذين صدقت عليهم البنية التحتية للمفاتيح العمومية/البنية التحتية للإدارة المتميزة في جهة أخرى في قطاع الصحة (وتمتد ذلك على الأقل إلى الحد الأدنى للتقييس فيما يتعلق بمراقبة النفاذ والسياسات الأخرى ذات العلاقة بقطاع الصحة). ولتحقيق ذلك، يمكن وضع استراتيجيات مختلفة يمكن أن تشمل الاعتراف المتبادل بالبنى التحتية المختلفة أو استخدام جِذر مشترك. واعتماد معايير تكنولوجيا وإمكانية التشغيل البيني من الناحية التقنية للبنى التحتية المختلفة وتقييس سياسات معينة يضمن قيام بيئة كاملة الكفاءة ومتكاملة لمعاملات الصحة في جميع أنحاء العالم.

2.5.6 نظام سالفورد للوصفات الطبية الإلكترونية

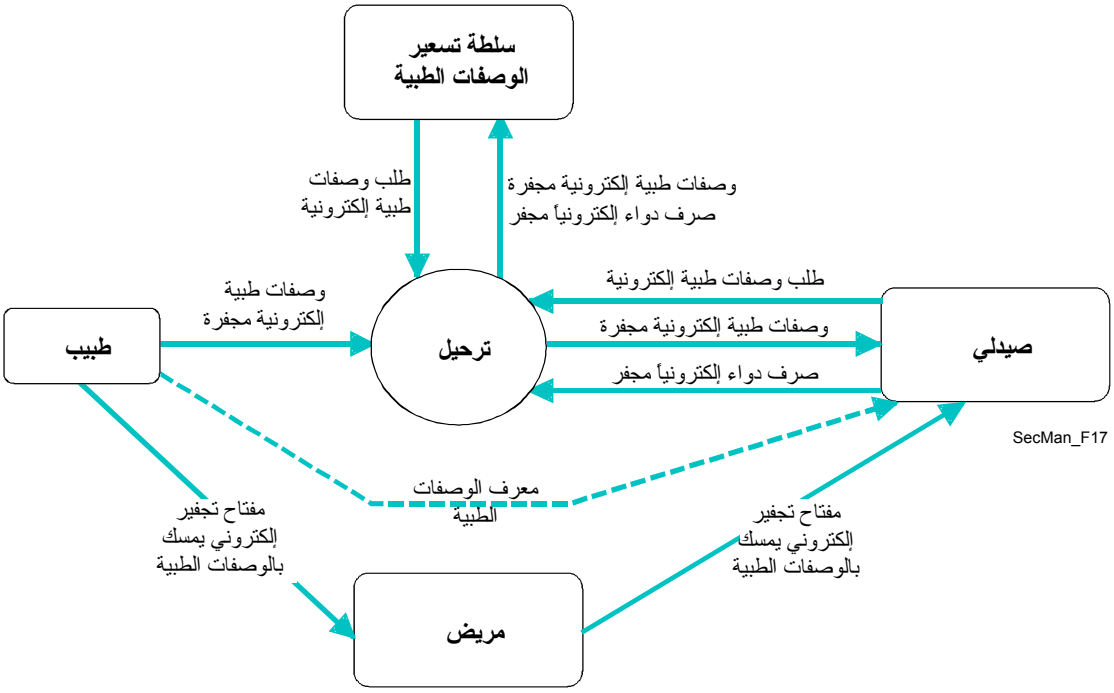
يعد نظام الوصفات الطبية الإلكترونية الوارد في [السياسة] مثالاً جيداً على تطبيق البنية التحتية للمفاتيح العمومية والبنية التحتية للإدارة المتميزة في مجال الصحة الإلكترونية. ونظراً لضخامة عدد المهنيين الذين يعملون في برنامج الإرسال الإلكتروني للوصفات الطبية (ETP) في المملكة المتحدة (500 34 ممارس عام و000 10 ممرضة سيرتفع عددهن إلى 000 120 خلال السنوات القليلة القادمة و000 44 صيدلي مسجل و000 22 طبيب أسنان) وضآلة عدد عمليات الاستيقان المطلوبة (أي مستويات التصاريح المختلفة لوصف العلاج وصرف الدواء واستحقاقات الوصفات الطبية ا انية)، يبدو أن مراقبات النفاذ القائمة على الأدوار (RBAC) هي آلية الاستيقان المثلى لاستخدام الإرسال الإلكتروني للوصفات الطبية. وعندما يقترن ذلك بعدد المرضى المحتملين في المملكة المتحدة (60 مليوناً)، وحقيقة أن الوصفات الطبية ا انية تمثل نسبة 85 في المائة من البنود التي تتضمنها الوصفات الطبية [FreePresc]، ينبغي استخدام مراقبات النفاذ القائمة على الأدوار أيضاً لمراقبة النفاذ إلى الوصفات الطبية ا انية إذا كان ذلك ممكناً. ونظراً لضخامة عدد الأشخاص الذين يلزم تخويلهم، فمن الضروري إدارة الأدوار التي توزع على السلطات المختصة، بدلاً من محاولة إخضاعها لسلطة مركزية، وإلا سيصبح من الصعب إدارة النظام.

وكل مهني يتبع هيئة رسمية تمنح له حق ممارسة مهنته. وا لمس الطبي العام في المملكة المتحدة هو المسؤول عن تسجيل الأطباء وشطبهم من قائمة الأطباء بسبب سوء السلوك. ويؤدي مجلس أطباء الأسنان العام نفس الدور لأطباء الأسنان، بينما يختص مجلس التمريض والقابلات بالترخيص للممرضات والكلية الملكية للصيدلة بالترخيص للصيادلة. وفي نظام الإرسال الإلكتروني للوصفات الطبية المبين فيما سبق، يكون تخصيص هذه الأدوار من حق هذه الهيئات، نظراً لأ ا وظيفة تؤديها على نحو جيد.

وقد تولت إدارة العمل والمعاشات التقاعدية (DWP) التي أنشئت في يونيو 2001، مسؤوليات الإدارات السابقة التي كانت معنية بالضمان الاجتماعي والتعليم والتوظيف. وهي مسؤولة عن دفع إعانات البطالة والمعاشات التقاعدية، كما أ ا - بالإضافة إلى سلطة تسعير الوصفات الطبية (PPA) - مسؤولة أيضاً عن تحديد استحقاق الوصفات الطبية ا انية. ويستحق عدد كبير من الأشخاص الوصفات الطبية ا انية، بما في ذلك: الأشخاص الذين يتجاوزون سن الستين والأطفال تحت سن 16 سنة والشباب الذين تبلغ أعمارهم 16 أو 17 أو 18 سنة من المتفرغين للتعليم، والأشخاص الذين يتلقون دعماً للدخل أو علاوة الباحثين عن عمل، والأشخاص الذين ترد أسماؤهم في شهادة المساعدة الكاملة ضمن نظام الصحة الوطنية (NHS) الحالي الذي يشمل ذوي الدخول المنخفضة، والنساء الحوامل والنساء اللاتي وضعن أطفالاً خلال الاثني عشر شهراً الماضية، والمتقاعدين المعوقين بسبب الحرب. وبناء على ذلك، توزع إدارة هذه المستحقات بين فروع مختلفة لإدارة العمل والمعاشات التقاعدية وسلطة تسعير الوصفات الطبية.

وتخصص كل هيئة مهنية لكل مهني شهادة خواص طبقاً للدور الذي يقوم به، وتخزن هذه الشهادات في دليل بروتوكول نفاذ الدليل خفيف الوزن (LDAP) تابع لتلك الهيئة المهنية. وبوسع نظام الإرسال الإلكتروني للوصفات الطبية اتخاذ قرارات بالتفويض بوصف العلاج وصرف الدواء إذا كان يستطيع النفاذ إلى أدلة بروتوكول نفاذ الدليل خفيف الوزن. وبالمثل، فإذا خصصت إدارة العمل والمعاشات التقاعدية شهادات خواص أدوار للأشخاص الذين يستحقون الحصول على وصفات طبية مجانية لأسباب مختلفة، وأمكن تخزين هذه الشهادات في دليل (أو أدلة) بروتوكول نفاذ الدليل خفيف الوزن، فسوف تتمكن إدارة العمل والمعاشات التقاعدية من اتخاذ قرارات حول استحقاق الوصفات الطبية إ انية بواسطة النفاذ إلى دليل بروتوكول نفاذ الدليل خفيف الوزن دون حاجة إلى أن يطلب الصيدلي من المريض أن يثبت ما إذا كان يستحق ذلك. ويكون ذلك مطلوباً فقط في الحالات التي يكون فيها المريض مستحقاً لأول مرة، مثلاً، عندما يشخص الطبيب أن امرأة حامل لأول مرة، ولا يوجد وقت كاف لإدارة العمل والمعاشات التقاعدية لإنشاء شهادة خواص رسمية.

وتستخدم هذه الأدوار فيما بعد آلة اتخاذ قرار بتخويل (مثل PERMIS، انظر www.permis.org) لتحديد أي الأطباء يسمح لهم بوصف العلاج وأي الصيادلة يسمح لهم بصرف الدواء وأي المرضى يسمح لهم بتلقي الوصفات الطبية مجاناً طبقاً لسياسة الإرسال الإلكتروني للوصفات الطبية. ويقوم كل تطبيق للإرسال الإلكتروني للوصفات الطبية (نظام وصف العلاج ونظام صرف الدواء ونظام سلطة تسعير الوصفات الطبية) بقراءة سياسة الإرسال الإلكتروني للوصفات الطبية قبل تنفيذ ما هو مطلوب، ثم عندما يطلب مهنيون محددون أعمالاً مثل وصف علاج أو صرف دواء، وتبحث آلية اتخاذ قرار التخويل عن دور الأشخاص في دليل بروتوكول نفاذ الدليل خفيف الوزن الملائم، وتتخذ قرارها طبقاً للسياسة المطبقة. ومن ثم، يمكن للمستعملين الحصول على النفاذ إلى تطبيقات متعددة، وكل ما يحتاجونه هو زوج مفاتيح البنية التحتية للمفاتيح العمومية. ويمكن تنفيذ إصدار شهادات خواص الأدوار دون اشتراك المستعمل، وليست هناك حاجة لمعرفة كيف أو أين يجري تخزينها واستخدامها من قبل النظام.



الشكل 17
نظام سالفورد للوصفات الطبية الإلكترونية

يحتوي الشكل 17 على مثال لتنفيذ نظام الوصفات الطبية الإلكترونية في المملكة المتحدة، ويوضح العديد من قضايا الأمن الرئيسية المرتبطة بتنفيذها. وتوجد في قلب النظام بنية تحتية للأمن لا توفر الاستيقان القوي فحسب (أي بنية تحتية للمفاتيح العمومية باستخدام شهادات المفاتيح العمومية)، بل توفر أيضاً التخويل القوي (أي بنية تحتية للإدارة المتميزة) تمنح فيها الحقوق المحددة التي يتمتع ا المهنيون الطبيون بحكم أدوارهم المخزنة في شهادات الخواص. وتستخدم النماذج التقليدية قوائم مراقبة النفاذ المبينة في كل تطبيق (مثل السجلات الطبية، وقواعد بيانات الوصفات الطبية، والتأمين، وما إلى ذلك)، وهي تتطلب من المستعملين (الأطباء، والصيادلة، والمرضى، وما إلى ذلك) الحصول على العديد من تصاريح الأمن الممكنة وإدار ا (مثل اسم المستعمل/كلمات السر، والبطاقات، وغير ذلك). وفي النموذج الجديد الذي يجمع بين البنية التحتية للمفاتيح العمومية والبنية التحتية للإدارة المتميزة، يحتاج المستعمل إلى إذن واحد فقط – هو شهادة المفتاح العمومي للمستعمل - للاستفادة من الخدمات والموارد المختلفة الموزعة جغرافياً و/أو طوبوغرافياً. ويتم الاحتفاظ بشهادات الخواص الخاصة بالمستعمل داخل النظام وليس مع المستعمل وتنتقل هذه الشهادات بين مكونات حسب الرغبة لمنح النفاذ. ونظراً لأن شهادات الخواص موقعة رقمياً من قِبل الجهات التي تصدرها، لا يمكن التلاعب فيها خلال عمليات الانتقال هذه.

وفي المثال المبين في الشكل 17، يحدد الطبيب الوصفات الطبية الإلكترونية ويوقع عليها رقمياً (لأغراض الاستيقان) ويتم تجفيرها تناظرياً باستخدام مفتاح دورة عشوائي (لضمان السرية) ثم ترسل إلى مكان التخزين المركزي. وتعطى 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 يسترد الوصفة الطبية ويفك تجفيرها. ويراقب المريض في النهاية من هو المخول له صرف دواء الوصفة الطبية، كما هو الحال مع الوصفة الطبية الورقية الحالية. إلا أن هذا لا يكفي. فمن الضروري وجود مراقبة على من هو المخول لوصف العلاج، وصرف أي أنواع الأدوية، ومن يحق له الحصول على وصفات طبية مجانية.

والوصف الوارد أعلاه يشير إلى نظام متكامل صارم، قابل بالفعل للتعميم، بحيث يكون دليل خواص الطبيب مختلفاً عن النظام المستخدم في الاستيقان من الصيادلة، أو الذي يقوم بتخزين حقوق وسياسات صرف الأدوية، وما إلى ذلك، مما يعتمد على أطراف أخرى موثوق ا للاستيقان من الأطراف المختلفة وتخويلها. وعلى الرغم من إمكانية تطبيق حلول لملكية البنية التحتية للمفاتيح العمومية والبنية التحتية للإدارة المتميزة، فإن استخدام حلول مثل الحلول التي تنص عليها التوصية ITU-T X.509 يمكن أن يساعد اليوم على تحقيق نفاذ أكثر شمولاً إلى الوصفات الطبية الإلكترونية على المستوى العالمي.

7 الخلاصة

عكف قطاع تقييس الاتصالات طوال مدة طويلة على وضع مجموعة من التوصيات الأساسية بشأن الأمن، منها: التوصية X.800 التي تعد وثيقة مرجعية بشأن معمارية الأمن للتوصيل البيني للأنظمة المفتوحة. وتتضمن سلسلة التوصيات X.816-X.810 تعريف الإطار العام للأمن في الأنظمة المفتوحة بما في ذلك الاستيقان، ومراقبة النفاذ، وعدم التنصل، وسرية البيانات، وسلامة وأمن البيانات، وتحذيرات المدققين. وحديثاً، وضع قطاع تقييس الاتصالات التوصية ITU-T X.805 التي توضح معمارية الأمن في الأنظمة التي توفر الاتصالات من طرف إلى طرف. وتتضمن التوصية X.805 تنقيحاً لمعمارية الأمن يأخذ في الاعتبار التهديدات المتزايدة وجوانب الضعف الناتجة عن ظهور شبكات متعددة وعن البيئة التي تعمل فيها وكالات متعددة لتقديم الخدمات. ومن المؤكد أن التوصية X.509 التي وضعها قطاع تقييس الاتصالات بشأن المفاتيح العمومية وأطر الخواص هي أكثر النصوص التي ترجع إليها الجهات المعنية في تطبيقات الأمن، سواء بشكل مباشر أو ضمني، في إطار المعايير الأخرى التي وضِعت على أساس المبادئ التي تنص عليها التوصية X.509.

وبالإضافة إلى هذه التوصيات الإطارية، قام قطاع تقييس الاتصالات بوضع أحكام للأمن في العديد من الأنظمة والخدمات وقام بتعريفها في صورة توصيات. ويتضمن هذا الكتيب توصيف بعض منها في القسم 6: نقل الصوت باستعمال بروتوكول الإنترنت بموجب التوصية H.323 أو الاتصالات الكبلية باستخدام بروتوكول الإنترنت وتأمين إرسال الفاكس وإدارة الشبكات. ويتضمن الكتيب أيضاً مثالاً على تطبيق المفاتيح العمومية وتطبيقات البنية التحتية للإدارة المتميزة في مجال الصحة الإلكترونية. وتوجد توصيات أكثر من ذلك صادرة عن قطاع تقييس الاتصالات تتناول احتياجات الأمن في الاتصالات و تكنولوجيا المعلومات، ينبغي تطبيقها بحذر. وتعكف لجان الدراسات التابعة لقطاع تقييس الاتصالات في الوقت الحاضر على دراسة هذه الجوانب وغيرها من الجوانب 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 حلقات العمل الدولية بشأن الأمن، أو المشاركة فيها، ووضع مشروع للأمن وإنشاء لجنة دراسات رئيسية تتولى الأعمال المتصلة بالأمن في قطاع تقييس الاتصالات.

المراجع

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

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

[Chadwick] D. W. Chadwick; "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] M. Euchner, P-A. Probst; "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] D. W. Chadwick, D. Mundy; "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 Communication System Security" www.itu.int/ITU-T/studygroups/com17/cssecurity.html (*Section 2* on the Catalogue of ITU-T Recommendations related to Communications System Security; *Section 3* on Compendium of Security Definitions in ITU-T Recommendations)

[Shannon] G. Shannon; "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] S. Mandil, J. Darbellay; "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

الملحق ألف: مصطلحات الأمن

تم اقتباس المختصرات والمصطلحات التالية من توصيات قطاع تقييس الاتصالات ومصادر خارجية أخرى، كما هو مبين فيما يلي. وللاطلاع على موارد تكميلية، يمكن الرجوع أيضاً إلى الملحق ألف-3.

ألف – 1 المختصرات التي يتكرر استعمالها في مجال الأمن

المختصر	التعريف
3DES	[H.235] معيار ثلاثي لتجفير البيانات
A	[M.3010] وكيل
A/M	[M.3010] وكيل/مدير
AA	[X.509] سلطة خواص
AAA	[X.805] الاستيقان والتخويل والمحاسبة
AARL	[X.509] قائمة إبطال سلطة الخواص
ACI	[X.810] معلومات مراقبة النفاذ
ACRL	[X.509] قائمة إبطال شهادة الخواص
AE	[M.3010] كيان تطبيق
AES	[H.235] [J.170] خوارزمية معيارية متطورة للتجفير
AH	[J.170] رأسية الملف، وهي بروتوكول أمن المستخدم لبروتوكول الإنترنت الذي يضمن سلامة الرسائل لرزم بروتوكول الإنترنت الكاملة بما في ذلك رأسية ملف بروتوكول الإنترنت
ASCII	[T.36] الشفرة الأمريكية المعيارية لتبادل المعلومات
ASD	[J.170] بيانات التطبيق المحدد. توفر مجال التطبيق المحدد في رأسية أمن بروتوكول الإنترنت مع عنوان مقصد بروتوكول الإنترنت رقم وحيد لكل تصاحب أمن.
ASN.1	[H.680] ترميز تركيب مجرد رقم 1
ASP	[X.805] مزود خدمة التطبيق
ATM	[X.805] أسلوب نقل لا تزامني
ATM	[M.3010] أسلوب نقل لا تزامني
AuF	[H.530] وظيفة الاستيقان، راجع توصية قطاع تقييس الاتصالات [6] H.510
B(n)	[T.36] قيمة قاعدة (n)
BE	[H.530] عنصر حد، راجع توصية قطاع تقييس الاتصالات [2] H.225. 0 Annex G
BES	[H.235] مخدم طرف خلفي
BML	[M.3010] طبقة إدارة الأعمال
B-OSF	[M.3010] طبقة إدارة الأعمال – وظيفة أنظمة العمليات
BPI+	[J.170] سطح بيني لخط أساسي خاص إضافي هو جزء الأمن من المعيار J.112 الذي يمر على طبقة شفرة الاستيقان من الرسائل
CA	[X.509] [J.170] [H.235] [H.234] سلطة إصدار شهادات. هي منظمة موثوق ا تقبل طلبات لإصدار الشهادات من كيانات وتقوم بالاستيقان من الطلبات وإصدار الشهادات وتحتفظ بحالة المعلومات عن الشهادات. [J.170] وكيل نداء. هو جزء من تركيب رسالة مجفرة يحتفظ بحالة الاتصالات ويراقب جانب خط الاتصالات.
CARL	[X.509] قائمة إبطال سلطة إصدار الشهادات
CBC	[H.235] تسلسل فدرة التجفير
CCA	[H.234] السلطة القطرية لإصدار الشهادات
CFB	[H.235] أسلوب التغذية الراجعة لتجفير
CH_n	[H.530] رقم التحدي n
CM	[J.170] مودم بكبل
CME	[X.790] كيان إدارة مطابق
CMIP	[M.3010] بروتوكول معلومات إدارة مشتركة
CMIS	[X.790] خدمة معلومات إدارة مشتركة

المختصر	التعريف
CMISE	[X.790] عنصر خدمة معلومات إدارة مشتركة
CMS	[J.170] تركيب رسالة مجفرة. [J.170] مخدم إدارة نداء يراقب التوصيلات السمعية. ويسمى أيضاً وكيل نداء في مصطلحات بروتوكول مراقبة باب الوسائط وبرتوكول مراقبة باب التشفير (وهذا مثال على مخدم التطبيقات).
CMTS	[J.112] نظام إ اء مودم بكبل
CNM	[X.790] إدارة شبكة العميل
CORBA	[SANCHO] معمارية وسيط لطلب غرض مشترك
CRL	[H.235] [X.509] قائمة إبطال الشهادات
DCF	[M.3010] وظيفة اتصال للبيانات
DCN	[M.3010] شبكة اتصالات البيانات
dCRL	[X.509] قائمة دلتا لإبطال الشهادات
DES	[H.235] [J.170] معيار تجفير البيانات
DH	[H.235] [H.350] ديفي – هلمان
DHCP	[J.170] [X.805] بروتوكول تشكيل مضيف دينامي
DIB	[X.509] قاعدة معلومات الدليل
DIT	[X.509] شجرة معلومات الدليل
DN	[X.790] اسم متميز
DNS	[H.235] [J.170] [X.805] مخدم اسم الميدان
DOCSIS	[J.170] مواصفات سطح بيني لخدمة البيانات عبر الكبل
DoS	[X.805] رفض الخدمة
DQoS	[J.170] نوعية خدمة دينامية
DS-3	[X.805] مستوى 3 لإشارة رقمية
DSA	[X.509] وكيل نظام الدليل
DSCP	[J.170] نقطة شفرة خدمة تفاضلية. هو مجال في كل رزمة لبروتوكول الإنترنت يعرف خدمة تفاضلية لكل سلوك قفزة. وفي الصيغة 4 لبروتوكول الإنترنت، يعاد تعريف بتة نوع الخدمة لتكون نقطة شفرة خدمة تفاضلية. وفي الصيغة 6 لبروتوكول الإنترنت، يستخدم أثمون نوع الحركة باعتباره نقطة شفرة خدمة تفاضلية. راجع الملحق جيم.
DSS	[H.235] معيار التوقيع الرقمي
DTMF	[H.235] [J.170] تردد متعدد بنغمة مزدوجة (نغمات)
DUA	[X.509] وكيل مستعمل دليل
EARL	[X.509] قائمة إبطال شهادات خواص كيان طرفي
ECB	[H.235] أسلوب كتاب الشفرات الإلكترونية
EC ،ECC	[H.235] نظام تجفير المنحني الإهليلجي (راجع القسم 7.8 من مواصفات أمن منتدى أسلوب النقل اللاتزامني للصيغة 1.1). نظام التجفير بمفتاح عمومي.
EC-GDSA	[H.235] توقيع رقمي لمنحني إهليلجي مع تذييل تماثلي لخوارزمية توقيع رقمية للمعهد الوطني للمعايير والتكنولوجيا (وكيل نظام دليل) (راجع أيضاً [ISO/IEC 15946-2، الفصل 5])
ECKAS-DH	[H.235] مخطط اتفاق مفتاح منحني إهليلجي – ديفي-هلمان. مخطط اتفاق مفتاح ديفي–هلمان باستخدام تجفير منحني إهليلجي
EML	[M.3010] طبقة إدارة العنصر
EOFB	[H.235] أسلوب معزز تغذية راجعة لخرج
E-OSF	[M.3010] طبقة إدارة عنصر – وظيفة نظام العمليات
EP	[H.235] نقطة طرفية
EP_{ID}	[H.530] معرف نقطة طرفية لمطراف متنقل، راجع توصية قطاع تقييس الاتصالات [1] H.225.0
EPRL	[X.509] قائمة إبطال شهادة كيان طرفي بمفتاح عمومي
ESH	[T.36] فرم واضح مخلط ومجفر (24 رقماً عشرياً)
ESIM	[T.36] رسالة سلامة مخلطة ومجفرة. عدد به 12 رقماً عشرياً
ESP	[J.170] أمن مغلف باستخدام أمن بروتوكول الإنترنت
ESSK	[T.36] مفتاح سري مجفر مخلط. عدد يقوم على 12 رقماً عشرياً

المختصر	التعريف
FDS	[M.3210.1] نظام اكتشاف الاحتيال
FEAL	[T.36] خوارزمية تجفير بيانات سريعة هي من عائلة الخوارزميات التي تقابل نصاً واضحاً لقدرات نص مجفر لـ 64 بتة بناء على مفتاح سري له 64 بتة. وهي تشبه معيار تجفير بيانات ولكنها أسهل من وظيفة f. وصممت من أجل السرعة والبساطة مما يجعلها مناسبة لحاسوب صغري أقل تعقيداً (مثل البطاقات الذكية). (في A. Menezes et al., Handbook of Applied Cryptography, CRC Press, 1997)
FIGS	[M.3210.1] نظام جمع معلومات عن الاحتيال
FQDN	[J.170] اسم مجال مؤهل بالكامل. راجع IETF RFC 821 للاطلاع على مزيد من التفاصيل
FTP	[X.805] بروتوكول نقل ملفات
FU	[X.790] وحدة وظيفية
GCA	[H.234] سلطة عامة لإصدار الشهادات
GDMI	[M.3210.1] مبادئ توجيهية لتعريف السطح البيني لإدارة شبكة إدارة الاتصالات
GDMO	[M.3010] مبادئ توجيهية لأغراض مسيرة إدارياً
GK	[H.235] [H.510] [H.530] بواب
GK_{ID}	[H.530] معرف بواب موقع الزيارة، راجع توصية قطاع تقييس الاتصالات [1] H.225.0
GNM	[X.790] نموذج شبكة عامة
GRJ	[H.530] رفض بواب
GRQ	[H.530] طلب بواب
GW	[H.235] بوابة
h[*]	[H.234] نتيجة الوظيفة h المنطبقة على*
H-BE	[H.530] استقبال عنصر حد
HFC	[J.165] ألياف مهجنة/متحدة المحور (كبل)
HFX	[T.30] [T.36] تجفير فاكس هوثورن
H-GK	[H.530] بواب محلي
HKM	[T.36] [T.30] خوارزمية إدارة مفاتيح هوثورن
HKMD1	[T.36] تجفير مزدوج باستخدام خوارزمية إدارة مفاتيح هوثورن
HLF	[H.530] وظيفة تحديد موقع محلي
HMAC	[J.170] شفرة الاستيقان من رسالة مفرومة. تقوم خوارزمية الاستيقان من الرسالة إما على أساس فرم خوارزمية فرم آمن رقم 1 أو ملخص رسالة رقم 5 والمعرفة في طلب تعليقات 2104.
HMAC-SHA1-96	[H.530] شفرة الاستيقان من رسالة مفرومة ذات خوارزمية فرم آمنة 1
$HMAC_z$	[H.530] شفرة الاستيقان من رسالة مفرومة لمفتاح/استجابة مع سر متقاسم Z، وإذا كان Z غير مبين ينطبق سر القفزة التالية
iCRL	[X.509] قائمة إبطال شهادات غير مباشرة
ICV	[H.235] قيمة سلامة التحقق
ID	[H.235] معرف
IDEA	[T.36] الخوارزمية الدولية لتجفير البيانات هي خوارزمية تجفير وضعها Xuejia Lai وJames Massey في سنة 1992 وتستخدم تجفير قدرة مع مفتاح 128 بتة (قدرات 64 بتة مع مفتاح 128 بتة) واعتبرت آمنة جداً بصورة عامة. وتعتبر من بين أفضل الخوارزميات المعروفة. وخلال السنوات العديدة التي استخدمت فيها، لم تنشر أي هجمات عملية عليها بالرغم من محاولة إيجاد بعض هذه الهجمات (http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14-gci213675,00.html)
Idx	[T.36] آخر ستة أرقام لتعريف الفاكس X (رقم هاتف فاكس)
Idy	[T.36] آخر ستة أرقام لتعريف الفاكس Y (رقم هاتف فاكس)
IKE	[J.170] بدالة مفتاح الإنترنت هي آلية إدارة مفتاح تستخدم للتفاوض واشتقاق المفاتيح المرتبطة بالأمن في أمن بروتوكول الإنترنت.
IKE-	[J.170] ترميز معرف للإشارة إلى استخدام بدالة مفتاح الإنترنت مع مفاتيح متقاسمة مسبقاً من أجل الاستيقان.

المختصر	التعريف
IM	[T.36] رسالة سلامة مستخدمة لتأكيد أو رفض سلامة رسالة مستقبلة (12 رقماً عشرياً)
IMT-2000	[M.3210.1] الاتصالات المتنقلة الدولية - 2000
Imy	[T.36] رسالة سلامة يولدها Y لتأكيد أو رفض سلامة رسالة مستقبلة. عدد يقوم على 12 رقماً عشرياً
IN	[M.3010] شبكة ذكية
IP	[X.805] بروتوكول الإنترنت
IPSec	[H.235] [H.530] [J.170] [X.805] أمن بروتوكول الإنترنت
ISAKMP	[H.235] بروتوكول إدارة المفاتيح المرتبطة بالأمن في استخدام الإنترنت
ISDN	[M.3010] شبكة رقمية متكاملة الخدمات
ISTP	[J.170] بروتوكول نقل تشوير الإنترنت
IV	[H.235] متجه التدميث
IVR	[J.170] نظام تفاعلي لاستجابة صوتية
K	[H.530] دورة دينامية/مفتاح وصلة
KDC	[J.170] مركز توزيع المفاتيح
LAN	[M.3010] شبكة منطقة محلية
LDAP	[H.235] بروتوكول نفاذ دليل خفيف الوزن
LLA	[M.3010] معمارية مبنية حسب الطبقات
MAC	[J.170] [H.235] شفرة الاستيقان من الرسائل. بند بيانات طوله ثابت يرسل مع رسالة لضمان سلامة البيانات والمعروف أيضاً بالتحقق من سلامة الرسالة. [J.170] مراقبة نفاذ الوسائط. وهي طبقة فرعية لطبقة وصلة بيانات. وتمر عادة على الطبقة المادية مباشرة.
MAF	[M.3010] وظيفة تطبيق الإدارة
MAN	[M.3010] شبكة منطقة حضرية
MAPDU	[X.790] وحدة بيانات بروتوكول تطبيق الإدارة
MCU	[H.235] وحدة صب متعددة. [H.323] وحدة مراقبة نقاط متعددة
MD5	[H.235] [J.170] ملخص الرسالة رقم 5
MG	[J.170] بوابة وسائط
MGC	[J.170] مراقب بوابة وسائط
MGCP	[J.170] بروتوكول مراقبة بوابة وسائط
MIB	[J.170] [M.3010] قاعدة معلومات الإدارة
MIS	[M.3010] خدمة معلومات الإدارة
MO	[M.3010] أغراض خاضعة للإدارة
mod n	[T.36] مقياس رياضي باستخدام القاعدة n
MPS	[H.235] رتل متعدد لحمولة نافعة
MPx	[T.36] بدائية متبادلة X. عدد يقوم على 16 رقماً عشرياً، يجري توليده فقط بواسطة X. وتنتج بدائية متبادلة بواسطة X باستخدام خوارزمية إدارة مفاتيح هوثورن مع بدائيات مشكلة من رقم تعريف وحيد X ورقم تجفير وحيد X ومعرف X وآخر ستة أرقام لتعريف الفاكس Y
Mpy	[T.36] بدائية متبادلة Y
MRP	[H.530] وكالة تسيير اتصالات متنقلة
MS	[M.3210.1] خدمات إدارة
MSB	[J.170] أكثر البتات دلالة
MT	[H.530] مطراف متنقل، راجع توصية قطاع تقييس الاتصالات [6] H.510
MTA	[J.170] مكيف مطراف الوسائط
NAT	[H.235] ترجمة عنوان الشبكة
NCS	[J.170] تشوير نداء الشبكة
NE	[X.790] [M.3010] عنصر الشبكة
NEF	[M.3010] وظيفة عنصر الشبكة

المختصر	التعريف
NEF-MAF	[M.3010] وظيفة عنصر الشبكة – وظيفة تطبيق الإدارة
NML	[M.3010] [M.3210.1] طبقة إدارة الشبكة
NOC	[X.790] مركز عمليات الشبكة
N-OSF	[M.3010] طبقة إدارة الشبكة – وظيفة أنظمة العمليات
NTP	[H.530] بروتوكول وقت الشبكة
O	[M.3010] اختياري
OA&M	[M.3010] العمليات والإدارة والصيانة
OAM&P	[SANCHO] العمليات والإدارة والصيانة والتوفير
OCSP	[H.235] بروتوكول حالة الشهادة على الخط
ODP	[X.810] معالجة موزعة مفتوحة
OFB	[H.235] أسلوب تغذية راجعة للخرج
OID	[H.235] [H.530] [J.170] [M.3010] معرف الغرض
OS	[M.3010] [X.790] نظام العمليات
OSF	[M.3010] وظيفة أنظمة العمليات
OSF-MAF	[M.3010] وظيفة أنظمة العمليات – وظيفة تطبيق الإدارة
OSI	[M.3010] [X.790] [X.805] [X.810] توصيل بيني للأنظمة المفتوحة
OSS	[J.170] دعم أنظمة العمليات. برمجيات المكتب الخلفي المستخدمة للتشكيل والأداء والأعطال والمحاسبة وإدارة الأمن.
OT	[T.36] مفتاح لمرة واحدة. عدد به من 6 إلى 64 رقماً عشرياً يتفق عليه كل من المستخدمين
Otx	[T.36] مفتاح لمرة واحدة كما استخدمه X لأول مرة في تسجيل X مع Y
Oty	[T.36] مفتاح لمرة واحدة كما استخدمه Y عندما بدأ Y التسجيل مع X لإتمام التسجيل المتبادل، سواء كان مختلفاً أو مماثلاً لمفتاح لمرة واحدة كما استخدمه X
P(n)	[T.36] قيمة الطور (n)
PBX	[M.3010] بدالة فرع خاص
PDU	[H.235] وحدة بيانات البروتوكول
PH	[T.36] فرم واضح لرسالة (24 رقماً عشرياً)
PKCROSS	[J.170] يستخدم مفتاح عمومي للاستيقان الأولي لتجفير إنشاء مفاتيح الحقول الداخلية المرتبطة بسياسات الحقول الداخلية التي تطبق عند إصدار بطاقات خدمة حقول متقاطعة بين الحقول والميادين للدعم الداخلي والخارجي لميادين تشوير من تركيب رسالة مجفرة إلى تركيب رسالة مجفرة.
PKCS	[H.235] [J.170] [X.509] معايير تجفير المفاتيح العمومية
PKI	[H.235] [H.530] [X.509] [J.170] بنية تحتية للمفاتيح العمومية. وهي عملية إصدار شهادات المفاتيح العمومية تشمل معايير وسلطات إصدار الشهادات والاتصالات بين السلطات والبروتوكولات لإدارة عمليات إصدار الشهادات.
PMI	[X.509] البنية التحتية للإدارة المتميزة
PRF	[H.235] وظيفة شبه عشوائية
Primitive	[T.36] عدد مركب من 64 رقماً مشكلاً من رقم هوية وحيد ورقم تجفير وحيد
procREGxy	[T.36] إجراء للتسجيل بين X و Y
procSTKxy	[T.36] إجراء للإرسال الآمن للمفتاح السري من X إلى Y
PRS	[T.36] تتابع شبه عشوائي
PSTN	[SANCHO] شبكة هاتفية عمومية مبدلة
PTO	[M.3010] مشغل الاتصالات العمومية
PTR	[X.790] تقرير جهة تقديم الخدمة عن أعطال
PVC	[X.805] دارة تقديرية دائمة
PW	[H.530] كلمة سر المستعمل المتنقل
QA	[M.3010] مكيف Q
QoS	[SANCHO] نوعية الخدمة

المختصر	التعريف
R	[M.3010] مورد
R_1	[H.530] عدد عشوائي
RADIUS	[J.170] خدمة الاستيقان عن بعد لمستعمل المراقمة الداخلية
RBAC	[X.509] مراقبة نفاذ قائمة على الأدوار
RC4	[J.170] تجفير رتل طولي لمفتاح متغير مقدم في مجموعة تجفير تستخدم لتجفير حركة وسائط في الاتصالات الكبلية باستخدام بروتوكول الإنترنت
RCN	[T.36] عدد تجفير مسجل. وهو عدد يقوم على 16 رقماً عشرياً
RDN	[X.790] اسم متميز نسبي
RIP	[H.530] الطلب الجاري
RKS	[J.170] مخدم يحتفظ بسجل. جهاز يجمع الرسائل المختلفة لحدث ويربط بينها.
RNCn	[T.36] عدد عشوائي غير سري مرتبط بمفتاح التحدي السري. عدد يقوم على 4 أرقام عشرية.
RNIM	[T.36] عدد عشوائي غير سري مرتبط بسلامة الرسالة. عدد يقوم على 4 أرقام عشرية.
RNK	[T.36] عدد عشوائي غير سري يستخدم لتوفير تغاير بدائيات مولدة من بدائية متبادلة X عند تجفير مفتاح سري. عدد يقوم على 4 أرقام عشرية.
RNSRn	[T.36] عدد عشوائي غير سري مرتبط بمفتاح استجابة سري n. عدد يقوم على 4 أرقام عشرية.
RNSSn	[T.36] عدد عشوائي غير سري مرتبط بمفتاح دورة سري n . عدد يقوم على 4 أرقام عشرية.
RRJ	[H.530] رفض التسجيل
RRQ	[H.530] طلب التسجيل
RSA	[T.36] [T.30] [H.235] ريفست وشامير وأدلمان (خوارزمية المفاتيح العمومية)
RSVP	[J.170] بروتوكول حجز موارد
RTCP	[J.170] [H.235] بروتوكول مراقبة النقل في الوقت الفعلي
RTO	[J.170] إمهال إعادة الإرسال
RTP	[J.170] [H.235] [H.225.0] بروتوكول الوقت الفعلي
SA	[J.170] الارتباط بالأمن
SAFER K-64	[T.36] روتين التجفير الآمن والسريع مع خوارزمية مفتاح له 64 بتة استعمله J. L. Massey سنة 1993، ومتكامل مع تجفير قدرة لنص واضح به 64 بتة وقدرات نص واضح (في A. Menezes et al., Handbook of Applied Cryptography, CRC Ress, 1997).
SCn	[T.36] مفتاح التحدي السري، العدد n. عدد يقوم على 12 رقماً عشرياً.
SDH	[M.3010] تراتبية عددية متزامنة
SDP	[J.170] بروتوكول وصف الدورة
SDU	[H.235] وحدة بيانات الخدمة
SG	[J.170] بوابة التشوير هي وكيل تشوير يتسلم/يرسل تشويراً أصلياً لمفتاح التحدي السري عند حافة شبكة بروتوكول الإنترنت. وتقوم وظيفة بوابة تشوير، بصفة خاصة، بترجمة متغيرات مفتاح نظام التشوير رقم 7 لجزء مستعمل الخدمة المتكاملة وبروتوكول تطبيق قدرات إدارة المعاملات في مفتاح نظام التشوير 7 – بوابة الإنترنت لصيغة مشتركة لجزء مستعمل الخدمة المتكاملة وبروتوكول تطبيق قدرات إدارة المعاملات.
SH	[T.36] فرم واضح مخلط (24 رقماً عشرياً)
SHA1	[H.235] خوارزمية الفرم الآمن رقم 1
SI	[X.810] معلومات الأمن
SIP	[X.805] [J.170] بروتوكول الشروع في الدورة. بروتوكول (تشوير) مراقبة طبقة التطبيق من أجل إقامة وتعديل وإ اء دورة مع مشارك أو أكثر.
SIP+	[J.170] بروتوكول الشروع في الدورة الإضافية. تمديد لبروتوكول الشروع في الدورة.
SK	[T.36] مفتاح سري قد يكون مفتاح التحدي السري ومفتاح الاستجابة السري ومفتاح الدورة السري، وما إلى ذلك. عدد يقوم على 12 رقماً عشرياً.
SMAPM	[X.790] آلة بروتوكول تطبيق نظام الإدارة
SMK	[M.3010] معرفة الإدارة المشتركة
SML	[M.3010] [M.3210.1] طبقة إدارة الخدمة
SMO	[X.790] نظرة شاملة على إدارة الأنظمة
SMTP	[X.805] بروتوكول نقل البريد البسيط

المختصر	التعريف
SNMP	[J.170] [X.805] بروتوكول إدارة الشبكة البسيطة
SNTP	[H.530] بروتوكول وقت الشبكة البسيطة
SOA	[X.509] مصدر السلطة
SONET	[X.805] شبكة بصرية متزامنة
S-OSF	[M.3010] طبقة إدارة الخدمة – وظيفة أنظمة العمليات
SRn	[T.36] مفتاح استجابة سري، عدد n. عدد يقوم على 12 رقماً عشرياً.
SRTP	[H.225.0] [H.235] بروتوكول الوقت الفعلي الآمن
SS	[T.36] مفتاح دورة سري مع خوارزمية سلامة البيانات HFX40-I (12 رقماً عشرياً)
SS7	[J.170] [X.805] نظام التشوير رقم 7 هو معمارية ومجموعة من البروتوكولات لأداء تشوير نداء خارج النطاق مع شبكة هاتف
SSK	[T.36] مفتاح سري مخلط. عدد يقوم على 12 رقماً عشرياً
SSL	[X.805] [H.235] طبقة مقبس آمن
SSn	[T.36] مفتاح دورة سري، العدد n، يستخدم مع تجفير الموجه الحاملة و/أو الفرم. عدد يقوم على 12 رقماً عشرياً
SSx	[T.36] مفتاح دورة سري يولده X ليستخدم مع خوارزمية سلامة البيانات HFX40-I (12 رقماً عشرياً)
TCAP	[J.170] بروتوكول تطبيق قدرات المعاملات. هو بروتوكول داخل الرصة في نظام التشوير رقم 7، يستخدم لأداء معاملات قاعدة البيانات عن بعد مع مراقبة تشوير.
TD	[J.170] إمهال لفك التوصيل
TF	[M.3010] وظيفة التحويل
TF-MAF	[M.3010] وظيفة التحويل - وظيفة تطبيق الإدارة
TFTP	[J.170] بروتوكول نقل الملفات غير المهمة
TGS	[J.170] مخدم إصدار البطاقات، وهو نظام فرعي لمركز توزيع مفاتيح مستخدم لمنح بطاقات Kerberos
TKx	[T.36] مفتاح نقل، وهو تجفير لبدائية متبادلة X يولدها X. عدد يقوم على 16 رقماً عشرياً
TLS	[H.235] أمن مستوى النقل
TMN	[X.790] [M.3210.1] [M.3010] شبكة إدارة الاتصالات
T_n	[H.530] ختم الوقت للعدد n
TSAP	[H.235] نقطة نفاذ خدمة النقل
TSP	[X.790] أولوية خدمة الاتصالات
TTP	[X.810] طرف ثالث موثوق به
TTR	[X.790] تقرير أعطال الاتصالات
UCN	[T.36] رقم تجفير وحيد، مثل رقم التجفير الوحيد X، و رقم التجفير الوحيد Y. عدد يقوم على 16 رقماً عشرياً معروف فقط للنظام
UDP	[J.170] بروتوكول كتلة بيانات المستعمل
UIN	[T.36] عدد سلامة وحيد، مثل عدد السلامة الوحيد X وعدد السلامة الوحيد Y، وهو عدد يقوم على 48 رقماً عشرياً معروف فقط للنظام
V-BE	[G.530] عنصر حد مزار
V-GK	[H.530] بواب مزار
VLF	[H.530] وظيفة تحديد مكان الزائر
VoIP	[X.805] نقل الصوت باستعمال بروتوكول الإنترنت
VPN	[X.805] شبكة تقديرية خاصة
W	[H.530] قيمة مركبة مع مركب رياضي لأنصاف مفاتيح ديفي-هلمان
WSF	[M.3010] وظيفة محطة العمل
WSSF	[M.3010] وظيفة دعم محطة العمل
WT	[H.530] إذنة واضحة متنقلة
X	[T.36] اسم كيان واحد

المختصر	التعريف
x	[T.36] لاحقة تعرف ملكية أو يولدها X
X<<Y>>	[H.234] شهادة Y يولدها X
XOR'd	[T.36] OR' d على وجه الحصر
Xp	[H.234] مفتاح عمومي لرفست وشامير وأدلمان لكيان X
Xp[*]	[H.234] تجفير/فك تجفير [*] مع مفتاح عمومي لرفست وشامير وأدلمان. وفي حالة رفست وشامير وأدلمان يجري أداء هذا بواسطة الآسية
Xs	[H.234] مفتاح سري لرفست وشامير وأدلمان لكيان X
Xs[*]	[H.234] تجفير/فك تجفير [*] مع لاحقة تعرف ملكية أو يولدها X. وفي حالة رفست وشامير وأدلمان يجري أداء هذا بواسطة الآسية
XT	[H.530] إذنة مجفرة للاستيقان من مطراف متنقل
Y	[T.36] اسم كيان ثانٍ
y	[T.36] لاحقة تعرف ملكية أو يولدها Y
ZZ	[H.530] سر/كلمة سر متقاسمة للمستعمل المتنقل تتقاسم مع وظيفة استيقان تتوافق معها
ZZMT	[H.530] سر متقاسم لمطراف متنقل متقاسم مع وظيفة استيقان تتوافق معه
ZZ_n	[H.530] سر متقاسم للعدد n

ألف - 2 التعاريف التي يتكرر استعمالها في مجال الأمن

المصطلح	التعريف
مراقبة النفاذ	[X.800] [H.235] منع استخدام غير مخول لمورد، بما في ذلك منع استخدام مورد بطريقة غير مخولة (X.800). [X.170] الحد من تدفق معلومات من موارد نظام إلى أشخاص مخولين أو برامج أو عمليات أو موارد نظام أخرى على الشبكة. [X.805] يحمي بعد الأمن لمراقبة النفاذ من الاستخدام غير المخول لموارد الشبكة. وتضمن مراقبة النفاذ أن الأشخاص أو الأجهزة المخولة يسمح لها بالنفاذ إلى عناصر الشبكة والمعلومات المخزنة وتدفقات المعلومات والخدمات والتطبيقات. وبالإضافة إلى ذلك، توفر مراقبة النفاذ القائمة على الأدوار مستويات نفاذ مختلفة لضمان أن الأفراد والأجهزة يمكنها النفاذ فقط وأداء عمليات على عناصر الشبكة والمعلومات المخزنة وتدفقات المعلومات المخولة.
قائمة مراقبة النفاذ	[X.800] قائمة كيانات، مع حقوق نفاذها، مخولة النفاذ إلى مورد.
عقدة النفاذ	[J.170] عقدة النفاذ، كما هي مستخدمة في هذه الوثيقة، هي طبقة لجهاز إ اء ثنائي ينهي طرف شبكة توصيل مودم بكبل. وهي تكنولوجيا محددة. وتسمى في الملحق ألف من J.112 مكيف تفاعلي لشبكة، بينما تسمى في الملحق باء نظام إ اء مودم بكبل.
المسؤولية	[X.800] الخاصية التي تضمن أن أعمال كيان ما يمكن تتبعها فقط إلى الكيان.
التهديد النشط	[X.800] ديد لتغيير متعمد غير مخول لحالة نظام. (ملاحظة - قد تكون أمثلة التهديدات النشطة المتعلقة بالأمن: إدخال تعديل على الرسائل والإجابة على الرسائل وإدراج رسائل هامشية والتنكر ككيان مخول ورفض الخدمة).
الوكيل	[X.790] كما جاء تعريفه في التوصية X.701 ، نظرة شاملة على إدارة الأنظمة، ولكن مع التقييد التالي. فيما يتعلق بخدمة (أو مورد) اتصالات، يمكن أن يدير خدمة مع نظام واحد يقوم بدور المدير، ويقوم الآخر بدور الوكيل.
الاسم المستعار	[X.790] اسم آخر، بجانب معرف غرض، يعرف بناء عليه تقرير أعطال أو يشار إليه أو يعرف (عادة من قبل زبون).

المصطلح	التعريف
الارتباط بالتطبيق	[X.790] علاقة تعاونية بين كياني تطبيق يتشكل بواسطة تبادل معلومات مراقبة بروتوكول تطبيق من خلال استخدامهما لخدمات تقديم.
سياق التطبيق	[X.790] مجموعة محددة بوضوح لعناصر خدمة التطبيق وخيارات ذات علاقة وأي معلومات ضرورية أخرى للعمل البيني لكيانات تطبيق على الارتباط بالتطبيق.
كيان التطبيق	[X.790] جوانب عملية متعلقة بالتوصيل البيني للأنظمة المفتوحة.
إنذارات متصاحبة	[X.790] إنذارات متعلقة مباشرة بعطل معرف.
خوارزمية تجفير لا تناظرية	[X.810] هي خوارزمية لأداء تجفير أو فك تجفير مصاحب تكون فيه المفاتيح المستخدمة للتجفير وفك التجفير مختلفة. (ملاحظة - مع بعض الخوارزميات ا فرة اللاتناظرية، يتطلب فك تجفير نص مجفر أو توليد توقيع رقمي استخدام أكثر من مفتاح خاص.)
الهجوم	[H.235] الأنشطة المضطلع ا لتجاوز أو استغلال جوانب القصور في آليات أمن النظام. وبالهجوم على نظام، تستغل الأنشطة جوانب القصور في الخوارزميات أو المبادئ أو خصائص آلية الأمن المهمة. ويجري أداء الهجوم غير المباشر عند تجاوز الآلية أو عندما يستخدم النظام الآلية بطريقة غير صحيحة.
الخواص	[X.790] معلومات تتعلق بغرض مسير إدارياً مستخدم لوصف (سواء جزئياً أو كلياً) ذلك الغرض المسير إدارياً. وتتألف هذه المعلومات من نوع الخواص وقيمة أو قيم الخواص المتطابقة (قيمة واحدة) أو (قيم متعددة).
سلطة تحديد الخواص	[X.509] سلطة تحديد الخواص هي السلطة التي تعين امتيازات من خلال إصدار شهادات الخواص.
قائمة إبطال سلطة الخواص	[X.509] قائمة إبطال سلطة الخواص هي قائمة تحتوي على مراجع لشهادات الخواص التي أصدر ا سلطات الخواص والتي لم تعد تعتبر صالحة من قبل السلطة التي أصدر ا.
شهادة الخواص	[X.509] هيكل بيانات وقعته رقمياً سلطة تحديد الخواص ويربط بعض قيم الخواص بمعلومات تعرف حامليها.
قائمة إبطال شهادة النعوت	[X.509] قائمة إبطال شهادة الخواص هي قائمة تحتوى على مراجع لشهادات الخواص التي لم تعد تعتبرها السلطة التي أصدر ا صالحة.
نوع الخواص	[X.790] مكونة خاصية تشير إلى نوع المعلومات التي تعطى لتلك الخاصية.
قيمة الخواص	[X.790] حالة خاصة لنوع المعلومات التي أشار إليها نوع الخواص.
مخدم سمعي	[J.170] مخدم سمعي يقدم بلاغات إعلامية على شبكة الاتصالات الكبلية باستخدام بروتوكول الإنترنت. وهناك حاجة لبلاغات وسائط من أجل الاتصالات التي لا تكتمل وتوفر خدمات معلومات معززة للمستعمل. وتقوم أجزاء مكونة المخدم السمعي بالعمل كأجهزة وسائط ومراقبي أجهزة الوسائط.
التدقيق	[X.800] انظر تدقيق الأمن
تسجيل تدقيق	[X.800] انظر تسجيل تدقيق الأمن

المصطلح	التعريف
الاستيقان	[H.235] [X.800] [X.811] تقديم ما يؤكد الهوية التي يدعيها كيان. انظر الاستيقان من أصل البيانات والاستيقان من الهوية النظيرة. (ملاحظة - لا يستخدم مصطلح "الاستيقان" فيما يتصل بسلامة البيانات؛ ويستخدم مصطلح "سلامة البيانات" بدلاً منه). [J.170] عملية التحقق من هوية الكيان الذي ينتحل هوية أخرى. [X.805] يقوم بعد أمن الاستيقان بالتأكد من هوية كيانات الاتصال. ويضمن الاستيقان صلاحية الهوية الطالبة للكيانات المشاركة في الاتصالات (مثل شخص أو جهاز أو خدمة أو تطبيق) ويضمن أن الكيان لا يحاول تقديم إجابة متنكرة أو غير مخولة على الاتصالات السابقة.
تبادل الاستيقان	[X.800] آلية القصد منها هو التأكد من هوية كيان بواسطة تبادل المعلومات.
وظيفة الاستيقان	[H.530] وظيفة الاستيقان هي كيان وظيفي للأمن في ميدان محلي يحافظ على علاقة الأمن مع المستعملين المتنقلين المشتركين والمطاريف المتنقلة المشتركة.
معلومات الاستيقان	[X.800] معلومات تستخدم للتحقق من هوية الطالب.
إذنة الاستيقان؛ (إذنة)	[X.509] معلومات تنقل خلال تبادل الاستيقان القوي، ويمكن أن تستخدم للاستيقان من هوية مرسلها.
ضمان الاستيقان	[J.170] القدرة على التأكد من أن المعلومات المعطاة لم يطرأ عليها تعديل أو تزوير ومن أن الكيان الذي أعطى المعلومات هو الذي أنتجها بالفعل.
السلطة	[X.509] كيان مسؤول عن إصدار الشهادات. وتم تحديد نوعين للسلطة في هذه المواصفة؛ سلطة إصدار الشهادات التي تصدر شهادات المفاتيح العمومية، وسلطة الخواص التي تصدر شهادات الخواص.
شهادة السلطة	[X.509] شهادة تصدر لسلطة (مثل سلطة إصدار الشهادات أو سلطة الخواص).
التخويل	[H.235] منح تصريح على أساس الاستيقان من الهوية. [J.170] إجراء منح النفاذ إلى خدمة أو جهاز إذا كان هناك تصريح بالنفاذ. [X.800] منح حقوق تشمل منح النفاذ على أساس حقوق النفاذ.
التيسر	[X.800] خاصية قابلية النفاذ والاستخدام عند الطلب من كيان مخول.
التيسر	[X.805] يضمنُ بعد أمن التيسر عدم وجود رفض لنفاذ مخول إلى عناصر الشبكة والمعلومات المخزنة وتدفقات المعلومات والخدمات والتطبيقات التي ترجع إلى أحداث تؤثر على الشبكة. وتشمل هذه الفئة الحلول الخاصة بإعادة الأوضاع إلى ما كانت عليه قبل حدوث الكوارث.
قاعدة قائمة إبطال الشهادات	[X.805] قائمة إبطال الشهادات هي التي تستخدم كأساس في توليد قائمة دلتا لإبطال شهادات.
طبقة إدارة الأعمال	[M.3010] طبقة الإدارة المسؤولة عن المؤسسة بكاملها ولا تخضع للتقييس.
شهادة- سلطة إصدار شهادات	[X.509] شهادة لسلطة واحدة لإصدار الشهادات تصدرها سلطة إصدار شهادات أخرى.
ملغى	[X.790] يمكن للمدير أن يطلب إلى الوكيل "إلغاء" تقرير الأعطال. ويريد المدير إجهاض تقرير الأعطال هذا (سواء بسبب دخوله خطأ أو بسبب عدم وجود حالة أعطال). وتحت أوضاع معينة (مثل عدم إرسال أو اختبار أعطال)، "يلغي" الوكيل تقرير الأعطال بواسطة تحيين حالته إلى "أغلق بناء على طلب زبون". وقد يكون "لإلغاء" تقرير الأعطال آثار على الأعمال أبعد من نطاق هذه التوصية (مثلاً إذا كان على الزبون أن يدفع مقابل تقرير الأعطال).

المصطلح	التعريف
المقدرة	[X.800] إذنة مستخدمة كمعرف لمورد بحيث أن امتلاك إذنة يضفي حقوق نفاذ للمورد.
الشهادة	[H.235] 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 (X.810). وفي هذه التوصية يشير المصطلح إلى شهادات "المفاتيح العمومية" التي تعتبر قيماً تمثل مالكي المفاتيح العمومية (والمعلومات التشغيلية الأخرى) كما تم الاستيقان منها ووقعتها السلطة الموثوق ا في شكل لا يمكن تزويره.
سياسة الشهادة	[X.509] مجموعة من القواعد تشير إلى قابلية تطبيق الشهادة على تجمع و/أو نوع معين من التطبيق له متطلبات أمن مشتركة. فمثلاً، قد تشير سياسة شهادة معينة إلى مدى قابلية تطبيق نوع من الشهادات على الاستيقان من معاملات تبادل البيانات الإلكترونية للاتجار في سلع في نطاق سعر معين.
قائمة إبطال الشهادات	[X.509] قائمة إبطال الشهادات هي قائمة موقعة تشير إلى مجموعة من الشهادات لم يعد يعتبرها مصدر الشهادة صالحة. وبالإضافة إلى المصطلح التنوعي قائمة إبطال الشهادات، تعرف بعض أنواع محددة لهذه القوائم لتشمل منظورات معينة.
الرقم المسلسل للشهادة	[X.509] هي قيمة صحيحة، وحيدة في السلطة الصادرة، متصاحبة بوضوح مع الشهادة التي أصدر ا سلطة إصدار الشهادات.
مستعمل الشهادة	[X.509] كيان يحتاج إلى معرفة المفتاح العمومي لكيان آخر على نحو مؤكد.
صلاحية الشهادة	[X.509] عملية ضمان أن شهادة كانت صالحة في وقت معين، بما في ذلك إمكانية إنشاء ومعالجة مسير شهادة وضمان أن جميع الشهادات في ذلك المسير كانت صالحة (أي لم تنته صلاحيتها أو أبطلت) في وقت معين.
نظام استخدام الشهادة	[X.509] تنفيذ الوظائف المعرفة في هذا الدليل. مواصفات يستخدمها مستعمل شهادة.
سلطة إصدار الشهادات	[X.509] سلطة إصدار الشهادات هي سلطة موثوق ا من مستعمل أو أكثر لخلق وتعيين شهادات مفاتيح عمومية. واختيارياً، قد تخلق سلطة إصدار شهادات مفاتيح مستعملين. [X.810] كيان يوثق به (في سياق سياسة الأمن) لخلق شهادات أمن تحتوي على نوع أو أكثر من البيانات المتعلقة بالأمن.
قائمة إبطال سلطة إصدار الشهادات	[X.509] قائمة إبطال سلطة إصدار الشهادات هي قائمة إبطال تحتوي على قائمة شهادات مفاتيح عمومية صدرت لسلطات إصدار الشهادات، لا يعتبرها مصدر الشهادة صالحة.
مسير إصدار الشهادات	[X.509] تتابع منتظم لشهادات أغراض في شجرة معلومات دليل يمكن، مع المفتاح العمومي للغرض الأولي في المسير، معالجته للحصول على غرض ائي في المسير.
القناة	[X.800] مسير نقل المعلومات.
التجفير	[H.235] خوارزمية مجفرة، تحويل رياضي. [J.170] خوارزمية تحول بيانات بين نص واضح ونص مجفر.
مجموعة التجفير	[J.170] مجموعة ينبغي أن تحتوي على كل من خوارزمية تجفير وخوارزمية الاستيقان من الرسالة (مثل شفرة الاستيقان من الرسالة أو شفرة الاستيقان من الرسالة المفرومة). وبصورة عامة، قد تحتوي على خوارزمية لإدارة المفاتيح لا تنطبق في سياق الاتصالات الكبلية التي تستخدم بروتوكول الإنترنت.
نص التجفير	[X.800] بيانات منتجة من خلال استخدام التجفير. ولا يتاح محتوى دلالات البيانات الناتجة. (ملاحظة - قد يكون النص المُجفر نفسه مدخلاً للتجفير، بحيث ينتج مخرج فوق مجفر.)

المصطلح	التعريف
تحرير تقارير الأعطال	[X.790] إصرار وكيل على أن الأعمال التي عرفت في تقرير الأعطال أو نشاط إصلاح مطابقات غرض قد تم أداؤها بشكل مرض لحل الأعطال، أو أن مثل هذه الأعمال لم تعد ضرورية، وفي أي من الحالتين يعتبر تقرير الأعطال مرشحاً للغلق.
نص واضح	[X.800] بيانات واضحة يكون محتوى دلالا ا متاحاً.
الزبون	[X.790] مستعمل خدمة يوفرها نظام أو شبكة.
مغلق	[X.790] يعتبر تقرير الأعطال "مغلقاً" عندما يقرر الوكيل أن تقرير الأعطال قد تم تحريره أو لم يعد موجوداً، ويحين الوكيل حالة تقرير الأعطال ليشير إلى أن تقرير الأعطال قد "أغلق". ويمكن للوكيل فقط أن يغير حالة تقرير الأعطال باعتباره "مغلقاً". وقد تتغير حالة تقرير الأعطال إلى "مغلق بناء على طلب الزبون" نتيجة طلب المدير بإلغاء تقرير الأعطال.
غلق تقارير الأعطال	[X.790] إصرار الوكيل على أن الأعطال قد تم حلها بحيث أن تقرير الأعطال المحرر يمكن معالجته فقط لابتكار سجل تاريخ الأعطال و/أو إلغاؤه.
الاتصالات	[X.805] يضمن ُبعد أمن الاتصالات تدفق المعلومات فقط بين النقاط الطرفية المخولة (لم تتحول المعلومات أو يتم اعتراضها بينما تتدفق بين النقاط الطرفية هذه).
كيان مشروط موثوق به	[X.810] كيان موثوق به في سياق سياسة الأمن، ولكن لا يمكن انتهاك سياسة الأمن دون اكتشافه.
السرية	[H.235] خاصية تمنع كشف المعلومات لأفراد أو كيانات أو عمليات غير مخولة. [J.170] طريقة لضمان أن المعلومات لا يكشف عنها لأحد غير الأطراف المقصودة. ويجري تجفير المعلومات لتوفير السرية. وتعرف أيضاً بالخصوصية (privacy). [X.800] خاصية لا تتيح المعلومات أو تكشف عنها لأفراد أو كيانات أو عمليات غير مخولة.
كيان الإدارة المطابق	[X.790] نظام حقيقي مفتوح يدعم قابلية التشغيل البيني المعرف في هذه التوصية.
التلامس	[X.790] شخص يمكنه توفير معلومات إضافية حول الأعطال نيابة عن مدير أو وكيل.
التفويض	[H.530] في هذه التوصية، يفهم التفويض [مثل HMACZZ(GKID) أوHMACZZ (W) على أنه جزء من بيانات طبقت فيه وظيفة الاستيقان تجفيرياً لسره المتقاسم الذي يتقاسمه مع مستعمل متنقل. وينقل التفويض ليثبت التخويل وتوقيت تأكيد التخويل.
التفويضات	[X.800] بيانات تنقل لتحديد هوية كيان الطالب.
نقطة توزيع قائمة إبطال الشهادات	[X.509] مدخل دليل أو مصدر توزيع آخر لقوائم إبطال الشهادات؛ وتوزع قائمة إبطال الشهادة من خلال نقطة التوزيع القائمة التي قد تحتوي على مداخل إبطال مجموعة فرعية فقط من مجموعة كاملة لشهادات أصدر ا سلطة إصدار الشهادات أو قد تحتوي على مداخل إبطال لسلطات إصدار شهادات متعددة.
تحليل التجفير	[J.170] عملية استرجاع نص واضح لرسالة أو مفتاح تجفير دون نفاذ إلى المفتاح. [X.800] تحليل نظام مجفر و/أو مداخله ومخارجه للتوصل إلى متغيرات سرية و/أو بيانات حساسة بما في ذلك نص واضح.
خوارزمية مجفرة	[H.235] دالة رياضية تحسب النتيجة من قيمة أو قيم عديدة لمداخل.

المصطلح	التعريف
سلسلة مجفرة	[X.810] أسلوب استخدام خوارزمية مجفرة تقوم الخوارزمية فيها بأداء تحويل يعتمد ذلك على قيم المداخل أو المخارج السابقة.
قيمة التحقق ا فرة	[X.800] معلومات مشتقة بواسطة أداء تحويل مجفر (انظر تجفير) في وحدة معطيات. (ملاحظة - يمكن أداء اشتقاق قيمة تحقق في خطوة أو أكثر وهو نتيجة لدالة رياضية لمفتاح ووحدة معطيات. ويستخدم عادة للتحقق من سلامة وحدة المعطيات.)
نظام مجفر	[X.509] النظام ا فر هو جمع تحويلات من نص واضح إلى نص مجفر والعكس بالعكس، وتختار مفاتيح تحويل (تحويلات) معينة. وتعرف الخوارزمية الرياضية عادة التحويلات.
علم التجفير	[X.800] التخصص الذي يجسد مبادئ ووسائل وطرق تحويل البيانات من أجل إخفاء محتوى المعلومات ويمنع تعديلها غير المكتشف و/أو يمنع استخدامها غير المخول. (ملاحظة - يحدد علم التجفير الطرق المستخدمة في التجفير وفك التجفير. ويعتبر الهجوم على مبدأ أو وسيلة أو طريقة مجفرة تحليلاً للتجفير).
الزبون	[X.790] الزبون هو مستعمل خدمات الاتصالات التي يوفرها مزود الخدمة. وعلى نحو خاص في سياق هذه التوصية، الزبون هو مستعمل يختار استخدام سطح بيني من أنظمة عمليات إلى أنظمة عمليات إدارة الشبكة عبر سلطات قضائية لتحقيق مراقبة خدمات الاتصالات (أو الموارد) المستخدمة. ويقوم الزبون (أو ممثل الزبون) بدور المدير. وليست هناك متطلبات بأن يقتصر السطح البيني على الحالات التي توجد فيها خدمة اتصالات تقليدية لزبون لخدمة علاقة مزود بين الأطراف. ويمكن لمزودين (شركتي اتصالات) لخدمة اتصالات استخدام السطح البيني هذا لتبادل تقارير الأعطال في الحالات التي تكون فيها شبكا م تعمل بينياً لتوفير الخدمة للمستعمل النهائي. وفي تلك الحالة، قد يتغير دور الزبون من حالة إلى أخرى. ومع ذلك، في أي حالة معينة، يمكن لشركة اتصالات واحدة أن تكون الزبون وتقوم بدور المدير، بينما تكون الشركة الأخرى هي المورد وتقوم بدور الوكيل.
شبكة اتصال البيانات	[M.3010] شبكة اتصالات داخل شبكة إدارة الاتصالات أو بين شبكات إدارة الاتصالات تدعم وظيفة اتصالات البيانات.
سرية البيانات	[X.509] يمكن أن تستخدم هذه الخدمة لتوفير حماية البيانات من إفشاء غير مخول. ويدعم إطار الاستيقان خدمة سرية البيانات. ويمكن أن تستخدم للحماية من اعتراض البيانات. [X.805] ويحمي بعد الأمن لسرية البيانات من عدم إفشاء غير مخول. وتضمن سرية البيانات أن محتوى البيانات لا يمكن فهمه بواسطة كيانات غير مخولة. والطرق التي تستخدم أحياناً لتوفير سرية البيانات هي التجفير وقوائم مراقبة النفاذ وتصاريح الملفات.
سلامة البيانات	[X.800] خاصية تضمن عدم تغيير البيانات أو تدمرها بطريقة غير مخولة. [X.805] ويضمن بعد الأمن لسلامة البيانات صحة أو دقة البيانات. ويجري حماية البيانات من التعديل أو الحذف أو التغيير الكامل أو الاستنساخ غير المخول ويوفر دلالة على حدوث هذه الأنشطة غير المخولة.
الاستيقان من أصل البيانات	[X.800] التأكد من أن مصدر البيانات التي يستقبلها الطالب هو المصدر المطلوب.
فك التشفير	[X.800] إبطال تشفير معكوس متناظر.
فك التجفير	[X.800] انظر فك التشفير.

المصطلح	التعريف
بؤجل	[X.790] تأجيل العمل بشأن تقرير الأعطال أو وضعه جانباً حتى يحين تلبية الشروط الملائمة ويمكن تطويره أكثر.
الوفد	[X.509] منح مزايا من كيان واحد يتمتع ا إلى كيان آخر.
مسير الوفد	[X.509] تتابع منتظم لشهادات يمكن، مع الاستيقان من الكيان المتميز المؤكد، معالجته للتحقق من الاستيقان المتميز للمؤكد.
قائمة دلتا لإبطال الشهادات	[X.509] قائمة دلتا لإبطال الشهادات هي قائمة إبطال جزئي تحتوي فقط على مدخلات لشهادات تغيرت حالة إبطالها منذ إصدار قاعدة قائمة إبطال الشهادات المشار إليها.
رفض الخدمة	[X.800] منع نفاذ مخول إلى الموارد أو تأخير عمليات التوقيت الحرجة.
بصمة إصبع رقمية	[X.810] خاصية بند بيانات مثل قيمة تحقق مجفرة أو نتيجة أداء وظيفة فرم بطريقة واحدة على بيانات تعتبر كافية بصورة معينة لبند بيانات لا يجدي حسابه لإيجاد بند بيانات آخر يمتلك نفس الخصائص.
توقيع رقمي	[X.800] بيانات مذيلة أو تحويل مجفر (انظر تجفير) لوحدة بيانات تسمح لمستقبل وحدة بيانات أن يتأكد من المصدر وسلامة وحدة البيانات ويحميها من التزوير، مثلا بواسطة مستقبل.
معرف متميز	[X.810] بيانات تعرف كياناً وحيداً.
في **الاتجاه الهابط**	[J.170] اتجاه من طرف رأس اتجاه تحديد موقع المشترك.
طبقة إدارة العنصر	[M.3010] طبقة إدارة مسؤولة عن إدارة عناصر الشبكة على أساس فردي أو جماعي.
التشفير	[H.235] التشفير (التجفير) عملية تجعل البيانات غير قابلة للقراءة لكيانات غير مخولة بواسطة تطبيق خوارزمية مجفرة. وفك تجفير هو عملية عكسية يتحول عن طريقها نص مجفر إلى نص واضح. [X.800] والتحويل ا فر للبيانات (انظر علم التجفير) هو إنتاج نص مجفر. (ملاحظة - قد لا يمكن عكس التجفير وفي هذه الحالة لا يمكن أداء عملية فك التجفير المتطابقة بأي حال.)
التجفير	[J.170] طريقة تستخدم لترجمة معلومات في نص واضح إلى نص مجفر. [X.800] انظر التشفير.
كيان ائي	[X.509] شخص له شهادة يستخدم مفتاحها الخاص لأغراض غير توقيع الشهادات أو كيان هو طرف ترحيل.
قائمة إبطال شهادات الخواص لكيان ائي	[X.509] قائمة إبطال شهادات الخواص لكيان ائي هي قائمة إبطال تحتوي على قائمة شهادات خواص صدرت لمستبقيها وهي ليست سلطات خواص ولا يعتبرها مصدر الشهادة صالحة.
قائمة إبطال شهادة مفتاح عمومي لكيان ائي	[X.509] هي قائمة إبطال تحتوي على قائمة شهادات مفاتيح عمومية صدرت لأشخاص، ليست سلطات لإصدار شهادات، ولا يعتبرها مصدر الشهادة صالحة.
نقطة طرفية	[J.170] مطراف أو بوابة أو وحدة مراقبة نقاط متعددة.
تشفير من طرف إلى طرف	[X.800] تشفير بيانات في أو عند مصدر نظام طرفي مع فك تشفير متناظر يحدث فقط في أو عند مقصد نظام طرفي. (انظر أيضاً تشفير من وصلة إلى وصلة).

المصطلح	التعريف
متغيرات بيئية	[X.509] الجوانب السياسية المطلوبة لقرار تخويل غير مجتوية في هياكل سكونية، ولكنها متاحة من خلال بعض الوسائل المحلية لمتحقق متميز (مثل وقت من اليوم أو رصيد حساب جارٍ).
تقرير أعطال متصاعد	[X.790] تعريف تقرير أعطال يستحق انتباهاً إشرافياً عاجلاً وفورياً لاستبانة الأعطال.
الحدث	[X.790] حدوث آني يغير الحالة الشاملة للغرض. وقد يكون تغيير الحالة مستمراً أو مؤقتاً، ومن ثم يسمح بالمراقبة والرصد والعنصر الوظيفي لقياس الأداء، وما إلى ذلك. وقد تولد أو لا تولد الأحداث تقارير؛ وقد تكون آنية أو مخططة؛ وقد تفجر أحداثاً أخرى أو يفجرها حدث أو أحداث أخرى.
رسالة لحدث	[J.170] رسالة تلتقط جزءاً واحداً من التوصيل.
سطح بيني F	[M.3010] سطح بيني يطبق عند نقاط مرجعية f.
نقاط مرجعية F	[M.3010] نقطة مرجعية موجودة بين فدرة وظيفة محطة العمل وفدرة وظيفة أنظمة العمليات.
إدارة الأعطال	[X.790] تتألف إدارة الأعطال من مجموعة من الوظائف التي تمكن من اكتشاف وعزل وتصحيح عملية شاذة لشبكة اتصالات وبيئتها.
قائمة إبطال الشهادات الكاملة	[X.509] قائمة إبطال كاملة تحتوي على مداخل لجميع الشهادات التي تم إبطالها لمنظور معين.
فدرة وظيفية	[M.3010] أصغر وحدة (قابلة للنشر) لعنصر وظيفي لإدارة شبكة إدارة اتصالات تخضع للتقييس.
نقاط مرجعية G	[M.3010] نقطة مرجعية موجودة خارج شبكة إدارة الاتصالات بين مستعملين بشريين وفدرة وظيفة محطة العمل. ولا تعتبر جزءاً من شبكة إدارة الاتصالات بالرغم من أ ا تنقل معلومات شبكة إدارة الاتصالات.
بوابة	[J.170] أجهزة تربط بين عالم الاتصالات الهاتفية للاتصالات الكبلية تستخدم بروتوكول الإنترنت والشبكة الهاتفية العمومية المبدلة. وأمثلة ذلك بوابة وسائط توفر أسطح بينية لدارة حمالة والشبكة الهاتفية العمومية المبدلة وتحويل شفرة رتل وسائط وبوابة التشوير التي ترسل وتستقبل تشوير شبكة الدارة المبدلة إلى حافة شبكة الاتصالات الكبلية التي تستخدم بروتوكول الإنترنت.
وظيفة الفرم	[X.509] وظيفة (رياضية) تقابل قيماً من ميدان كبير (ومن الممكن كبير جداً) إلى ميدان أصغر مدى. وظيفة فرم "جيدة" هي التي ينتج عنها تطبيق الوظيفة على مجموعة (كبيرة) من القيم في ميدان يوزع (من الواضح عشوائياً) في النهاية عبر المدى. [X.810] وظيفة (رياضية) تقابل قيماً من مجموعة كبيرة (من الممكن كبيرة جداً) من القيم بمدى قيم أصغر.
رأسية	[J.170] معلومات مراقبة البروتوكول موجودة في بداية وحدة بيانات البروتوكول.
المستبقي	كيان ميز سواء مباشرة من مصدر سلطة أو بطريقة غير مباشرة من خلال سلطة خواص أخرى.
عنصر الحد المحلي	[H.530] عنصر الحد المحلي هو عنصر حد موضوع في ميدان محلي.
سياسة أمن قائمة على الهوية	[X.800] سياسة أمن قائمة على الهويات و/أو نعوت المستعملين أو زمرة المستعملين أو كيانات تعمل نيابة عن مستعملين وموارد/أشخاص يجري نفاذها.
قائمة إبطال شهادة غير مباشرة	[X.509] قائمة إبطال شهادة غير مباشرة هي قائمة إبطال تحتوي على الأقل على معلومات إبطال عن شهادات أصدر ا سلطات من غير السلطات التي أصدرت قائمة إبطال شهادة.

المصطلح	التعريف
سلامة البيانات	[H.235] خاصية تضمن عدم تعديل البيانات بطريقة غير مخولة. [J.170] وهي طريقة للتأكد من أن المعلومات لم يطرأ عليها تعديل من جانب أطراف غير مخول لهم القيام بذلك. [X.800] انظر سلامة البيانات.
السطح البيني	[M.3010] مفهوم معماري يوفر التوصيل البيني لقدرات مادية عند نقاط مرجعية.
الولاية القضائية	[X.790] تشير هذه إلى فصل وظيفي لشبكات الاتصالات. والولاية القضائية هي إحدى الأنواع الأربعة التالية: (أ) شبكة موجات حاملة لبدالة محلية؛ (ب) شبكة موجات حاملة بين البدالات؛ (ج) شبكة مستعمل نائي؛ (د) بعض تركيب ما ورد أعلاه.
Kerberos	[J.170] بروتوكول استيقان شبكة مفاتيح سرية تستخدم خيار خوارزميات مجفرة للتجفير وقاعدة بيانات مركزية للاستيقان.
مفتاح	[J.170] خرج قيمة رياضية في خوارزمية مجفرة مختارة. [X.800] تتابع رموز تتحكم في عمليات التجفير وفك التجفير.
اتفاق مفاتيح	[X.509] طريقة للتفاوض بشأن قيمة مفتاح على الخط دون نقل المفتاح، حتى في شكل مجفر، مثل تقنية ديفي-هلمان (انظر ISO/IEC 11770-1 لمزيد من المعلومات عن آليات اتفاق المفاتيح).
بدالة مفاتيح	[J.170] تبادل مفاتيح عمومية بين كيانات تستخدم لتجفير الاتصالات بين الكيانات.
إدارة مفاتيح	[X.800] [H.235] توليد وتخزين وتوزيع وإلغاء والحفظ في الأرشيف وتطبيق مفاتيح طبقاً لسياسة الأمن.
إدارة-مفاتيح	[J.170] عملية توزيع مفاتيح متناظرة متقاسمة مطلوبة لإدارة بروتوكول الأمن.
تشفير وصلة بوصلة	[X.800] تطبيق فردي لتشفير البيانات على كل وصلة في نظام الاتصالات. انظر أيضاً تشفير من طرف إلى طرف. (ملاحظة - تطبيق التشفير وصلة بوصلة هو أن تكون البيانات في شكل نص واضح في كيانات ترحيل).
معمارية مبنية حسب الطبقات	[M.3010] مفهوم معماري ينظم وظائف الإدارة في تجمع طبقات الإدارة ويصف العلاقات بين الطبقات.
نقاط مرجعية M	[M.3010] نقطة مرجعية موجودة خارج شبكة إدارة الاتصالات بين قدرة وظيفة مكيف Q والكيانات المسيرة إدارياً التي لا تتطابق مع توصيات شبكة إدارة الاتصالات.
مورد مسير إدارياً	[M.3010] تجريد لجوانب موارد الاتصالات (منطقية أو مادية) مطلوبة لإدارة الاتصالات.
وظيفة تطبيق الإدارة	[M.3010] وظيفة تمثل (جزء) من عنصر وظيفي لخدمة إدارة أو أكثر.
ميدان الإدارة	[M.3010] مجموعة موارد مسيرة إدارياً تخضع لسياسة إدارة مشتركة.
وظيفة إدارة	[M.3010] أصغر جزء في خدمة إدارة كما يدركها مستعمل الخدمة.
مجموعة وظائف الإدارة	[M.3010] مجموعة وظائف إدارة شبكة إدارة الاتصالات هي تجمع لوظائف إدارة شبكة إدارة الاتصالات ترتبط مع بعضها سياقياً، أي أ ا ترتبط بمقدرة إدارة محددة (مثل وظائف الإبلاغ عن إنذارات ومراقبة إدارة الحركة). ومجموعة وظائف إدارة شبكة إدارة الاتصالات هي أصغر بند يعاد استخدامه للمواصفات الوظيفية. وينبغي النظر إلى مجموعة وظائف إدارة شبكة إدارة الاتصالات ككل. فهي تشبه جزءاً من متطلبات التوصيل البيني للأنظمة المفتوحة ووظيفة إدارة النظام).

المصطلح	التعريف
خدمة الإدارة	[M.3010] خدمة الإدارة هو عرض لتلبية احتياجات محددة لإدارة الاتصالات.
طبقة الإدارة	[M.3010] مفهوم معماري يعكس جوانب معينة للإدارة ويتضمن تجميع معلومات الإدارة التي تدعم ذلك الجانب.
المدير	[X.790] كما عرف في التوصية X.701، نظرة شاملة على إدارة الأنظمة، ولكن مع التقييد التالي. فيما يتعلق بمطابقة خدمة (أو مورد) اتصالات معينة، يمكن له إدارة الخدمة مع نظام واحد يقوم بدور المدير ويقوم الآخر بدور الوكيل.
كشف التلاعب	[X.800] آلية تستخدم لكشف ما إذا كانت البيانات قد تم تعديلها (سواء عرضياً أو عمداً).
التنكر	[X.800] وجود كيان على أنه كيان آخر.
رتل الوسائط	[H.235] يمكن أن يكون رتل الوسائط من نوع سمعي أو فيديوي أو بيانات أو تجميع من أي منها. وتنقل بيانات رتل الوسائط بيانات المستعمل أو البيانات التطبيقية (حمولة نافعة) وليس البيانات المراقبة.
وكالة تسيير التنقلية	[H.530] وكالة تسيير التنقلية هي كيان وظيفي اختياري يعمل ككيان وظيفي وسيط وينهي تصاحب الأمن لوصلة قفزة بقفزة.
عنصر الشبكة	[M.3010] مفهوم معماري يمثل معدات اتصالات (أو مجموعات/أجزاء من معدات اتصالات) ويدعم معدات أو أي بند أو مجموعة بنود تعتبر أ ا تخص بيئة الاتصالات وتؤدي وظائف عناصر الشبكة.
وظيفة عنصر الشبكة	[M.3010] قدرة وظيفية تمثل وظائف الاتصالات وتتصل مع قدرة وظيفة شبكة إدارة الاتصالات ووظيفة أنظمة العمليات لغرض رصدها و/أو مراقبتها.
طبقة إدارة الشبكة	[M.3010] طبقة إدارة مسؤولة عن الإدارة بما في ذلك تنسيق النشاط لرؤية الشبكة.
عدم التنصل	[H.235] حماية من رفض واحد من الكيانات العاملة في الاتصالات تشارك في جميع الاتصالات أو جزء منها. [J.170] المقدرة على منع المرسل إنكار فيما بعد أنه أرسل رسالة أو أدى عملاً. [X.805] ويوفر بعد أمن عدم التنصل وسيلة لمنع أي فرد أو كيان من إنكار أداء عمل معين يتعلق ببيانات من خلال دليل متاح عن أعمال مختلفة متعلقة بالشبكة (مثل إثبات التزام أو نية؛ إثبات أصل البيانات وإثبات ملكية وإثبات استخدام مورد). ويضمن إتاحة دليل يمكن تقديمه لطرف ثالث ويستخدم لإثبات أن نوعاً من الأحداث أو الأعمال قد تم.
شهادة الاستيقان	[X.800] تسجيل بيانات مع طرف ثالث موثوق به يسمح بضمان دقة خصائصه مثل المحتوى والأصل والوقت والتسليم.
طريقة غرض	[X.509] عمل يمكن تنفيذه بشأن مورد (مثلاً يجوز لنظام ملفات أن يقرأ ويكتب وينفذ طرق أغراض).
دالة وحيدة الاتجاه	[X.509] دالة f (رياضية) يمكن حسا ا بسهولة، ولكن بقيمة عامة y في المدى، ومن الصعب حسا ا لإيجاد قيمة x في الميدان حيث f(x) = y. وقد توجد قيم y قليلة وليس من الصعب إيجاد x حسابياً. [X.810] دالة (رياضية) من السهل حسا ا ولكن، عند معرفة النتيجة، من غير ا دي حسا ا لإيجاد أي قيم قد تكون موفرة للحصول عليها.

المصطلح	التعريف
دالة فرم وحيدة الاتجاه	[X.810] دالة (رياضية) هي دالة وحيدة الاتجاه ودالة فرم.
نظام العمليات	[M.3010] قدرة مادية تؤدي وظائف أنظمة العمليات.
وظيفة أنظمة العمليات	[M.3010] قدرة وظيفية تعالج معلومات متعلقة بإدارة الاتصالات لغرض الرصد/التنسيق و/أو مراقبة وظائف الاتصالات بما في ذلك وظائف الإدارة (أي شبكة إدارة الاتصالات نفسها).
انقطاع	[X.790] عدم إتاحة الخدمة أو المورد.
ديد سلبي	[X.800] ديد بإفشاء غير مخول لمعلومات دون تغيير حالة النظام.
كلمة السر	[X.800] [H.530] معلومات الاستيقان السرية تتألف عادة من سلسلة سمات.
الاستيقان من كيان نظير	[X.800] تأكيد أن الكيان النظير المتصاحب هو المطلوب.
خطورة محسوسة	[X.790] خطورة مشكلة كما يراها الشخص المبلغ عن الأعطال.
قدرة مادية	[M.3010] مفهوم معماري يمثل تحقيق قدرة وظيفية أو أكثر.
أمن مادي	[X.800] تدابير مستخدمة لتوفير حماية مادية لموارد من ديدات متعمدة وعرضية.
سياسة	[X.800] انظر سياسة الأمن.
تقابل السياسة	[X.509] التسليم، عندما تصدق سلطة إصدار الشهادات في ميدان واحد على سلطة إصدار الشهادات في ميدان آخر، بأ ا تعتبر سلطة الميدان الأول أن سياسة شهادة معينة في ميدان ثانٍ مكافئة (ولكن ليس بالضرورة مماثلة في جميع الجوانب) لسياسة شهادة معينة في الميدان الأول.
الأولوية	[X.790] درجة العجلة التي يطلب بناء عليها المدير حلاً للمشكلة.
الخصوصية	[H.235] أسلوب اتصالات يمكن من خلاله فقط لأطراف قادرة أن تفسر الاتصالات بوضوح. ويتحقق هذا من خلال تجفير وتقاسم مفتاح (مفاتيح) من أجل التجفير. [J.170] طريقة لضمان أن المعلومات لا تفشى لأي أحد غير الأطراف المقصودة. وعادة ما تكون المعلومات مجفرة لتوفير الخصوصية. [X.800] حق الأفراد في مراقبة أو التأثير على أي معلومات قد تتعلق م جمعت وخزنت من يجوز لهم إفشاء هذه المعلومات. (ملاحظة - بسبب أن هذا المصطلح يتعلق بحق الأفراد، لا يمكن أن يكون دقيقاً وينبغي تجنب استخدامه باستثناء الدافع وراء طلب الأمن). [X.805] ويوفر بعد أمن الخصوصية حماية المعلومات التي قد تشتق من ملاحظة أنشطة الشبكة. وترد أمثلة هذه المعلومات في مواقع الويب التي زارها المستعمل والمكان الجغرافي للمستعمل وعناوين بروتوكول الإنترنت وأسماء أجهزة اسم ميدان في شبكة مزود الخدمة.
قناة خاصة	[H.235] بالنسبة لهذه التوصية، القناة الخاصة هي قناة ناتجة عن مفاوضات مسبقة بشأن قناة آمنة. وفي هذا السياق، قد تستخدم لمناولة أرتال الوسائط.
مفتاح خاص	[J.170] المفتاح المستخدم في تجفير المفاتيح العمومية التي تخص كياناً فردياً وينبغي الاحتفاظ به سرياً. [X.810] المفتاح المستخدم مع خوارزمية لا تناظرية مجفرة يكون امتلاكها مقيداً (عادة لكيان واحد فقط).

المصطلح	التعريف
مفتاح خاص؛ مفتاح سري (لا ينصح به)	[X.509] (في نظام تجفير مفتاح عمومي) هو مفتاح لمفتاح زوجي لمستعمل معروف فقط لذلك المستعمل.
امتياز	[X.509] خواص أو ملكية معينة لكيان من قبل سلطة.
مؤكد امتياز	[X.509] استخدام صاحب الامتياز لشهادة الخواص أو شهادة المفتاح العمومي لتأكيد الامتياز.
بنية تحتية لإدارة الامتياز	[X.509] البنية التحتية القادرة على دعم إدارة الامتيازات لدعم خدمة الاستيقان شاملة وفي علاقة مع بنية تحتية لمفتاح عمومي.
سياسة الامتياز	[X.509] سياسة توجز شروط متحققي الامتياز لتوفير/أداء خدمات حساسة لمؤكدي الامتياز المؤهلين. وتتعلق السياسة المتميزة بخواص مرتبطة بخدمات وكذلك خواص مرتبطة بمؤكدي الامتياز.
متحقق الامتياز	[X.509] كيان يتحقق من شهادات مقابل سياسة الامتياز.
الوكالة	[J.170] مرفق يوفر بطريقة غير مباشرة بعض الخدمة أو يعمل كممثل في تسليم المعلومات وبالتالي يقضي على الحاجة إلى المضيف لدعم الخدمة.
مفتاح عمومي	[J.170] مفتاح مستخدم في تجفير المفاتيح العمومية التي تخص كياناً فردياً ويوزع بشكل عام. وتستخدم كيانات أخرى هذا المفتاح لتجفير بيانات ترسل إلى مالك المفتاح. [X.810] مفتاح يستخدم مع خوارزمية لا تناظرية مجفرة ويمكن إتاحته بشكل عام.
شهادة مفتاح عمومي	[J.170] ربط بين مفتاح عمومي لكيان ونعت أو أكثر يتعلق .وبته، ويعرف أيضاً بالشهادة الرقمية.
تجفير مفتاح عمومي	[H.235] نظام تجفير يستخدم مفاتيح لا تناظرية (للتجفير/فك التجفير) تكون فيها للمفاتيح علاقة رياضية كل بالآخر – ولا يمكن حسا ا بشكل معقول. [J.170] إجراء يستخدم مفتاحاً زوجياً ومفتاحاً عمومياً ومفتاحاً خاصاً للتجفير وفك التجفير، ويعرف أيضاً بالخوارزمية اللاتناظرية. ويتاح المفتاح العمومي للمستعمل بشكل عام للآخرين لاستخدامه في إرسال رسالة إلى مالك المفتاح. ويحتفظ بالمفتاح الخاص للمستعمل بشكل سري وهو المفتاح الوحيد لفك تجفير رسالة أرسلت مجفرة من قبل المفتاح العمومي للمستعمل.
البنية التحتية للمفاتيح العمومية	[X.509] بنية تحتية قادرة على دعم إدارة المفاتيح العمومية التي تتمكن من دعم خدمات الاستيقان أو التجفير أو سلامة البيانات أو عدم التنصل.
مشغل الاتصالات العمومية	[M.3010] يستخدم من أجل الإيجاز ويشمل إدارات الاتصالات ووكالات التشغيل المعترف ا والإدارات الخاصة (الزبون والطرف الثالث) و/أو المنظمات الأخرى العاملة أو المستخدمة لشبكة إدارة الاتصالات.
مفتاح - عمومي	[X.509] (في نظام تجفير مفتاح عمومي) هو مفتاح زوجي لمستعمل معروف بشكل عام.
شهادة مفتاح - عمومي	[X.509] مفتاح عمومي للمستعمل، مع بعض معلومات أخرى، لا يمكن تزويره بواسطة تجفير مفتاح خاص لسلطة شهادة قد أصدر ا.
مكيف Q	[M.3010] قدرة مادية تتميز بقدرة وظيفية مكيف Q محتواة وتوصل كيانات مادية لمشابه عنصر الشبكة أو مشابه نظام العمليات مع أسطح بينية متوافقة مع غير شبكة إدارة الاتصالات (عند النقاط المرجعية m) بالأسطح البينية Q.
سطح بيني Q	[M.3010] سطح بيني يطبق عند النقاط المرجعية q.

المصطلح	التعريف
نقاط مرجعية Q	[M.3010] نقطة مرجعية موجودة بين وظيفة عنصر الشبكة ووظيفة أنظمة العمليات وبين وظيفة المكيف Q ووظيفة أنظمة العمليات وبين وظيفة أنظمة عمليات ووظيفة أنظمة عمليات.
نقطة مرجعية	[M.3010] مفهوم معماري مستخدم ليصف قدرات وظيفية للإدارة ويعرف حدود الخدمة بين قدرتي وظيفة الإدارة.
طرف يعتمد عليه	[X.509] مستعمل أو وكيل يعتمد على البيانات في الشهادة لاتخاذ القرارات.
الرفض	[X.800] إنكار أحد الكيانات العاملة في الاتصالات بأنه شارك في جميع أو جزء من الاتصالات.
شهادة الإبطال	[X.810] شهادة أمن تصدرها سلطة الأمن وتشير إلى أن شهادة أمن معينة قد أبطلت.
شهادة قائمة الإبطال	[X.810] شهادة أمن تعرف قائمة شهادات أمن قد أبطلت.
شهادة مواصفة الدور	[X.509] شهادة تحتوي على خواص دور وتعيين دور أو أكثر لشخص/صاحب شهادة.
شهادة تحديد الدور	[X.509] شهادة تحتوي على تعيين ميزات لدور.
مفتاح خاص للجذر	[J.170] مفتاح التوقيع الخاص لأعلى سلطة إصدار شهادات. ويستخدم عادة لتوقيع شهادات مفاتيح عمومية لأقل مستوى سلطات إصدار شهادات أو كيانات أخرى.
مراقبة التسيير	[X.800] تطبيق قواعد خلال عملية التسيير من أجل اختيار أو تجنب شبكات أو وصلات أو ترحيلات محددة.
سياسة أمن قائمة على القواعد	[X.800] سياسة أمن قائمة على قواعد شاملة تفرض على جميع المستعملين. وتعتمد هذه القواعد على مقارنة حساسية الموارد التي يجري النفاذ إليها وامتلاك خواص متطابقة لمستعملين أو مجموعة مستعملين أو كيانات تعمل نيابة عن مستعملين.
الختم	[X.810] قيمة تحقق مجفرة تدعم سلامة البيانات ولكنها لا تحمي من تزوير المستقبِل (أي، لا توفر عدم التنصل). وعندما يتصاحب الختم مع عنصر بيانات، يقال إن عنصر البيانات هذا قد ختم. (ملاحظة - بالرغم من أن الختم في حد ذاته لا يوفر عدم التنصل، تستفيد بعض آليات عدم التنصل من خدمة سلامة البيانات التي توفرها الأختام، مثلاً لحماية الاتصالات مع أطراف ثالثة موثوق ا).
مفتاح سري	[X.810] مفتاح يستخدم مع خوارزمية لا تناظرية مجفرة. وامتلاك مفتاح سري مقيد (عادة لكيانين).
قواعد تفاعلية آمنة	[X.810] قواعد سياسة الأمن التي تنظم التفاعلات بين ميادين الأمن.
إداري الأمن	[X.810] شخص مسؤول عن تعريف أو فرض جزء أو أكثر من سياسة الأمن.
تدفيق الأمن	[X.800] استعراض وفحص مستقلين لسجلات وأنشطة نظام من أجل اختبار دقة مراقبة نظام لضمان الامتثال للسياسة القائمة والإجراءات التشغيلية لكشف اختراقات الأمن والتوصية بأي تغييرات قد أشير إليها في المراقبة والسياسة والإجراءات.
تسجيل تدفيق الأمن	[X.800] بيانات مجمعة واحتمال استخدامها لتيسير تدقيق الأمن.
سلطة الأمن	[X.810] كيان مسؤول عن تعريف أو تنفيذ أو فرض سياسة الأمن.

المصطلح	التعريف
شهادة الأمن	[X.810] مجموعة بيانات متعلقة بالأمن تصدرها سلطة أو طرف ثالث موثوق به مع معلومات أمن تستخدم لتوفير سلامة البيانات وخدمات الاستيقان من أصل البيانات. (ملاحظة - تعتبر جميع الشهادات أ ا شهادات أمن (انظر التعاريف ذات الصلة في ISO 7498-2). واعتمد مصطلح شهادة الأمن لتجنب تضارب المصطلحات مع توصية قطاع تقييس الاتصالات X.509 | ISO/IEC 9594-8؛ أي معيار الاستيقان من الدليل).
سلسلة شهادات الأمن	[X.810] تتابع منظم لشهادات الأمن تحتوي الشهادة الأولى على معلومات متعلقة بالأمن وتحتوي كل شهادة تالية على معلومات أمن يمكن أن تستخدم في التحقق من شهادات الأمن السابقة.
ميدان الأمن	[X.810] مجموعة عناصر وسياسة أمن وسلطة أمن ومجموعة أنشطة متعلقة بالأمن تخضع فيها مجموعة عناصر إلى سياسة الأمن لأنشطة محددة، وتدير سياسة الأمن سلطة أمن ميدان الأمن.
سلطة ميدان الأمن	[X.810] سلطة أمن مسؤولة عن تنفيذ سياسة الأمن لميدان الأمن.
معلومات الأمن	[X.810] معلومات مطلوبة لتنفيذ خدمات الأمن.
وسم الأمن	[X.800] توسيم مرتبط بمصدر (قد يكون وحدة معطيات) ُيسمى أو يعين نعوت الأمن لذلك المصدر. (ملاحظة - قد يكون التوسيم و/أو الربط واضحاً أو ضمنياً).
سياسة الأمن	[X.509] مجموعة قواعد تضعها سلطة الأمن التي تراقب استخدام وتوفير خدمات وتسهيلات الأمن. [X.800] مجموعة معايير لتوفير خدمات الأمن (انظر سياسة أمن قائمة على الهوية وقائمة على القواعد). (ملاحظة – تتناول سياسة أمن كاملة بالضرورة شواغل كثيرة خارج نطاق التوصيل البيني للأنظمة المفتوحة).
قواعد سياسة الأمن	[X.810] تمثيل سياسة الأمن لميدان أمن في نظام حقيقي.
مظهر جانبي للأمن	[H.235] مجموعة (مجموعة فرعية) لإجراءات خصائص متسقة وقابلة للتشغيل البيني من قطاع تقييس الاتصالات [H.235] مفيدة لتأمين اتصالات وسائط متعددة H.323 فيما بين كيانات عاملة في سيناريو محدد.
استرجاع الأمن	[X.810] أعمال متخذة وإجراءات منفذة عند انتهاك الأمن سواء كشفت أو يشك في حدوثها.
خدمة الأمن	[X.800] خدمة، توفرها طبقة أنظمة الاتصالات المفتوحة، تضمن الأمن الكافي للأنظمة أو لنقل البيانات.
إذنة الأمن	[X.810] مجموعة بيانات تحميها خدمة الأمن أو أكثر مع معلومات أمن تستخدم في توفير خدمات أمن تنقل بين كيانات الاتصالات.
حماية مجالات انتقائية	[X.800] حماية مجالات محددة في رسالة ترسل.
الحساسية	[X.509] خاصية مورد تتضمن قيمته أو أهميته. [X.800] خاصية مورد تتضمن قيمته أو أهميته وقد تشمل تعرضها للتأثر.
الخدمة	[X.790] يمثل هذا المصطلح مقدرات اتصالات يشتريها أو يؤجرها زبون من مزود خدمة. والخدمة هي تجريد رؤية موجهة نحو الشبكة – عنصر أو موجهة نحو المعدات. ويمكن أن توفر عناصر الشبكة المختلفة خدمات مماثلة ويمكن توفير خدمات مختلفة من قبل نفس عناصر الشبكة.

المصطلح	التعريف
طبقة إدارة الخدمة	[M.3010] طبقة إدارة تتعلق بالجوانب التعاقدية ومسؤولة عنها، بما في ذلك مناولة طلبات الخدمة ومناولة الشكاوى والفوترة لخدمات تقدم إلى زبائن أو متاحة لزبائن محتملين جدد.
وكالة تقديم الخدمات	[X.790] نظام أو شبكة توفر خدمة الاتصالات إلى الزبون. وفي سياق هذه الوثيقة، يعتبر مزود الخدمة مزوداً محدداً لخدمات الاتصالات يعرض توصيلاً بينياً لأنظمة مفتوحة من نظام العمليات إلى نظام العمليات ليتيح للزبون مقدرة إدارة الشبكة عبر ولايات قضائية لمراقبة خدمات (أو موارد) يجري توفيرها (انظر الزبون). ويقوم مزود الخدمة بدور الوكيل. وليست هناك متطلبات تقصر السطح البيني على الحالات التي توجد فيها خدمة اتصالات تقليدية من زبون إلى مزود خدمة اتصالات والعلاقة بين الأطراف. ومن الممكن أن تستخدم شركتا اتصالات تعمل شبكا ما بينياً لتوفير خدمة الاتصالات مستعملاً بائياً لهذا السطح البيني. وفي تلك الحالة، قد تتغير أدوار الزبون والمزود من حالة إلى حالة. ومع ذلك، وفي أي حالة معينة، تكون إحدى شركتي الاتصالات هي الزبون ولها دور المدير، بينما تكون الأخرى المورد ولها دور الوكيل.
علاقة الخدمة	[H.530] مراجع تصاحب أمن قائمة بين كيانين وظيفيين، مع افتراض وجود مفتاح متقاسم على الأقل.
سر متقاسم	[H.530] يشير إلى مفتاح الأمن لخوارزميات مجفرة؛ قد يكون مشتقاً من كلمة السر.
التوقيع	[X.800] انظر التوقيع الرقمي.
الاستيقان بسيط	[X.509] الاستيقان بواسطة ترتيبات كلمة السر البسيطة.
مصدر السلطة	[X.509] مصدر سلطة هو سلطة خواص تثق في متحقق الامتياز لمورد معين باعتبارها السلطة النهائية لتعيين مجموعة من المميزات.
بريد إلكتروني غير مرغوب	[H.235] هجوم رافض للخدمة عند إرسال بيانات غير مخولة تتجاوز النظام. وحالة خاصة هي بريد إلكتروني غير مرغوب للوسائط عند إرسال رزم بروتوكول الوقت الفعلي على منافذ بروتوكول بيانات المستعمل. وعادة ما يفيض النظام برزم؛ وتستهلك المعالجة موارد النظام الثمينة.
حالة تقرير الأعطال	[X.790] المرحلة التي وصل إليها تقرير الأعطال منذ استطباقه/وضعه بينما يجري حل الأعطال.
الاستيقان القوي	[X.509] الاستيقان بواسطة تفويضات مشتقة مجفرة.
خوارزمية تناظرية (قائمة على مفتاح سري) مجفرة	[H.235] خوارزمية لأداء التشفير أو خوارزمية متطابقة لأداء فك التجفير يطلب فيها نفس المفتاح لكل من التشفير وفك التشفير (X.810).
خوارزمية تناظرية مجفرة	[X.810] خوارزمية لأداء التشفير أو خوارزمية متطابقة لأداء فك التشفير يطلب فيها نفس المفتاح لكل من التشفير وفك التشفير.
شبكة إدارة الاتصالات	[M.3010] معمارية للإدارة بما في ذلك تخطيط وتوفير وتركيب وصيانة وتشغيل وإدارة معدات وشبكات وخدمات الاتصالات.
التهديد	[H.235] احتمال انتهاك الأمن (X.800). [X.800] احتمال انتهاك الأمن.

المصطلح	التعريف
دلالة الوقت	[X.790] قيمة وقت مستخدم يشير إلى وقت حدوث نشاط أو عمل الحدث.
تحليل الحركة	[X.800] استدلال معلومات من ملاحظة تدفقات الحركة (وجودها وغيا ا وكميتها واتجاهها وترددها).
سرية تدفق الحركة	[X.800] خدمة سرية لحماية تحليل الحركة.
تحشية الحركة	[X.800] ابتكار حالات هامشية للاتصالات ووحدات بيانات هامشية و/أو بيانات هامشية في وحدات البيانات.
وظيفة التحويل	[M.3010] قدرة وظيفية تترجم بين نقطة مرجعية لشبكة إدارة الاتصالات ونقطة مرجعية لغير شبكة إدارة الاتصالات (سواء سلوكة أو مقيسة). ويكون الجزء غير شبكة إدارة الاتصالات للقدرة الوظيفية هذه خارج حدود شبكة إدارة الاتصالات.
الأعطال	[X.790] أي سبب يؤدي أو يساهم في إدراك المدير أن نوعية الخدمة لخدمات شبكة أو أكثر أو موارد الشبكة تدار تتدهور.
إدارة الأعطال	[X.790] تتألف إدارة الأعطال من مجموعة وظائف تمكّن من الإبلاغ عن الأعطال وتتبع حالتها. وتشمل خدمة إدارة الأعطال نسق طلب تقرير الأعطال وإدخال تقرير الأعطال وإضافة معلومات عن الأعطال وإلغاء تقرير الأعطال وحالة طلب تقرير الأعطال واستعراض تاريخ الأعطال وإخطار بتغيير قيمة الخواص (مثل، حالة تقرير الأعطال/الوقت الملتزم به) وضع/إلغاء غرض (تقرير الأعطال) التحقق من انتهاء إصلاح الأعطال وتعديل معلومات إدارة الأعطال.
سجل تاريخ الأعطال	[X.790] سجل معلومات مختارة من تقرير الأعطال تم الاحتفاظ به لأغراض تاريخية بعد غلق تقرير الأعطال.
إدارة الأعطال	[X.790] إبلاغ وتتبع الأعطال بين تشغيل بيني لكيانات إدارة مطابقة تعاونياً تجاه حل العطل. (ليس هناك تمييز بين السطوح البينية داخل الولاية القضائية أو ضمن ولاية قضائية.)
إبلاغ عن الأعطال	[X.790] إجراء اتصال باكتشاف الأعطال حتى تعمل إدارة الأعطال على حلها.
توضيح الأعطال	[X.790] هي عملية تشخيص وإجراء الإصلاح المطلوب لحل المشكلة. وتشمل عملية تعيين بنود أعمال محددة أو مسؤولية شاملة لحلها وغلق تقرير الأعطال.
تتبع الأعطال	[X.790] المقدرة على تتبع تطور تقرير الأعطال منذ بدايته حتى غلقه.
نوع الأعطال	[X.790] وصف الأعطال التي اكتشفت وفئا ا.
الثقة	[X.509] عامة، يقال إن كيان "يثق" في كيان ثانٍ عندما يفترض (الكيان الأول) أن الكيان الثاني يسلك الطريقة التي يتوقعها الكيان الأول. وتنطبق هذه الثقة فقط على وظيفة محددة. والدور الرئيسي للثقة في هذا السياق هو وصف العلاقة بين كيان موثق وسلطة؛ ويكون الكيان المتأكد من أنه يثق في سلطة لإصدار الشهادات صالحة ويعتمد عليها فقط. [X.810] ويقال إن الكيان X يثق في الكيان Y للقيام بمجموعة أنشطة إذا، وفقط إذا، اعتمد الكيان X على الكيان Y بأنه يسلك بطريقة معينة فيما يتعلق بالأنشطة.
كيان موثوق به	[X.810] كيان يمكن أن ينتهك سياسة الأمن سواء بواسطة أداء أعمال لا ينبغي القيام ا أو بواسطة الفشل في أداء أعمال من المفترض القيام ا.
عنصر وظيفي موثوق به	[X.800] عنصر وظيفي تم إدراكه على أنه صحيح فيما يتعلق ببعض المعايير، مثلاً كما وضعتها سياسة الأمن.

المصطلح	التعريف
طرف ثالث موثوق به	[X.810] سلطة أمن أو وكيلها الموثوق به فيما يتعلق ببعض الأنشطة المتعلقة بالأمن (في سياق سياسة الأمن).
كيان موثوق به غير مشروط	[X.810] كيان موثوق به يمكنه انتهاك سياسة الأمن دون اكتشافه.
مستعمل	[M.3010] شخص أو عملية تطبق خدمات الإدارة لغرض إنجاز عمليات الإدارة.
عنصر حد مزار	[H.530] عنصر الحد المزار هو عنصر حد موضوع في ميدان مزار.
محطة العمل	[M.3010] قدرة مادية تؤدي وظائف محطة العمل.
وظيفة محطة العمل	[M.3010] قدرة وظيفة تفسر معلومات شبكة إدارة اتصالات لمستعمل بشري والعكس بالعكس.
سطح بيني X	[M.3010] سطح بيني يطبق على نقاط مرجعية X.
نقاط مرجعية X	[M.3010] نقطة مرجعية توجد بين قدرات وظيفية لأنظمة العمليات في شبكات إدارة الاتصالات مختلفة. (ملاحظة - قد تكون الكيانات الموجودة خارج النقطة المرجعية X كجزء من شبكة إدارة الاتصالات (وظيفة أنظمة العمليات) فعلية أو جزء من بيئة غير شبكة إدارة الاتصالات (مشابه لوظيفة أنظمة العمليات). وهذا التصنيف غير واضح عند النقاط المرجعية X.)
شهادة X.509	[J.170] مواصفات شهادة مفتاح عمومي وضعت كجزء من دليل معايير قطاع تقييس الاتصالات X.500.

ألف – 3 مصطلحات وموارد تعريف أخرى لقطاع تقييس الاتصالات

توفر قاعدة بيانات قطاع تقييس الاتصالات على الخط SANCHO (*مختصرات وتعاريف القطاع لمسرد موجه نحو الاتصالات*) النفاذ إلى "المصطلحات والتعاريف" أو "المختصرات" بالإنكليزية والفرنسية والإسبانية التي تم تعريفها في منشورات قطاع تقييس الاتصالات. وهذا مورد مجاني على الخط يمكن النفاذ إليه على www.itu.int/sancho. ويجري أيضاً نشر صيغة على قرص متراص بذاكرة قراءة (CD-ROM) بانتظام. ويمكن الوصول إلى جميع المصطلحات والتعاريف الواردة أعلاه في SANCHO مع قائمة بالتوصيات التي استخدم فيها المصطلح أو التعريف.

ووضعت لجنة الدراسات 17 التابعة لقطاع تقييس الاتصالات مجموعة من تعاريف الأمن المستخدمة في توصيات قطاع تقييس الاتصالات التي توجد على www.itu.int/ITU-T/studygroups/com17/cssecurity.html.

الملحق باء: كتالوج توصيات قطاع تقييس الاتصالات المتعلقة بالأمن

باء – 1 جوانب الأمن الواردة في هذا الكتيب

التوصية F.400 *نظام مناولة الرسائل ونظرة شاملة على الخدمة*

توفر هذه التوصية نظرة شاملة لتعريف النظام الشامل وخدمة نظام مناولة الرسائل وتقدم نظرة عامة لنظام مناولة الرسائل. وهذه النظرة هي واحدة من مجموعة توصيات تصف نموذج النظام وعناصر خدمة نظام مناولة الرسائل وخدماته. وتستعرض هذه التوصية قدرات نظام مناولة الرسائل التي تستخدمها وكالة توفير الخدمة من أجل توفير خدمات عمومية لمناولة الرسائل تمكّن المستعملين من تبادل الرسائل على أساس التخزين وإعادة الإرسال. ويصمم نظام مناولة الرسائل طبقاً لمبادئ نموذج مرجعي لتوصيل بيني لأنظمة مفتوحة للتطبيقات في قطاع تقييس الاتصالات (X.200) ويستخدم تقديم خدمات الطبقة وخدمات عناصر الخدمة تطبيقات أخرى أكثر عمومية. ويمكن إنشاء نظام مناولة الرسائل باستخدام أي شبكة تناسب نطاق التوصيل البيني للأنظمة المفتوحة. وتكون خدمة نقل الرسائل التي توفرها خدمة نقل الرسائل مستقلة التطبيق. ومن أمثلة التطبيقات المقيسة خدمة المراسلة فيما بين الأشخاص (F.420 + X.420) وخدمة مراسلة تبادل البيانات الإلكترونية (F.435 + X.435) وخدمة مراسلة صوتية (F.440 + X.440). ويمكن للأنظمة الطرفية أن تستخدم خدمة نقل الرسائل لتطبيقات محددة معروف أ ا ثنائية. وتخص خدمات مناولة الرسائل التي يوفرها مزودو الخدمة زمرة خدمات تلماتية. ويرد تعريف الخدمات العمومية المبنية على نظام مناولة الرسائل وكذلك النفاذ إلى ومن نظام مناولة الرسائل للخدمات العمومية في سلسلة توصيات F.400. ويرد تعريف الجوانب التقنية لنظام مناولة الرسائل في سلسلة توصيات X.400. وترد معمارية النظام الشامل لنظام مناولة الرسائل في التوصية X.402 لقطاع تقييس الاتصالات. وعناصر الخدمة هي خصائص الخدمة الموفرة من خلال عمليات التطبيق. وتعتبر عناصر الخدمة مكونات الخدمات الموفرة للمستعملين وهي إما عناصر خدمة أساسية أو أ ا تسهيلات اختيارية للمستعملين وهي مصنفة على أ ا 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 (معرفة في الملحق باء) **وإدارة الأمن** وإعالات أمن نظام مناولة الرسائل وأمن المراسلة فيما بين الأشخاص. المسألة 11/17

التوصية F.440 *خدمة مناولة الرسائل: خدمة المراسلة الصوتية*

تحدد هذه التوصية جوانب الخدمة العامة والاختيارية ونوعيتها لخدمة المراسلة الصوتية العمومية الدولية، وهو نوع محدد من خدمة مناولة الرسائل، وهي خدمة اتصالات دولية تقدمها إدارات تمكّن المشتركين من إرسال رسالة لمستقبل أو أكثر وتسلم رسائل عبر شبكة الاتصالات باستخدام الجمع بين التخزين وإعادة الإرسال وتقنيات التخزين والاسترداد. وتمكّن 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 رسالة على حدة أو لفترة من الوقت تعاقدية متفق عليها، إذا كانت توفرها الإدارة. ويمكن توفير مراسلة اتصال بيني مع خدمة مراسلة فيما بين الأشخاص كخيار في خدمة المراسلة الصوتية. ويتعين أن تتيح الإدارة دولياً خصائص أساسية. وتصنف الخصائص غير الأساسية، الواضحة للمشترك، إما على أ ا أساسية أو إضافية. وينبغي للإدارة أن تتيح دولياً الخصائص الأساسية الاختيارية. ويمكن أن تتيح بعض الإدارات الخصائص الإضافية الاختيارية للاستخدام الوطني والدولي على أساس اتفاق ثنائي. وتسمى الخصائص غير الأساسية تسهيلات اختيارية للمستعمل. ويمكن توفير خدمة المراسلة الصوتية باستخدام أي شبكة اتصالات. ويمكن عرض خدمة المراسلة الصوتية على نحو منفصل أو الجمع بين خدمات التلماتية المختلفة أو اتصالات البيانات. وترد في سلسلة توصيات X.400 المواصفات والبروتوكولات المستخدمة في خدمة المراسلة الصوتية.

الملحق زاي: عناصر **آمنة** لمراسلة صوتية لخدمة

الملحق حاء: نظرة شاملة على **أمن** المراسلة الصوتية المسألة 11/17

التوصية F.851 *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 المشاركة 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 المستعمل للاتصالات الشخصية العالمية"، وكخيار لخاصية المستعمل يوجد الاستيقان من وكالة تقديم خدمة الاتصالات الشخصية العالمية. ويرد في القسم 4.4 تفاصيل متطلبات الأمن. المسألة 3/2

التوصية 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 القسم 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. المسألة G/16

التوصية 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 ا التجفير وفك تجفير البيانات المرسلة. وإذا تمكن طرف ثالث من النفاذ إلى المفاتيح المستخدمة، يصبح نظام الخصوصية غير آمن. ومن ثم، تصبح صيانة المستعملين للمفاتيح جزءاً مهماً من نظام الخصوصية. وترد في هذه التوصية طرق عملية بديلة لإدارة المفاتيح. المسألة G/16

التوصية H.235 *أمن وتجفير المطاريف متعددة الوسائط للسلسلة H (المطاريف H.323 وغيرها من نمط H.245)*

تتضمن عادة اتصالات الوقت الحقيقي الآمنة عبر شبكات غير آمنة الاستيقان والخصوصية (تجفير بيانات). وتصف هذه التوصية تعزيز إطار المؤتمرات التفاعلية لتتضمن خدمات الأمن مثل الاستيقان من النقطة الطرفية وخصوصية الوسائط، وتصف البنية التحتية للأمن وتقنيات محددة للخصوصية يجري استخدامها. وينطبق المخطط المقترح على كل من مؤتمرات بسيطة من نقطة إلى نقطة ومتعددة النقاط لأي مطاريف تستخدم بروتوكول مراقبة التوصية H.245. وتمثل هذه الصيغة (11/00) تجفيراً لمنحني إهليلجي ومظاهر جانبية للأمن (توقيعات قائمة على كلمة سر بسيطة ورقمية متطورة) وتدابير عكس الأمن (مناهضة الرسائل الاقتحامية للوسائط) وخوارزمية تجفير متقدمة وخدمة طرفية خلفية ومعرفات أغراض (انظر دليل المنفذين التوصية H.323). المسألة G/16

التوصية H.235 الملحق واو *الملامح العامة للأمن المهجن*

يصف هذا الملحق مظهراً جانبياً مهجناً للأمن قائماً على بنية تحتية للمفاتيح العمومية، فعالاً ويمكن قياسه، ينتشر بتوقيعات 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 لتوقيع في التوصية H.235 الملحق هاء على نحو غير مهم؛ وما تزال التوقيعات الرقمية تتطابق مع إجراءات خوارزمية التجفير المتقدمة. ومع ذلك، تنتشر التوقيعات 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 عوائق 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 توقيعات 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. ويلزم المظهر الجانبي المهجن للأمن نموذج بواب متفرع ويقوم على أساس تقنيات أنفاق التوصية H.245؛ أما دعم نماذج غير بواب متفرع فيحتاج لمزيد من الدراسة. المسألة G/16

التوصية H.323 *نظام اتصالات لوسائط متعددة قائم على الرزم (الملحق ياء: أمن أنواع بسيطة لنقاط طرفية)*

تصف هذه التوصية مطاريف وكيانات أخرى توفر الوقت الفعلي لخدمات اتصالات سمعية وفيديوية وبيانات و/أو متعددة الوسائط عبر شبكات قائمة على رزم قد لا تضمن نوعية الخدمة. إن الدعم السمعي إلزامي، أما البيانات والفيديو فهما اختياريان، أما إذا تم دعمهما، تكون 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 ضمنية أو شبكات توصيل بيني (بما في ذلك الإنترنت) أو توصيلات من نقطة إلى نقطة أو جزء واحد من شبكة أو شبكة للتوصيل البيني 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 ترتبط 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 المبدلة و/أو الشبكات اللاسلكية، ويمكن تكاملها في الحواسيب الشخصية أو تنفيذها في أجهزة وحيدة مثل الهواتف المرئية. المسألة G/16

التوصية H.530 *أمن التوصية H.510 في بيئات الوسائط المتعددة المتنقلة للتوصية H.323*

الغرض من هذه التوصية توفير 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.323 في صيغة 1 و2 لمناولة الأمن في بيئات سكونية للتوصية H.323. ويمكن أن تحقق تلك البيئات وأنظمة الوسائط المتعددة بعض الانتقال المحدود في مناطق بوابين؛ وتوفر التوصية H.323 بشكل عام والتوصية H.235 بشكل خاص الدعم القليل فقط لتجول آمن للمستعملين المتنقلين والمطاريف عبر ميادين مختلفة مع كيانات كثيرة متضمنة في بيئة تنقل موزعة مثلاً. وتعرض سيناريوهات تنقل التوصية H.323 الموصوفة في التوصية H.510 فيما يتعلق بالتنقل الطرفي حالة جديدة مع سمة مرنة وديناميه أيضاً من وجهة نظر الأمن. ويتعين الاستيقان من المستعملين الجوالين للتوصية H.323 والمطاريف المتنقلة بواسطة 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 ومعين له كلمة سر، لا يعرف الميدان المزار المستعمل المتنقل في البداية. وفي هذه الحالة، لا يتقاسم الميدان المزار مع أي علاقة أمن قائمة مع المستعمل المتنقل والمطراف المتنقل. ومن أجل أن يحقق الميدان المزار الاستيقان وضمان تخويل المستعمل المتنقل والمطراف المتنقل، يرحل الميدان المزار بعض مهمات الأمن مثل التحقق من التخويل 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 من ناحية المبدأ تكون البيئات المتنقلة للتوصية H.323 مفتوحة أكثر من الشبكات المغلقة للتوصية H.323، هناك حاجة أيضاً لتأمين مهمات إدارة المفاتيح على نحو صحيح. ومن الحقيقي أيضاً أن الاتصالات في الميادين المتنقلة وعبرها تستحق الحماية من التلاعب الخبيث. المسألة G/16

التوصية J.93 *متطلبات النفاذ المشروط في التسليم الثانوي لتلفزيون رقمي أو أنظمة تلفزيون بكبل*

تعرف هذه التوصية خصوصية البيانات ومتطلبات النفاذ لحماية شفرات تلفزيون رقمي لفريق خبراء الصور المتحركة التي تمر عبر شبكات التلفزيون الكبلية بين طرف رأسية الكبل والمشترك النهائي. ولا توجد خوارزميات مجفرة دقيقة مستخدمة في هذه العملية في التوصية J.93 كما تحدد إقليمياً و/أو تحددها الصناعة. لجنة الدراسات 9

التوصية J.96 التعديل 1 *الطريقة التقنية لضمان خصوصية إرسال تلفزيون دولي لمسافة بعيدة لفريق خبراء الصور المتحركة 2 المتطابقة مع التوصية J.89*

تحتوي هذه التوصية على معيار مشترك لنظام نفاذ مشروط لإرسال دولي لمسافة بعيدة لتلفزيون رقمي يتطابق مع مظهر جانبي مهني لفريق خبراء الصور المتحركة 2 (4:2:2). وتصف نظاماً أساسياً لتخليط التشكيل البيني القائم على مواصفات إذاعة فيديوية رقمية - خوارزمية تخليط مشتركة باستخدام المفاتيح الواضحة الثابتة تسمى كلمات الدورة. ويقدم أسلوب متلائم خلفي آخر آلية إضافية لإدراج كلمات الدورة ا فرة، بينما يحتفظ في نفس الوقت بقابلية التشغيل البيني. المسألة 6/9

التوصية J.170 *مواصفات أمن الاتصالات الكبلية باستخدام بروتوكول الإنترنت (J.sec)*

تعرف هذه التوصية معمارية الأمن وبروتوكولات وخوارزميات ومتطلبات وظيفية متصاحبة وأي متطلبات تقنية يمكن توفيرها لأمن نظام شبكة الاتصالات الكبلية باستخدام بروتوكول الإنترنت. وينبغي توفير الاستيقان ومراقبة النفاذ ورسـالة وسلامة محتوى الحمالة والسـرية وخدمات الأمن وعـدم التنصل كما عرفت لكل الأسطح البينية لعنـاصر الشـبكة. لجنة الدراسات 9

التوصية M.3010 *مبادئ شبكة إدارة الاتصالات*

تعرف 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. وتتناول بعض أجزاء هذه التوصية الأمن. ويتوفر نموذج مرجعي منطقي لتقسيم وظيفية الإدارة ومعمارية بشكل طبقات. وتعرف هذه التوصية أيضاً كيفية بيان تطابق وامتثال شبكة إدارة الاتصالات لغرض تحقيق قابلية التشغيل البيني. وتشمل متطلبات شبكة إدارة الاتصالات القادرة على ضمان نفاذ آمن إلى معلومات الإدارة بواسطة مستعملين مخولين لمعلومات 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 متصاحبة مع تطبيقات شبكة إدارة الاتصالات. المسألة 7/4

التوصية M.3016 *نظرة شاملة على أمن شبكة إدارة الاتصالات (M.3sec)*

توفر هذه التوصية نظرة شاملة وإطاراً يعرف ـديدات الأمن على شبكة إدارة الاتصالات وتوجز كيفية تطبيق خدمات الأمن المتاحة في سياق معمارية وظيفية لشبكة إدارة الاتصالات، كما وصفت في التوصية M.3010. وهذه التوصية تنوعية في طابعها ولا تعرف أو تتناول متطلبات لسطح بيني محدد لشبكة إدارة الاتصالات. المسألة 7/4

التوصية M.3210.1 *إدارة الأمن من فئة الاتصالات المتنقلة الدولية 2000 - متطلبات*

هذه التوصية هي واحدة من سلسلة توصيات خدمة إدارة شبكة إدارة الاتصالات التي توفر وصفاً لخدمات الإدارة وأهدافها وسياقها لجوانب إدارة شبكات الاتصالات المتنقلة الدولية 2000. وتبنى هذه التوصية على مجموعة الوظائف المعرفة في التوصية M.3400 لقطاع تقييس الاتصالات بواسطة تحديد مجموعات وظائف جديدة ووظائف ومعلمات وإضافة دلالات وتقييدات. وتصف هذه التوصية مجموعة فرعية لخدمات إدارة الأمن لتوفير متطلبات وتحليل إدارة الأمن والمظهر الجانبي لإدارة احتيالية 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 كوسيلة لرصد مجموعة محددة من أنشطة المشتركين تحد من تعرضهم المالي إلى فواتير كبيرة غير مسددة وجدت في حسابات المشترك بينما يقوم هذا المشترك بالتجول. المسألة 14/4

التوصية M.3320 *متطلبات للسطح البيني X*

هذه التوصية هي جزء من سلسلة توصيات تتناول نقل المعلومات لإدارة شبكات وخدمات الاتصالات، وتتناول بعض الأجزاء فقط جوانب الأمن. والغرض من هذه التوصية هو 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 ا ومشغلي شبكات آخرين وزبائن وكيانات أخرى. المسألة 9/4

التوصية M.3400 *وظائف إدارة شبكة إدارة الاتصالات*

هذه التوصية هي 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) متصاحبة مع المهام 2 (وصف سياق إدارة شبكة إدارة الاتصالات) في منهجية مواصفات السطح البيني لشبكة إدارة الاتصالات المحددة في التوصية M.3020 لقطاع تقييس الاتصالات. وعند أداء تحليل سياق إدارة شبكة إدارة الاتصالات، من المستصوب النظر في الاستخدام الأمثل موعات وظائف إدارة شبكة إدارة الاتصالات المتاحة في هذه التوصية. المسألة 7/4

التوصية Q.293 *الفترات التي تنفذ فيها تدابير الأمن*

هذا مقتطف من الكتاب الأزرق ويحتوي على الأقسام من 5.8 (الفترات التي تنفذ فيها تدابير الأمن) إلى 9.8 (طريقة تقاسم الحمولة) من التوصية Q.293. لجنة الدراسات 4

التوصية Q.813 *عناصر أمن خدمة تحويل التطبيقات من أجل عناصر خدمة العمليات عنُ بعد (STASE-ROSE)*

توفر هذه التوصية مواصفات لدعم تحويلات الأمن مثل التجفير والفرم ومنع التسرب والتوقيع مع التركيز على عناصر خدمة العمليات عنُ بعد لوحدات بيانات البروتوكول. وتستخدم تحويلات الأمن لتوفير خدمات أمن مختلفة مثل الاستيقان والسرية وسلامة البيانات وعدم التنصل. وتصف هذه التوصية منهجاً لتوفير تحويلات أمن تنفذ في طبقة تطبيق وتتطلب عدم وجود عنصر وظيفي محدد لأمن في أي من طبقات بطاريات التوصيل البيني للأنظمة المفتوحة. المسألة 18/4

التوصية Q.815 *مواصفات وحدة الأمن لحماية رسالة كاملة*

تحدد هذه التوصية وحدة تشغيل أمن تستخدم مع التوصية Q.814، مواصفات لوكيل بيانات إلكترونية متبادلة تفاعلية، وتوفر خدمات الأمن لوحدات بيانات البروتوكول الكاملة، وتدعم، بصورة خاصة، وحدة الأمن عدم التنصل للأصل والمستقبل وكذلك سلامة الرسالة الكاملة. المسألة 18/4

التوصية Q.817 *بنية تحتية للمفاتيح العمومية لشبكة إدارة الاتصالات - شهادات رقمية ومظاهر جانبية لقوائم إبطال الشهادات*

تشرح هذه التوصية كيفية استخدام الشهادات الرقمية ومظاهر جانبية لقوائم إبطال الشهادات في شبكة إدارة الاتصالات وتقدم متطلبات عن استخدام تمديد الشهادة 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 من هذه التوصية هو توفير آلية تشغيل بيني يمكن قياسها لتوزيع المفاتيح والإدارة في شبكة إدارة الاتصالات عبر جميع الأسطح البينية وكذلك لدعم خدمة عدم التنصل عبر السطح البيني X. وتنطبق على جميع الأسطح البينية وتطبيقات شبكة إدارة الاتصالات. وهي مستقلة عن بطاريات بروتوكول الاتصالات أو بروتوكول إدارة الشبكة المستخدمة. ويمكن استخدام تسهيلات البنية التحتية للمفاتيح العمومية لمدى واسع من وظائف الأمن مثل الاستيقان

وسلامة البيانات وعدم التنصل وتبديل المفاتيح (M.3016). ومع ذلك، لا تحدد هذه التوصية كم عدد الوظائف التي ينبغي تنفيذها مع بنية تحتية للمفاتيح العمومية أو بدو ا. المسألة 18/4

التوصية Q.1531 *متطلبات أمن الاتصالات الشخصية العالمية لخدمة من ا موعة 1*

تحدد هذه التوصية متطلبات أمن الاتصالات الشخصية العالمية لكل من الشبكة إلى المستعمل واتصالات شبكة التوصيل البيني المطبقة على خدمة الاتصالات الشخصية العالمية من ا موعة 1 كما عرفت في التوصية 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. لجنة الدراسات 15

التوصية Q.1741.1 *مراجع الاتصالات المتنقلة الدولية- 2000 لتحرير 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 لمتطلبات أمن 3GPP التالية:

TS 21.133: ديدات الأمن ومتطلباته
TS 22.100: المرحلة 1 للنظام العالمي للاتصالات المتنقلة
TS 22.101: مبادئ خدمة النظام العالمي للاتصالات المتنقلة
TS 33.102: معمارية الأمن
TS 33.103: مبادئ توجيهية لسلامة الأمن
TS 33.105: متطلبات الخوارزمية ا فرة
TS 33.106: متطلبات الاعتراض القانوني
TS 33.107: معمارية اعتراض قانوني ووظائفها
TS 33.120: أهداف ومبادئ الأمن لجنة الدراسات الخاصة

التوصية Q.1741.2 *مراجع الاتصالات المتنقلة الدولية – 2000 لتحرير 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 لمتطلبات أمن 3GPP التالية:

TS 21.133: أمن 3G؛ ديدات الأمن ومتطلباته
TS 22.048: آليات الأمن موعة أدوات تطبيق وحدة (عالمية) لهوية مشترك؛ المرحلة 1
TS 22.101: جوانب الخدمة؛ مبادئ الخدمة
TS 33.102: أمن 3G؛ معمارية الأمن
TS 33.103: أمن 3G؛ مبادئ توجيهية للسلامة
TS 33.105: متطلبات الخوارزمية ا فرة
TS 33.106: متطلبات الاعتراض القانوني
TS 33.107: أمن 3G؛ معمارية اعتراض قانوني ووظائفها
TS 33.120: أهداف ومبادئ الأمن
TS 33.200: أمن ميدان الشبكة – نظام فرعي للتطبيق المتنقل
TS 35.205. 206, 207 and 208: أمن 3G؛ مواصفات مجموعة خوارزميات MILENAGE: مثال مجموعة خوارزميات الاستيقان 3GPP ووظائف ابتكار المفاتيح f1 و*f1 وf2 وf3 وf4 و*f5؛ (205: عام؛ 206: مواصفات خوارزمية؛ 207: بيانات اختبار المنفذين؛ بيانات اختبار تطابق التصميم) لجنة الدراسات الخاصة

التوصية Q.1741.3 *مراجع الاتصالات المتنقلة الدولية- 2000 لتحرير 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 لمتطلبات أمن 3GPP التالية:

TS 22.101: جوانب الخدمة؛ مبادئ الخدمة
TS 33.102: أمن 3G؛ معمارية الأمن

TS 33.106: متطلبات الاعتراض القانوني
TS 33.107: أمن 3G؛ معمارية الاعتراض القانوني ووظائفها
TS 33.108: أمن 3G؛ سطح بيني لتسليم الاعتراض القانوني
TS 33.200: أمن ميدان الشبكة - نظام فرعي للتطبيق المتنقل
TS 33.203: أمن 3G؛ أمن نفاذ لخدمات قائمة على بروتوكول الإنترنت
TS 33.210: الأمن؛ أمن ميدان الشبكة؛ أمن طبقة الشبكة باستخدام بروتوكول الإنترنت
TS 35.205, 206, 207, 208 and 209: أمن 3G؛ مواصفات مجموعة خوارزميات MILENAGE: مثال مجموعة خوارزميات الاستيقان 3GPP ووظائف ابتكار مفاتيح f1، *f1 و f2 و f3 وf4 و *f5؛ (205: عام؛ 206: مواصفات خوارزمية؛ 207: بيانات اختبار المنفذين؛ بيانات اختبار تطابق التصميم؛ 909: موجز ونتائج التصميم والتقييم) لجنة الدراسات الخاصة

التوصية Q.1742.1 *مراجع الاتصالات المتنقلة الدولية 2000 - للمعهد الأمريكي الوطني للمعايير- 41 الذي طور الشبكة الأساسية مع نفاذ متعدد لتقسيم شفري 2000 لشبكة النفاذ*

تصاحب هذه التوصية معايير الشبكة الأساسية الصادرة عن منظمات تنمية المعايير مع مواصفات 3GPP2 التي تمت الموافقة عليها في 17 يوليو 2001 لعضو أسرة الاتصالات المتنقلة الدولية-2000 "للمعهد الأمريكي الوطني للمعايير-41 الذي طور شبكة اللب مع نفاذ متعدد لتقسيم شفري 2000 لشبكة النفاذ." وسوف تصاحب مواصفات 3GPP2 التي تمت الموافقة عليها في يوليو 2002 معايير شبكة اللب الصادرة في التوصية Q.1742.2 لقطاع تقييس الاتصالات. ويصاحب السطح البيني الراديوي وشبكة النفاذ الراديوية والمعايير من منظمات التنمية معايير لعضو أسرة الاتصالات المتنقلة الدولية-2000 التوصية M.1457 لقطاع تقييس الاتصالات. وتحدد الارتباطات لأعضاء أسرة الاتصالات المتنقلة الدولية-2000 في سلسلة التوصية Q.174x. وتجمع هذه التوصية وتصاحب معايير الشبكة الأساسية ذات الصلة من عدد من منظمات تنمية المعايير لعضو أسرة الاتصالات المتنقلة الدولية-2000 في توصية شاملة. لجنة الدراسات الخاصة

التوصية 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 لتقسيم شفري 2000 لشبكة النفاذ*

ترتبط هذه التوصية بمعايير الشبكة الأساسية الصادرة عن منظمات إقليمية لتنمية المعايير مع مواصفات 3GPP2 التي تمت الموافقة عليها في 11 يوليو 2002 لعضو أسرة الاتصالات المتنقلة الدولية-2000 "للمعهد الأمريكي الوطني للمعايير-41 الذي طور الشبكة الأساسية مع نفاذ متعدد لتقسيم شفري 2000 لشبكة النفاذ." وصاحبت مواصفات 3GPP2 التي تمت الموافقة عليها في 17 يوليو 2001 معايير الشبكة الأساسية الصادرة عن المنظمات الإقليمية لتنمية المعايير في التوصية Q.1742.1 لقطاع تقييس الاتصالات. وسوف تصاحب مواصفات 3GPP2 التي تمت الموافقة عليها في يوليو 2003 معايير الشبكة الأساسية الصادرة في التوصية Q.1742.3 لقطاع تقييس الاتصالات. ويصاحب السطح البيني الراديوي وشبكة النفاذ الراديوية ومعايير من منظمات تنمية المعايير لعضو أسرة الاتصالات المتنقلة الدولية-2000 التوصية M.1457 لقطاع تقييس الاتصالات. وتعرف الارتباطات لأعضاء أسرة الاتصالات المتنقلة الدولية-2000 في سلسلة التوصية Q.174x. وتجمع هذه التوصية وتصاحب المعايير الإقليمية لشبكة اللب لعضو أسرة الاتصالات المتنقلة الدولية-2000 في توصية شاملة. لجنة الدراسات الخاصة

التوصية Q.1742.3 *توصيات تقنية مرجعية في التوصية Q.1742.3 مع جوانب الأمن*

توصيات 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)

مواصفات بيانات الرزم:

P.S0001-A معيار شبكة لاسلكية باستخدام بروتوكول الإنترنت (الصيغة 3.0.0؛ 16 يوليو 2001)

P.S0001-B معيار شبكة لاسلكية 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 لاسلكية (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 معرف المعدات المتنقلة 3G (الصيغة 1.0؛ MEID) (10 مايو 2001)

S.S0053 خوارزمية مجفرة مشتركة (الصيغة 1.0؛ 21 يناير 2002)

S.S0054 مواصفات السطح البيني لخوارزمية 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 (الصيغة 1.0؛ 18 أبريل 2002)

S.R0073 إدارة تشكيل سماعات يد على الهواء للإنترنت (الصيغة 1.0؛ IOTA) المرحلة 1 (12 ديسمبر 2002)

S.S0078-0 خوارزميات الأمن المشتركة (الصيغة 1.0؛ 12 ديسمبر 2002) لجنة الدراسات الخاصة

التوصية T.30 *إجراءات لإرسال وثيقة بالفاكس في الشبكة الهاتفية العمومية المبدلة*

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 ريفس وشامير وأدلمان. لجنة الدراسات 16

التوصية T.36 *مقدرات الأمن لاستخدام مطاريف الفاكس من الزمرة 3*

تعرف 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 ريفس وشامير وأدلمان. لجنة الدراسات 16

التوصية T.123rev الملحق باء *توصيلات نقل متعددة*

يقوم هذا الملحق بتنقيح التوصية T.123 لبروتوكول مفاوضات التوصيل الذي 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 اليدوية وبروتوكول أمن طبقة النقل X.274/ISO ونظام فرعي أرضي- سطح بيني لبرنامج تطبيق. المسألة 1/16

التوصية T.503 *مظهر جانبي لتطبيق وثيقة لمبادلة وثائق الفاكس من الزمرة 4*

تعرف هذه التوصية المظهر الجانبي لتطبيق وثيقة قد يستخدم بواسطة أي خدمة تلماتية. والغرض منها هو تحديد نسق مبادلة وثائق الفاكس من الزمرة 4 تحتوي فقط على رسوم بيانية تنقيطية. ويجري مبادلة الوثائق في شكل منسوق يمكن المستقبل من عرض أو طبع الوثيقة كما يتوخاها مرسلها. لجنة الدراسات 16

التوصية T.563 *الخصائص المطرافية لأجهزة الفاكس من الزمرة 4*

تعرف هذه التوصية الجوانب العامة لأجهزة الفاكس من الزمرة 4 والسطح البيني للشبكة المادية. لجنة الدراسات 16

التوصية T.611 *السطح البيني لبرمجة اتصالات* ***السطح البيني للتطبيق المحلي ولتطبيقات الاتصالات*** *لفاكس من الزمرة 3 وفاكس من الزمرة 4 وتيلكس وبريد إلكتروني وخدمات نقل الملفات*

تعرف هذه التوصية السطح البيني لبرمجة اتصالات تسمى "**السطح البيني للتطبيق المحلي ولتطبيقات الاتصالات**" يوفر نفاذاً موحداً لخدمات اتصالات مختلفة مثل فاكس من الزمرة 3 أو خدمات تلماتية. وتصف هذه التوصية هيكل ومحتويات الرسائل وطريقة تبادلها بين كيانين (أي تطبيق محلي وسلطة إصدار شهادات وتطبيق اتصالات). *وأي اتصالات تسبقها عملية نفاذ إلى شبكة وانتهائها بعملية خروج من الشبكة، تيسر كلا العمليتين تنفيذ مخططات أمن مهمة بصورة خاصة في أنظمة المستعملين المتعددين. وتوفران أيضاً وسائل لتنفيذ آليات الأمن بين التطبيق المحلي وسلطة إصدار الشهادات*. وتشكل هذه التوصية مستوى مرتفع من سطح بيني لبرمجة تطبيق يحمي جميع خصائص الاتصالات ولكن يوفر مراقبة قوية ورصداً لنشاط اتصالات مصممي التطبيق. لجنة الدراسات 8

التوصية X.217 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - تعريف خدمة عنصر خدمة مراقبة التصاحب*

تعرف هذه التوصية خدمات عنصر خدمة مراقبة الارتباط لمراقبة التطبيق - الارتباط في بيئة التوصيل البيني للأنظمة المفتوحة. ويدعم عنصر خدمة مراقبة الارتباط أنساق التوصيل الموجه وعدم التوصيل للاتصالات. وتعرف ثلاث وحدات وظيفية في عنصر خدمة مراقبة الارتباط. وتستخدم وحدة النواة الوظيفية الإلزامية لإنشاء وتحرير التطبيقات - الارتباطات. ويشمل عنصر خدمة مراقبة الارتباط وحدتين وظيفيتين اختياريتين، واحدة منهما هي وحدة وظيفية لاستيقان اختياري توفر تسهيلات إضافية لتبادل المعلومات لدعم الاستيقان خلال إنشاء الارتباط دون إضافة خدمات جديدة. ويمكن استخدام تسهيلات استيقان عنصر خدمة مراقبة الارتباط لدعم نوع محدود من طرق الاستيقان.

التعديل 1: دعم آليات الاستيقان لنسق عدم التوصيل المسألة 11/17

التوصية X.227 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - بروتوكول موجه نحو توصيل عنصر خدمة مراقبة الارتباط: مواصفة البروتوكول*

تعرف مواصفات البروتوكول هذا الإجراءات التي تطبق في حالات اتصالات بين أنظمة تود التوصيل البيني مع بيئة توصيل بيني لأنظمة مفتوحة في نسق موجه نحو التوصيل، أي بروتوكول نسق موجه نحو توصيل عنصر الخدمة - تطبيق من أجل مراقبة التطبيق - ارتباط وعنصر خدمة مراقبة الارتباط. وتشمل مواصفات بروتوكول وحدة النواة الوظيفية المستخدمة لإنشاء وتحرير التطبيقات - الارتباطات. وتوفر الوحدة الوظيفية للاستيقان من التسهيلات الإضافية لتبادل المعلومات لدعم الاستيقان خلال إنشاء الارتباط دون إضافة خدمات جديدة. ويمكن استخدام تسهيلات الاستيقان عنصر خدمة مراقبة الارتباطات لدعم نوع محدود من طرق الاستيقان. وتوفر الوحدة الوظيفية للمفاوضات بشأن سياق التطبيق تسهيلاً إضافياً لاختيار سياق التطبيق خلال إنشاء التصاحب. وتشمل مواصفة هذا البروتوكول ملحقاً يصف آلة

بروتوكول، المشار إليها في آلة بروتوكول المراقبة، على أساس جدول حالة. وتشمل مواصفات هذا البروتوكول ملحقاً يصف آلية الاستيقان 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 "سلسلة رسوم بيانية". المسألة 11/17

التوصية X.237 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - بروتوكول عدم توصيل عنصر خدمة مراقبة الارتباط: مواصفات البروتوكول*

يشمل التعديل 1 على هذه التوصية وسم قابلية تمديد ترميز التركيب ا ,رد رقم 1 في وحدة تصف البروتوكول. ويعزز أيضا مواصفة بروتوكول عنصر خدمة مراقبة الارتباط عدم التوصيل لتوفير الدعم لنقل معلمات الاستيقان في A-UNIT-DATA APDU. المسألة 11/17

التوصية X.257 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - بروتوكول عدم توصيل عنصر خدمة مراقبة الارتباط: شكل إعلان عن مطابقة تنفيذ البروتوكول*

توفر هذه التوصية شكل إعلان عن مطابقة تنفيذ بروتوكول لبروتوكول عدم التوصيل لتوصيل بيني لأنظمة مفتوحة لعنصر خدمة مراقبة الارتباط المحدد في التوصية X.237. ويمثل شكل إعلان عن مطابقة تنفيذ البروتوكول، في شكل مجدول، العناصر الإلزامية والاختيارية لبروتوكول عدم التوصيل لتوصيل بيني لأنظمة مفتوحة. ويستخدم شكل البروتوكول هذا لتعريف خصائص واختيارات تنفيذ بروتوكول عدم التوصيل لتوصيل بيني لأنظمة مفتوحة. المسألة 11/17

التوصية X.272 *انضغاط البيانات والخصوصية عبر شبكات ترحيل الرتل*

تعرف هذه التوصية خدمة انضغاط البيانات وخدمة الخصوصية لشبكات ترحيل الرتل بما في ذلك المفاوضات وتغليف انضغاط البيانات وانضغاط البيانات الآمنة والاستيقان والتجفير عبر ترحيل الرتل. ويزيد وجود خدمة انضغاط البيانات في شبكة الصبيب الفعال للشبكة. ويتطلب الطلب على إرسال بيانات حساسة عبر الشبكات العمومية تسهيلات لضمان خصوصية البيانات. ومن أجل تحقيق معدلات انضغاط مثلي، من الضروري ضغط البيانات قبل تجفيرها. وبالتالي، فمن المستصوب توفير تسهيلات في خدمة انضغاط البيانات للمفاوضات مع بروتوكولات تجفير البيانات كذلك. ونظراً لأن مهمة الانضغاط ثم التجفير للبيانات هي مكثفة حسابياً، تتحقق الفعالية 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 غير المرقمة المغلفة باستخدام التوصية Q.933 الملحق هاء. ويتناول انضغاط البيانات والخصوصية في كل من التوصيلات التقديرية الدائمة والتوصيلات التقديرية المبدلة. المسألة 10/17

التوصية X.273 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - بروتوكول أمن طبقة الشبكة*

تحدد هذه التوصية البروتوكول لدعم خدمات سلامة البيانات والسرية والاستيقان ومراقبة النفاذ المعرفة في نموذج أمن التوصيل البيني للأنظمة المفتوحة كما تطبق على بروتوكولات طبقة شبكة بأسلوب التوصيل وبأسلوب عدم التوصيل. ويدعم البروتوكول هذه الخدمات من خلال استخدام آليات مجفرة ووسم الأمن ونعوت الأمن المعينة مثل المفاتيح ا مفرة. المسألة 11/17

التوصية X.274 *تكنولوجيا المعلومات - تبادل الاتصالات والمعلومات بين الأنظمة - بروتوكول أمن طبقة النقل*

تحدد هذه التوصية البروتوكول الذي يمكن أن يدعم خدمات سلامة البيانات والسرية والاستيقان ومراقبة النفاذ المعرفة في نموذج أمن التوصيل البيني للأنظمة المفتوحة كما تتعلق بطبقة النقل. ويدعم البروتوكول هذه الخدمات من خلال استخدام آليات مجفرة ووسم الأمن وخواص الأمن المعينة مثل المفاتيح ا فرة. المسألة 11/17

التوصية X.400/F.400 *نظام مناولة الرسائل ونظرة شاملة على الخدمة*

تحدد هذه التوصية عناصر نظام مناولة الرسائل 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 لخدمات أمن السرية وسلامة البيانات وعدم التنصل ومراقبة النفاذ المحددة على أ ا تتعلق بطبقة التطبيق. (انظر F.400) المسألة 11/17

التوصية X.402 *تكنولوجيا المعلومات - أنظمة مناولة الرسائل - المعمارية العامة*

تحدد هذه التوصية إجراءات الأمن ومعرفات الأغراض لاستخدامها في بروتوكولات أنظمة مناولة الرسائل لتحقيق خدمات السرية وسلامة البيانات وعدم التنصل ومراقبة النفاذ المحددة على أ ا تتعلق بطبقة التطبيق. المسألة 11/17

التوصية X.411 *تكنولوجيا المعلومات – أنظمة مناولة الرسائل – نظام نقل الرسائل: تعريف وإجراءات الخدمة ا ردة*

تحدد هذه التوصية آليات وإجراءات تدعم خدمات السرية وسلامة البيانات والاستيقان وعدم التنصل المحددة على أ ا تتعلق بطبقة التطبيق. ويدعم البروتوكول هذه الخدمات من خلال استخدام آليات مجفرة ووسم أمن وتوقيعات رقمية كما عرفت في التوصية X.509. وبالرغم من أن التوصية تحدد البروتوكول الذي يستخدم التقنيات اللاتناظرية ا فرة، إلا أن التقنيات التناظرية ا فرة يجري دعمها أيضاً. المسألة 11/17

التوصية X.413 *تكنولوجيا المعلومات - أنظمة مناولة الرسائل: مخزن رسائل: تعريف الخدمة ا ردة*

تحدد هذه التوصية آليات وبروتوكول وإجراءات تدعم خدمات سلامة البيانات ومراقبة النفاذ والاستيقان وعدم التنصل المعرفة على أ ا تتعلق بطبقة التطبيق. ويدعم البروتوكول هذه الخدمات نيابة عن مستعمل مخزن رسائل مباشر.المسألة 11/17

التوصية X.419 *تكنولوجيا المعلومات - أنظمة مناولة الرسائل: مواصفات البروتوكول*

تحدد هذه التوصية إجراءات وسياقات التطبيق لتعريف النفاذ الآمن لكيانات أنظمة مناولة الرسائل والمستعملين عنُ بعد من خلال توفير خدمات الاستيقان ومراقبة النفاذ المحددة على أ ا تتعلق بطبقة التطبيق. المسألة 11/17

التوصية 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 ومراقبة النفاذ المحددة على أ ا تتعلق بطبقة التطبيق. المسألة 11/17

التوصية 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 نيابة عن مستعملها المباشر. وخدمات الأمن التي تدعمها هي سلامة البيانات والسرية والاستيقان ومراقبة النفاذ كما حددت على أ ا تتعلق بطبقة التطبيق. المسألة 11/17

التوصية 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 ومراقبة النفاذ كما حددت على أ ا تتعلق بطبقة التطبيق. المسألة 11/17

التوصية X.500 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - الدليل: نظرة شاملة على المفاهيم والنماذج والخدمات*

تحدد هذه التوصية الدليل وخصائصه المتعلقة بالأمن. المسألة 9/17

التوصية X.501 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - الدليل: نماذج*

تحدد هذه التوصية استخدام الدليل لمفتاحه العمومي للتوصية X.509 وأطر شهادات الخواص. المسألة 9/17

التوصية X.509 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - الدليل:*

--- إطار الاستيقان (طبعة 1993 – الطبعة/المنقحة الثانية)

--- إطار الاستيقان (طبعة 1997 – الطبعة/المنقحة الثالثة)

--- أطر المفاتيح العمومية وشهادات الخواص (طبعة 2000 – الطبعة/المنقحة الرابعة)

تعرف هذه التوصية إطار شهادات المفاتيح العمومية وشهادات الخواص وتعرف إطار توفير خدمات الاستيقان من قبل دليل إلى مستعمليه. وتصف مستويين من الاستيقان: الاستيقان البسيط، باستخدام كلمة سر للتحقق من الهوية الطالبة؛ والاستيقان القوي الذي يتضمن تفويضات مشكلة باستخدام تقنيات مجفرة. وبينما يوفر الاستيقان البسيط بعض الحماية المحدودة من النفاذ غير المخول، ينبغي استخدام الاستيقان القوي فقط كأساس لتوفير الخدمات الآمنة. ويمكن أن تستخدم الأطر المعرفة لوضع مظهر جانبي لتطبيق البنى التحتية للمفاتيح العمومية والبنى التحتية لإدارة الامتياز. ويشمل إطار شهادات المفاتيح العمومية مواصفات أغراض البيانات المستخدمة لتمثل الشهادات نفسها وكذلك إشعارات إبطال للشهادات الصادرة التي ينبغي عدم الثقة فيها. وبينما تعرف بعض مكونات حرجة لبنى تحتية للمفاتيح العمومية، فهي لا تعرفها بالكامل. ومع ذلك، توفر أساساً يمكن أن تبنى عليه بنية تحتية للمفاتيح العمومية ومواصفا ا. ويشمل إطار شهادات الخواص مواصفات أغراض البيانات التي تستخدم لتمثل الشهادات نفسها وكذلك إشعارات إبطال للشهادات الصادرة التي ينبغي عدم الثقة فيها. وبينما تعرف بعض مكونات حرجة لبنية تحتية لإدارة متميزة، فهي لا تعرفها بالكامل. ومع ذلك، توفر أساساً يمكن أن تبنى عليه بنى تحتية لإدارة متميزة ومواصفا ا. وتعرف أيضاً أغراض المعلومات للاحتفاظ بأغراض البنية التحتية لمفاتيح عمومية والبنية التحتية لإدارة متميزة في الدليل ومن أجل مقارنة القيم المقدمة مع القيم المخزنة. المسألة 9/17

التوصية X.519 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - الدليل: مواصفة البروتوكول*

تحدد هذه التوصية الإجراءات وسياقات التطبيق لتعريف النفاذ الآمن خلال إسناد كيانات الدليل. المسألة 9/17

التوصية X.733 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - إدارة الأنظمة: وظيفة الإخبار عن الإنذار*

تعرف هذه التوصية وظيفة إدارة الأنظمة التي قد تستخدم بواسطة عملية تطبيق في بيئة إدارة مركزية أو لا مركزية للتفاعل من أجل إدارة الأنظمة. وتعرف هذه التوصية وظيفة تتألف من تعاريف تنوعية وخدمات ووحدات وظيفية موجودة في طبقة التطبيق لنموذج مرجعي للتوصيل البيني للأنظمة المفتوحة. وتوفر التبليغات عن الإنذار التي تعرفها هذه الوظيفة معلومات قد يحتاجها المدير للعمل بشأن الحالة التشغيلية لنظام ونوعية الخدمة. المسألة 17/4

التوصية X.735 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - إدارة الأنظمة: وظيفة مراقبة لوغاريتمية*

تعرف هذه التوصية وظيفة إدارة الأنظمة التي قد تستخدم بواسطة عملية تطبيق في بيئة إدارة مركزية أو لامركزية للتفاعل من أجل غرض الأنظمة. وتعرف هذه التوصية وظيفة مراقبة لوغاريتمية وتتألف من خدمات ووحدتين وظيفيتين. وتوجد هذه الوظيفة في طبقة التطبيق. المسألة 17/4

التوصية X.736 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - إدارة الأنظمة: وظيفة الأمن للإخبار عن الإنذار*

تعرف هذه التوصية | هذا المعيار الدولي وظيفة الأمن للإخبار عن الإنذار. وهذه الوظيفة هي وظيفة إدارة الأنظمة التي قد تستخدمها عملية التطبيق في بيئة إدارة مركزية أو لامركزية لتبادل المعلومات لغرض إدارة الأنظمة كما عرفت في ISO/IEC 7498-4 | CCITT Rec. X.700. وتوجد هذه التوصية | هذا المعيار الدولي في طبقة التطبيق وتعرف طبقاً للنموذج الذي تقدمه ISO/IEC 9545 | CCITT Rec. X.200. ويرد وصف دور وظائف إدارة الأنظمة في ISO/IEC 10040 | CCITT Rec. X.701. وتوفر تبليغات الأمن عن إنذارات التي تعرفها وظيفة إدارة الأنظمة معلومات تتعلق بالحالة التشغيلية ونوعية الخدمة المتعلقة بالأمن. المسألة 14/4

التوصية X.740 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - إدارة الأنظمة: وظيفة التسجيل الدقيق للأمن*

تعرف هذه التوصية | هذا المعيار الدولي وظيفة التسجيل الدقيق للأمن. وهذه الوظيفة هي وظيفة إدارة الأنظمة التي قد تستخدمها عملية التطبيق في بيئة إدارة مركزية أو لامركزية لتبادل المعلومات والأوامر لغرض إدارة الأنظمة كما عرفت في ISO/IEC 7498-4 | CCITT Rec. X.700. وتوجد هذه التوصية | هذا المعيار الدولي في طبقة التطبيق وتعرف طبقاً للنموذج الذي تقدمه ISO/IEC 9545 | CCITT Rec. X.200. ويرد وصف دور وظائف إدارة الأنظمة في ISO/IEC 10040 | CCITT Rec. X.701. المسألة 14/4

التوصية X.741 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - إدارة الأنظمة: أغراض وخواص لمراقبة النفاذ*

تعرف هذه التوصية | هذا المعيار الدولي نموذج الأمن لمراقبة النفاذ ومعلومات الإدارة الضرورية لابتكار وإدارة مراقبة النفاذ المتصاحب مع إدارة الأنظمة للتوصيل البيني للأنظمة المفتوحة. ولا تحدد سياسة الأمن المعتمدة لأي حالة استخدام وتترك باعتبارها خياراً للتنفيذ. وهذه المواصفة ذات تطبيق تنوعي وتطبق على إدارة الأمن لأنواع تطبيق كثيرة. المسألة 14/4

التوصية X.800 *معمارية الأمن للتوصيل البيني للأنظمة المفتوحة لتطبيقات اللجنة CCITT*

تعرف 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 تضع توصيات جديدة في سياق توصيل بيني للأنظمة المفتوحة من أجل السماح بتأمين الاتصالات، ومن ثم توفير منهج متسق للأمن في التوصيل البيني للأنظمة المفتوحة. وتتوسع هذه التوصية في النموذج المرجعي لتشمل 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 قد يوفرها النموذج المرجعي؛ وتعرف الحالات في النموذج المرجعي حيث يمكن توفير الخدمات والآليات. المسألة 10/17

التوصية 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 والمادية). وتصف المفاهيم المعمارية المشتركة لهذه الطبقات وأساس التفاعلات المتعلقة بالأمن بين الطبقات ووضع بروتوكولات الأمن في الطبقات السفلى. المسألة 10/17

التوصية 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 والدورة) للنموذج المرجعي للتوصيل البيني للأنظمة المفتوحة. المسألة 10/17

التوصية X.805 *معمارية أمن لأنظمة توفر الاتصالات من طرف إلى طرف*

تعرف هذه التوصية العناصر المعمارية العامة المتعلقة بالأمن التي عند تطبيقها على نحو ملائم، ولا سيما في بيئة بائع متعدد، يمكن ضمان حماية الشبكة بشكل ملائم من الهجمات الخبيثة وغير المتعمدة وتعمل على توفير معلمات الأداء مثل التوافر العالي ووقت الاستجابة الملائم وسلامة البيانات وقابلية للتدريج ووظيفة الفوترة الدقيقة. المسألة 10/17

التوصية X.810 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - أطر الأمن للأنظمة المفتوحة: نظرة شاملة*

تعرف هذه التوصية الإطار الذي تحدد فيه خدمات أمن الأنظمة المفتوحة. ويصف هذا الجزء من أطر الأمن تنظيم إطار الأمن ويعرف مفاهيم الأمن المطلوبة في أكثر من جزء واحد لإطار الأمن وتصف علاقة الخدمات والآليات المعرفة في الأجزاء الأخرى للإطار. ويصف هذا الإطار جميع جوانب الاستيقان نظراً لأ ا تطبق على الأنظمة المفتوحة وعلاقة الاستيقان مع وظائف الأمن الأخرى مثل مراقبة النفاذ ومتطلبات إدارة الاستيقان. المسألة 10/17

التوصية X.811 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - أطر الأمن للأنظمة المفتوحة: إطار الاستيقان*

تعرف هذه التوصية إطاراً عاماً لتوفير الاستيقان. والهدف الأولي للاستيقان هو مواجهة ديدات التنكر والإجابة. المسألة 10/17

التوصية X.812 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - أطر الأمن للأنظمة المفتوحة: إطار مراقبة النفاذ*

تعرف هذه التوصية إطاراً عاماً لتوفير مراقبة النفاذ. والهدف الأولي لمراقبة النفاذ هو مواجهة التهديدات من عمليات غير مخولة تتضمن حاسوباً أو نظام اتصالات؛ وغالباً تنقسم هذه التهديدات إلى أنواع تعرف بالاستخدام غير المخول والكشف والتعديل والتدمير ورفض الخدمة. المسألة 10/17

التوصية X.813 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - أطر الأمن للأنظمة المفتوحة: إطار عدم التنصل*

تعرف هذه التوصية إطاراً عاماً لخدمات عدم التنصل. وهدف خدمة عدم التنصل هو الجمع والاحتفاظ والإتاحة والتحقق من دليل لا يقبل الجدل فيما يتعلق بتحديد مرسلين ومستقبلين متضمنين في نقل المعطيات. المسألة 10/17

التوصية X.814 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - أطر الأمن للأنظمة المفتوحة: إطار السرية*

تعرف هذه التوصية إطاراً عاماً لتوفير خدمات السرية. والسرية هي خاصية أن المعلومات لا تتاح أو يكشف عنها لأفراد أو كيانات أو عمليات غير مخولة. المسألة 10/17

التوصية X.815 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - أطر الأمن للأنظمة المفتوحة: إطار سلامة البيانات*

تعرف هذه التوصية إطاراً عاماً لتوفير خدمات سلامة البيانات . وتسمى خاصية عدم تعرض البيانات للتعديل أو التدمر بطريقة غير مخولة بخاصية السلامة . المسألة 10/17

التوصية X.816 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - أطر الأمن للأنظمة المفتوحة: إطار التسجيل الدقيق للأمن*

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 التسجيل الدقيق للأمن. المسألة 10/17

التوصية X.830 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - أمن الطبقات العليا التنوعية: نظرة شاملة ونماذج وترميز*

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 ما يلي: أ) نماذج عامة لوظائف بروتوكول تبادل الأمن وتحويلات الأمن؛ ب) مجموعة من الأدوات الترميزية لدعم مواصفة متطلبات الحماية الانتقائية للمجالات في مواصفة قواعد التركيب ا ,رد ولدعم مواصفة بدالات وتحويلات الأمن؛ ج) مجموعة من الإرشادات الغنية بالمعلومات فيما يتعلق بتطبيق تسهيلات أمن الطبقة العليا التنوعية التي تغطيها هذه السلسلة من التوصيات. المسألة 10/17

التوصية X.831 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - أمن الطبقات العليا التنوعية: تعريف خدمة عنصر خدمة تبادل الأمن (SESE)*

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 الخدمة التي يوفرها عنصر خدمة تبادل الأمن. وهذا العنصر هو عنصر- خدمة- تطبيق (ASE) ييسر اتصال معلومات الأمن لدعم توفير خدمات الأمن في طبقة التطبيق للتوصيل البيني للأنظمة المفتوحة. المسألة 10/17

التوصية X.832 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - أمن الطبقات العليا التنوعية: 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 يوفر عنصر خدمة تبادل الأمن. وهذا العنصر هو عنصر- خدمة- تطبيق ييسر اتصال معلومات الأمن لدعم توفير خدمات الأمن في طبقة التطبيق للتوصيل البيني للأنظمة المفتوحة. المسألة 10/17

التوصية X.833 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - أمن الطبقات العليا التنوعية: مواصفة حماية قواعد تركيب النقل*

تنتمي هذه التوصية إلى سلسلة من التوصيات التي تقدم مجموعة من التسهيلات للمساعدة على بناء بروتوكولات الطبقة العليا التي تدعم توفير خدمات الأمن. تعرف هذه التوصية | هذا المعيار الدولي لقواعد تركيب النقل المحمية المتصاحبة مع دعم طبقة تقديم خدمات الأمن في طبقة التطبيق. المسألة 10/17

التوصية X.834 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - أمن الطبقات العليا التنوعية: شكل الإعلان عن تطابق تنفيذ بروتوكول عنصر خدمة تبادل الأمن*

تنتمي هذه التوصية إلى سلسلة توصيات بشأن أمن الطبقات العليا التنوعية، وهي شكل الإعلان عن تطابق تنفيذ بروتوكول عنصر خدمة تبادل الأمن المحدد في التوصية X.832 لقطاع تقييس الاتصالات وتبادل الأمن الوارد في التوصية X.830 لقطاع تقييس الاتصالات.

الملحق جيم - توفر هذه التوصية وصفاً لمقدرات مقيسة وخيارات على شكل يدعم تقييم تطابق تنفيذ معين. المسألة 10/17

التوصية X.835 *تكنولوجيا المعلومات - التوصيل البيني للأنظمة المفتوحة - أمن الطبقات العليا التنوعية: شكل الإعلان عن تطابق تنفيذ بروتوكول حماية قواعد تركيب النقل*

تنتمي هذه التوصية إلى سلسلة توصيات بشأن أمن الطبقات العليا التنوعية، وهي شكل الإعلان عن تطابق تنفيذ بروتوكول حماية قواعد تركيب لنقل المحدد في التوصية X.833 لقطاع تقييس الاتصالات. توفر هذه التوصية وصفاً لمقدرات مقيسة وخيارات على شكل يدعم تقييم تطابق تنفيذ معين. المسألة 10/17

التوصية X.841 *تكنولوجيا المعلومات - تقنيات الأمن - أغراض معلومات أمن لمراقبة النفاذ*

توفر هذه التوصية أغراض معلومات أمن لمراقبة نفاذ تعاريف مطلوبة مشتركة في معايير الأمن لتجنب تعاريف متعددة ومختلفة لنفس العنصر الوظيفي. وتتحقق الدقة في هذه التعاريف باستخدام ترميز تركيب مجرد رقم 1. وتشمل هذه التوصية الجوانب السكونية فقط لأغراض معلومات الأمن. المسألة 10/17

التوصية 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 ا وكيانات تستخدم خدما ا. وتعرف هذه التوصية الفئات الرئيسية المختلفة لخدمات الطرف الثالث الموثوق به بما في ذلك دلالة الوقت وعدم التنصل وإدارة المفتاح وإدارة الشهادة والموثق الإلكتروني. المسألة 10/17

التوصية X.843 *تكنولوجيا المعلومات - تقنيات الأمن - مواصفة خدمات الطرف الثالث الموثوق به لدعم تطبيق التوقيعات الرقمية*

تعرف هذه التوصية الخدمات المطلوبة لدعم تطبيق التوقيعات الرقمية لعدم التنصل عند وضع الوثيقة. ونظراً لأن هذا يتضمن سلامة الوثيقة والاستيقان من واضعها، ويمكن جمع الخدمات الموصوفة لتنفيذ خدمات سلامة البيانات والاستيقان. المسألة 10/17

التوصية X.901 *تكنولوجيا المعلومات - معالجة موزعة مفتوحة - نموذج مرجعي: نظرة شاملة*

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 يمكن في داخلها تكامل دعم التوزيع والتشغيل البيني وقابلية الحمل. وتحتوي هذه التوصية على نظرة شاملة عن المعالجة الموزعة المفتوحة موضحة أسبا ا وتبريرها وشرحاً لمفاهيمها الرئيسية وموجزاً لمعيارية المعالجة الموزعة المفتوحة. وتحتوي على مواد تفسيرية عن كيفية تفسير النموذج المرجعي هذا واستخدامه من قبل المستعملين الذين قد يشملون كتاباً عن المعايير ومهندسين لأنظمة المعالجة الموزعة المفتوحة. كما أن التوصية تحتوي أيضاً على تصنيف مجالات التقييس المطلوبة التي تتعلق بالنقاط المرجعية حول المطابقة المعرفة في التوصية X.903. ويتعين تأمين أنظمة المعالجة الموزعة المفتوحة، أي ينبغي بناؤها وصيانتها بطريقة تضمن حماية تسهيلات وبيانات النظام من نفاذ غير مخول والاستخدام غير القانوني وأي ديدات أو هجوم. وتصبح متطلبات الأمن أكثر صعوبة لتلبية التفاعلات عن بعد وقابلية أجزاء النظام ومستعملي النظام للحركة. وقد تعرف قواعد أمن المعالجة الموزعة المفتوحة: قواعد اكتشاف التهديدات على الأمن؛ وقواعد الحماية من التهديدات على الأمن؛ وقواعد الحد من أي ضرر تتسبب فيه أي انتهاكات للأمن. المسألة 26/17

التوصية X.902 *تكنولوجيا المعلومات - معالجة موزعة مفتوحة - نموذج مرجعي: الأسس*

تحتوي هذه التوصية على تعريف المفاهيم والإطار التحليلي لوصف مقيس لأنظمة المعالجة الموزعة (الاعتباطية). وتقدم مبادئ التطابق مع معايير المعالجة الموزعة المفتوحة والطريقة التي تطبق ا. وهذا فقط على مستوى كاف من التفاصيل لدعم التوصية X.903 ولوضع المتطلبات لتقنيات المواصفة الجديدة. المسألة 26/17

التوصية X.903 *تكنولوجيا المعلومات - معالجة موزعة مفتوحة - نموذج مرجعي: المعمارية*

تحتوي هذه التوصية على مواصفة الخصائص المطلوبة التي تؤهل المعالجة الموزعة على أ ا مفتوحة. وهذه هي التقييدات التي ينبغي أن تتطابق معها معايير المعالجة الموزعة المفتوحة. وتستخدم تقنيات الوصفية من التوصية X.902. المسألة 26/17

التوصية X.904 *تكنولوجيا المعلومات – معالجة موزعة مفتوحة – نموذج مرجعي: علم الدلالات المعمارية*

تحتوي هذه التوصية على مقياس مفاهيم وضع النماذج للمعالجة الموزعة المفتوحة المعرفة في التوصية X.902، المادتان 8 و9. ويتحقق المقياس من خلال تفسير كل مفهوم على أساس تركيبات التقنيات المختلفة للوصف الشكلي المقيس. المسألة 26/17

باء-2 جوانب الأمن التي لم يشملها هذا الكتيب (الاعتمادية والحماية المادية للمنشآت الخارجية)

إن حماية المنشآت الخارجية من التآكل والآثار البيئية والحرائق والأنشطة البشرية ومن الأشكال الأخرى لتدمير جميع أنواع كبلات الاتصالات العامة والهياكل المتصاحبة هي أحد العناصر التي تبرز مستوى أمن نقل المعلومات من وجهة نظر إتاحة الشبكة والاعتماد عليها. إن معدات وكبلات الإنشاء والتركيب والرصد ضرورية لضمان أداء جيد للوصلة. وكلما كانت نوعية المعلومات المنقولة عالية، كلما كانت أهمية الحماية المادية للمنشأة عالية. وتشمل سلسلة التوصيات L تقنيات تمكّن من زيادة مستوى أمن المنشأة وبالتالي ترحيل المعلومات من جانب إلى آخر.

L.3 *تدريع الكبلات*

مع الكبلات الموضوعة مباشرة في التربة، يساهم التدريع في المنشآت الآمنة واعتمادية التشغيل من خلال ضمان حماية الكبلات من الضرر الميكانيكي الذي تتسبب فيه الأحجار والمعدات أو أدوات الحفر والقوارض والحشرات والتآكل الكيميائي أو الإلكتروليتي وآثار الانبعاثات الجوية وظواهر الدلالات التي ترجع إلى قرب الخطوط الكهربائية. المسألة 8/6

L.4 *أغلفة الكبلات الألومينية*

إن الاستخدام العام للألومنيوم لتغليف الكبلات مستصوب عندما لا تزداد تكاليف الكبلات بالمقارنة باستخدام الرصاص وعندما تلبي أيضاً الأغلفة الألومينية المتطلبات التقنية إلى مدى كبير. إن استخدام كبلات ذات أغلفة من الألومنيوم مهم بصورة خاصة في حالة كبلات الخط الرئيسي. المسألة 8/6

L.5 *أغلفة الكبلات المصنوعة من مواد غير الرصاص أو الألومنيوم*

يمكن استخدام أنواع أخرى من التدريع مثل الألومنيوم المموج وشرائط النحاس وما إلى ذلك يتوقف على تطبيقات معينة. المسألة 8/6

L.7 *تطبيق حماية مهبطية مشتركة*

تعني حماية مهبطية مشتركة لعديد من الهياكل المعدنية تحت الأرض الحماية من تآكل هذه الهياكل بواسطة أجهزة حماية مشتركة. ويتألف نظام الحماية المشتركة من العديد من هياكل معدنية تحت الأرض لروابط كهربائية بين الهياكل وأجهزة حماية مشتركة تمثل لحماية مهبطية ومعدات تصريف كهربائية. وتعزز تقنيات الحماية المشتركة الاعتماد على الهياكل المدفونة وتحسن كفاءة أجهزة الحماية المهبطية وتخفض أيضاً مجموع تكاليف الاستثمار والصيانة لنظام الحماية. المسألة 7/6

L.16 *مواد إيصالية بلاستيكية كأغطية لحماية الأغطية المعدنية للكبلات*

إن أهم فوائد المواد الإيصالية البلاستيكية للكبلات هي الحماية من التآكل والصواعق وآثار الخطوط الكهربائية والسكك الحديدية وخفض تكاليف الصيانة ولا سيما من أجل التأريض وتبسيط مشروعات الحماية. المسألة 8/6

L.20 *وضع شفرة أمن للحرائق في مرافق الاتصالات*

بالنسبة للمباني الحالية وتصميم المباني الجديدة وبنائها، ينبغي للإدارات التي توجد فيها منشآت اتصالات وضع شفرة داخلية للأمن من الحرائق طبقاً للاستخدام المتوقع المحدد لكل مبنى ويحتوي على خطوط توجيهية دنيا للسلامة من الحرائق والحماية منها. المسألة 2/6

L.21 *أنظمة اكتشاف الحرائق والإنذارات وأجهزة الاكتشاف وأجهزة السبر*

من أجل حماية الممتلكات والحياة، عندما تنطبق، يمكن تركيب أنظمة اكتشاف الحرائق والإنذارات للبدء في عدد من الأنشطة المختلفة مثل اكتشاف وتحديد أماكن الحرائق وتوفير المساعدة على احتوائها و/أو إطفاء الحرائق وإجراءات الإخلاء في حالات الطوارئ واستدعاء قوات مكافحة الحرائق. المسألة 2/6

L.22 *الوقاية من الحرائق*

مع الأخذ في الاعتبار الضرر الخطير الذي يمكن أن يحدث عندما تندلع حرائق وأهمية الوقاية من الحرائق على الأمن وتوفير الخدمة واقتصاد أنظمة الاتصالات، توجد جوانب عديدة ينبغي النظر فيها مثل خفض معامل حمل الحريق وتقسيم المباني إلى أقسام (قطاعات حرائق) لخفض وتأخير انتشار الحريق وإحصائيات الحرائق. المسألة 2/6

L.23 *إطفاء الحرائق - تصنيف وأماكن منشآت ومعدات إطفاء الحرائق*

إن وسائل مكافحة الحرائق التي يتعين اعتمادها في مباني الاتصالات قد تتفاوت طبقاً للاستخدام ومكان المقر وما إذا كانت مشغولة. وتوجد عوامل تحدد كمية خدمة المساعدة في مكافحة الحرائق المخصصة مبدئياً في حالة نشوب حريق. المسألة 2/6

L.25 *صيانة شبكة كبلية من ألياف بصرية*

إن أنظمة الصيانة وإجراءا ا قادرة على رصد نوعية شبكة ألياف بصرية مستقلة عن معدات الإرسال. المسألة 5/6

L.28 *حماية إضافية خارجية لكبلات أرضية بحرية*

بالنسبة لكبلات المياه الضحلة، يكون احتمال حدوث عطب أعلى من تطبيق المياه العميقة ويرجع ذلك للظواهر البيئية (مثل حركة أمواج البحر وزلازل المياه الجوفية والا يارات الأرضية) والأنشطة البشرية التي تؤثر على قاع البحر (مثل الصيد ووضع الكبلات والخدمات الأخرى وصيانتها).

وبالإضافة إلى التدريع المختلف الذي يعتمد عادة لوضع الكبلات – مثلاً التدريع الصخري (RA) وتدريع أسلاك الصلب مثل تدريع أوحد (SA) أو تدريع مزدوج (DA)، ينبغي اعتماد حماية إضافية خارجية إذا احتاج الأمر. ويمكن استخدام هذه الحماية في كل من الساحل القريب من المياه الضحلة وعلى الشاطئ في الجزء الواقع بين حافة المياه والشاطئ المشترك أو على طول طريق الكبل حيث يمكن لعوامل خارجية أو سمات قاع البحر أن تحدث أضراراً بالكبلات. المسألة 10/6

L.32 *أجهزة الوقاية من اختراقات كبلات خلالية لفواصل قطاع الحرائق*

بالنظر إلى العدد الكبير لاختراقات الكبلات الخلالية في حدود قطاع الحرائق في مبنى للاتصالات، الذي يقلل من فعالية نظام إطفاء الحرائق، تتألف الاستراتيجية الملائمة من إعتماد تدابير للتحكم السلبي في الدخان والنار مثل سد أماكن اختراق الكبل الخلالي بواسطة مواد توقف انتشار النار أو استخدام أنظمة (لحماية) إدارة الكبلات. المسألة 2/6

L.45 *تقليل الأثر إلى أدنى حد على البيئة من منشآت خارجية في شبكات الاتصالات*

يجري تفصيل المنهجية المعتمدة لتقليل الأثر إلى أدنى حد (مثل الطاقة وثاني أكسيد الكربون) التي تتسبب فيه منشأة خارجية في البيئة. ويقوم هذا على أساس تحليل دورة الحياة، أي *من المهد إلى اللحد* لملكية المنتجات. المسألة 1/6

L.46 *حماية كبلات ومنشآت الاتصالات من هجوم بيولوجي*

تصف عمليات الهجوم البيولوجي والتدابير المناهضة لها لحماية كبلات الاتصالات. وتتناول جميع أنواع الهجوم البيولوجي وضعف الكبلات وخصائص الضرر وتنظر في طرق بديلة لحماية المنشأة بما في ذلك الاعتماد على وضع الكبلات. المسألة 1/6

تتناول التوصيات التالية إتاحة شبكات تراتب رقمي متزامن وشبكات نقل بصري:

G.841 *أنماط وخصائص معماريات الحماية لشبكات التراتب الرقمي المتزامن*

تصف هذه التوصية آليات الحماية المختلفة لشبكات التراتب الرقمي المتزامن وأهدافها وتطبيقا ا.

وتصنف مخططات الحماية باعتبارها حماية تسجيل التراتب الرقمي المتزامن (في طبقة قسم أو مسير) كحماية لتوصيل شبكة فرعية لتراتب رقمي متزامن (مع رصد داخلي ورصد غير مقحم ورصد طبقة فرعية). المسائل Q.15 و16 و17 و18/15

G.842 *التشغيل البيني لمعماريات حماية شبكة التراتب الرقمي المتزامن*

تصف هذه التوصية آليات التشغيل البيني لمعماريات حماية الشبكة. ويجري وصف التشغيل البيني للتوصيل البيني لعقدة واحدة ومزدوجة لحركة تبديل بين الحلقات. ويمكن تشكيل كل حلقة لحماية خدمة صيانة متقاسمة أو حماية توصيل الشبكة الفرعية. المسائل Q.15 و16 و17 و18/15

G.808.1 *تبديل الحماية التنوعية - تسجيل خطي وحماية الشبكة الفرعية*

توفر هذه التوصية نظرة شاملة على تبديل الحماية الخطية. وتشمل شبكات النقل البصرية وشبكات التراتب الرقمي المتزامن وشبكات أسلوب النقل اللاتزامني القائمة على مخططات الحماية. وسيجري توفير نظرة شاملة على حماية الحلقة ومخططات التوصيل البيني للشبكة الفرعية (مثلاً الحلقة) لعقدة مزدوجة في توصيات أخرى. المسائل Q.15 و16 و17 و18/15

G.873.1 *شبكة النقل البصري - الحماية الخطية*

تعرف هذه التوصية بروتوكول تبديل الحماية الأتوماتية وعملية تبديل الحماية لمخططات الحماية الخطية لشبكة النقل البصري عند مستوى وحدة بيانات القناة البصرية. ومخططات الحماية التي ينظر فيها في هذه التوصية هي حماية تسجيل وحدة بيانات القناة البصرية؛ حماية توصيل الشبكة الفرعية لوحدة بيانات القناة البصرية مع الرصد الداخلي؛ حماية توصيل الشبكة الفرعية لوحدة بيانات القناة البصرية مع رصد غير مقحم؛ حماية توصيل الشبكة الفرعية لوحدة بيانات القناة البصرية مع رصد الطبقة الفرعية. المسائل Q.15 و16 و17 و18/15

G.781 *وظائف طبقة التزامن*

اعتمادية مصدر توقيت التراتب الرقمي المتزامن والتراتب الرقمي متقارب التزامن. تحدد هذه التوصية مكتبة من توزيع تزامن أساسي لبناء الفدرات، يشار إليها "بالوظائف الذرية" ومجموعة من القواعد التي بمقتضاها تجمع معاً لوصف العنصر الوظيفي لتزامن معدات الإرسال الرقمية. المسائل Q.15 و16 و17 و18/15

G.911 *معلمات الاعتمادية والتيسر وطرق حسا ا في أنظمة الألياف البصرية*

الاعتمادية وتوافر أنظمة الألياف البصرية: تعرف هذه التوصية الحد الأدنى موعة معلمات ضرورية لتمييز الاعتمادية وتوافر أنظمة الألياف البصرية. وترد معلمات مختلفة للاعتمادية وصيانة النظام من أجل اعتمادية جهاز بصري نشط ومن أجل اعتمادية جهاز بصري سلبي ومن أجل اعتمادية الألياف البصرية والكبلات. وتوفر هذه التوصية أيضاً خطوطاً توجيهية وطرقاً لحساب الاعتمادية المتوقعة للأجهزة والوحدات والأنظمة. وتشمل أمثلة. المسائل Q.15 و16 و17 و18/15

G.784 *إدارة التراتب الرقمي المتزامن*

إدارة التراتب الرقمي المتزامن. تتناول التوصية G.784 العطب والتشكيل والحسابات والأداء ووظائف إدارة الأمن لعناصر شبكة إدارة التراتب الرقمي المتزامن. أما جوانب إدارة الأمن في هذه التوصيات "فيجري دراستها" حالياً. المسألة Q.14/15

G.874 *جوانب إدارة عنصر شبكة النقل البصري*

إدارة شبكات نقل بصري. تتناول التوصية G.874 العطب والتشكيل والحسابات والأداء ووظائف إدارة الأمن لعناصر شبكة إدارة شبكة النقل البصري. أما جوانب إدارة الأمن في هذه التوصيات "فيجري دراستها" حالياً. المسألة Q.14/15

G.7712/Y.1703 *معمارية ومواصفة شبكة بيانات الاتصالات*

تشمل هذه التوصية جوانب أمن شبكات إدارة الاتصالات وشبكات تشوير الاتصالات. وتدعم وظائف بيانات الاتصالات الواردة في هذه التوصية خدمات الشبكة الأقل توصيلاً. وقد تضاف وظائف إضافية في صيغ هذه التوصية في المستقبل لدعم خدمات شبكات موجهة نحو التوصيل. المسألة Q.14/15

ملاحظة: قد تحتوي التوصيات في السلسلة G.650, 660-690, 950-970 على بعض العناصر المتعلقة بالاعتمادية.

الملحق جيم: قائمة لجان الدراسات والمسائل المتعلقة بالأمن

تقوم لجان الدراسات التقنية بعمل التقييس في قطاع تقييس الاتصالات ويقوم فيها مثلو أعضاء قطاع تقييس الاتصالات بوضع توصيات (معايير) لمختلف مجالات الاتصالات الدولية. وتقوم لجان الدراسات بعملها في شكل مسائل للدراسة. وتتناول هذه المسائل دراسات تقنية في مجال معين من تقييس الاتصالات. ويوجد لكل لجنة دراسات رئيس وعدد من نواب الرئيس تقوم بتعيينهم الجمعية العالمية لتقييس الاتصالات. وفيما يلي قائمة بلجان الدراسات التابعة لقطاع تقييس الاتصالات في الفترة الدراسية 2001-2004 وعناوينها واختصاصا ا وقائمة بمسائل الدراسة التي تتناول عمل الأمن.

لجنة الدراسات 2	الجوانب التشغيلية لتوفير الخدمات والشبكات والأداء *لجنة الدراسات الرئيسية المعنية بدراسة تعريف الخدمة والترقيم والتسيير والتنقلية العالمية*
الاختصاصات: مسؤولة عن الدراسات المتعلقة بمبادئ تقديم الخدمات والمتطلبات التشغيلية لمحاكاة الخدمات؛ متطلبات الترقيم والتسمية والعنونة وتحديد المصادر بما في ذلك معايير وإجراءات الحجز والتخصيص؛ متطلبات التسيير والتشغيل البيني؛ العوامل البشرية؛ الجوانب التشغيلية للشبكات ومتطلبات الأداء المرتبطة ا، بما في ذلك إدارة حركة الشبكات، ونوعية الخدمة (هندسة الحركة، وأداء التشغيل وقياسات الخدمات)؛ الجوانب التشغيلية للتشغيل البيني فيما بين شبكات الاتصالات التقليدية والشبكات الجديدة؛ تقييم المعلومات المرتدة من جهات التشغيل، وشركات التصنيع والمستعملين بشأن الجوانب المختلفة لتشغيل الشبكات. المسائل الرئيسية المتعلقة بالأمن: - Q.5/2 - نوعية خدمة الشبكات	

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

لجنة الدراسات 4	إدارة الاتصالات، بما في ذلك شبكة إدارة الاتصالات *لجنة الدراسات الرئيسية المعنية بدراسة شبكة إدارة اتصالات*
باعتبارها لجنة الدراسات الرئيسية المعنية بدراسة أنشطة الإدارة، يتناول عمل لجنة الدراسات 4 ا الات التالية: أ) الاعتبارات المعمارية ومتطلبات الأسطح 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.	

تعرف إدارة شبكة الاتصالات على مستويات مختلفة من التجريد، من معلومات مستوى عنصر شبكة الإدارة إلى خدمات الإدارة التي تقدم إلى الزبون. وتعتمد متطلبات الأمن للمعلومات المتبادلة بين أنظمة الإدارة وبين عناصر الشبكة على ما إذا كانت شبكات الإدارة في إدارة واحدة أو موزعة بين إدارتين. وعلى أساس المبادئ المعمارية، تم تعريف متطلبات واضحة وآليات وبروتوكول دعم في التوصيات الحالية ويجري تطوير توصيات إضافية أخرى.

المسائل الرئيسية المتعلقة بالأمن:

- Q.16/4 - إدارة شبكة الاتصالات لدعم الاتصالات المتنقلة الدولية – 2000 والشبكات الذكية

لجنة الدراسات 5	الحماية من الآثار البيئية الكهرمغنطيسية

تكون لجنة الدراسات 5 مسؤولة عن الدراسات المتصلة بحماية الشبكات والتجهيزات من التداخل والصواعق وكذلك أيضاً عن الدراسات المتصلة بالملاءمة الكهرمغنطيسية. وخلال الإيفاء بمهمتها، تناولت لجنة الدراسات 5 مسائل عديدة ووضعت عدداً من التوصيات والكتيبات التي تساهم في أمن الشبكة من التهديدات الكهرمغنطيسية. وتشمل هذه التهديدات ظواهر عابرة عالية القدرة خبيثة من صنع الإنسان مثل النبضة الكهرمغنطيسية عالية الارتفاع والموجات الصغرية عالية القدرة. وقد يتضمن الأمن الكهرمغنطيسي أيضاً تسرب معلومات من شبكات اتصالات من خلال إرسالات راديوية غير متوقعة من المعدات.

ويتشابه طابع التهديدات الخبيثة وتقنيات التخفيف المتطابقة التي تطبق على الاضطرابات الكهرمغنطيسية الطبيعية أو غير المتعمدة. ومن ثم، تساهم الأنشطة التقليدية للجنة الدراسات 5 المتعلقة بالحماية من الصواعق والتحكم في التداخل الكهرمغنطيسي في أمن الشبكة من التهديدات الخبيثة من صنع الإنسان. وتوجد حالياً ست مسائل موزعة على لجنة الدراسات 5 تتعلق بالأمن الكهرمغنطيسي لشبكة الاتصالات.

وبينما يوجد تشابه كبير بين التهديدات الكهرمغنطيسية الخبيثة التي هي من صنع الإنسان والبيئة الكهرمغنطيسية غير المتعمدة أو الطبيعية، هناك بالتأكيد بعض الاختلافات المهمة. وخلال الإيفاء بمهمتها، تناولت لجنة الدراسات 5 مسائل عديدة ووضعت عددا من التوصيات والكتيبات التي تساهم في أمن الشبكة من التهديدات الكهرمغنطيسية.

وا الان الرئيسيان للأمن الكهرمغنطيسي هما:

- مقاومة وحصانة شبكات ومعدات الاتصالات من ظواهر عابرة عالية القدرة خبيثة من صنع الإنسان. وتشمل هذه التهديدات:
  - مجالات كهرمغنطيسية تنتجها التفجيرات النووية على ارتفاعات عالية - النبضات الكهرمغنطيسية عالية الارتفاع.
  - مولدات كهرمغنطيسية عالية القدرة تشمل الموجات الصغرية عالية القدرة ومصادر النطاق العريض جداً.
- إمكانية تسرب معلومات من شبكات الاتصالات من خلال إرسالات راديوية غير متوقعة من المعدات.

لقد زاد الوعي مؤخراً بتهديدات الأمن المترتبة على هذه الظواهر نتيجة لظهور مقالات وتحقيقات إخبارية وبرامج تلفزيونية تتعلق ذه القضايا في وسائل الإعلام.

هناك تشابه بين التهديدات الكهرمغنطيسية الخبيثة التي هي من صنع الإنسان والاضطرابات الكهرمغنطيسية غير المتعمدة أو الطبيعية. فمثلاً، هناك تشابه بين نبضة كهرمغنطيسية عالية الارتفاع والنبضة الكهرمغنطيسية التي تولدها صاعقة. وتقلل إلى أدنى حد تقنيات الحجب والترشيح التي تخفض إرسالات الطاقة الراديوية غير المطلوبة من المعدات إمكانية تسرب الطاقة غير المتعمد. ومن ثم، تساهم الأنشطة التقليدية للجنة الدراسات 5 المتعلقة بالحماية من الصواعق والتحكم في التداخل الكهرمغنطيسي في أمن الشبكة من التهديدات الخبيثة التي هي من صنع الإنسان. ويوضح الجدول التالي المسائل المدرجة على جدول أعمال لجنة الدراسات 5 للفترة الدراسية 2001-2004 فيما يتعلق بالتأثير على أمن الشبكة.

المسائل الرئيسية المتعلقة بالأمن:

- Q.2/5 – الملاءمة الكهرمغنطيسية المتعلقة بأنظمة النفاذ عريض النطاق (*التحكم في الإرسالات غير المطلوبة من أنظمة نفاذ عريض النطاق تساهم في تقليل إمكانية تسرب المعلومات*).
- Q.4/5 – مقاومة أنواع جديدة من معدات الاتصالات وشبكات النفاذ (*تحسن مقاومة المعدات للصواعق وتحسين مقاومة المعدات للتمورات التي تحدثها النبضة الكهرمغنطيسية عالية الارتفاع*).
- Q.5/5 – الحماية من الصواعق للأنظمة الثابتة والمتنقلة واللاسلكية (*توفر أيضاً التقنيات المستخدمة للحماية من الصواعق درجة مقاومة المرفق للنبضة الكهرمغنطيسية عالية الارتفاع والموجات الصغرية عالية القدرة*).
- Q.6/5 – ربط التشكيلات وتأريض أنظمة الاتصالات في البيئة العالمية (*تدابير ربط وتأريض ملائمة تساعد في مقاومة المرفق للنبضات الكهرمغنطيسية عالية الارتفاع والموجات الصغرية عالية القدرة*).
- Q.12/5 – صيانة وتعزيز توصيات الملاءمة الكهرمغنطيسية الحالية (*تحسن الملاءمة الكهرمغنطيسية لمعدات الاتصالات وتحسين حصانة المعدات من بيئة النبضات الكهرمغنطيسية عالية الارتفاع المسيرة والمشعة وكذلك بيئة الموجات الصغرية عالية القدرة المشعة. وتخفض كذلك الملاءمة الكهرمغنطيسية لمعدات الاتصالات إمكانية تسرب المعلومات*).
- Q.13/5 – صيانة وتعزيز توصيات المقاومة الحالية (*مقاومة المعدات للصواعق تؤدي إلى تحسين مقاومة المعدات للتمورات التي تحدثها النبضات الكهرمغنطيسية عالية الارتفاع*).

لجنة الدراسات 6	المنشآت الخارجية

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

المسائل الرئيسية المتعلقة بالأمن:

-Q.1/6 – القضايا البيئية لمنشآت الاتصالات

-Q.2/6 – السلامة من الحرائق

-Q.5/6 – صيانة شبكات كبلات الألياف البصرية

لجنة الدراسات 9	شبكات الكبلات المتكاملة عريضة النطاق والإرسال التلفزيوني والصوتي *لجنة الدراسات الرئيسية لدراسة الكبلات المتكاملة عريضة النطاق والشبكات التلفزيونية*

لجنة الدراسات المعنية بـ"شبكات الكبلات المتكاملة عريضة النطاق والإرسال التلفزيوني والصوتي" (لجنة الدراسات 9) هي لجنة الدراسات الرئيسية لدراسة شبكات الكبلات المتكاملة عريضة النطاق والإرسال التلفزيوني. وتعد هذه اللجنة توصيات بشأن المسائل التالية، وتحتفظ بها:

- استعمال الشبكات الكبلية والشبكات الهجينة المصممة أساساً لتوصيل البرامج التلفزيونية والصوتية إلى المنازل حيث إن الشبكات المتكاملة عريضة النطاق تحمل أيضاً الخدمات الصوتية أو الخدمات الأخرى التي يتسم فيها الوقت بأهمية حرجة وخدمات الفيديو عند الطلب والخدمات التفاعلية، وما إلى ذلك.
- استخدام أنظمة الاتصالات للمساهمة والتوزيع الأولي والتوزيع الثانوي للتلفزيون والبرامج الصوتية وخدمات البيانات المشابهة.

وبناء على هذا الدور، تتولى لجنة الدراسات 9 تقييم التهديدات وجوانب الضعف في الشبكات عريضة النطاق والخدمات وأهداف أمن الوثائق والتدابير المضادة وتعرف معماريات الأمن. ومجالات الأمن الرئيسية التي تم تناولها هي تأمين الخدمات عريضة النطاق، وتأمين خدمات نقل الصوت باستعمال بروتوكول الإنترنت، وتأمين خدمات التوصيل الشبكي للشبكات المحلية، وتأمين بيئات التطبيق للخدمات التلفزيونية التفاعلية.

وركزت الأنشطة المتعلقة بالأمن على ا الات التالية:

- *تأمين الخدمات عريضة النطاق*: توفير خدمات الأمن لشبكات النفاذ عريضة النطاق، أي الاستيقان من مودم الكبل، وإدارة المفاتيح ا فرة، والخصوصية وسلامة البيانات المرسلة، وتأمين تحميل برمجيات مودم الكبل.
- *تأمين خدمات نقل الصوت باستعمال بروتوكول الإنترنت*: إن الاتصالات الكبلية باستعمال بروتوكول الإنترنت هي مشروع خاص بشأن الخدمات التفاعلية في الوقت الحرج عبر شبكة تلفزيون الكبل باستخدام بروتوكول الإنترنت، ولا سيما نقل الصوت والصورة باستعمال بروتوكول الإنترنت. وتشمل خدمات الأمن في الاتصالات الكبلية باستعمال بروتوكول الإنترنت الاستيقان من مكيف المطراف متعدد الوسائط لوكالة تقديم الخدمة، والاستيقان من وكالة تقديم الخدمة لمكيف المطراف متعدد الوسائط، وتأمين توفير الجهاز والتشكيل، وتأمين إدارة الجهاز، وتأمين التشوير، وتأمين الوسائط.
- *تأمين خدمات الشبكات المنـزلية*: يمكن لأجهزة مودم الكبل المتطورة أن توفر للمنازل خدمات توصيل شبكي مع تجهيزات الأمن، وترجمة عناوين الشبكة. وتشمل خدمات الأمن المتوافرة لأجهزة مودم الكبل المتطورة الاستيقان من المطراف متعدد الوسائط التابع لوكالة تقديم الخدمات، والاستيقان من وكالة تقديم الخدمات لمكيف المطراف متعدد الوسائط، وتأمين توفير خدمة وتشكيل وتأمين إدارة الجهاز، وعنصر وظيفي لرزمة ترشيح/وظيفة تجهيزات الأمن، وإدارة تجهيزات الأمن، وتأمين تحميل برمجيات مودم الكبل المتطورة.
- *تأمين بيئات التطبيق للخدمات التلفزيونية التفاعلية*: تعتمد الخدمات التلفزيونية التفاعلية على خدمات الأمن المعرفة في برنامج Java ومواصفة القاعدة المحلية متعددة الوسائط.

المسائل الرئيسية المتعلقة بالأمن:

-Q.6/9 – طرق وممارسات النفاذ المشروط وحماية نسخة للتوزيع الرقمي لتلفزيون الكبل في المنازل.

-Q.13/9 – تطبيقات نقل الصوت والصورة باستعمال بروتوكول الإنترنت عبر شبكات تلفزيون الكبل.

لجنة الدراسات 11	متطلبات وبروتوكولات التشوير *لجنة الدراسات الرئيسية المعنية بدراسة الشبكات الذكية*

الاختصاصات: مسؤولة عن الدراسات المتصلة بمتطلبات وبروتوكولات التشوير اللازمة للوظائف المتصلة ببروتوكول الإنترنت، وبعض الوظائف المتصلة بالتنقلية، ووظائف الوسائط المتعددة، وتحسين التوصيات الحالية بشأن النفاذ وبروتوكولات تشوير الشبكات البينية لأسلوب النقل اللاتزامني (ATM)، والشبكات الرقمية متكاملة الخدمات ضيقة النطاق (N-ISDN) والشبكات الهاتفية العمومية المبدلة (PSTN).

المسائل الرئيسية المتعلقة بالأمن:

-Q.1/11 – متطلبات التشوير من أجل دعم تشوير الخدمات الجديدة وخدمات القيمة المضافة القائمة على بروتوكول الإنترنت وعلى الشبكات الذكية.

-Q.6/11 – متطلبات التشوير من أجل دعم تشوير الخدمات البينية ومراقمة النفاذ إلى الإنترنت والخدمات الصوتية والبيانات والاتصالات متعددة الوسائط على الشبكات القائمة على بروتوكول الإنترنت.

-Q.12/11 – تشوير النفاذ والشبكة للخدمات المتطورة الضيقة والعريضة النطاق.

لجنة الدراسات 12	أداء الإرسال من طرف إلى طرف للشبكات والمطاريف *لجنة الدراسات الرئيسية المعنية بدراسة نوعية الخدمة والأداء*

الاختصاصات: مسؤولة عن التوجيهات الخاصة بأداء الإرسال من طرف إلى طرف للشبكات والمطاريف والتفاعل فيما بينها، فيما يتصل بنوعية وتقبل المستعملين لتطبيقات النصوص والكلام والصور. ويشمل هذا العمل الأمور المتصلة بتأثير إرسال جميع الشبكات (مثل الشبكات القائمة على الترتيب الرقمي متقارب التزامن، والترتيب الرقمي المتزامن، وأسلوب النقل اللاتزامني، وبروتوكول الإنترنت)، وجميع مطاريف الاتصالات (مثل الأجهزة اليدوية، والأجهزة حرة اليدين، وأجهزة الرأس، والأجهزة المتنقلة، والأجهزة السمعية المرئية، والاستجابة الصوتية التفاعلية).

المسائل الرئيسية المتعلقة بالأمن:

-Q.12/12 – اعتبارات أداء الإرسال لخدمات النطاق الصوتي التي تنفذ على شبكات تستخدم بروتوكول الإنترنت.

-Q.13/12 – متطلبات نوعية خدمة/أداء الوسائط المتعددة

لجنة الدراسات 13	الشبكات متعددة البروتوكولات والشبكات القائمة على بروتوكول الإنترنت وتشغيلها البيني *لجنة الدراسات الرئيسية المعنية بدراسة المسائل المتصلة ببروتوكول الإنترنت والشبكات الرقمية متكاملة الخدمات عريضة النطاق والبنية التحتية العالمية للمعلومات والمسائل الساتلية*

نتيجة لطابع مسؤولية لجنة الدراسات 13 والدراسات المتعلقة

- بالربط الشبكي للشبكات متغايرة الخصائص التي تشمل ميادين متعددة،
- البروتوكولات المتعددة والتكنولوجيات المبتكرة التي تهدف إلى تشغيل شبكات عالية الجودة يمكن الاعتماد عليها،
- جوانب محددة تشملها المعمارية والتشغيل البيني وتكييفها، واعتبارات الإرسال من طرف إلى طرف، والتسيير ومتطلبات النقل.

وباعتبارها لجنة الدراسات الرئيسية المعنية بدراسة مسائل تتعلق ببروتوكول الإنترنت، سوف تتأثر بأعمالها الشبكات الرقمية متكاملة الخدمات عريضة النطاق والبنية التحتية العالمية للمعلومات والمسائل الساتلية ومشروع العدد غير الجغرافي (NGN) لكثير من مسائل الأمن بالمعنى الواسع.

وتقليدياً، تناولت لجنة الدراسات 13 التابعة لقطاع تقييس الاتصالات بوضوح جوانب الأمن عند تناول مسائل المعمارية وهيكل الشبكة، لعلمها بأن من الضروري أن تشمل أعمالها مثل هذه المسائل (من وجهة نظر المعمارية والتنفيذ) لضمان شبكة قابلة للتشغيل ويعتمد عليها.

وتزداد الصعوبات مع جوانب الأمن عند تنفيذ تكنولوجيات تبديل الرزم الرقمية الجديدة – المفتوحة إلى حد ما – والبيئة المتحررة المبينة، مثل مفهوم البنية التحتية العالمية للمعلومات (GII). وهذا يصدق بصورة خاصة عندما يتضمن أطرافاً ثالثة، في مفهوم "سلسلة القيمة المضافة" طبقاً لنهج البنية التحتية العالمية للمعلومات (أو مجموعته الفرعية الخاصة بالعدد غير الجغرافي). وفي أمن هذه البيئة مع كل جوانبه تصبح المسألة أكثر أهمية وينبغي تناولها بطريقة واضحة.

ولهذا قررت لجنة الدراسات 13 أن تدرج في كل توصية جديدة أو منقحة قسماً عن الأمن كمراجع لأقسام التوصية التي تتناول جوانب الأمن. وحتى لو لم تكن هناك جوانب أمن في التوصية، ينبغي تسجيل هذه الحقيقة في القسم الخاص بالأمن. وقد سلمت لجنة الدراسات 17 هذا القرار واقترحت عرضه على جميع لجان الدراسات التابعة لقطاع تقييس الاتصالات.

وتقرر أيضاً في لجنة الدراسات 13 وجوب الإبلاغ عن التوصيات التي تتضمن مواصفات متعلقة بالأمن إلى لجنة الدراسات 17 للسماح بتحديث "كتالوج توصيات الأمن المعتمدة" في الوقت المناسب، وكذلك تحديث "مجموعة قطاع تقييس الاتصالات لتعاريف الأمن المعتمدة"

ويتناول المشروع الجديد الخاص بالعدد غير الجغرافي أيضاً جوانب الأمن في أقسام عديدة ويوليه اهتماماً خاصاً في القسم 6.6.

المسائل الرئيسية المتعلقة بالأمن:

- Q.1/13 – مبادئ ومتطلبات وأطر ومعماريات بيئة الشبكة متغايرة الخصائص
- Q.3/13 – العمليات والإدارة والصيانة وإدارة الشبكة في الشبكات القائمة على بروتوكول الإنترنت والشبكات الأخرى
- Q.4/13 – إدارة النطاق العريض والموارد المتعلقة ببروتوكول الإنترنت
- Q.6/13 – أداء الشبكات القائمة على بروتوكول الإنترنت والبنية التحتية العالمية للمعلومات التي بدأت تظهر
- Q.7/13 – نقل خلايا الشبكات الرقمية متكاملة الخدمات – عريضة النطاق/أسلوب النقل اللا تزامني وتيسر الأداء
- Q.8/13 – خطأ الإرسال وتيسر الأداء
- Q.10/13 – معمارية الشبكة الأساسية ومبادئ التشغيل البيني
- Q.11/13 – الآليات التي تسمح بتشغيل الخدمات القائمة على بروتوكول الإنترنت على الشبكات العمومية

لجنة الدراسات 15	الشبكات البصرية وشبكات النقل الأخرى *لجنة الدراسات الرئيسية المعنية بدراسة النقل على شبكة النفاذ والتكنولوجيا البصرية*

المسألة 14 في لجنة الدراسات 15 (Q.14/15) مسؤولة عن تحديد متطلبات الإدارة والمراقبة ودعم نماذج المعلومات لمعدات النقل. وقد اقتدت دراسة المسألة Q.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 Q.14/15.

- متطلبات إدارة معدات النقل: تتناول G.7710/Y.1701, G.784, G.874 وظائف إدارة المعدات داخل عنصر شبكة النقل المشتركة مع تكنولوجيات متعددة محددة لعنصر الشبكة لتراتب رقمي متزامن وعنصر شبكة النقل البصرية على التوالي. ويجري توصيف التطبيقات من حيث التاريخ والوقت، وإدارة الأعطال، وإدارة التشكيل، وإدارة الحسابات، وإدارة الأداء، وإدارة الأمن. ويترتب على ذلك تحديد مواصفات وظائف إدارة المعدات ومتطلبا ا. وتجري حالياً دراسة متطلبات إدارة الأمن في هذه التوصيات.
- معمارية شبكة بيانات الاتصالات ومتطلبا ا: تعرف G.7712/Y.1703 متطلبات المعيارية لشبكة بيانات الاتصالات التي قد تدعم اتصالات إدارة موزعة تتعلق بشبكة إدارة الاتصالات، واتصالات التشوير الموزعة التي تتعلق بشبكة نقل مبدلة أوتوماتية، والاتصالات الموزعة الأخرى (مثل اتصالات خدمة الخط، أو الاتصالات الصوتية، أو تحميل البرمجيات). وتتطلب التطبيقات المختلفة (مثل شبكة إدارة الاتصالات، وشبكة النقل المبدلة الأوتوماتية، وما إلى ذلك) شبكة اتصالات قائمة على الرزم لنقل المعلومات بين المكونات المختلفة. فمثلاً، تتطلب شبكة إدارة الاتصالات، التي يشار إليها بشبكة اتصالات الإدارة، لنقل رسائل الإدارة بين مكونات شبكة إدارة الاتصالات (مثل، مكون وظيفة عنصر شبكة، ومكون وظيفة نظام العمليات). وتتطلب شبكة النقل المبدلة الأوتوماتية شبكة الاتصالات، التي يشار إليها بشبكة تشوير الاتصالات، لنقل رسائل التشوير بين مكونات شبكة النقل المبدلة الأوتوماتية (مثل مكونات مراقبة النداء). وتتضمن التوصيتان G.7712/Y.1703 مواد مرجعية للتوصية M.3016 فيما يتعلق بمتطلبات أمن شبكة اتصالات الإدارة. وتعريف متطلبات أمن شبكة اتصالات الأمن وارد في G.7712/Y.1703.
- النداء الموزع وإدارة التوصيل: توفر G.7713/Y.1704 متطلبات النداء الموزع وإدارة التوصيل لكل من السطح البيني لشبكة المستعمل والسطح البيني لعقدة الشبكة. وتحدد المتطلبات في هذه التوصية الاتصالات عبر الأسطح البينية للقيام بعمليات نداء أوتوماتية وعمليات التوصيل. وتحدد خواص الأمن، والخواص الأخرى، السماح بالتحقق من عمليات النداء والتوصيل (وقد يشمل ذلك المعلومات التي تسمح بالاستيقان من طلب النداء وربما أيضاً سلامة التأكد من طلب النداء).
- معمارية ومتطلبات التسيير في الشبكات البصرية المبدلة أوتوماتياً: تحدد G.7715/Y.1706 متطلبات ومعمارية وظائف التسيير المستخدمة لإقامة توصيلات مبدلة وتوصيلات دائمة للبرمجيات في إطار الشبكة البصرية المبدلة أوتوماتياً. وتشمل ا ،الات الرئيسية في هذه التوصية معمارية تسيير الشبكة البصرية المبدلة أوتوماتياً وبعض المكونات الوظيفية بما في ذلك انتقاء مسير وخواص التسيير، والرسائل ا .ردة والرسوم البيانية للحالة. وتتضمن هذه التوصية بيانات مرجعية للتوصيتين M.3016 وX.800 فيما يتعلق باعتبارات الأمن. وتقرر بصورة خاصة، أنه اعتماداً على سياق استخدام بروتوكول التسيير، وأهداف الأمن الشاملة المعرفة في التوصية M.3016 الصادرة عن قطاع تقييس الاتصالات فإن السرية، وسلامة البيانات، والمساءلة، والتوافر قد تتفاوت أهميتها. وينبغي أن يتناول تحليل .ديد بروتوكول التسيير المقترح البنود التالية القائمة على التوصية X.800 لقطاع تقييس الاتصالات، وهي التنكر، والتنصت، والنفاذ غير المخول، وضياع أو إتلاف المعلومات (بما في ذلك تكرار الهجوم) والتنصل، والتزوير ورفض الخدمة.
- إطار إدارة الشبكة البصرية المبدلة أوتوماتياً: تتناول التوصية G.fame جوانب إدارة مستوي مراقبة الشبكة البصرية المبدلة أوتوماتياً والتفاعلات بين مستوي الإدارة ومستوي مراقبة الشبكة البصرية المبدلة أوتوماتياً. وسوف تشمل متطلبات إدارة الأعطال، وإدارة التشكيل، وإدارة الحسابات، وإدارة الأداء وإدارة أمن مكونات مستوى الرقابة.

المسائل الرئيسية المتعلقة بالأمن:

-Q.14/15 – إدارة الشبكة لأنظمة النقل ومعدا ا

لجنة الدراسات 16	الخدمات متعددة الوسائط والأنظمة والمطاريف *لجنة الدراسات الرئيسية المعنية بدراسة الخدمات متعددة الوسائط والأنظمة والمطاريف والأعمال الإلكترونية والتجارة الإلكترونية*

لجنة الدراسات 16 هي لجنة الدراسات الرئيسية المعنية بدراسة الخدمات متعددة الوسائط والأنظمة والمطاريف والأعمال الإلكترونية والتجارة الإلكترونية. وتشمل المسألة G (WP2/16) "أمن الأنظمة والخدمات متعددة الوسائط" وتتناول مسائل الأمن التالية.

تطبيقات الوسائط المتعددة المتطورة مثل المهاتفة عبر الشبكات القائمة على الرزم ونقل الصوت باستعمال بروتوكول الإنترنت والمؤتمرات التفاعلية والتعاون؛ والمراسلة متعددة الوسائط متقدمة الانسياب الصوتي/الفيديوي وأشكال المراسلة الأخرى التي تتعرض لتهديدات على الأمن حرجة ومتنوعة في بيئة متغايرة. وتعتبر هجمات سوء الاستخدام والتلاعب الخبيث والتنصت ورفض الخدمة من بين المخاطر المحتملة القليلة ولا سيما على الشبكات القائمة على بروتوكول الإنترنت.

ومن المسلم به أن هذه التطبيقات لها احتياجات مشتركة للأمن يمكن أن تلبي تدابير الأمن التنوعية؛ مثلاً بواسطة أمن الشبكة. ومع ذلك، تخضع تطبيقات الوسائط المتعددة المتطورة لاحتياجات تطبيقات محددة للأمن يمكن الوفاء ا عن طريق تدابير الأمن عند طبقة التطبيق. وتركز المسألة G على مسائل أمن التطبيقات في الوسائط المتعددة المتطورة مع مراعاة الأساليب التكميلية لأمن الشبكة، حسب مقتضى الحال.

المسائل الرئيسية المتعلقة بالأمن:

-Q.G/16 – أمن الأنظمة والخدمات متعددة الوسائط

لجنة الدراسات 17	شبكات البيانات وبرمجيات الاتصالات *لجنة الدراسات الرئيسية المعنية بدراسة ترحيل الرتل وأمن نظام الاتصالات ولغات وتقنيات الوصف*

الاختصاصات: هذه اللجنة مسؤولة عن الدراسات المتعلقة بشبكات توصيل البيانات والدراسات المتصلة بتطبيق النظام المفتوح للاتصالات، بما في ذلك التشغيل البيني والدليل والأمن، وعن اللغات التقنية وطريقة استخدامها والمسائل الأخرى المتعلقة بجوانب برمجيات أنظمة الاتصالات.

المسائل الرئيسية المتعلقة بالأمن:

-Q.9/17 خدمات وأنظمة الدليل

-Q.10/17 متطلبات الأمن والنماذج والمبادئ التوجيهية لأنظمة وخدمات الاتصالات (ملاحظة: وافقت لجنة الدراسات 17 على تقسيم المسألة 10/17 إلى ست مسائل منفصلة: G/17 - مشروع الأمن؛ H/17 - معمارية وإطار الأمن؛ I/17 - الأمن السيبراني؛ J/17 - إدارة الأمن؛ K/17 - القياسات الحيوية في الاتصالات؛ وL/17 - تأمين خدمات الاتصال).

لجنة الدراسات الخاصة	لجنة الدراسات الخاصة المعنية بالاتصالات المتنقلة الدولية – 2000 وما بعدها *لجنة الدراسات الرئيسية للدراسة المعنية بالاتصالات المتنقلة الدولية – 2000 وما بعدها وبشأن التنقلية*
ضمنت لجنة الدراسات الخاصة المعنية بالاتصالات المتنقلة الدولية – 2000 وما بعدها الأمن كجانب رئيسي لتوصيا ا المرجعية لأعضاء أسرة الاتصالات المتنقلة الدولية – 2000 (3G) المحددة في توصيتها Q.1741.x (3GPP) وسلسلة توصيات Q.1742.x (3GPP2). وتشمل هذه تقييم التهديدات الواردة وقائمة بمتطلبات الأمن للتصدي لهذه التهديدات وأهداف ومبادئ الأمن ومعمارية أمن معرفة (أي خصائص وآليات الأمن) ومتطلبات خوارزمية مجفرة ومتطلبات اعتراض قانوني ومعمارية ووظائف اعتراض قانوني. وقد تم تناول هذه الدراسات في المسائل 3 و6 و7 للجنة الدراسات الخاصة. والهدف الرئيسي لدراسات الاعتراض القانوني هو تحديد الاعتراض المفيد والرصد المتعلق بالمعلومات الذي يحتاج إلى أن يوفره مزودو الخدمة إلى الوكالات الوطنية لتنفيذ القانون. وقد يكون الاعتراض المتعلق بالمعلومات ومحتوى الاتصالات مستقلاً تكنولوجياً أو يعتمد على 3G أو متطوراً مع شبكات متنقلة 3G.	
المسائل الرئيسية المتعلقة بالأمن: -3/SSG – تعريف أنظمة الاتصالات المتنقلة الدولية – 2000 الحالية والمتطورة -6/SSG – تنسيق أنظمة الاتصالات المتنقلة الدولية – 2000 المتطورة -7/SSG – تقارب أنظمة الاتصالات المتنقلة الدولية – 2000 الثابتة والحالية	

قدرات بناء الأمن لقطاع تقييس الاتصالات

إطار معمارية الامن

- X.800 – معمارية الأمن
- X.802 – نموذج الأمن في الطبقات السفلى
- X.803 – نموذج الأمن في الطبقات العليا
- X.805 – معمارية الأمن لأنظمة توفر الاتصالات من طرف إلى طرف
- X.810 – إطر الأمن للأنظمة المفتوحة: نظرة شاملة
- X.811 – إطر الأمن للأنظمة المفتوحة: إطار الاستيقان
- X.812 – إطر الأمن للأنظمة المفتوحة: إطار مراقبة النفاذ
- X.813 – إطر الأمن للأنظمة المفتوحة: إطار عدم التنصل
- X.814 – إطر الأمن للأنظمة المفتوحة: إطار السرية
- X.815 – إطر الأمن للأنظمة المفتوحة: إطار سلامة البيانات
- X.816 – إطر الأمن للأنظمة المفتوحة: إطار تدقيق مقتضيات الأمن والإنذار

البروتوكولات

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

الامن في ترحيل الرتل

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

تقنيات الامن

- 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 الخواص
- X.519 – مواصفات البروتوكول

امن إدارة الشبكة

- M.3010 – مبادئ شبكة إدارة الاتصالات
- M.3016 – نظرة شاملة على امن شبكة الاتصالات
- 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 الانظمة

- 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

الفاكس

- T.30 الملحق زاي– تدابير لإرسال فاكس من الزمرة 3 آمنة 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 – مظهر جانبي لتطبيق وثيقة مبادلة وثائق الفاكس من الزمرة 4
- T.563 – الخصائص المطرافية لأجهزة الفاكس من الزمرة 4

اجهزة التلفزيون وانظمة 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 امن الاتصالات الكبلية باستخدام بروتوكول الإنترنت

انصالات متعددة الوسائط

- H.233 – نظام السرية في الخدمات السمعية المرئية
- H.234 – إدارة مفاتيح التجفير ونظام الاستيقان للخدمات السمعية المرئية
- H.235 – أمن وتجفير لمطاريف متعددة الوسائط للسلسلة H (المطاريف H.323 وغيرها من نمط H.245)
- H.323 الملحق ياء– أنظمة اتصالات متعددة الوسائط قائمة على رزم – أمن 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

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

يشمل عمل الأمن المهم الحالي في الاتحاد الدولي للاتصالات

المصطلحات وإدارة الأمن وأمن التنقلية واتصالات حالات الطوارئ

لمزيد من المعلومات عن الاتحاد الدولي للاتصالات ولجان دراساته: http://www.itu.int/ITU-T