|  |  |  |  |
| --- | --- | --- | --- |
| itu_logo | **الجمعية العالمية لتقييس الاتصالات (WTSA-16)**  **الحمامات، 25 أكتوبر - 3 نوفمبر 2016** | | CCITT/ITU-T 60th Anniversary logo |
|  |  | |  |
|  | |  | |
| الجلسة العامة | | الوثيقة 20-A | |
|  | | يونيو 2016 | |
|  | | الأصل: بالإنكليزية | |
|  | | | |
| لجنة الدراسات 17 لقطاع تقييس الاتصالات | | | |
| الأمن | | | |
| تقرير ل‍جنة الدراسات 17 لقطاع تقييس الاتصالات إلى ال‍جمعية العال‍مية لتقييس الاتصالات لعام 2016 (WTSA-16): ال‍جـزء الثاني - مسائل تُقترح دراستها في فترة الدراسة التالية (2020‑2017) | | | |
|  | | | |

|  |  |
| --- | --- |
| تضم هذه المساهمة، من لجنة الدراسات 17 إلى ال‍جمعية العال‍مية لتقييس الاتصالات لعام 2016، المسائل التي تُقترح دراستها في فترة الدراسة التالية (2020‑2017). | **ملخص**: |

ملاحظة من مكتب تقييس الاتصالات:

يرد تقرير لجنة الدراسات 17 إلى الجمعية العالمية لتقييس الاتصالات لعام 2016 (WTSA‑16) في الوثيقتين التاليتين:

الجـزء الأول: **الوثيقة 19** - اعتبارات عامة، بما في ذلك التغييرات المقترحة للقرار 2 لل‍جمعية العالمية لتقييس الاتصالات الوارد في الملحق 2

الجـزء الثاني: **الوثيقة 20** - مسائل تُقترح دراستها في فترة الدراسة 2020‑2017

# 1 قائمة بالمسائل التي تقترحها لجنة الدراسات 17

|  |  |  |
| --- | --- | --- |
| رقم المسألة | عنوان المسألة | الحالة |
| A/17 | تنسيق أمن أنظمة الاتصالات/تكنولوجيا المعلومات والاتصالات | استمرار المسألة 1/17 |
| B/17 | معمارية الأمن وإطاره | استمرار المسألة 2/17 |
| C/17 | إدارة أمن معلومات الاتصالات | استمرار المسألة 3/17 |
| D/17 | الأمن السيبراني | استمرار المسألة 4/17 |
| E/17 | مكافحة الرسائل الاقتحامية بالوسائل التقنية | استمرار المسألة 5/17 |
| F/17 | الجوانب الأمنية لخدمات وشبكات الاتصالات | استمرار المسألة 6/17 |
| G/17 | خدمات التطبيقات المأمونة | استمرار المسألة 7/17 |
| H/17 | أمن الحوسبة السحابية | استمرار المسألة 8/17 |
| I/17 | القياسات الحيوية في الاتصالات | استمرار المسألة 9/17 |
| J/17 | معمارية وآليات إدارة الهوية | استمرار المسألة 10/17 |
| K/17 | التكنولوجيات العامة (الدليل، البنية التحتية للمفتاح العمومي (PKI)، البنية التحتية لإدارة الامتيازات (PMI)، قواعد التركيب المجردة 1 (ASN.1)، معرفات الأشياء (OID)) لدعم التطبيقات المأمونة | استمرار المسألة 11/17 |
| L/17 | اللغات الشكلية لبرمجيات الاتصالات والاختبار | استمرار المسألة 12/17 |

# 2 نصوص المسائل

مشروع المسألة A/17

تنسيق أمن أنظمة الاتصالات/تكنولوجيا المعلومات والاتصالات

(استمرار المسألة 1/17)

### 1 الدوافع

تتزايد مخاطر الأمن التي تتعرض لها البنية التحتية للاتصالات وتكنولوجيا المعلومات والاتصالات (ICT) - سواء من حيث تواترها أو تعقدها. وعلى مر السنين، كانت الجهود التي بذلت لتأمين البنية التحتية مجزأة إلى حد ما وتقوم على أساس رد الفعل، ولم تحقق حتى الآن المستوى المرجو للحماية من تلك المخاطر. ويضاعف من تعقيد هذه المسألة العدد الكبير من المنظمات العاملة بشأن مختلف الجوانب الأمنية. وهذا يجعل من التنسيق والتعاون أمراً عسيراً وشاقاً.

وبالنظر إلى أن كثيراً جداً من المعاملات التجارية في العالم تتم عبر وصلات الاتصالات، فإن ضمان الأمن المرتبط باستعمال هذه البنية التحتية السيبرانية أمر بالغ الأهمية لضمان الأداء السلس للأعمال التجارية، ولرفاهة المواطنين، والتسيير الفعال للمهام التي تضطلع بها حكوماتهم. وقد تضررت ملايين الحواسيب وشبكات الاتصالات في أنحاء العالم من جراء الديدان والفيروسات وغيرها من هجمات التشفير الخبيثة. وكان لهذه الهجمات أثرها الاقتصادي الهائل. وتقتضي مكافحة هذه التهديدات بذل جهود مكثفة ومتواصلة ومركزة.

وموضوع الأمن شاسع في نطاقه. فالأمن يكاد ينطبق على جميع جوانب الاتصالات وتكنولوجيا المعلومات. وهناك نُهج مختلفة لتناول المتطلبات الأمنية، من بينها ما يلي:

• نهج "من القاعدة إلى أعلى" يقوم فيه الخبراء باستنباط تدابير أمنية لتعزيز وحماية مجال معين في الشبكة عن طريق استعمال تدابير مضادة محددة وتقنيات من قبيل القياسات الحيوية والتشفير. ورغم أن هذا النهج شائع إلى حد ما، إلا أنه مجزأ وغالباً ما يؤدي إلى حدوث تباين في تحديد التدابير الأمنية وتطبيقها.

• نهج "من القمة إلى أسفل"، يشكل أسلوباً استراتيجياً رفيع المستوى لمواجهة مشكلة الأمن. ويقتضي هذا النهج معرفة الصورة العامة. وهو نهج أصعب نسبياً نظراً لصعوبة العثور على خبراء ذوي معرفة شاملة بكل أجزاء الشبكة واحتياجاتها الأمنية مما هو الحال بالنسبة لخبراء ذوي معرفة تفصيلية في مجال واحد أو مجالين محددين.

• مزيج بين نهجي "من القاعدة إلى أعلى" و"من القمة إلى أسفل"، مع بذل جهود التنسيق للجمع بين هذين النهجين المختلفين. وقد ثبت في أحيان كثيرة أن هذا نهج بالغ الصعوبة عندما تناول الأمر مصالح وأولويات متباينة.

وفي خلال فترة الدراسة السابقة، حققت هذه المسألة العديد من النواتج التي يعتبرها قطاع تقييس الاتصالات نواتج قيمة لتعزيز أعماله ونواتجه. ومن الأمثلة على هذه النواتج خارطة طريق معايير الأمن وكتيب الأمن ومجموعة وثائق الأمن. وستواصل هذه المسألة التركيز على تنسيق وتنظيم كامل طائفة الأنشطة الأمنية في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات داخل قطاع تقييس الاتصالات، كما ستواصل وضع وتحديث الوثائق لدعم أنشطة التنسيق والتوعية. وسيستخدم نهج "من القمة إلى أسفل" إزاء الأمن بالتعاون مع لجان الدراسات الأخرى ومع منظمات وضع المعايير (SDO). وهذا النشاط موجه صوب زيادة تركيز الجهود على مستوى المشاريع والمستوى الاستراتيجي داخل لجنة الدراسات 17 وخارجها على السواء.

وعمل لجنة الدراسات 17 في مجال الأمن يأخذ بعين الاعتبار قرارات الجمعية العالمية لتقييس الاتصالات 7، 11، 40، 50، 52، 58، 64، 65، 67، 70، 73، 75، 76 و78؛ وقرارات مؤتمر المندوبين المفوضين 101، 123، 130، 136، 174، 177، 178، 179، 181، 188، 189، 197، 199، 200 و201؛ قرارات المؤتمر العالمي لتنمية الاتصالات 23، 30، 34، 45، 47، 54، 63، 67، 69 و80.

وتدعم لجنة الدراسات 17 أيضاً خط عمل القمة العالمية لمجتمع المعلومات جيم5 "بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات" والهدف 3 من خطة عمل دبي الذي اعتُمد في المؤتمر العالمي لتنمية الاتصالات لعام 2014 بشان تعزيز الأمن وبناء الثقة في استخدام تطبيقات تكنولوجيا المعلومات والاتصالات.

التقارير التقنية التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 23 مارس 2016: تقرير تقني عن "الأمن في مجال الاتصالات وتكنولوجيا المعلومات".

النصوص قيد التطوير: التقرير التقني عن الاستخدام الناجح للمعايير الأمنية (X.TRsuss).

### 2 المسألة

تتناول الدراسة البنود التالية دون أن تقتصر عليها:

 ﺃ ) ما هي نواتج هذه المسألة؟

ﺏ) ما هي العمليات وبنود العمل وأساليب العمل والجدول الزمني للمسألة لكي تحقق نواتجها؟

ﺝ) ما هي وثائق التوعية (خارطة الطريق والمجموعات الأمنية والتقارير التقنية والنشرات وصفحات الويب وما إلى ذلك) التي يتعين على الاتحاد إصدارها وتحديثها؟

د ) ما هي ورش العمل الأمنية اللازمة وكيف يمكن تنظيمها؟

ه ) ماذا يلزم لبناء روابط فعالة مع المنظمات الأخرى لوضع المعايير لغرض النهوض بالأعمال المتعلقة بالأمن؟

ﻭ ) ما هي المراحل الرئيسية ومعايير النجاح؟

ﺯ ) كيف يمكن تنشيط اهتمام أعضاء القطاعات والإدارات في الأعمال المتعلقة بالأمن وكيف يمكن الحفاظ على قوة الدفع؟

ﺡ) كيف يمكن زيادة جاذبية الخصائص الأمنية للاتصالات/تكنولوجيا المعلومات والاتصالات في الأسواق؟

ﻁ) كيف يمكن الترويج على أفضل وجه لدى الحكومات والقطاع الخاص للأهمية الحاسمة لأمن الاتصالات، والحاجة الماسة إلى حماية المصالح الاقتصادية العالمية، التي تعتمد على البنية التحتية القوية والمأمونة في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات؟

ﻱ) ما هي أنشطة الأمن قيد التطوير في لجان الدراسات الأخرى في الاتحاد وفي منظمات التقييس الأخرى؟

### 3 المهام

تشمل المهام البنود التالية دون أن تقتصر عليها:

 ﺃ ) العمل كجهة اتصال رئيسية للجنة الدراسات 17 لشؤون تنسيق الأمن في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات.

ﺏ) متابعة خارطة معايير أمن تكنولوجيا المعلومات والاتصالات وتحديثها.

ﺝ) متابعة مجموعة وثائق الأمن لدى قطاع تقييس الاتصالات وتحديثها.

ﺩ ) مساعدة مكتب تقييس الاتصالات وتزويده بالمدخلات لغرض تحديث كتيب الأمن المنشور كتقرير تقني عنوانه "الأمن في الاتصالات وتكنولوجيا المعلومات".

ﻫ ) مواصلة إعداد تقرير تقني عن الاستخدام الناجح للمعايير الأمنية.

ﻭ ) المساعدة في تحديد الثغرات في الأعمال المتعلقة بمعايير أمن الاتصالات/تكنولوجيا المعلومات والاتصالات وتعزيز الجهود الرامية إلى معالجة هذه الثغرات.

ﺯ ) توفير الإرشاد بشأن تنفيذ معايير الأمن في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات.

ﺡ) تعزيز التعاون والتآزر بين الجهات العاملة في مجال وضع معايير الأمن بشأن الاتصالات/تكنولوجيا المعلومات والاتصالات.

ﻁ) استعراض التوصيات ورسائل الاتصال من لجان الدراسات الأخرى ومنظمات وضع المعايير حسب الاقتضاء، لتقييم آثار التنسيق في مجال الأمن.

ﻱ) المساعدة في الجهود الرامية إلى ضمان التنسيق الأمني الفعال حيثما كان ذلك ضرورياً.

ﻙ) المساعدة في توجيه مسؤولي الاتصال من الأفرقة الخارجية إلى لجان الدراسات الملائمة في قطاع تقييس الاتصالات.

ﻝ) الاسترشاد بقطاع تقييس الاتصالات في تنظيم وتخطيط ورش العمل والحلقات الدراسية بخصوص الأمن، حسب الاقتضاء.

 ﻡ) ضمان المشاركة على نحو يتسم بالكفاءة والفعالية في تنسيق الجهود الأمنية مع المنظمات الأخرى.

ﻥ) المساعدة في تحسين كفاءة عمل لجنة الدراسات 17 (من خلال إنشاء نماذج، على سبيل المثال، أو أدوات أو إجراءات).

ﺱ) تشجيع السلطات وشركات التشغيل الوطنية من البلدان النامية في أقاليم على العمل معاً والمساهمة بشكل أفضل في أنشطة لجنة الدراسات 17 لقطاع تقييس الاتصالات وبما يتماشى مع ولاية لجنة الدراسات 17 وفي تنفيذ توصيات لجنة الدراسات 17 بشأن الأمن، ومثال ذلك الفريق الإقليمي لإفريقيا الذي أسسته لجنة الدراسات 17 رسمياً.

ﻉ) مساعدة لجنة الدراسات 17 في سد فجوة التقييس بهدف دعم القرار 44 للجمعية العالمية لتقييس الاتصالات والقرار 123 لمؤتمر المندوبين المفوضين والقرار 47 للمؤتمر العالمي لتنمية الاتصالات.

ﻑ) تحقيق مشاركة تتميز بالكفاءة والفعالية في جهود التنسيق المتعلقة بالأمن التي تجري داخل لجنة الدراسات 17، لضمان أن يجسد برنامج عمل اللجنة ما تقوم به حالياً من أنشطة الأمن وأن يعالج شواغل أعضاء قطاع تقييس الاتصالات.

### 4 الروابط

التوصيات:

• توصيات السلسلة X والتوصيات الأخرى ذات الصلة بأمن الاتصالات/تكنولوجيا المعلومات والاتصالات

المسائل:

• المسائل B/17 وC/17 وD/17 وE/17 وF/17 وG/17 وH/17 وI/17 وJ/17 وK/17 وL/17 لقطاع تقييس الاتصالات

لجان الدراسات:

• لجان الدراسات 2 و5 و9 و11 و13 و15 و16 و20 لقطاع تنمية الاتصالات وقطاع الاتصالات الراديوية وقطاع تقييس الاتصالات؛ الفريق الاستشاري لتقييس الاتصالات، بما في ذلك أنشطة التنسيق المشتركة والأفرقة المتخصصة ذات الصلة.

هيئات التقييس:

• تحالف حلول صناعة الاتصالات (ATIS)؛ رابطة المعايير الكندية (CSA)؛ المعهد الأوروبي لتقييس الاتصالات (ETSI)؛ معهد المهندسين الكهربائيين والإلكترونيين (IEEE)؛ فريق مهام هندسة الإنترنت (IETF)؛ اللجنة الخاصة 6 واللجنة الخاصة 27 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1)؛ اللجنة التقنية 292 التابعة للمنظمة الدولية للتوحيد القياسي (ISO TC 292)؛ هيئة الإدارة التقنية التابعة للمنظمة الدولية للتوحيد القياسي (ISO TMB)؛ منظمة النهوض بمعايير المعلومات المنظمة (OASIS)؛ مشروع الشراكة لتكنولوجيات الجيل الثالث (3GPP)؛ المشروع الثاني لشراكة الجيل الثالث (3GPP2)

هيئات أخرى:

• الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA)؛ المعهد الوطني للمعايير والتكنولوجيا (NIST)؛ المنتدى الإقليمي لتبادل أمن المعلومات في آسيا (RAISE).

مشروع المسألة B/17

معمارية الأمن وإطاره

(استمرار المسألة 2/17)

### 1 الدوافع

تصف التوصيات X.800 وX.802 وX.803 الصادرة عن قطاع تقييس الاتصالات الأمن في سياق الأنظمة المفتوحة. وترد في التوصية ITU‑T X.805 معمارية الأمن للأنظمة التي توفر الاتصالات من طرف إلى طرف. وقد تم وضع مجموعة شاملة من أطر الأمن التي تغطي جوانب أمنية من قبيل الاستيقان والتحكم في النفاذ وعدم الرفض والسرية وسلامة البيانات وتدقيق الأمن والإنذارات الأمنية (X.810 وX.811 وX.812 وX.813 وX.814 وX.815 وX.816). ووضعت التوصيات X.830 وX.831 وX.832 وX.833 وX.834 وX.835 لتحديد أمن الطبقات العليا العمومية (GULS). وبالتعاون مع اللجنة الفرعية ISO/IEC JTC 1/SC 27 وضعت التوصيات X.841 وX.842 وX.843 بشأن أغراض معلومات الأمن، وخدمات الطرف الثالث الموثوق به.

ويستدعي الأمر بذل جهد متواصل للحفاظ على هذه التوصيات الأمنية وتحسينها بما يفي باحتياجات التكنولوجيات الناشئة (مثل شبكات الجيل التالي (NGN) والشبكات القائمة على بروتوكول الإنترنت، والجوانب الأمنية للتوصيل الشبكي ال‍معرَّف بالبرم‍جيات (SDN)/التمثيل الافتراضي لوظيفة الشبكة (NFV) والتطور طويل الأمد/تطور معمارية النظام (LTE/SAE) وإرشادات التنفيذ التقني للأنظمة التي تقدم الاتصالات من طرف إلى طرف) والخدمات المتصلة بها. وينعكس هذا الجهد في التوصيتين X.1035 وX.1036 اللتين تبينان تفاصيل بروتوكولات تبادل المفاتيح المستيقنة بكلمة السر وتوزيع السياسات وإنفاذها.

وبالنظر إلى حالة التقارب والتنقلية في عالم الاتصالات، فإن الشبكات الناقلة للاتصالات وأنظمة المعلومات المرتبطة بها معرضة لأشكال جديدة من المخاطر الأمنية. وأصبح بوسع المهاجمين التوغل داخل الشبكات بمستويات أقل من المهارة واحتمالات أعلى بإيقاع الضرر. وانتشرت على نطاق واسع الهجمات الفيروسية وعمليات القرصنة الحاسوبية وإنكار الخدمة وأثرت تأثيراً ضاراً على عناصر الشبكات وعلى أنظمة الدعم على حد سواء.

وتسعى صناعات الاتصالات وتكنولوجيا المعلومات إلى إيجاد حلول أمنية شاملة وفعالة من حيث التكلفة ومؤثرة تكنولوجياً من أجل حماية طائفة عريضة من الخدمات والتطبيقات. ومن أجل تحقيق هذه الحلول في بيئة متعددة البائعين، ينبغي أن يصمم تأمين الشبكات وفقاً لمعمارية أمن معيارية وتكنولوجيات معيارية. وبالنظر إلى مخاطر الأمن التي تتعرض لها بيئة الاتصالات وأوجه التقدم الراهنة في تدابير الأمن المضادة لمواجهة هذه المخاطر، ينبغي البحث في متطلبات وحلول أمنية جديدة. ويلزم وضع توصيات جديدة تبين كيفية الجمع بين معايير التكنولوجيا وأطر الأمن من أجل تنفيذ الأمن الشامل للشبكات والخدمات الناشئة.

وتشمل التوصيات والإضافات التي تندرج في إطار مسؤولية هذه المسألة ما يلي اعتباراً من 29 أبريل 2016: X.800 وX.802 وX.803 وX.805 وX.810 وX.811 وX.812 وX.813 وX.814 وX.815 وX.816 وX.830 وX.831 وX.832 وX.833 وX.834 وX.835 وX.841 وX.842 وX.843 وX.1031 و X.1032و X.1033وX.1034 وX.1035 وX.1036 وX.1037 والإضافات X.Suppl.2 و X.Suppl.3و X.Suppl.15و X.Suppl.16 وX.Suppl.23.

النصوص قيد الإعداد: X.salcm و X.sdnsec-2و X.sgmvno و X.tigsc و X.voLTEsec-1.

### 2 المسألة

تتناول الدراسة البنود التالية دون أن تقتصر عليها:

 ﺃ ) ما هو السبيل إلى تحديد حل شامل ومتماسك لأمن الاتصالات؟

ﺏ) ما هي المعمارية المطلوبة لحل شامل ومتماسك لأمن الاتصالات؟

ﺝ) ما هو الإطار اللازم لتطبيق معمارية الأمن لغرض إيجاد حلول أمنية جديدة؟

ﺩ ) ما هو الإطار اللازم لتطبيق معمارية الأمن من أجل تقييم (ومن ثم تحسين) الحلول الأمنية القائمة؟

ﻫ ) ما هي المرتكزات المعمارية للأمن؟

’1‘ ما هي المعمارية من أجل الأمن من طرف إلى طرف؟

’2‘ ما هي معمارية الأمن للأنظمة المفتوحة؟

’3‘ ما هي معمارية الأمن للبيئة المتنقلة؟

’4‘ ما هي معمارية الأمن للشبكات المتطورة؟

’5‘ ما هي معمارية الأمن لخدمات التطبيق بالتعاون مع المسألة G/17؟

و ) ما هي معمارية الأمن الجديدة والتوصيات الإطارية المطلوبة لتوفير حلول أمنية في بيئة متغايرة؟

ز ) كيف يتعين تنظيم المعايير المعمارية فيما يتعلق بالتوصيات القائمة بشأن الأمن؟

ح) كيف يتعين تنظيم المعايير المعمارية فيما يتعلق بالتكنولوجيات الأمنية المتقدمة الحالية؟

ط) كيف يتعين تعديل توصيات إطار الأمن لكي تتكيف مع التكنولوجيات الناشئة، وما هي التوصيات الإطارية الجديدة المطلوبة؟

ي) كيف تطبق خدمات الأمن لغرض توفير حلول أمنية؟

ك) كيف يطبق رصد البنية التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات لتوفير حلول أمنية؟

### 3 المهام

تشمل المهام البنود التالية دون أن تقتصر عليها:

 ﺃ ) وضع مجموعة شاملة من معماريات الأمن والتوصيات الإطارية لتوفير حلول أمنية معيارية للاتصالات بالتعاون مع المنظمات الأخرى لوضع المعايير ولجان الدراسات لقطاع تقييس الاتصالات في الاتحاد.

ﺏ) إجراء الدراسات ووضع التوصيات بشأن معمارية موثوق بها لشبكة الاتصالات تدمج فيها أوجه التقدم التكنولوجي المتعلقة بالأمن.

ﺝ) الحفاظ على التوصيات والإضافات في السلسلة X.800 والسلسلة X.103x وتحسينها.

### 4 الروابط

التوصيات:

• السلسلة X وغيرها مما يتصل بالأمن

المسائل:

• المسائل A/17 وC/17 وD/17 وE/17 وF/17 وG/17 وH/17 وI/17 وJ/17 وK/17 لقطاع تقييس الاتصالات.

لجان الدراسات:

• لجنة الدراسات 2 لقطاع تنمية الاتصالات؛ فرقة العمل 6B لقطاع الاتصالات الراديوية؛ لجان الدراسات 2 و9 و11 و13 و16 و20 لقطاع تقييس الاتصالات

هيئات التقييس:

• تحالف حلول صناعة الاتصالات (ATIS)؛ المعهد الأوروبي لتقييس الاتصالات (ETSI)؛ منتدى النفاذ الدولي غير المنتظم إلى الشبكات (FIINA)؛ اللجنة الخاصة 27 واللجنة الخاصة 37 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1)؛ اللجنة التقنية 25 التابعة للجنة الكهرتقنية الدولية (IEC TC 25)؛ اللجنة التقنية 12 التابعة للمنظمة الدولية للتوحيد القياسي (ISO TC12)؛ فريق مهام هندسة الإنترنت (IETF)؛ مشروع شراكة الجيل الثالث (3GPP)؛ المشروع الثاني لشراكة الجيل الثالث (3GPP2).

مشروع المسألة C/17

إدارة أمن معلومات الاتصالات

(استمرار المسألة 3/17)

### 1 الدوافع

إن مرافق الاتصالات والشبكات ووسائط الإرسال أصول تجارية هامة من أصول الاتصالات بالنسبة لمنظمات الاتصالات والإعلام والعمليات الداعمة. ولكي تتمكن منظمات الاتصالات من إدارة هذه الأصول التجارية بصورة ملائمة، ولكي تواصل نشاطها التجاري بشكل سليم، تعد مسألة إدارة أمن المعلومات ضرورية للغاية. ولهذا السبب، وضعت التوصية ITU‑T X.1051 لكي توفر مبادئ توجيهية هامة بشأن إدارة أمن المعلومات لمنظمات الاتصالات.

واستناداً إلى المبادئ التوجيهية لإدارة أمن المعلومات، تم أيضاً تطوير مجالات إدارة مفصلة ومحددة، بما فيها الحوكمة وإطار الإدارة والمخاطر والحوادث والأصول. وهناك مجالات جديدة تتعلق بالتوصية ITU‑T X.1051 ينبغي المضي في فحصها. وفي الوقت ذاته يتعين الحفاظ على توصيات السلسلة وتحديثها لكي تعكس آخر المعلومات عن قضايا إدارة أمن المعلومات. والهدف من ذلك هو وضع مجموعة من التوصيات بشأن إدارة أمن الاتصالات استناداً إلى التوصية ITU‑T X.1051 في قطاع تقييس الاتصالات في الاتحاد.

كما ينبغي، بالتوازي مع وضع التوصيات لمجالات الإدارة المفصلة والمحددة استناداً إلى التوصية ITU‑T X.1051، النظر في المجالات الجديدة للاتصالات/تكنولوجيا المعلومات والاتصالات بما في ذلك الحوسبة ’السحابية‘ والانتقال في بروتوكول الإنترنت من الصيغة IPv4 إلى الصيغة IPv6 وحماية معلومات تعرّف الهوية الشخصية والتي تتطلب اتخاذ تدابير مضادة ناشئة وعالمية. ولذلك يتعين النظر في الدراسات التي تركز بصفة خاصة على جوانب الإدارة في المجالات الجديدة المشار إليها أعلاه.

وفي أثناء إجراء هذه الدراسات، ستجري مواصلة التعاون الكامل بين قطاع تقييس الاتصالات واللجنة التقنية الأولى المشتركة بين المنظمة الدولية للتوحيد القياسي واللجنة الكهرتقنية الدولية (ISO/IEC JTC 1) لضمان تحقيق أوسع قدر ممكن من توافق الحلول الأمنية. ويلزم أيضاً دراسة الحلول الناجحة التي تم استحداثها كمعايير وطنية في بلدان كثيرة.

وتختلف هذه المسألة عن المسائل المندرجة في إطار لجنة الدراسات 2 من حيث إن لجنة الدراسات 2 تعنى بتبادل المعلومات المتعلقة بإدارة الشبكات بين عناصر الشبكات وأنظمة الإدارة وبين أنظمة الإدارة في بيئة تتعلق بشبكة إدارة الاتصالات (TMN). وتتناول هذه المسألة في المقام الأول حماية الأصول التجارية، بما في ذلك المعلومات والعمليات، في سبيل إدارة أمن المعلومات.

والتوصيات التي تندرج في إطار مسؤولية المسألة اعتباراً من 23 مارس 2016 هي: E.409 (بالاشتراك مع لجنة الدراسات 2) وX.1051 و X.1052وX.1054 وX.1055 و X.1056وX.1057 والإضافة X.Suppl.13.

النصوص قيد الإعداد: X.gpim وX.sgsm و X.sup-gisb وX.sup-gpim.

### 2 المسألة

تتناول الدراسة البنود التالية دون أن تقتصر عليها:

 ﺃ ) كيف ينبغي تحديد قضايا إدارة الأمن المحددة لمنظمات الاتصالات؟

ﺏ) كيف ينبغي تنفيذ قضايا إدارة الأمن المحددة لمنظمات الاتصالات الصغيرة والمتوسطة (SMTO)؟

ﺝ) كيف ينبغي أن تنفَّذ على النحو الملائم إدارة أمن المعلومات لمنظمات الاتصالات باستعمال المعايير القائمة (ITU‑T وISO/IEC وغيرها)؟

ﺩ ) كيف ينبغي تحديد وإدارة عملية قياس إدارة أمن المعلومات في مجال الاتصالات؟

ﻫ ) كيف ينبغي تنفيذ إدارة أمن المعلومات على النحو الملائم في بيئة الحوسبة ’السحابية‘؟

ﻭ ) كيف تنبغي حماية معلومات تعرّف الهوية الشخصية على النحو الملائم؟

ﺯ ) كيف ينبغي تنفيذ إدارة أمن المعلومات في بيئة بروتوكول الإنترنت الشاملة للانتقال من الإصدار الرابع لبروتوكول الإنترنت إلى الإصدار السادس لبروتوكول الإنترنت؟

ﺡ) ما هي التحسينات المطلوب إدخالها على التوصيات الحالية قيد الاستعراض أو التوصيات الجديدة قيد الإعداد والتي يلزم اعتمادها للحد من الأثر الناشئ على تغير المناخ (من قبيل وفورات الطاقة والحد من انبعاثات غازات الدفيئة وتنفيذ أنظمة المراقبة) بصورة مباشرة أو غير مباشرة في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات أو في مجالات الصناعات الأخرى؟

### 3 المهام

تشمل المهام البنود التالية دون أن تقتصر عليها:

 ﺃ ) دراسة ووضع إطار لوظائف إدارة أمن المعلومات على النحو المبين في التوصية ITU‑T X.1051.

ﺏ) دراسة ووضع منهجية لتنفيذ نظام لإدارة أمن المعلومات لمنظمات الاتصالات استناداً إلى المعايير القائمة (ITU‑T وISO/IEC وغيرها).

ﺝ) دراسة ووضع مبادئ توجيهية لتنفيذ إدارة الأمن لمنظمات الاتصالات الصغيرة والمتوسطة (SMTO)

ﺩ ) دراسة ووضع مبادئ توجيهية لإنشاء إدارة أمن المعلومات لبيئة الحوسبة "السحابية".

ﻫ ) دراسة ووضع مبادئ توجيهية أو إطار لإنشاء إدارة أمن المعلومات في بيئة الصيغة IPv6 من بروتوكول الإنترنت.

ﻭ ) دراسة ووضع توصيات لإعداد مبادئ توجيهية بشأن حماية معلومات تعرّف الهوية الشخصية.

ﺯ ) اقتراح مخطط لتوصيات جديدة.

ﺡ) تقييم نواتج الأنشطة المذكورة أعلاه في ضوء إمكانية استخدامها في مرافق الاتصالات وفي الخدمات.

ﻁ) إعداد مشاريع توصيات.

ﻱ) الحفاظ على التوصيات في السلسلة X.105x وتحسينها.

### 4 الروابط

التوصيات:

• السلاسل X.800- وX.1000- وX.1100- وX.1200- وX.1300-

المسائل:

• المسائل A/17 وB/17 وD/17 وE/17 وF/17 وG/17 وH/17 وI/17 وJ/17 وK/17 و14/15 لقطاع تقييس الاتصالات

لجان الدراسات:

• قطاع تنمية الاتصالات؛ قطاع الاتصالات الراديوية؛ لجان الدراسات 2 و9 و11 و13 و15 و16 لقطاع تقييس الاتصالات

هيئات التقييس:

• رابطة المعايير الكندية (CSA)؛ المعهد الأوروبي لتقييس الاتصالات (ETSI)؛ اللجنة الخاصة 27 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1)؛ للمنظمة الدولية للتوحيد القياسي/اللجنة التقنية 215 (ISO/TC 215)؛ المعهد الوطني للمعايي‍ر والتكنولوجيا (NIST)؛ لجنة تكنولوجيا الاتصالات (TTC)؛ مشروع شراكة الجيل الثالث (3GPP).

مشروع المسألة D/17

الأمن السيبراني

(استمرار المسألة 4/17)

### 1 الدوافع

يلاحظ أن مشهد الاتصالات في حالة تغير دائب يصحبه في ذلك ما يرتبط به من أمن الاتصالات/تكنولوجيا المعلومات والاتصالات. وفي هذه البيئة السيبرانية ثمة حاجة قوية إلى تأمين البروتوكولات والبنى التحتية والتطبيقات التي تستخدم كجزء لا يتجزأ من اتصالاتنا اليومية.

وينطوي الأمن السيبراني على تأمين وحماية الخدمات، والمعلومات الشخصية، وحماية معلومات تعرّف الهوية الشخصية (PII)، وتوفير أمن المعلومات (IA) فيما بين الكيانات المتفاعلة.

وما فتئت تنتشر الهجمات السيبرانية على نطاق واسع، وهي تتسبب في طائفة معقدة من المشاكل للمستعملين ومزودي الخدمات والشبكات. وتقتضي مواجهة الهجمات السيبرانية بأساليب تقنية وضع أطر ومتطلبات لتحري الهجمات السيبرانية والحماية منها والتخفيف من آثارها والتعافي منها، ولتبادل معلومات الأمن السيبراني.

وتشمل التوصيات والإضافات التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 23 مارس 2016 ما يلي: X.1205 وX.1206 وX.1207 و X.1208و X.1209و X.1210و X.1211و X.1303 وX.1303مكرراً و X.1500وX.1500.1 وX.1520 وX.1521 وX.1524 و X.1525 و X.1526وX.1528 وX.1528.1 وX.1528.2 وX.1528.3 وX.1528.4 وX.1541 وX.1544 وX.1546 وX.1570 وX.1580 وX.1581 و X.1582والإضافات وX.Suppl.8 وX.Suppl.9 وX.Suppl.10 وX.Suppl.18 وX.Suppl.20.

والنصوص قيد الإعداد هي: X.1542 (X.simef) و X.cogent و X.metric و X.nessa و X.samtn وX.sbb.

### 2 المسألة

تتناول الدراسة البنود التالية دون أن تقتصر عليها:

 ﺃ ) كيف يتعين على مزودي خدمات الاتصالات/تكنولوجيا المعلومات والاتصالات تأمين بنيتهم التحتية والحفاظ على سلامة العمليات واستخدام آليات التحقق من الأمن في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات؟

ﺏ) ما هي المتطلبات الأمنية اللازمة للبرمجيات وبروتوكولات الاتصالات ومصممي أنظمة الاتصالات وصانعيها، لغرض النظر في تصميم ووضع وتقاسم أفضل الممارسات في مجال البيئة السيبرانية؟

ﺝ) كيف ينبغي تقاسم معلومات قابلية التأثر على نحو يتسم بالكفاءة من أجل المساعدة في معالجة قابلية التأثر أثناء دورة حياة المعلومات؟

ﺩ ) ما هي المتطلبات والحلول اللازمة لضمان تجاوز العثرات والأمن والسلامة في ما يمكن إنشاؤه من أنظمة الاتصالات/ تكنولوجيا المعلومات والاتصالات؟

ﻫ ) ما هي المتطلبات والحلول اللازمة من حيث المساءلة والاستجابة للأحداث ورصد التهديدات والإبلاغ عن المخاطر في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات؟

ﻭ ) ما هي الآليات اللازمة لتبادل المعلومات المتعلقة بالأمن والضمان بشأن الأنظمة المفعَّلة سيبرانياً، بما فيها تلك القائمة على الخدمة السحابية، وتلك المدمجة والقابلة للإنشاء؟

ﺯ ) كيف يمكن استخدام الشبكات في توفير الخدمات الحرجة، من قبيل استخدام بروتوكول الإنذار المشترك، بصورة مأمونة أثناء حالات الطوارئ الوطنية؟

ﺡ) ما هي المبادئ التوجيهية والممارسات الفضلى الأمنية الضرورية لتحديد التهديدات السيبرانية، التي تتضمن البرمجيات الخبيثة والحرمان من الخدمة الموزَّع والهندسة الاجتماعية، وللتخفيف منها والحد من أثرها؟

ﻁ) ما هي التحسينات المدخلة على التوصيات الحالية قيد الاستعراض أو التوصيات الجديدة قيد الإعداد والتي ينبغي اعتمادها للحد من الأثر على تغيرات المناخ (مثل وفورات الطاقة والحد من انبعاثات غازات الدفيئة وتنفيذ أنظمة المراقبة) بصورة مباشرة أو غير مباشرة في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات أو في مجالات صناعات أخرى؟

### 3 المهام

تشمل المهام البنود التالية دون أن تقتصر عليها:

 ﺃ ) التعاون مع لجان الدراسات لقطاع تقييس الاتصالات والمعهد الأوروبي لمعايير الاتصالات (ETSI) والمنتدى العالمي لفرق الاستجابة للطوارئ وأمن المعلومات (FIRST) وفريق مهام هندسة الإنترنت (IETF) ومعهد المهندسين الكهربائيين والإلكترونيين (IEEE) والمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1) ومنظمة تحسين معايير المعلومات المبنية (OASIS) والاتحاد المفتوح للاتصالات المتنقلة (OMA) وفريق الحوسبة الموثوقة (TCG) ومشروع شراكة الجيل الثالث (3GPP) والمشروع الثاني لشراكة الجيل الثالث (3GPP2) والهيئات الأخرى لوضع المعايير في مجال الأمن السيبراني.

ﺏ) العمل على وضع أطر وتوصيات بشأن كيفية قيام مزودي الاتصالات/تكنولوجيا المعلومات والاتصالات بتأمين البنى التحتية لديهم والحفاظ على أمن العمليات وتبادل معلومات الأمن السيبراني.

ﺝ) وضع مجموعة من التوصيات لتوفير حلول أمنية بشأن المساءلة والضمان والتصدي للحوادث في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات.

ﺩ ) دراسة وتحديد التقنيات والقدرات الأمنية لمقدمي الخدمات لغرض تنسيق وتبادل المعلومات بشأن مواطن الضعف والمنصات والهجمات السيبرانية، وما إلى ذلك.

ﻫ ) تحديد كيفية تطبيق آلية المساءلة والضمان والتصدي للحوادث في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات.

ﻭ ) وضع مبادئ توجيهية وأساليب تقنية لحماية المعلومات الشخصية وكذلك لحماية معلومات تعرّف الهوية الشخصية (PII) باستخدام أساليب إطار تبادل معلومات الأمن السيبراني (CYBEX).

ﺯ ) تقديم المساعدة إلى لجان الدراسات الأخرى في قطاع تقييس الاتصالات في تطبيق توصيات الأمن السيبراني ذات الصلة فيما يتعلق بحلول أمنية محددة.

ح) وضع الممارسات الفضلى والمبادئ التوجيهية لتبادل المعلومات بشأن الثغرات الأمنية وسبل علاجها من أجل المساعدة في معالجة عمليات دورة حياة الثغرة الأمنية.

### 4 الروابط

التوصيات:

• سلسلة التوصيات X والتوصيات الأخرى ذات الصلة بالأمن

المسائل:

• A/17 وB/17 وC/17 وE/17 وF/17 وG/17 وH/17 وI/17 وJ/17 وK/17 و7/11 لقطاع تقييس الاتصالات.

لجان الدراسات:

• لجان الدراسات 2 و9 و11 و13 (المسألة 7/13) و16 لقطاع تقييس الاتصالات؛ لجنة الدراسات 2 لقطاع تنمية الاتصالات (المسألة 3/2)

هيئات التقييس:

• المعهد الأوروبي لتقييس الاتصالات (ETSI)؛ معهد المهندسين الكهربائيين والإلكترونيين (IEEE)؛ فريق مهام هندسة الإنترنت (IETF)؛ اللجنة التقنية 57 التابعة للجنة الكهرتقنية الدولية (IEC TC 57)؛ اللجنة التقنية 65 التابعة للجنة الكهرتقنية الدولية/فريق العمل 10 (IEC TC 65/WG10)؛ اللجنة الخاصة 27 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SC 27)؛ المعهد الوطني للمعايير والتكنولوجيا (NIST)؛ منظمة النهوض بمعايير المعلومات المنظمة (OASIS)؛ الاتحاد المفتوح للاتصالات المتنقلة (OMA)؛ فريق إدارة الأشياء (OMG)؛ مشروع شراكة الجيل الثالث (3GPP)؛ المشروع الثاني لشراكة الجيل الثالث (3GPP2)

هيئات أخرى:

• فريق العمل المعني بمكافحة التصيد (APWG)؛ فريق مواجهة الطوارئ الحاسوبية/مركز التنسيق (CERT/CC)؛ الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA)؛ جمعية النظام العالمي للاتصالات المتنقلة (GSMA)؛ المنتدى العالمي لفرق الاستجابة للطوارئ وأمن المعلومات (FIRST)؛ الشراكة العالمية المتعددة الأطراف لمكافحة الإرهاب السيبراني (IMPACT)؛ منظمة التعاون والتنمية في الميدان الاقتصادي (OECD).

مشروع المسألة E/17

مكافحة الرسائل الاقتحامية بالوسائل التقنية

(استمرار المسألة 5/17)

### 1 الدوافع

أصبحت الرسائل الاقتحامية مشكلة واسعة الانتشار تتسبب في احتمال خسارة في إيرادات مقدمي خدمات الإنترنت ومشغلي خدمات الاتصالات الثابتة أو المتنقلة ومستعملي خدمات الأعمال في شتى بقاع العالم. وعلاوة على ذلك، تتسبب الرسائل الاقتحامية بمشكلات تواجه أمن شبكات المعلومات والاتصالات كما تستخدم وسيلة للاحتيال ونشر الفيروسات والديدان وبرمجيات التجسس وغيرها من أشكال البرمجيات الخبيثة، وما إلى ذلك. ولهذا، كلفت الجمعية العالمية لتقييس الاتصالات (WTSA‑08) في القرار 52 لجان الدراسات ذات الصلة بأن تقوم بدعم العمل الجاري، خاصة في لجنة الدراسات 17، المتعلق بمكافحة الرسائل الاقتحامية والإسراع بأعمالها في هذا الشأن وذلك للتصدي للتهديدات الحالية والمستقبلية والتي تدخل في إطار اختصاص قطاع تقييس الاتصالات وخبرته، حسب الاقتضاء. وهي مكلفة أيضاً بأن تواصل التعاون مع المنظمات ذات الصلة وأن تواصل وضع توصيات تقنية، كمسألة ملحة، بغية ضمان تبادل أفضل للممارسات ونشر المعلومات عن طريق ورش العمل، والدورات التدريبية، وما إلى ذلك؛ كما تكلف لجنة الدراسات 17 بأن ترفع تقارير منتظمة إلى الفريق الاستشاري لتقييس الاتصالات عن التقدم المحرز في تنفيذ هذا القرار.

وقد اعترف بأن مكافحة الرسائل الاقتحامية تمثل مشكلة عالمية تتطلب نهجاً شاملاً متعدد الوجوه. ولجنة الدراسات 17، بوصفها لجنة الدراسات الرئيسية فيما يتعلق بأمن الاتصالات ودعم الأنشطة التي نص عليها القرار 52 للجمعية العالمية لتقييس الاتصالات، في وضع متميز لدراسة طائفة التدابير التقنية الممكنة لمكافحة الرسائل الاقتحامية بقدر ما تتصل هذه التدابير بثبات شبكة الاتصالات ومتانتها. وعلاوة على ذلك، أرسيت بنية تقنية للتوصيات القائمة والمحتملة لمكافحة الرسائل الاقتحامية بأساليب تقنية وذلك في سبيل تيسير وضع التوصية. وإضافة إلى ذلك، ينبغي نشر توصيات جديدة لمكافحة أشكال جديدة من الرسائل الاقتحامية.

وتشمل التوصيات والإضافات التي تندرج في إطار مسؤولية هذه المسألة ما يلي اعتباراً من 23 مارس 2016: X.1231 وX.1240 وX.1241 وX.1242 و X.1243وX.1244 وX.1245 وX.1246 وX.1247 وX.Suppl.6 وX.Suppl.11 وX.Suppl.12 وX.Suppl.14 و X.Suppl.25.

النص قيد الإعداد: X.cspim وX.gcspi وX.tfcma وX.ticsc.

### 2 المسألة

تتناول الدراسة البنود التالية دون أن تقتصر عليها:

 ﺃ ) كيف نفهم ونعرف ما هي الرسائل الاقتحامية؟

ﺏ) ما هي الأشكال الجديدة للرسائل الاقتحامية في الشبكات القائمة والمقبلة؟

ﺝ) ما هي الآثار الخطيرة التي تترتب على الرسائل الاقتحامية؟

ﺩ ) ما هي العوامل التقنية التي تسهم في صعوبات تحديد مصادر الرسائل الاقتحامية؟

ﻫ ) كيف يمكن للتكنولوجيات والخدمات والتطبيقات الجديدة، مثل المراسلة الفورية والتواصل الاجتماعي والتطبيق المتنقل والصوت عبر التطور طويل الأمد (VoLTE)/مجموعة الاتصالات الغنية (RCS) وغيرها، أن تفضي إلى فرص لاستحداث الرسائل الاقتحامية ونشرها؟

ﻭ ) ما هي الأعمال التقنية المضطلع بها فعلاً في إطار فريق مهام هندسة الإنترنت (IETF) ومشروع شراكة الجيل الثالث (3GPP) وجمعية النظام العالمي للاتصالات المتنقلة (GSMA) فريق العمل المعني بمكافحة إساءة استعمال المراسلة (M3AAWG) وفي محافل أخرى ومن جانب كيانات القطاع الخاص تصدياً لمشكلة الرسائل الاقتحامية؟

ﺯ ) ما هي أعمال تقييس شبكة الاتصالات، إن وجدت، الضرورية لمكافحة الرسائل الاقتحامية مكافحة فعّالة بقدر ما تتصل بثبات شبكة الاتصالات ومتانتها؟

ﺡ) ما هي الحلول التي تتسم بالفعالية والكفاءة لمكافحة الرسائل الاقتحامية؟

ﻁ) كيف توضع متطلبات عامة ومحددة لتبادل المعلومات بشأن مكافحة الرسائل الاقتحامية؟

ﻱ) ما هي أفضل الممارسات لمكافحة الرسائل الاقتحامية؟

### 3 المهام

تشمل المهام البنود التالية دون أن تقتصر عليها:

 ﺃ ) التصرف بوصفها اللجنة الرائدة في القطاع بخصوص الأساليب التقنية لمكافحة الرسائل الاقتحامية، تبعاً لوصف لجنة الدراسات 2 لهذه الرسائل.

ﺏ) تحديد وفحص مخاطر أمن شبكات الاتصالات (في أطراف الشبكة وفي صلبها) التي تنطوي عليها الطبيعة المتغيرة باستمرار للرسائل الاقتحامية.

ﺝ) وضع قائمة شاملة ومستحدثة بمصادر التدابير التقنية الراهنة لمكافحة الرسائل الاقتحامية في شبكة الاتصالات، سواء المستخدمة أم قيد التطوير.

ﺩ ) وضع توصيات جديدة بشأن مكافحة الأشكال القائمة والناشئة للرسائل الاقتحامية.

ﻫ ) وضع متطلبات عامة ومحددة لتبادل المعلومات بشأن مكافحة الرسائل الاقتحامية؟

و ) تقرير ما إذا كان من شأن وضع توصيات جديدة أو تعزيز توصيات قائمة، بما في ذلك طرائق مكافحة نشر برمجيات التجسس وممارسات التدليس وغير ذلك من المحتويات المؤذية، أن تفيد جهود الأعضاء في مكافحة الرسائل الاقتحامية مكافحة فعّالة بقدر ما تتصل بثبات شبكة الاتصالات ومتانتها.

ﺯ ) تقديم تحديثات منتظمة إلى الفريق الاستشاري لتقييس الاتصالات وإلى مدير مكتب تقييس الاتصالات لتضمينها في التقرير السنوي إلى المجلس.

### 4 الروابط

التوصيات:

• السلسلة X

المسائل:

• المسائل A/17 وB/17 وC/17 وD/17 وF/17 وG/17 وH/17 وI/17 وJ/17 لقطاع تقييس الاتصالات

لجان الدراسات:

• ولجنتا الدراسات 1 و2 لقطاع تنمية الاتصالات ؛ ولجان الدراسات 2 و11 و13 و16 لقطاع تقييس الاتصالات

هيئات التقييس:

• اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1)؛ وفريق مهام هندسة الإنترنت (IETF)؛ والمعهد الأوروبي لتقييس الاتصالات (ETSI)؛ ومشروع شراكة الجيل الثالث (3GPP)؛ والمشروع الثاني لشراكة الجيل الثالث (3GPP2)؛ والاتحاد المفتوح للاتصالات المتنقلة (OMA)؛ وغيرها من منظمات المعايير الوطنية والدولية ذات الصلة

هيئات أخرى:

• جمعية النظام العالمي للاتصالات المتنقلة (GSMA)؛ وفريق العمل المعني بمكافحة إساءة استعمال المراسلة (M3AAWG)، ومنتدى أفرقة الاستجابة لحوادث الأمن (FIRST)، والمعهد الوطني للمعايي‍ر والتكنولوجيا (NIST) ومنظمة التعاون والتنمية في الميدان الاقتصادي (OECD).

مشروع المسألة F/17

الجوانب الأمنية لخدمات وشبكات الاتصالات

(استمرار المسألة 6/17)

### 1 الدوافع

توفر التوصية ITU‑T X.1101 المتطلبات والإطار بشأن الأمن في اتصالات تعدد الإرسال. وتصف التوصيات ITU‑T X.1111 وX.1112 وX.1113 وX.1114 الإطار الأمني للشبكة المن‍زلية بما في ذلك موجز شهادة الجهاز وآلية الاستيقان وإطار الترخيص. وتوفر التوصيات ITU‑T X.1121 وX.1122 وX.1123 وX.1124 وX.1125 مواصفة شاملة بشأن أمن الشبكة المتنقلة. وتحدد التوصيات ITU‑T X.1171 وX.1311 وX.1312 إطار الخصوصية لخدمات أرقام تعرّف الجنسية (NID) المتنقلة وإطار الأمن لشبكة الاستشعار الشمولية (USN) والمبادئ التوجيهية لأمن البرمجيات الوسيطة USN ومتطلبات الأمن لتسيير شبكات المحاسيس اللاسلكية، على التوالي. وتصف التوصيات ITU‑T X.1191 وX.1192 وX.1193 وX.1194 وX.1195 وX.1196 وX.1197 وX.1198 مجموعة شاملة من المتطلبات والآليات وإطاراً لأمن خدمات تلفزيون بروتوكول الإنترنت (IPTV). وتعرض الإضافتان X.Suppl.19 وX.Suppl.24 جوانب الأمن بخصوص الهواتف المتنقلة. ويحتاج الأمر إلى مواصلة الجهود من أجل الحفاظ على توصيات وإضافات الأمن هذه وتعزيزها لكي تلبي احتياجات التكنولوجيات والخدمات الناشئة.

وتشير عبارة ’خدمات وشبكات الاتصالات‘ إلى الخدمة التي تتيح للجميع النفاذ إلى أي معلومات مطلوبة بطريقة سهلة الاستعمال في أي وقت وفي أي مكان وباستعمال أي أجهزة كانت. وما فتئت صناعة الاتصالات تشهد حالة من النمو المذهل في مجال خدمات الاتصالات التي تقوم على التكنولوجيا المتنقلة. وعلى وجه الخصوص، يتسم أمن خدمات وشبكات الاتصالات والخاصة بكل مجال فيما بين الأجهزة غير المتجانسة من أجل التكنولوجيات على مستوى التطبيقات، مثل شبكة الاستشعار (بما فيها إنترنت الأشياء (IoT) وأنظمة النقل من آلة إلى آلة (M2M) وأجهزة النقل الذكية وشبكات الجيل الخامس) والشبكة المحلية والجوانب الأمنية للتوصيل الشبكي ال‍معرَّف بالبرم‍جيات (SDN)/التمثيل الافتراضي لوظيفة الشبكة (NFV) والشبكة الذكية والشبكة المتنقلة (بما في ذلك اتصالات المجال القريب (NFC) ووحدة هوية المشترك المدمجة (eSIM) والهواتف الذكية) وشبكة البث المتعدد وشبكة تلفزيون بروتوكول الإنترنت، بأهمية حاسمة في دفع عجلة الصناعة وهيئات تشغيل الشبكات وتوفير الخدمات.

وتقييس أفضل التطبيقات الأمنية الشاملة أمر حيوي لمشغلي الشبكات ومزودي الخدمات الذين يعملون في بيئة اتصالات دولية متعددة البائعين. وبالنظر إلى بعض الخصائص التي تنفرد بها الاتصالات المتنقلة (مثل الإرسال على الهواء ومحدودية القدرة الحاسوبية وحجم الذاكرة في الأجهزة المتنقلة الصغيرة)، فإن توفير الأمن مهمة عسيرة حقاً وتتطلب الاهتمام والدراسة بصورة خاصة.

وتشمل التوصيات والإضافات التي تندرج في إطار مسؤوليات هذه المسألة اعتباراً من 23 مارس 2016 ما يلي: X.1101 وX.1111 وX.1112 وX.1113 وX.1114 وX.1121 وX.1122 وX.1123 وX.1124 وX.1125 وX.1171 وX.1191 وX.1192 و X.1193 وX.1194 وX.1195 وX.1196 وX.1197 وX.1198 وX.1311 وX.1312 وX.1313 وX.1314 والإضافات X.Suppl.19 وX.Suppl.24 و X.Suppl.26.

النصوص قيد الإعداد: X.iotsec-1 و X.iotsec-2 و X.itsec-1 و X.itssec-2 و X.msec-9 وX.msec-11 وX.sdnsec-1 وX.sgsec-2 وX.sotavsu.

### 2 المسألة

تتناول الدراسة البنود التالية دون أن تقتصر عليها:

 ﺃ ) كيف ينبغي تحديد وتعريف جوانب الأمن المتعلقة بخدمات وشبكات الاتصالات في إطار الاتصالات المتنقلة؟

ﺏ) كيف ينبغي تحديد ومعالجة المخاطر التي تهدد خدمات وشبكات الاتصالات؟

ﺝ) ما هي التكنولوجيات الأمنية لدعم خدمات وشبكات الاتصالات؟

ﺩ ) كيف ينبغي ضمان التوصيلية المأمونة بين خدمات وشبكات الاتصالات والحفاظ على هذه التوصيلية؟

ﻫ ) ما هي أساليب وآليات وبروتوكولات الأمن اللازمة للخدمات والشبكات الناشئة في إطار الاتصالات، ولا سيما الخدمات الناشئة لحماية المحتوى الرقمي؟

ﻭ ) ما هي الحلول الأمنية العالمية لخدمات وشبكات الاتصالات (بما في ذلك مثلاً أنظمة خدمات الشبكات الذكية وأنظمة النقل الذكية القائمة على شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات)؟

ﺯ ) ما هي أفضل الممارسات أو المبادئ التوجيهية للخدمات المأمونة للاتصالات وما هي تطبيقاتها؟

ﺡ) ما هي التحسينات المطلوب إدخالها على التوصيات الحالية قيد الاستعراض أو التوصيات الجديدة قيد الإعداد والتي يلزم اعتمادها للحد من الأثر الناشئ على تغير المناخ (مثل وفورات الطاقة والحد من انبعاثات غازات الدفيئة وتنفيذ أنظمة المراقبة) بصورة مباشرة أو غير مباشرة في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات أو في مجالات الصناعات الأخرى؟

ﻁ) ما هي الآليات اللازمة لحماية المعلومات المحددة لهوية شخص (PII) وإدارتها في خدمات وشبكات الاتصالات المأمونة؟

### 3 المهام

تشمل المهام البنود التالية دون أن تقتصر عليها:

 ﺃ ) القيام بالتعاون مع لجان الدراسات الأخرى لقطاع تقييس الاتصالات ومنظمات وضع المعايير، ولا سيما فريق مهام هندسة الإنترنت (IETF) والمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/ SCs 6, 25, 27 & 31)، بوضع مجموعة من التوصيات لتوفير حلول أمنية شاملة للخدمات والشبكات المأمونة للاتصالات.

ﺏ) استعراض التوصيات/المقاييس الحالية لقطاع تقييس الاتصالات والمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC) في مجال الشبكة المنزلية والشبكة الذكية والشبكة المتنقلة (بما في ذلك أمن الهواتف الذكية)، والخدمة المتنقلة لإنترنت الأشياء (IoT) وشبكة الاستشعار، لغرض تحديد خدمات وشبكات مأمونة للاتصالات.

ﺝ) مواصلة الدراسة لغرض تحديد الجوانب الأمنية لخدمات وشبكات الاتصالات في بيئة دولية عمومية متعددة البائعين، وبالنسبة لخدمات جديدة ناشئة (بالنسبة مثلاً لأنظمة النقل الذكية والشبكة الكهربائية الذكية التي تستند إلى شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات).

ﺩ ) دراسة وتحديد المسائل الأمنية والمخاطر في مجال الخدمات والشبكات المأمونة للاتصالات.

ﻫ ) دراسة وتطوير آليات أمنية للخدمات المأمونة للاتصالات الشمولية.

ﻭ ) دراسة وتطوير آليات التوصيلية البينية للخدمات والشبكات المأمونة للاتصالات في بيئة اتصالات عمومية تضم موردين فرادى أو متعددين.

ﺯ ) دراسة وتحديد الإشكالات والتهديدات التي تعترض حماية المعلومات المحددة لهوية شخص في خدمات وشبكات الاتصالات المأمونة.

ﺡ) دراسة ووضع الآليات اللازمة لحماية المعلومات المحددة لهوية شخص وإدارتها في خدمات وشبكات الاتصالات المأمونة.

### 4 الروابط

التوصيات:

• سلسلة التوصيات X والتوصيات الأخرى ذات الصلة بالأمن

المسائل:

• المسائل A/17 وB/17 وC/17 وD/17 وE/17 وG/17 وH/17 وI/17 وJ/17 وK/17 و7/13 و13/16 و21/16 لقطاع تقييس الاتصالات

لجان الدراسات:

• قطاع الاتصالات الراديوية؛ لجان الدراسات 9 و11 و13 و15 و16 20 لقطاع تقييس الاتصالات؛ نشاط التنسيق المشترك–إنترنت الأشياء (JCA-IoT) ونشاط التنسيق المشترك–تلفزيون بروتوكول الإنترنت (JCA‑IPTV)؛ التعاون بشأن معايير الاتصالات المتعلقة بأنظمة النقل الذكية (CITS).

هيئات التقييس:

• جمعية النظام العالمي للاتصالات المتنقلة (GSMA)؛ فريق مهام هندسة الإنترنت (IETF)؛ فريق تقييم الأنظمة 6 لدى اللجنة الكهرتقنية الدولية (IEC SEG) (الشبكة الكهربائية الصغرية)، فريق العمل 3 واللجنة التقنية 57 لدى هيئة إدارة التقييس في اللجنة الكهرتقنية الدولية (IEC SMB WG3 & TC57)، اللجنتان التقنيتان 57، 65 لدى اللجنة الكهرتقنية الدولية (IEC)، اللجان الخاصة 6 و25 و27 و31 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SCs 6, 25, 27 & 31)؛ اللجنة التقنية 204 التابعة للمنظمة الدولية للتوحيد القياسي (ISO TC 204)؛ الاتحاد المفتوح للاتصالات المتنقلة (OMA)؛ مشروع شراكة الجيل الثالث (3GPP)؛ المشروع الثاني لشراكة الجيل الثالث (3GPP2)

هيئات أخرى:

• تحالف حلول صناعة الاتصالات (ATIS)؛ رابطة تقييس الاتصالات الصينية (CCSA)؛ المعهد الأوروبي لتقييس الاتصالات (ETSI) (TC CYBER, TC ITS)؛ تحالف الاتصالات من آلة إلى آلة (M2M Alliance)؛ منتدى اتصالات المجال القريب (NFC Forum)؛ المعهد الوطني للمعايي‍ر والتكنولوجيا (NIST)؛ شراكة الاتصالات من آلة إلى آلة (oneM2M)؛ لجنة تكنولوجيا الاتصالات (TTC)؛ رابطة تكنولوجيا الاتصالات (TTA)؛ منتدى البروتوكول الشامل للتوصيل والتشغيل (UPnP).

مشروع المسألة G/17

خدمات التطبيقات المأمونة

(استمرار المسألة 7/17)

### 1 الدوافع

توفر التوصيات X.1141 وX.1142 وX.1143 وX.1144 لقطاع تقييس الاتصالات مجموعة من التوصيات التي تتناول علامات الأمن من أجل الاستيقان/الترخيص ومعماريات الأمن لخدمات رسائل الشبكات. وتحدد التوصيات ITU‑T X.1151 و X.1152 وX.1153 وX.1154 وX.1155 وX.1156 وX.1157 وX.1158 وX.1159 مبادئ توجيهية بشأن استيقان مأمون يقوم على أساس كلمة سر في خدمات تبادل المفاتيح ومختلف خدمات الطرف الثالث الموثوق به (TTP). وتحدد التوصيات ITU‑T X.1161 وX.1162 وX.1163 وX.1164 إطاراً شاملاً وآليات لأمن الخدمات من الند إلى الند (P2P). ويلزم مواصلة الجهد المبذول لدعم وتحسين هذه التوصيات التي تتناول مسألة الأمن لغرض تلبية الاحتياجات الناشئة في مجال تكنولوجيات وخدمات الاتصالات.

وما فتئت صناعة الاتصالات تشهد مرحلة نمو مذهل في خدمات الطرف الثالث الموثوق به. ويتسم أمن خدمات التطبيقات القائمة على الاتصالات، بما فيها خدمات الشبكات الاجتماعية والخدمات من الند إلى الند وخدمات الطرف الثالث الموثوق به، بأهمية حاسمة للمضي في تطوير صناعة الاتصالات. وتؤدي بروتوكولات تطبيقات الأمن دوراً حرجاً جداً في توفير خدمات التطبيقات الآمنة. ويشكل تقييس أفضل الحلول الأمنية الشاملة أمراً حيوياً للصناعة ومشغلي الشبكات ومقدمي الخدمات الذين يعملون في بيئة دولية متعددة البائعين. ويلزم أيضاً دراسة وتطوير أنواع أخرى من خدمات التطبيقات الأمنية مثل خدمات خاتم التوقيت وخدمات الموثق العمومي المأمونة والخدمات المالية الرقمية (الدفع الإلكتروني، الصيرفة الإلكترونية، التجارة الإلكترونية) المأمونة وخدمات تحليل البيانات وخدمات تقصي البرمجيات الخبيثة والتصدي لها، بما في ذلك تحليل سلوك البرمجيات الخبيثة في بيئات مُحكمة، واستخدام تأكيدات الأمن كبديل عوضاً عن استخدام الشهادات في البروتوكولات القائمة على البنية التحتية للمفاتيح العمومية (PKI) وخدمات تطبيقات البنية التحتية للمفاتيح العمومية، وغير ذلك. وأصبحت تكنولوجيات الأمن، مثل تأكيد الأمن وتأكيد التحكم في النفاذ، ذات أهمية بالغة في شبكات الاتصالات.

وتشمل التوصيات التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 23 مارس 2016 ما يلي: X.1141 وX.1142 وX.1143 وX.1144 وX.1151 وX.1152 وX.1153 وX.1154 وX.1155 وX.1156 وX.1157 وX.1158 وX.1159 وX.1161 وX.1162 وX.1163 وX.1164 والإضافات X.Suppl.17 و X.Suppl.21 وX.Suppl.22.

النصوص قيد الإعداد: X.websec-6 وX.websec-7 وX.websec-8.

### 2 المسألة

تتناول الدراسة البنود التالية دون أن تقتصر عليها:

 ﺃ ) كيف ينبغي تحديد المخاطر التي تتهدد خدمات التطبيقات المأمونة ومعالجتها؟

ﺏ) ما هي التقنيات الأمنية اللازمة لخدمات التطبيقات المأمونة؟

ﺝ) كيف ينبغي الحفاظ على التوصيلية البينية المأمونة وصونها؟

ﺩ ) ما هي التقنيات أو البروتوكولات الأمنية اللازمة لخدمات التطبيقات المأمونة؟

ﻫ ) ما هي التقنيات أو البروتوكولات الأمنية اللازمة لخدمات التطبيقات المأمونة الناشئة؟

ﻭ ) ما هي الحلول العالمية لخدمات التطبيقات المأمونة وما هي تطبيقاتها؟

### 3 المهام

تشمل المهام البنود التالية دون أن تقتصر عليها:

 ﺃ ) القيام، بالتعاون مع لجان الدراسات الأخرى لقطاع تقييس الاتصالات ومنظمات وضع المعايير، ولا سيما المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SC 27)، بوضع مجموعة شاملة من التوصيات لتوفير حلول أمنية شاملة لخدمات التطبيقات المأمونة.

ﺏ) استعراض التوصيات/المعايير القائمة لدى قطاع تقييس الاتصالات والهيئة ISO/IEC في مجال خدمات التطبيقات المأمونة.

ﺝ) المضي في الدراسة لتحديد الجوانب الأمنية لخدمات التطبيقات المأمونة وللخدمات الجديدة الناشئة.

ﺩ ) دراسة وتطوير المسائل والمخاطر الأمنية في خدمات التطبيقات المأمونة.

ﻫ ) دراسة وتطوير الآليات الأمنية من أجل خدمات التطبيقات المأمونة.

### 4 الروابط

**التوصيات:**

• سلسلة التوصيات X.800 والتوصيات الأخرى ذات الصلة بالأمن

**المسائل:**

• المسائل A/17 وB/17 وC/17 وD/17 وE/17 وF/17 وH/17 وI/17 وJ/17 وK/17 و7/13 و13/16 لقطاع تقييس الاتصالات

**لجان الدراسات:**

• لجان الدراسات 2 و9 و11 و13 و16 و20 لقطاع تقييس الاتصالات

**هيئات التقييس:**

• فريق مهام هندسة الإنترنت (IETF)؛ المعهد الأوروبي لتقييس الاتصالات (ETSI)؛ جمعية النظام العالمي للاتصالات المتنقلة (GSMA)؛ اللجنة الخاصة 27 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SC 27)؛ المنظمة الدولية للتوحيد القياسي/اللجنة التقنية 68 (ISO/TC 68)؛ مبادرة قنطرةKantara ؛ منظمة النهوض بمعايير المعلومات المنظمة (OASIS)؛ الاتحاد المفتوح للاتصالات المتنقلة (OMA)؛ اتحاد شبكة الويب العالمية (W3C)

**هيئات أخرى:**

• المجلس الأوروبي (COE)؛ الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA)؛ تحالف الهوية السريعة على شبكة الإنترنت (FIDO)؛ الشراكة العالمية المتعددة الأطراف لمكافحة الإرهاب السيبراني (IMPACT).

مشروع المسألة H/17

أمن الحوسبة السحابية

(استمرار المسألة 8/17)

### 1 الدوافع

الحوسبة السحابية عبارة عن نموذج لتمكين مستعمل الشبكة من النفاذ الشبكي من كل مكان وفي أي وقت بسهولة وعند الحاجة إلى مجموعة مشتركة من موارد الحوسبة القابلة للتشكيل (مثل الشبكات والمخدمات والتخزين والتطبيقات والخدمات)، التي يمكن توفيرها وتسليمها بسرعة مع أدنى حد من الجهد الإداري أو التدخل من جانب مورّد الخدمة. ويتألف نموذج الحوسبة السحابية من خمس خصائص أساسية (الخدمة بناءً على الطلب والتسليم عبر نفاذ شبكي واسع وتجميع الموارد وسرعة المرونة والخدمات الذاتية والمقيسة)، وخمس فئات لخدمة الحوسبة السحابية أي البرمجيات كخدمة (SaaS) والاتصال كخدمة (CaaS) والمنصات كخدمة (PaaS) والبنية التحتية كخدمة (IaaS) والشبكات كخدمة (NaaS) ونماذج النشر المختلفة (العامة والخاصة والهجينة...). وقد أدى ظهور نهج الحوسبة السحابية، بوصفه الأداة المفضلة للاكتشاف وإخراج البيانات والتركيب وإعادة استعمال الخدمة في إطار سير العمل والتطبيقات المدعومة بالاتصالات، إلى التأكيد من جديد على الحاجة إلى الأمن.

وتشمل الفوائد المتوقعة من الحوسبة السحابية توفير موارد مرنة ودينامية وإدارة أكثر بساطة وتلقائية للبنية التحتية لتكنولوجيا المعلومات. وتمكن التقنية الافتراضية من تقاسم موارد غير محدودة تقريباً، مع تحسينات في التوسعية وتخفيضات هائلة في تكاليف إدارة البنية التحتية. ومع ذلك، تثير الأنظمة المفتوحة وتقاسم الموارد في إطار نظام الحوسبة السحابية العديد من المخاوف المتعلقة بالأمن وربما كان ذلك أهم حاجز يحول دون اعتماد الحوسبة السحابية. فالانتقال إلى الحوسبة السحابية ينطوي على التحول من أنظمة تكنولوجيا المعلومات التقليدية الداخلية والآمنة إلى بنى تحتية مفتوحة "محوسبة سحابياً" وغير آمنة. وبالتالي فإنه يتطلب إعادة التفكير المتعمق في مسألة الأمن.

واعتبرت الحوسبة السحابية لعدة سنوات بمثابة تكنولوجيا معلومات تركز على الخدمة وتسيطر عليها الجهات الفاعلة المعنية بشبكة الإنترنت. ومع ذلك، بإمكان الجهات الفاعلة في مجال الاتصالات أداء دور هام في سوق الحوسبة السحابية الناشئة وبيئتها. وبما أن الخدمات السحابية تتاح من خلال شبكات الاتصالات، فإنه ينبغي على الجهات الفاعلة في مجال الاتصالات كفالة مستوى عال من الضمان. ومن شأن إتاحة حماية قوية ولكنها مرنة أن تكون داعماً رئيسياً لمجمل سوق الحوسبة السحابية وبيئتها.

وبالإضافة إلى ذلك، سوف تمكن المرونة في استخدام الموارد الغنية في بيئات الحوسبة السحابية من إتاحة خدمات أمنية جديدة لا يمكن لآليات الدفاع الحالية توفيرها (خدمات مكافحة البرمجيات الخبيثة كخدمة سحابية، على سبيل المثال). وبالتالي، هناك حاجة إلى دراسة ما يمكن للحوسبة السحابية أن تقدمه من أنواع التدابير الأمنية في المستقبل القريب.

وتوفر التوصيات ITU-T X.1601 وX.1602 وX.1631 مجموعة من التوصيات بشأن الخدمات الأمنية لإتاحة خدمات تتعلق بالوضع العام لأمن الحوسبة السحابية والمعمارية والإطار وأمن الحوسبة السحابية عبر الطبقات وأمن خدمات الشبكات خصوصاً. وتوجد حالياً حاجة ماسة لتأمين الخدمات التي تدعمها الحوسبة السحابية ومنها خدمات الصوت والوسائط المتعددة والخدمات القائمة على الهوية وخدمات ضمان المعلومات وخدمات الهوية والبيانات والخدمات في حالات الطوارئ. وتهدف هذه المسألة إلى بلورة توصيات جديدة تستند إلى الجزء 5 من التقرير التقني للفريق المتخصص المعني بالحوسبة السحابية من أجل ما يلي:

• وضع أفضل الممارسات والمبادئ التوجيهية للاسترشاد بها في كيفية توفير الأمن في بيئة قائمة على الحوسبة السحابية؛

• توضيح المسؤولية وتعريف متطلبات الأمن وتحديد التهديدات الأمنية لفائدة الجهات الفاعلة الرئيسية وأدوارها ذات الصلة في بيئة الحوسبة السحابية؛

• معمارية أمنية قائمة على أساس المعمارية المرجعية الواردة في المسألة 18/13؛

• إدارة الأمن وتكنولوجيا التدقيق من أجل إدارة المسائل المتعلقة بالثقة.

وسوف تتعاون المسألة H/17 مع المسائل ذات الصلة مثل B/17 وC/17 وD/17 وG/17 وJ/17 وK/17 لوضع توصيات بشأن أمن الحوسبة السحابية.

التوصيات التي تندرج ضمن مسؤولية هذه المسألة اعتباراً من 23 مارس 2016: X.1601 وX.1602 وX.1631 وX.1642.

النصوص قيد الإعداد: X.1641 (X.CSCDataSec) وX.dsms وX.SRIaaS.

### 2 المسألة

تشمل الدراسة البنود التالية دون أن تقتصر عليها:

 ﺃ ) ما هي التوصيات الجديدة أو الأنواع الأخرى من الوثائق التي ينبغي وضعها لتستفيد منها الجهات الفاعلة الرئيسية مثل مقدمي الخدمات ومستعملي الخدمات والشركاء في الخدمات وغيرهم من أصحاب المصلحة الرئيسية في دوائر صناعة الاتصالات لتعزيز أمن الحوسبة السحابية؟

ﺏ) ما هي التوصيات الجديدة التي ينبغي وضعها بشأن معمارية الأمن وتنظيم الوظائف الأمنية وفقاً للمعمارية المرجعية؟

ﺝ) ما هي التوصيات الجديدة التي ينبغي وضعها بشأن آليات الضمان وتكنولوجيات التدقيق وما يرتبط بها من تقدير المخاطر لبناء الثقة بين مختلف الجهات الفاعلة؟

ﺩ ) ما هو مجال التعاون اللازم للحد من ازدواجية الجهود مع المسائل الأخرى ولجان الدراسات ومنظمات وضع المعايير؟

ﻫ ) كيف ينبغي تطوير الأمن كخدمة لحماية أنظمة الاتصالات/تكنولوجيا المعلومات والاتصالات؟

### 3 المهـام

تشمل المهام البنود التالية دون أن تقتصر عليها:

 ﺃ ) وضع توصيات أو أي نوع آخر من الوثائق لتعزيز أمن الحوسبة السحابية.

ﺏ) وضع توصيات لتحديد المتطلبات الأمنية والتهديدات الأمنية من أجل تأمين خدمات الحوسبة السحابية على أساس المتطلبات العامة للحوسبة السحابية التي تحددها لجنة الدراسات 13 لقطاع تقييس الاتصالات.

ﺝ) وضع توصيات لتحديد معمارية إدارة الأمن وتنظيم الوظائف الأمنية على أساس المعمارية المرجعية التي تحددها لجنة الدراسات 13 لقطاع تقييس الاتصالات.

ﺩ ) وضع توصيات لتحديد معمارية قوية ومرنة للأمن وتنفيذه لأنظمة الحوسبة السحابية.

ﻫ ) وضع توصيات لتحديد آليات الضمان وتكنولوجيات التدقيق وتقييم المخاطر وذلك بهدف التوصل إلى إقامة علاقات ثقة داخل بيئة الحوسبة السحابية.

ﻭ ) الاضطلاع بجميع الأنشطة المتعلقة بأمن الحوسبة السحابية في إطار لجنة الدراسات 17.

ﺯ ) تمثيل لجنة الدراسات 17 فيما يتعلق بعملها المعني بأمن الحوسبة السحابية، في إطار نشاط التنسيق المشترك المعني بالحوسبة السحابية.

### 4 الروابط

التوصيات:

• توصيات السلسلة Y بشأن الحوسبة السحابية

**المسائل:**

• المسائل A/17 وB/17 وC/17 وD/17 وG/17 وJ/17 وK/17 لقطاع تقييس الاتصالات

**لجان الدراسات:**

• لجان الدراسات 2 و13 و16 و20 لقطاع تقييس الاتصالات

**هيئات التقييس:**

• فريق مهام هندسة الإنترنت (IETF)؛ اللجنة الخاصة 27 واللجنة الخاصة 38 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1)؛ منظمة النهوض بمعايير المعلومات المنظمة (OASIS)؛ وغيرها من الهيئات المعنية التي يجري تحديدها

**هيئات أخرى:**

• التحالف المعني بأمن الحوسبة السحابية (CSA)؛ فريق مهام إدارة سطح المكتب (DMTF).

مشروع المسألة I/17

القياسات الحيوية في الاتصالات

(استمرار المسألة 9/17)

### 1 الدوافع

هيأت المسألة 9/17، أثناء فترة الدراسة السابقة، الظروف لاستخدام القياسات الحيوية في تطبيقات الاتصالات ووفرت التوصيات اللازمة في هذا الشأن. وبالنظر إلى أن القياس الحيوي أصبح مقبولاً على نطاق واسع في عملية التحقق من الهوية في تطبيقات من قبيل التجارة الإلكترونية والصحة الإلكترونية، فلقد شكلت أنظمة تطبيق القياسات الحيوية تحديات شتى تتعلق بحماية الخصوصية وضمان الموثوقية وأمن بيانات القياسات الحيوية في تطبيقات السلامة الحيوية والأمن الحيوي. وتزداد هذه التحديات تعقيداً وصعوبة لدى اعتماد الاستيقان بالقياس الحيوي في بيئة الشبكات المفتوحة.

وفي الوقت الراهن، تتطلب تطبيقات الاتصالات التي تستخدم المطاريف المتنقلة وخدمات الإنترنت أساليب استيقان لا توفر درجة عالية من الأمن فحسب بل توفر أيضاً بيئة مريحة للمستعملين. ومن الأمثلة على هذه التطبيقات الناشئة ’الصيرفة على الخط‘ باستعمال هاتف متنقل ورقابة فيديوية باستعمال كاميرات الشبكات أو التلفزيون بدارة مغلقة (CCTV)، حيث من المتوقع أن يفي الاستيقان عن طريق القياس الحيوي بهذه المتطلبات. ولذا من الضروري تحديد المتطلبات المتصلة باستخدام التوصيات المتعلقة بالأمن والسلامة وحماية الخصوصية. وعلاوة على ذلك، من المطلوب معالجة مسائل مثل اختبار التوافق وقابلية التشغيل البيني للتوصيات، فضلاً عن تموين قاعدة بيانات القياسات الحيوية في الاتصالات.

وتشمل التوصيات التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 23 مارس 2016 ما يلي: X.1080.1 وX.1081 وX.1082 وX.1083 وX.1084 وX.1086 وX.1088 وX.1089 وX.1090 وX.1091 وX.1092.

النصوص قيد الإعداد: X.bhsm و X.pbact وX.tam وX.th2 وX.th3 وX.th4 وX.th5 وX.th6 وX.th13.

### 2 المسألة

تتناول الدراسة البنود التالية دون أن تقتصر عليها:

 ﺃ ) كيف يمكن تحسين أو مراجعة التوصيات الحالية من أجل نشرها واستعمالها على نطاق واسع؟

ﺏ) ما هي متطلبات الاستيقان بالقياس الحيوي في شبكة على درجة عالية من الخصائص الوظيفية مثل شبكات الجيل التالي؟

ﺝ) كيف ينبغي تقييم التدابير المضادة للأمن بالنسبة لتطبيقات معينة من تطبيقات القياسات الحيوية في الاتصالات؟

ﺩ ) كيف ينبغي تصميم أنظمة القياسات الحيوية وعملياتها لكي تكون متماشية مع المتطلبات الأمنية لأي تطبيق من تطبيقات القياسات الحيوية في الاتصالات بما في ذلك خدمات الحوسبة السحابية؟

ﻫ ) كيف يمكن تحسين التعرف على هوية المستعملين واستيقانها في جوانب السلامة والأمن عن طريق استعمال نماذج قابلة للتشغيل البيني لطرائق القياس الحيوي في الاتصالات؟

ﻭ ) ما هي الآليات التي يلزم دعمها لضمان التعامل الذي يتسم بالسلامة والأمن لبيانات القياسات الحيوية في أي من تطبيقات القياس الحيوي في الاتصالات، سواء الحالية أو الناشئة، مثل الصحة الإلكترونية والطب عن بُعد والتجارة الإلكترونية والصيرفة على الخط والرقابة الفيديوية؟

### 3 المهام

تشمل المهام البنود التالية دون أن تقتصر عليها:

 ﺃ ) تحسين ومراجعة التوصيات الراهنة للاستيقان بالقياس الحيوي في الاتصالات وتموين قاعدة بيانات القياسات الحيوية في الاتصالات.

ﺏ) استعراض أوجه التشابه والتباين بين التوصيات القائمة المتعلقة بالقياس الحيوي في الاتصالات في قطاع تقييس الاتصالات في الاتحاد والمعايير في المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC).

ﺝ) دراسة ووضع المتطلبات والمبادئ التوجيهية المتعلقة بالأمن لأي تطبيق يتعلق بالقياسات الحيوية في الاتصالات يستعمل المعماريات والأطر بما فيها تلك الموضوعة في إطار المسألة B/17.

ﺩ ) دراسة ووضع المتطلبات المتعلقة بتقييم الأمن والتوافق وقابلية التشغيل البيني في إطار أساليب حماية الخصوصية بالنسبة لأي من تطبيقات القياسات الحيوية في الاتصالات.

ﻫ ) دراسة ووضع المتطلبات المتعلقة بتطبيقات القياسات الحيوية في الاتصالات في الشبكات التي تتمتع بدرجة عالية من الخصائص الوظيفية.

ﻭ ) دراسة ووضع الأطر المتكاملة والمتطلبات اللازمة لمعماريات القياس الحيوي في الاتصالات من أجل بيئات الحوسبة السحابية وتخزين البيانات.

ﺯ ) دراسة ووضع المتطلبات اللازمة للاستيقان بالقياس الحيوي في الاتصالات من أجل إطار الهوية الموثوق بها.

ﺡ) دراسة ووضع المتطلبات اللازمة لوضع بروتوكولات نوعية ملائمة توفر السلامة والأمن وحماية الخصوصية والموافقة "على معاملة بيانات القياسات الحيوية" في أي من تطبيقات القياس الحيوي في الاتصالات، مثل الصحة الإلكترونية والطب عن بُعد والتجارة الإلكترونية والصيرفة على الخط والدفع الإلكتروني والرقابة الفيديوية.

ط) دراسة ووضع بروتوكولات البيولوجيا إلى الآلة (B2M) لإرسال مقاييس بيولوجية تعمل بينياً مع بروتوكولات الآلة إلى الآلة (M2M).

ي) دراسة ووضع تطبيقات القياسات الحيوية في الاتصالات باستخدام إشارات حيوية في التطبيقات لأغراض تشمل، على سبيل الذكر لا الحصر، الاستيقان وتحديد الهوية ومراقبة المعلومات الصحية.

ك) دراسة ووضع بروتوكول الاتصالات الحيوية المجسمة.

### 4 الروابط

التوصيات:

• X.200 وX.273 وX.274 وX.509 وX.680 وX.805 وX.1051

المسائل:

• A/17 وB/17 وC/17 وD/17 وE/17 وF/17 وG/17 وH/17 وJ/17 وK/17 و7/13 و14/15 لقطاع تقييس الاتصالات

لجان الدراسات:

• لجنة الدراسات 2 لقطاع تنمية الاتصالات ولجنة الدراسات 7 لقطاع الاتصالات الراديوية ولجان الدراسات 2 و5 و9 و11 و13 و15 و16 لقطاع تقييس الاتصالات

هيئات التقييس:

• اللجنة الكهرتقنية الدولية/اللجنة التقنية 25 (IEC/TC 25)، اللجنة الكهرتقنية الدولية/اللجنة التقنية 25/فريق العمل المشترك 1 (IEC/TC 25/JWG 1)؛ معهد المهندسين الكهربائيين والإلكترونيين (IEEE)؛ فريق مهام هندسة الإنترنت (IETF)؛ اللجان الخاصة 17 و27 و37 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SCs 17, 27 & 37)؛ المنظمة الدولية للتوحيد القياسي/اللجان التقنية 12 و68 و215 (ISO/TCs 12, 68 and 215)؛ المنظمة الدولية للتوحيد القياسي/اللجنة التقنية 12/فريق العمل المشترك 20 (ISO/TC 12/JWG 20)

هيئات أخرى:

• المكتب الدولي للأوزان والمقاييس (BIPM)؛ اللجنة الدولية للوحدات والمقاييس الإشعاعية (ICRU)؛ تحالف الهوية السريعة على شبكة الإنترنت (FIDO)؛ منظمة العمل الدولية (ILO)؛ منظمة الصحة العالمية (WHO).

مشروع المسألة J/17

معمارية وآليات إدارة الهوية

(استمرار المسألة 10/17)

### 1 الدوافع

إدارة الهوية (IdM) هي إدارة دورة الحياة واستخدام (بمعنى استحداث وحفظ واستخدام وتزويد وإلغاء) وثائق الإثبات ومعرّفات الهوية والنعوت والاستيقان والشهادة والأنماط التي تعرف بها الكيانات (مثل مقدمي الخدمات والمستعملين النهائيين والشبكات الاجتماعية والمنظمات وأجهزة الشبكات والتطبيقات والخدمات) بمستوى ما من الثقة. ووفقاً للسياق، يمكن لكيان وحيد أن يتخذ هويات متعددة بمتطلبات أمنية متباينة وفي مواقع متعددة. وتناقش عملية إدارة الهوية، في الشبكات السحابية والعامة، تبادل المعلومات الموثوق بها بين الكيانات المأذون لها على أساس التحقق من الهويات وتأكيدها عبر أنظمة موزعة. وتتيح عملية إدارة الهوية حماية المعلومات وتكفل اقتصار النشر على المعلومات المأذون بها. وإدارة الهوية عنصر رئيسي في العمليات الملائمة في شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات، (من قبيل إنترنت الأشياء (IoT) والحوسبة السحابية والمتنقلة والخدمات والمنتجات)، لأنها تدعم إقامة وصيانة الاتصالات الموثوق بها. وهذه العملية لا تدعم استيقان هوية كيان معين فحسب وإنما تسمح أيضاً بترخيص الامتيازات وتسهل من تغيير الامتيازات إذا طرأ تغيير على الدور الذي يقوم به الكيان، كما أنها تتيح إمكانية التفويض والترحال وغير ذلك من الخدمات الهامة القائمة على الهوية.

وإدارة الهوية عنصر حاسم الأهمية في إدارة أمن الشبكات وتمكين النفاذ، من خلال خدمات الترحال والخدمات بناءً على الطلب، إلى الشبكات وإلى الخدمات الإلكترونية التي يتوقعها اليوم المستعملون النهائيون. وتساعد عملية إدارة الهوية، إلى جانب الآليات الدفاعية الأخرى، على منع الاحتيال وسرقة الهوية ومن ثم فإنها تزيد من ثقة المستعملين في أمن وموثوقية المعاملات الإلكترونية، (من قبيل أنظمة إنترنت الأشياء (IoT) والحوسبة السحابية والمتنقلة التي لا تتحكم فيها مباشرة منظمة المستعمل).

وستكون هناك مواصفات وحلول وطنية/إقليمية محددة بشأن إدارة الهوية، وستواصل هذه المواصفات والحلول تطورها. ومن الأهمية بمكان، بالنسبة إلى الاتصالات العالمية، تحقيق الاتساق بين مختلف المناهج الوطنية/الإقليمية لإدارة الهوية والمواصفات والحلول المتباينة المتعلقة بها. وتحقيقاً لهذا الهدف، يحتاج الأمر إلى وضع معايير في مجال إدارة الهوية تستخدم بيئات تراعي المطور وتشجع التطوير على نطاق واسع للتطبيقات والأدوات باستخدام مختلف تكنولوجيات الويب (من قبيل HTTP وJSON وOAUTH وOpenID Connect).

وهذه المسألة مكرسة لتحديد الرؤية وتنسيق وتنظيم كامل طائفة أنشطة إدارة الهوية المضطلع بها داخل قطاع تقييس الاتصالات. وسوف يستخدم نهج "من القمة إلى أسفل" إزاء موضوع إدارة الهوية بالتعاون مع لجان الدراسات الأخرى والمنظمات والاتحادات الأخرى لوضع المعايير (SDO). ومن المسلم به أن هناك مسائل أخرى ستشارك في جوانب محددة من عملية إدارة الهوية (أي البروتوكولات والمتطلبات ومعرفات تجهيزات الشبكة).

وتشمل التوصيات والإضافات التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 23 مارس 2016 ما يلي: X.1250 وX.1251 وX.1252 وX.1253 وX.1254 وX.1255 وX.1256 وX.1257 وX.1275 والإضافة X.Suppl.7.

النصوص قيد الإعداد: X.1258 (X.eaaa) وX.te.

### 2 المسألة

تتناول الدراسة البنود التالية دون أن تقتصر عليها:

 ﺃ ) ما هي المفاهيم الوظيفية لبنية تحتية موحدة لإدارة الهوية (IdM)؟

ﺏ) ما هو النموذج الملائم لإدارة الهوية الذي يتمتع بالاستقلال عن تكنولوجيات الشبكات ويدعم المشاركة من جانب المستعملين ويشكل تعبيراً عن المعلومات المتصلة بإدارة الهوية ويدعم التبادل المأمون لمعلومات إدارة الهوية بين الكيانات المعنية (أي المستعملين والأطراف الواثقة ومزودي الهوية)؟

ﺝ) ما هي المكونات اللازمة لكي تضم معاً إدارة الهوية في الشبكات الاجتماعية والمتنقلة والمؤسسية بما يعزز سلامة المعاملات الرقمية؟

ﺩ ) ما هي الجوانب الوظيفية لنماذج إدارة الهوية؟

ﻫ ) ما هي المتطلبات المحددة لإدارة الهوية من جانب مقدمي الخدمات ومستهلكيها؟

ﻭ ) ما هي النعوت التي يمكن لمقدمي الهوية أن يتشاركوا بها ضمن أطر الثقة؟

ﺯ ) ما هي المتطلبات والقدرات وربما الاستراتيجيات اللازمة لتحقيق إمكانية التشغيل بين مختلف أنظمة إدارة الهوية (أي ضمان الهوية، التشغيل البيني)؟

ﺡ) ما هي الآليات المرشحة لقابلية التشغيل البيني في مجال إدارة الهوية بما يشمل تحديد وتعريف النماذج المطبقة للتقليل من مسائل قابلية التشغيل البيني؟

ﻁ) ما هي متطلبات وآليات حماية معلومات تعرّف الهوية الشخصية (PII) ومنع الإفصاح عنها؟

ﻱ) ما هي متطلبات حماية أنظمة إدارة الهوية من الهجمات السيبرانية؟

ﻙ) ما هي القدرات في مجال إدارة الهوية التي يمكن استخدامها في مجال مكافحة الهجمات السيبرانية؟

ﻝ) كيف ينبغي إدماج إدارة الهوية في تكنولوجيات الأمن المتقدمة؟

 ﻡ) ما هي المتطلبات الفريدة في مجال إدارة الهوية والمرتبطة بالحوسبة السحابية؟

ﻥ) ما هي المتطلبات الفريدة في مجال إدارة الهوية والمرتبطة بالحوسبة المتنقلة؟

ﺱ) ما هي المتطلبات الفريدة في مجال إدارة الهوية والمرتبطة بمختلف البيئات الموزعة من قبيل إنترنت الأشياء والمواقع السحابية؟

ﻉ) كيف يمكن تضمين تدقيق بيانات الهوية في أنظمة إدارة الهوية؟

ﻑ) كيف يمكن تضمين إدارة بيانات الاعتماد المأمونة في أنظمة إدارة الهوية؟

ﺹ) كيف يمكن تضمين تكنولوجيات الاستيقان في أنظمة إدارة الهوية؟

### 3 المهام

تشمل المهام البنود التالية دون أن تقتصر عليها:

 ﺃ ) تحديد إطار لإدارة الهوية يدعم خصائص نموذج الاكتشاف والسياسة والثقة والاستيقان والترخيص والتأكيدات وإدارة دورة حياة بيانات الاعتماد المطلوبة لإدارة الهوية في بيئات تتطور.

ﺏ) تحديد المفاهيم المعمارية الوظيفية لإدارة الهوية بحيث تشمل تقريب إدارة الهوية بين الشبكات وفيما بين أنظمة إدارة الهوية على أن تؤخذ في الاعتبار تكنولوجيات الأمن المتقدمة.

ﺝ) تحديد المتطلبات (واقتراح الآليات) لتأكيد الهوية، ووضع معايير المقابلة/العمل المتبادل بين مختلف طرائق تأكيد الهوية التي يمكن اعتمادها في شبكات شتى. وفي هذا السياق، يشمل تأكيد الهوية أنماط الهوية والسمعة.

ﺩ ) اقتراح مبادئ توجيهية لقابلية التشغيل بين أنظمة إدارة الهوية.

ﻫ ) توصيف المتطلبات (واقتراح الآليات) لحماية أنظمة إدارة الهوية، بما في ذلك كيفية استخدام قدرات إدارة الهوية كوسيلة يستخدمها مزودو الخدمات في تنسيق وتبادل المعلومات بشأن الهجمات السيبرانية.

ﻭ ) الاحتفاظ بقائمة متجددة لمصطلحات وتعاريف إدارة الهوية وتنسيقها ومواصلة العمل الجاري في هذا الصدد.

ﺯ ) دراسة وتوصيف المخاطر والتهديدات الأمنية المتعلقة بإدارة الهوية.

### 4 الروابط

التوصيات:

• توصيات السلسلتين X وY

المسائل:

• المسائل A/17 وC/17 وD/17 وF/17 وG/17 وH/17 لقطاع تقييس الاتصالات

لجان الدراسات:

• لجنتا الدراسات 1 و2 لقطاع تنمية الاتصالات؛ ولجان الدراسات 2 و3 و11 و13 و16 و20 لقطاع تقييس الاتصالات؛ والفريق الاستشاري لتقييس الاتصالات

هيئات التقييس:

• فريق مهام هندسة الإنترنت (IETF)؛ المعهد الأوروبي لتقييس الاتصالات (ETSI)؛ المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1 SCs 6, 27 & 37)

هيئات أخرى:

• المعهد الوطني للمعايير والتكنولوجيا (NIST)؛ منظمة النهوض بمعايير المعلومات المنظمة (OASIS)؛ مشروع شراكة الجيل الثالث (3GPP)؛ المشروع الثاني لشراكة الجيل الثالث (3GPP2).

مشروع المسألة K/17

التكنولوجيات العامة (كالدليل، البنية التحتية للمفتاح العمومي (PKI)،  
قواعد التركيب المجردة (ASN.1)، معرفات الأشياء) لدعم التطبيقات المأمونة

(استمرار المسألة 11/17)

### 1 الدوافع

تدعم هذه المسألة مواصلة وضع طائفة شتى من التكنولوجيات العامة التي تستخدم على نطاق واسع في دعم التطبيقات المأمونة. وهي تشمل ما يلي:

• خدمات الأدلة (السلسلة X.500)؛

• البنى التحتية للمفاتيح العمومية PKI) - (X.509؛

• البنية التحتية لإدارة الامتيازات PMI) - (X.509؛

• ASN.1 (السلسلتان X.680 وX.690)، معرّفات الأشياء وسلطات تسجيلها (السلسلتان X.660 وX.670)؛

• خدمات الويب السريعة وInfoset السريعة (السلسلة X.890)؛

• الحفاظ على التوصيل البيني للأنظمة المفتوحة (OSI) وعلى التجهيز المفتوح الموزع (ODP).

## 1.1 دوافع العمل بخصوص الأدلة والبنية التحتية للمفاتيح العمومية (PKI) والبنية التحتية لإدارة الامتيازات (PMI)

تتسم توصيات السلسلة ITU-T X.500 بأثر كبير في دوائر صناعة الاتصالات. وهذه التوصيات عبارة عن مكونات رئيسية في تكنولوجيات منشورة على نطاق واسع، مثل البنية التحتية للمفاتيح العمومية (PKI) وبروتوكول النفاذ السريع إلى الدليل (LDAP)، وهي تستعمل في مجالات عديدة، مالية وطبية وقانونية. وعندما يحتاج الأمر إلى خدمات أدلة معززة الأمن، في المجال العسكري مثلاً، فإن توصيات السلسلة X.500 هي الحل الأمثل.

وتوفر التوصية ITU-T X.500 درجة عالية من التحكم في النفاذ وحماية خصوصية البيانات. وهي مواصفة مفتوحة قابلة للتكيف مع العديد من التطبيقات المختلفة. وهي قابلة للتمديد بما يسمح بتلبية متطلبات مقبلة. والبروتوكول LDAP الواسع الاستخدام مبني على نموذج دليل X.500. وقد شملت التوصية ITU-T X.500 مقدرات للتعامل مع البروتوكول LDAP. وتشكل حلول التوصية ITU-T X.500 والبروتوكول LDAP جزءاً هاماً من إدارة الهوية (IdM). ويعمد بائعو الأدلة إلى تسويق حلول الأدلة في هيئة أنظمة لإدارة الهوية. ويمكن تلبية عدد من متطلبات إدارة الهوية وشبكات الجيل التالي (للتطبيقات القائمة على أساس العلامة مثلاً) باستخدام خدمة الأدلة.

وتتسم التوصية ITU-T X.509 بأهمية خاصة، كما تستخدم شهادات المفاتيح العمومية على نطاق واسع. ففي كل دورة تصفح مأمونة تستخدم أمن طبقة النقل (TLS) هنالك شهادة تستخدم لاستيقان مخدم الويب وللاتفاق على مفتاح تجفير يستخدم لحماية المعلومات المتبادلة في تلك الدورة. وتستخدم شهادة المفاتيح العمومية أيضاً لاستيقان وحماية البريد الإلكتروني. وتقوم أعمال فرقة العمل PKIX في إطار الفريقIETF ، ومنتدى تصفح هيئة إصدار الشهادات، والتواقيع الإلكترونية والبنية التحتية (ESI) في إطار المعهد الأوروبي لمعايير الاتصالات (ETSI)، كلها على الأساس الذي أرسي في التوصية ITU‑T X.500.

وتوفر شهادات النعوت طريقة آمنة لنقل الامتيازات ولا سيما في أنظمة إدارة الهوية الاتحادية. وتقوم مواصفات OASIS SAML على أساس شهادات نعوت التوصية ITU-T X.509. وشهادات النعوت مفيدة بصفة خاصة عندما تنسب الامتيازات من جانب سلطات أخرى غير السلطات التي تصدر شهادات المفاتيح العمومية وعندما يتطلب الأمر امتيازات طويلة الأمد وقابلة للاسترجاع، مثل عضويات المجموعات.

وتحتاج توصيات السلسلة ITU-T X.500 إلى أن تتطور لكي تلبي المتطلبات المقبلة بشأن إدارة الهوية وشبكات الجيل التالي واتصالات المجال القريب.

وتحتاج التوصية ITU-T X.509، بالتعاون مع مجموعات أخرى، إلى أن تتطور ويحافظ عليها لكي تعكس التجارب المكتسبة في مجال البنية التحتية للمفاتيح العمومية (PKI) وفي مجال البنية التحتية لإدارة الامتيازات (PMI) وتستفيد منها. وتدعو الحاجة لتعزيز التوصية ITU-T X.509 كي تتناول المتطلبات الجديدة كالاتصالات من آلة إلى آلة وأمن شبكة الكهرباء الذكية وأمن إنترنت الأشياء.

وتشمل التوصيات التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 23 مارس 2016 ما يلي: E.104 (بالاشتراك مع لجنة الدراسات 2)، وE.115 (بالاشتراك مع لجنة الدراسات 2)، وF.500 وF.510 وF.511 وF.515 وX.500 وX.501 وX.509 وX.511 وX.518 وX.519 وX.520 وX.521 وX.525 وX.1341.

النصوص قيد الإعداد: X.pki-em (إقامة البنية التحتية للمفاتيح العمومية وصيانتها) وX.pki-prof (البيانات الوصفية للبنية التحتية للمفاتيح العمومية).

## 2.1 دوافع العمل بشأن قواعد التركيب المجردة رقم واحد (ASN.1)، ومعرّفات الأشياء وسلطات تسجيلها

ستوضع، حسب الحاجة، توصيات إضافية بما يتوافق مع أوجه التقدم في التكنولوجيا، ومتطلبات إضافية من مستعملي قواعد التركيب المجردة رقم واحد (ASN.1)، وقواعد ترميزها، والمتطلبات الإضافية من مستعملي ومزودي سلطات التسجيل لمعرفات الأشياءالدولية.

ولقد ثبت أن قواعد التركيب ASN.1 هي الخيار المفضل لدى الكثير من أفرقة التقييس التابعة لقطاع تقييس الاتصالات، ويواصل الكثير منها إصدار طلبات تدعو لإزالة حالات اللبس وعدم الوضوح في الإضافات والتعديلات الأحدث عهداً التي أدخلت على تلك التوصيات.

وأثبتت معرّفات الأشياء(OID) أنها أصبحت مكاناً أثيراً لتحديد الأسماء على نحو يقوم أساساً على هيكل متشعب لهيئات التسجيل التراتبية التي تعرف هويتها بقيمة صحيحة. ويلقى التوسيع الحديث العهد لمعرفات الأشياء الدولية، على نحو يسمح بتحديد الأقواس المعرفة ببطاقات Unicode موحدة الترميز، أيضاً الطلب من أجل مختلف التطبيقات والتوزيعات، ومن المحتمل أن يسفر عن متطلبات تلتمس زيادة تطويرها وتوسيع نطاقها.

وهناك حاجة متواصلة إلى توفير المشورة والمساعدة إلى لجان الدراسات الأخرى والمنظمات الخارجية لوضع المعايير (SDO) والبلدان، ليس بشأن المسائل المتصلة بقواعد ASN.1 فحسب وإنما وبصورة متزايدة بشأن إدارة أماكن أسماء معرفات الأشياء. ومن المتوقع أن تزداد الحاجة إلى المساعدة والمشورة مع إدخال نظام معرفات الأشياء الدولية وزيادة استخدام هيئات التسجيل القطرية من جانب البلدان النامية. ولذلك فإن هناك حاجة متواصلة إلى "مشروع معرفات الأشياء" الذي يضطلع به قطاع تقييس الاتصالات وتعيين رئيس للمشروع لتوفير هذه المشورة والمساعدة.

ويتعين التنسيق مع لجنة الدراسات 2 لقطاع تقييس الاتصالات بشأن تطوير أي استعمال مبتكر لمعرفات الأشياء.

وتشمل التوصيات التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 23 مارس 2016 ما يلي: X.660 وX.662 وX.665 وX.666 وX.667 وX.668 وX.669 وX.670 وX.671 وX.672 و X.674 و X.675 وX.680 وX.681 وX.682 وX.683 وX.690 وX.691 وX.692 وX.693 وX.694 وX.695 و X.696 وX.891 وX.892 وX.893.

النصوص قيد الإعداد: X.894 (X.cms) وX.jsoner وX.oid-iot (مبادئ توجيهية لاستخدام معرفات الأشياء في إنترنت الأشياء)، و X.oiddev (تكنولوجيا المعلومات – استخدام معرفات الأشياء للتعرف على الأجهزة في إنترنت الأشياء)، وX.cms (قواعد تركيب الرسالة التجفيرية).

## 3.1 دوافع العمل بشأن الحفاظ على التوصيل البيني للأنظمة المفتوحة (OSI)

يمكن تنفيذ الأنظمة القائمة على هذه التوصيات المتعلقة بالتوصيل البيني للأنظمة المفتوحة على مدى فترة طويلة نسبياً. وقد تؤدي التجارب العملية في مجال الأنظمة المنفذة استناداً إلى هذه التوصيات إلى استكشاف أخطاء تقنية أو تحسينات مستصوبة لهذه التوصيات. ولذلك فإن هناك حاجة إلى مواصلة عملية التحديث الجارية حالياً لسلسلة التوصيات X بشأن التوصيل البيني للأنظمة المفتوحة.

وقد تم الانتهاء من الأعمال المتعلقة بالتوصيات الأساسية من أجل التوصيل البيني للأنظمة المفتوحة (OSI).

وتشمل التوصيات التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 23 مارس 2016 ما يلي: F.400 وF.401 وF.410 وF.415 وF.420 وF.421 وF.423 وF.435 وF.440 وF.471 وF.472 و X.200 وX.207 وX.210 وX.211 وX.212 وX.213 وX.214 وX.215 وX.216 وX.217 وX.217bis وX.218 وX.219 وX.220 وX.222 وX.223 وX.224 وX.225 وX.226 وX.227 وX.227bis وX.228 وX.229 وX.233 وX.234 وX.235 وX.236 وX.237 وX.237bis وX.245 وX.246 وX.247 وX.248 وX.249 وX.255 وX.256 وX.257 وX.260 وX.263 وX.264 وX.273 وX.274 وX.281 وX.282 وX.283 وX.284 وX.287 وX.400 وX.402 وX.404 وX.408 وX.411 وX.412 وX.413 وX.419 وX.420 وX.421 وX.435 وX.440 وX.445 وX.446 وX.460 وX.462 وX.467 وX.481 وX.482 وX.483 وX.484 وX.485 وX.486 وX.487 وX.488 وX.610 وX.612 وX.613 وX.614 وX.622 وX.623 وX.625 وX.630 وX.633 وX.634 وX.637 وX.638 وX.639 وX.641 وX.642 وX.650 وX.851 وX.852 وX.853 وX.860 وX.861 وX.862 وX.863 وX.880 وX.881 وX.882.

النصوص قيد الإعداد: لا توجد.

**4.1 دوافع العمل بشأن الحفاظ على التجهيز المفتوح الموزع (ODP)**

ثمة جانب رئيسي في تطوير أنظمة الاتصالات وهو توفر البرمجيات لدعم التجهيز المفتوح الموزع (ODP). ويتطلب توفير هذا التجهيز تقييس النماذج المرجعية والمعماريات والوظائف والسطوح البينية واللغات (السلسلة ITU‑T X.900).

وتشمل التوصيات التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 23 مارس 2016 ما يلي: X.901 وX.902 وX.903 وX.904 وX.906 وX.910 وX.911 وX.920 وX.930 وX.931 وX.950 وX.952 وX.960.

### 2 المسألة

تتناول المسألة البنود التالية دون أن تقتصر عليها:

## 1.2 بنود الدراسة المتصلة بالأعمال الخاصة بالأدلة والبنية التحتية للمفاتيح العمومية (PKI) والبنية التحتية لإدارة الامتيازات (PMI)

فيما يتعلق بخدمات الأدلة:

 ﺃ ) ما الذي يلزم من تعاريف الخدمات الجديدة أو تعديلات في السلسلة F لتحديد مدى إمكانية استخدام القدرات الحالية، وما هي المتطلبات الجديدة في التوصية ITU‑T X.500؟

ﺏ) ما هي التحسينات التي يلزم إدخالها على سلسلة التوصيات E لكي تلبي متطلبات الخدمات الجديدة؟

ﺝ) ما هي التحسينات المطلوب إدخالها على الدليل لدعم المتطلبات الجديدة للبنية التحتية للمفاتيح العمومية (PKI)؟

ﺩ ) ما هي متطلبات الأمن والخصوصية الجديدة فيما يتعلق بمعلومات الدليل؟

ﻫ ) ما هي قواعد التشفير الأخرى للتوصية ITU‑T X.500، مثل لغة التوسيم الموسعة (XML)، التي قد تكون مطلوبة لتعزيز جدوى التوصية ITU‑T X.500؟

ﻭ ) ما هي التحسينات الإضافية المطلوب إدخالها على شهادات المفاتيح العمومية والنعوت بما يتيح استخدامها في بيئات متنوعة، مثل البيئات مقيدة الموارد، وبيئات الاتصالات من آلة إلى آلة والشبكات الكبيرة؟

ﺯ ) ما هي التحسينات الإضافية التي يلزم إدخالها في شهادات المفاتيح العمومية والنعوت لزيادة فائدتها في مجالات من قبيل عمليات القياس الحيوي والاستيقان والتحكم في النفاذ والتجارة الإلكترونية؟

ﺡ) ما هي التغييرات التي يلزم إدخالها على التوصية ITU‑T X.509 لغرض تحديد التحسينات وتقويم أوجه النقص؟

وسيتم القيام بهذا العمل بالتعاون مع المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SC 6) فيما تقوم به من أعمال بشأن توسيع نطاق استعمال النظام ISO/IEC 9594. وسيتواصل التعاون مع فريق مهام هندسة الإنترنت لا سيما في مجالات بروتوكول النفاذ السريع إلى الدليل والبنية التحتية للمفاتيح العمومية.

# 2.2  دراسة البنود المتصلة بالأعمال في مجال قواعد التركيب المجردة رقم واحد (ASN.1) ومعرّفات الأشياء وهيئات التسجيل

 ﺃ ) ما هي التحسينات المطلوب إدخالها على قواعد التركيب المجردة رقم واحد (ASN.1) وقواعد الترميز المرتبطة به لتلبية احتياجات التطبيقات في المستقبل؟

ﺏ) ما هو نشاط التعليم اللازم لدعم استعمال معرفات الأشياء في بيئات متنوعة؟

ﺝ) ما هي هيئات التسجيل الإضافية أو إجراءاتها الإضافية اللازمة لدعم الأعمال المضطلع بها في إطار هذه المسألة وغيرها من المسائل؟

ﺩ ) ما هو التعاون المطلوب، خارج نطاق الاتفاقات الراهنة، مع الهيئات الأخرى التي تصدر عنها معايير قانونية أو فعلية لضمان أن تظل أعمال قطاع تقييس الاتصالات في الاتحاد بشأن قواعد التركيب المجردة رقم واحد ومعرفات الأشياء في طليعة الأعمال المضطلع بها في مجال توفير القواعد لتحديد البروتوكولات ووضع التسميات الواضحة؟

## 3.2  بنود الدراسة المتصلة بالأعمال في مجال الحفاظ على التوصيل البيني للأنظمة المفتوحة (OSI)

 ﺃ ) مواصلة الإبقاء على توصيات معمارية التوصيل البيني للأنظمة المفتوحة وفرادى الطبقات لتوفير أي تحسينات لازمة وتقويم أي أخطاء مبلغ عنها؛

ﺏ) مواصلة الإبقاء على التوصيات المتعلقة بخدمة وأنظمة معالجة الرسائل والنقل الموثوق به والعمليات النائية والالتزام والتوافق والاستعادة ومعالجة المعامَلات، وذلك لغرض أي تحسينات لازمة وتقويم أي أخطاء مبلغ عنها.

ومن المستصوب جداً أن يتم التعاون والاتصال بدرجة وثيقة مع لجان الدراسات الأخرى وسائر الأفرقة الدولية التي تقوم بتنفيذ التوصيل البيني للأنظمة المفتوحة، وذلك لضمان إمكانية تطبيق ما ينجم من توصيات على أوسع نطاق.

وسيجري الاضطلاع بهذا العمل بالتعاون مع اللجنة التقنية المشتركة الأولى للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1) ولجانها الفرعية.

# 4.2  بنود الدراسة المتصلة بالأعمال في مجال الحفاظ على التجهيز المفتوح الموزع (ODP)

مواصلة إدارة التوصيات المعنية بالتجهيز المفتوح الموزع.

ومن المستصوب جداً أن يتم التعاون والاتصال بدرجة وثيقة مع لجان الدراسات الأخرى وسائر الأفرقة الدولية التي تقوم بتنفيذ التجهيز المفتوح الموزع، وذلك لضمان إمكانية تطبيق ما ينجم من توصيات على أوسع نطاق.

وسيجري الاضطلاع بهذا العمل بالتعاون مع المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SC 7/WG 19).

### 3 المهام

تشمل المهام البنود التالية دون أن تقتصر عليها:

### 1.3 المهام المتصلة بالأعمال في مجال الأدلة والبنية التحتية للمفاتيح العمومية (PKI) والبنية التحتية لإدارة الامتيازات (PMI)

 ﺃ ) تحديث الدليل من خلال إعداد تقارير الأخطاء وإدخال التصويبات التقنية.

ﺏ) تحديد متطلبات الدليل الجديدة دعماً للتكنولوجيات الجديدة والراهنة.

ﺝ) وضع الإصدار الثامن من سلسلة التوصيات ITU‑T X.500.

ﺩ ) وضع تحسينات للتوصية ITU-T X.509 وللنصين X.pki-prof وX.pki-em لتلبية المتطلبات الجديدة.

### 2.3 المهام المتصلة بالأعمال في قواعد التركيب المجردة رقم واحد (ASN.1) ومعرفات الأشياء وهيئات التسجيل

 ﺃ ) المراقبة والتقدم في نشر كل الأعمال المتبقية في نهاية فترة الدراسة الأخيرة.

ﺏ) التعاون مع اللجنة ISO/IEC JTC 1 SC 6 في مجالات الاهتمام المشترك.

ﺝ) تحديث سلاسل التوصيات ITU‑T X.660 وX.670 وX.680 وX.690 وX.890 خلال فترة الدراسة استجابة لاحتياجات المستعملين، وإصدار طبعات جديدة عند الاقتضاء.

ﺩ ) القيام، حينما تكون هناك حاجة إلى تحسين نقل البيانات، بمساعدة المسائل الأخرى في جميع لجان الدراسات من أجل توفير نماذج قواعد التركيب المجردة رقم واحد (ASN.1) مكافئة لمخططات لغة التوسيم الموسعة (XML) المعرفة في توصيات قطاع تقييس الاتصالات (سواء الموجودة منها أم التي قيد الإعداد)، ولا سيما في حالات النطاق العريض المنخفض.

ﻫ ) المراقبة والمساعدة في عملية نشر التوصيات الموافق عليها والمعايير الدولية والتصويبات التقنية.

ﻭ ) البت في كل تقارير العيوب في بداية فترة الدراسة (وأي تقارير جديدة تنشأ أثناء فترة الدراسة) والتقدم في التصويبات التقنية حسب الضرورة.

ﺯ ) التأكد من معالجة بيانات الاتصال المتعلقة بترميز قواعد التركيب المجردة رقم 1 (ASN.1) ومعرفات الأشياء على نحو مناسب وحسن التوقيت.

ﺡ) وضع أي برمجيات تعليم أو صفحات ويب من المحتمل أن تساعد مستعملي قواعد التركيب المجردة رقم واحد (ASN.1) أو معرفات الأشياء.

ﻁ) التوصل إلى اتفاق في اللجنة ISO/IEC JTC 1/SC 6 ولجنة الدراسات 17 بشأن أي توزيعات إضافية لمعرفات الأشياء تعتبر ضرورية.

ﻱ) القيام، في إطار مسؤولية رئيس مشروع معرفات الأشياء بما يلي:

- توفير المشورة العامة للمستعملين بشأن معرفات الأشياء؛

- تعزيز استعمال قواعد التركيب المجردة رقم واحد (ASN.1) ومعرفات الأشياء الدولية داخل لجان الدراسات الأخرى والمنظمات الأخرى لوضع المعايير (SDO)؛

- مساعدة البلدان على إنشاء وصيانة هيئات التسجيل الوطنية لمعرفات الأشياء (بما في ذلك معرفات الأشياء الدولية).

### 3.3 المهام المتصلة بالأعمال في مجال الحفاظ على التوصيل البيني للأنظمة المفتوحة (OSI)

أ ) وضع التصويبات أو إدخال التحسينات على التوصيات المتعلقة بالتوصيل البيني للأنظمة المفتوحة، حسب الحاجة، استناداً إلى المساهمات الواردة والبت في أي عيوب مبلغ عنها؛

ب) الإبقاء على الدليل الإرشادي للمنفِّذين في مجال التوصيل البيني للأنظمة المفتوحة.

### 4.3 المهام المتصلة بالأعمال في مجال الحفاظ على التجهيز المفتوح الموزع (ODP)

وضع التصويبات أو إدخال التحسينات على التوصيات المتعلقة بالتجهيز المفتوح الموزع، حسب الحاجة، استناداً إلى المساهمات الواردة والبت في أي عيوب مبلغ عنها.

### 4 الروابط

التوصيات:

• السلسلة H.200 وH.323 والسلسلة H.350 وT.120 والسلاسل X.600-X.609 والسلسلة X.700 والسلاسل X.800-X.849 والسلسلة Z

المسائل:

• جميع مسائل قطاع تقييس الاتصالات المتصلة بالتوصيات الواردة أعلاه

لجان الدراسات:

• لجان الدراسات 2 و4 و11 و13 و16 و20 لقطاع تقييس الاتصالات وجميع لجان الدراسات التي تستخدم ASN.1 أو معرفات الأشياء أو التي تحتاج إليهما

هيئات التقييس:

• الفريق التوجيهي لهندسة الإنترنت (IESG)؛ فريق مهام هندسة الإنترنت (IETF)؛ اللجنة الكهرتقنية الدولية/اللجنة التقنية 57 (IEC/TC 57)؛ المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1 SCs 6, 7, 27 & 31)؛ اللجنتان التقنيتان 68 و204 لدى المنظمة الدولية للتوحيد القياسي؛ منظمة النهوض بمعايير المعلومات المنظمة (OASIS)؛ فريق إدارة الأشياء (OMG)؛ اتحاد شبكة الويب العالمية (W3C)

هيئات أخرى:

• الاتحاد البريدي العالمي (UPU).

مشروع المسألة L/17

اللغات الشكلية لبرمجيات الاتصالات والاختبار

(استمرار المسألة 12/17)

### 1 الدوافع

تدعم هذه المسألة الاستمرار في وضع مجموعة شتى من اللغات الشكلية المستخدمة على نطاق واسع في تصميم أنظمة الاتصالات واختبارها.

واستعمال لغات تصميم أنظمة شكلية في الاتحاد الدولي للاتصالات بغية تحديد المتطلبات والمعمارية وسلوك أنظمة الاتصالات: لغات المتطلبات، ووصف البيانات، ومواصفة السلوك، ولغات الاختبار والتنفيذ. وتستخدم اللغات الشكلية لمجالات الهندسة هذه على نطاق واسع في دوائر صناعة الاتصالات وتدعمها في ذلك أدوات قطاع تقييس الاتصالات والأدوات التجارية. ويمكن تطبيق هذه اللغات جماعياً أو إفرادياً من أجل مواصفة المعايير وتصنيع المنتجات. ولغات تصميم أنظمة الاتحاد ذات الشأن هي:

• ويطبق ترميز متطلبات المستعمل من أجل تحليل الأهداف وتعريف حالات الاستعمال، ولا سيما في المراحل الأولى من التصميم.

• وقد أثبتت قواعد ASN.1 أنها الخيار الأمثل في الترميز لدى العديد من أفرقة التقييس من أجل مواصفة المعلومات التي تمر بين الكيانات وهي تضمن، مع قواعد التشفير التي تصحبها، إمكانية تمرير المعلومات بما يتسم بالوضوح والأمن والكفاءة.

• وتمكن لغة التوصيف والوصف من تحديد سلوك ’التحريض والاستجابة‘ لدى الكيانات، ويمكن دمجها مع توصيف وحدات البيانات في قواعد الترميز ASN.1.

• وهي توفر البيانات الوصفية للغة نمذجة موحدة (UML) من أجل لغة التوصيف والوصف، وتقيد نماذج UML في إطار سلوك محدد على نحو جيد يتجنب التفاوتات الدلالية المتأصلة في معيار (OMG) وفي أجزاء من فريق إدارة الأغراض لا تدعو الحاجة إليها من أجل السلوك الذي تشمله لغة التوصيف والوصف.

• ويمكن وصف ترميز خارطة تتابع الرسائل التي تتيح تتابع الرسائل بين الكيانات ويمكن استعماله أيضاً لتعقب أسلوب سلوك نظام ما.

• ويمكّن الاختبار والإصدار 3 من ترميز التحكم في الاختبار (TTCN-3) من إجراء اختبارات لمعرفة أنظمة الوظيفية وقابلية التشغيل البيني الواجب توصيفها وطواقم الاختبار النوعية الواجب كتابتها. ويُستخدم TTCN-3 في اختبار توصيات قطاع تقييس الاتصالات التي تضعها لجان دراسات تقييس الاتصالات ذات الصلة لا سيما لجنة الدراسات 11، باعتبارها اللجنة الرئيسية المعنية بمواصفات الاختبار واختبار المطابقة وقابلية التشغيل البيني. ويُصدر قطاع تقييس الاتصالات في الاتحاد عدداً كبيراً من التوصيات. وبغية تحقيق قابلية التشغيل البيني، من الضروري أن يكون تنفيذ هذه التوصيات متماشياً مع ما تتضمنه تلك التوصيات.

• وقد استخدمت CHILL – وهي لغة البرمجية في قطاع تقييس الاتصالات – على نطاق واسع في الماضي ولكن نُهجاً بديلة استخدمت في السنوات الأخيرة مثل توليد الشفرة من لغة الوصف والتوصيف.

وتعرِّف التوصيات المندرجة ضمن نطاق هذه المسألة كل لغات تصميم النظام هذه لدى الاتحاد الدولي للاتصالات، إلا لغة ASN.1 (وقواعد التشفير المرتبطة بها).

وفضلاً عن تعريف اللغات، تقدم الوثائق المندرجة ضمن نطاق هذه المسألة توجيهات بشأن تعريف واستخدام وتطبيق لغات (بما فيها لغة ASN.1 إلى حد ما) للجان الدراسات الأخرى، ولمنظمات وضع المعايير الخارجية والبلدان. وتورد التوصيات ITU‑T Z.110 وZ.450 وZ.500 والإضافة Z.Sup1 توجيهات بشأن استخدام وتطبيق اللغات. وترد في التوصيتين ITU‑T Z.111 وZ.119 مبادئ توجيهية بشأن الكيفية التي ينبغي أن تُكتب بها أي توصية لغة جديدة، وهي تُستخدم كمراجع مدرجة في التوصيات الأخرى (ولا سيما سلسلة Z.100 وسلسلة Z.150).

وتشمل التوصيات والإضافات وأدلة المنفذين التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 23 مارس 2016 ما يلي: X.292 وZ.100 وZ.101 وZ.102 وZ.103 وZ.104 وZ.105 وZ.106 وZ.107 وZ.109 وZ.110 وZ.111 وZ.119 وZ.120 وZ.121 وZ.150 وZ.151 وZ.161 وZ.161.1 وZ.161.2 وZ.161.3 وZ.161.4 وZ.161.5 وZ.162 وZ.163 وZ.164 وZ.165 وZ.165.1 وZ.166 وZ.167 وZ.168 وZ.169 وZ.170 وZ.200 وZ.450 وZ.500 وZ.Sup1 وZ.Imp100.

النصوص قيد الإعداد: لا توجد.

### 2 المسألة

تتناول الدراسة البنود التالية دون أن تقتصر عليها:

أ ) ما هي الإدارة اللازمة لتعاريف لغات تصميم النظام القائمة (عدا ASN.1) لدى الاتحاد والمكيفة لكي تلائم متطلبات المستعمل المعاصر والمعماريات والأطر الجديدة الناشئة.

ب) ما هي اللغات الجديدة اللازمة لكي تلائم متطلبات المستعمل المعاصر والمعماريات والأطر الجديدة الناشئة (مثل إنترنت الأشياء) مع أخذ التوصية ITU-T Z.110 في الحسبان؟

### 3 المهام

تشمل المهام البنود التالية دون أن تقتصر عليها:

أ ) إدارة التوصيات المندرجة في إطار مسؤولية هذه المسألة؛

ب) توفير مشورة عامة لمستعملي اللغة (اللغات) والمنهجية (المنهجيات) والإطار (الأطر) من أجل اللغة (اللغات) التي تشملها دراسة المسألة؛

ج) النهوض باستخدام المنهجيات والأطر واللغات التي تشملها دراسة المسألة ضمن لجان دراسات أخرى ومنظمات خارجية لوضع المعايير.

### 4 الروابط

التوصيات:

• السلسلة X.690/X.680

المسائل:

• المسألة K/17؛ وجميع مسائل قطاع تقييس الاتصالات التي تستخدم لغات تصميم أنظمة

لجان الدراسات:

• لجنة الدراسات 11، ولجنة الدراسات الرئيسية المعنية بمواصفات الاختبار، وباختبار المطابقة وقابلية التشغيل البيني، وجميع لجان الدراسات التي تستخدم لغات تصميم أنظمة الاتحاد (خصوصاً لجان الدراسات 2 و11 و13 و16 و20) أو التي تحدد الاختبارات (خصوصاً لجان الدراسات 2 و9 و11 و13 و15 و16 و20)، والفريق الاستشاري لتقييس الاتصالات

لجان الدراسات الأخرى:

نشاط التنسيق المشترك الخاص باختبار المطابقة وقابلية التشغيل البيني (JCA-CIT) في قطاع تقييس الاتصالات

هيئات التقييس:

• المعهد الأوروبي لتقييس الاتصالات (ETSI) (TC MTS)؛ فريق مهام هندسة الإنترنت (IETF)؛ المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1) ولجانها الفرعية التي تستخدم لغات تصميم أنظمة الاتحاد الدولي للاتصالات

هيئات أخرى:

• فريق إدارة الأشياء (OMG)؛ جمعية منتدى لغة المواصفات والوصف.

\_\_\_\_\_\_\_\_\_\_\_