|  |  |
| --- | --- |
| الجمعية العالمية لتقييس الاتصالات (WTSA-20)جنيف، 1-9 مارس 2022 |  |
|  |  |
|  |  |
| الجلسة العامة | الوثيقة 20-A |
|  | ديسمبر 2021 |
|  | الأصل: بالإنكليزية |
|  |
| لجنة الدراسات 17 لقطاع تقييس الاتصالات |
| الأمن |
| تقرير لجنة الدراسات 17 لقطاع تقييس الاتصالاتإلى الجمعية العالمية لتقييس الاتصالات لعام 2020 (WTSA-20):ال‍جـزء الثاني - مسائل تُقترح دراستها في فترة الدراسة 2024‑2022 |
|  |
| **ملخص:** | تتضمن هذه المساهمة تقرير لجنة الدراسات 17 لقطاع تقييس الاتصالات إلى الجمعية العالمية لتقييس الاتصالات لعام 2020 (WTSA-20) بشأن أنشطة لجنة الدراسات في فترة الدراسة 2021-2017. |

|  |  |  |
| --- | --- | --- |
| **للاتصال:** | هونغ يول يومرئيس لجنة الدراسات 17 لقطاع تقييس الاتصالاتجمهورية كوريا | البريد الإلكتروني: hyyoum@sch.ac.kr |

ملاحظة من مكتب تقييس الاتصالات:

يرد تقرير لجنة الدراسات 17 إلى الجمعية العالمية لتقييس الاتصالات لعام 2020 (WTSA‑20) في الوثيقتين التاليتين:

الجـزء الأول: **الوثيقة 19** - اعتبارات عامة

الجـزء الثاني: **الوثيقة 20** - مسائل تُقترح دراستها في فترة الدراسة 2024-2021

مقدمة

تتضمن هذه الوثيقة نصوص المسائل التي وافقت لجنة الدراسات 17 على تقديمها إلى الجمعية العالمية لتقييس الاتصالات لعام 2020.

وترد في الجدول 1 قائمة المسائل وعلاقتها بمجموعة المسائل سارية المفعول التي أقرها الفريق الاستشاري لتقييس الاتصالات في اجتماعه الذي عُقد في الفترة 11-18 يناير 2021.

الجدول 1 – التقابل بين المسائل المقترحة من لجنة الدراسات 17 (مبينة في الجزء الأيمن)
والمسائل السابقة (مبينة في الجزء الأيسر)

| الرقم | العنوان الحالي للمسألة | الحالة | الرقم السابق | العنوان السابق للمسألة |
| --- | --- | --- | --- | --- |
| 1/17 | استراتيجية وتنسيق تقييس الأمن | استمرار | 1/17 | استراتيجية وتنسيق تقييس الأمن |
| 2/17 | معمارية الأمن وأمن الشبكات  | استمرار | 2/17 | معمارية الأمن وأمن الشبكات  |
| 3/17 | إدارة أمن معلومات الاتصالات وخدمات الأمن  | استمرار | 3/17 | إدارة أمن معلومات الاتصالات وخدمات الأمن  |
| 4/17 | الأمن السيبراني ومكافحة الرسائل الاقتحامية  | استمرار | 4/17 | الأمن السيبراني ومكافحة الرسائل الاقتحامية |
| 6/17 | الأمن لخدمات الاتصالات وإنترنت الأشياء  | استمرار | 6/17 | الأمن لخدمات الاتصالات وإنترنت الأشياء |
| 7/17 | خدمات التطبيقات المأمونة  | استمرار | 7/17 | خدمات التطبيقات المأمونة |
| 8/17 | أمن البنية التحتية للحوسبة السحابية والبيانات الضخمة | استمرار | 8/17 | أمن البنية التحتية للحوسبة السحابية والبيانات الضخمة |
| 10/17 | معمارية وآليات إدارة الهوية والقياسات البيومترية عن بُعد | استمرار | 10/17 | معمارية وآليات إدارة الهوية والقياسات البيومترية عن بُعد |
| 11/17 | التكنولوجيات العامة (مثل الدليل، البنية التحتية للمفاتيح العمومية (PKI)، اللغات الشكلية، معرفات الأشياء) لدعم التطبيقات المأمونة | استمرار | 11/17 | التكنولوجيات العامة (مثل الدليل، البنية التحتية للمفاتيح العمومية (PKI)، اللغات الشكلية، معرفات الأشياء) لدعم التطبيقات المأمونة |
| 13/17 | أمن نظام النقل الذكي  | استمرار | 13/17 | أمن نظام النقل الذكي |
| 14/17 | أمن تكنولوجيا السجلات الموزعة (DLT)  | استمرار | 14/17 | أمن تكنولوجيا السجلات الموزعة (DLT) |
| 15/17 | الأمن من أجل/من خلال التكنولوجيات الناشئة بما في ذلك الأمن القائم على التكنولوجيا الكمومية | استمرار | 15/17 | الأمن من أجل/من خلال التكنولوجيات الناشئة بما في ذلك الأمن القائم على التكنولوجيا الكمومية |

نص المسائل

المسألة 1/17

استراتيجية وتنسيق تقييس الأمن

(استمرار للمسألة 1/17)

# 1 المسوغات

لا تزال التهديدات الأمنية للاتصالات وتكنولوجيات المعلومات والاتصالات (ICT) والبنية التحتية معقدة على نحو متزايد. وعلى مر السنين، كانت الجهود التي بذلت لتأمين البنية التحتية مشتتة إلى حد ما وتقوم على أساس رد الفعل، ولم تحقق حتى الآن المستوى المرجو للحماية من تلك التهديدات في أوانها. وما برح التأثير الاقتصادي لمثل هذه الهجمات والتهديدات هائلاً ومكبداً الحكومات والكيانات خسائر مالية وتنظيمية عديدة. وتقتضي مكافحة هذه التهديدات بذل جهود مكثفة ومتواصلة ومركزة.

وهذا الجهد معقد ويتطلب مشاركة عدد كبير من المنظمات العاملة في مختلف جوانب الأمن، كل منها ضمن مجال خبرتها وولايتها. وإذ يتطلب ذلك التنسيق والتآزر والتعاون بين مختلف أصحاب المصلحة، فهو يشكل مهمة صعبة وعسيرة.

وموضوع الأمن شاسع في نطاقه. فالأمن يكاد ينطبق على جميع جوانب الاتصالات وتكنولوجيا المعلومات والشبكات. 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 البيومترية 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.

وتحقق هذه المسألة العديد من النواتج التي يعتبرها قطاع تقييس الاتصالات نواتج أساسية لتعزيز أعماله ونواتجه. وهي تقدم أيضاً موارد قيِّمة للاتحاد والمنظمات الخارجية. ومن الأمثلة على هذه النواتج خارطة طريق معايير الأمن وكتيب الأمن ومجموعة وثائق الأمن والاستخدام الناجح لمعايير الأمن في مجال تكنولوجيا المعلومات والاتصالات. وستبلور هذه المسألة رؤية وستقترح المعمارية التنظيمية للجنة الدراسات 17. 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. وتدعم هذه المسألة أنشطة لجنة الدراسات 17 للتأكد من أنها تعبر عن كفاءة عملية قادرة على وضع معايير اتصالات/تكنولوجيا معلومات واتصالات عالية الجودة في الوقت المناسب ووفق متطلبات السوق. وتتناول هذه المسألة أيضاً احتياجات البلدان النامية والأفرقة الإقليمية التابعة للجان الدراسات من خلال تنفيذ القرار 44 للجمعية العالمية لتقييس الاتصالات بشأن سد الفجوة التقييسية.

وتُعد استراتيجية تقييس الأمن أحد أهم الموضوعات في جميع المسائل لدى لجنة الدراسات 17. وتحتاج لجنة الدراسات 17 إلى النظر في الكيفية التي يمكن بها لمعمارية وتصميم معايير الأمن تحسين تطوير بنود العمل الحالية والمستقبلية في مجال الأمن.

وعمل لجنة الدراسات 17 في مجال الأمن يأخذ بعين الاعتبار قرارات الجمعية العالمية لتقييس الاتصالات 2 و7 و11 و18 و32 و40 و44 و50 و52 و54 و58 و64 و65 و67 و73 و75 و76 و77 و78 و80 و84 و86 و89 و90 و92 و93 و94 و96 و97 و98؛ وقرارات مؤتمر المندوبين المفوضين 101 و123 و130 و136 و174 و177 و178 و179 و181 و188 و189 و197 و199 و200 و201 و204 و205 و206؛ وقرارات المؤتمر العالمي لتنمية الاتصالات 30 و34 و43 و45 و47 و63 و67 و69 و79 و80 و84.

وتدعم لجنة الدراسات 17 أيضاً خط عمل القمة العالمية لمجتمع المعلومات جيم5 "بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات" والهدف 2 من خطة عمل بوينس آيرس التي اعتُمدت في المؤتمر العالمي لتنمية الاتصالات لعام 2017 بشأن "بنية تحتية حديثة وآمنة للاتصالات/تكنولوجيا المعلومات والاتصالات: تعزيز تنمية البنية التحتية والخدمات بما في ذلك بناء الثقة والأمن في استخدام الاتصالات/تكنولوجيا المعلومات والاتصالات".

التقارير التقنية التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 7 يناير 2022: TR.sec-manual وTR.Suss.

النصوص قيد الإعداد: اعتباراً من 7 يناير 2022: X.arch-design.

# 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؟

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

و ) ما هي المراحل الرئيسية ومعايير النجاح ومقاييس الأداء الداعمة؟

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

ح) كيف يمكن أن تصبح الخصائص الأمنية للاتصالات/تكنولوجيا المعلومات والاتصالات أوثق صلة بالأسواق؟

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؟

ك) كيف تمكن تلبية احتياجات البلدان النامية والأفرقة الإقليمية التابعة للجان الدراسات من أجل تنفيذ القرار 44 للجمعية العالمية لتقييس الاتصالات؟

ل) ما هي استراتيجية التقييس لدعم حل أمن الاتصالات الشامل والمتماسك؟

م ) كيف ينبغي أن تشمل استراتيجية التقييس التوصيات القائمة بشأن الأمن؟

# 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) إعداد وصيانة خارطة طريق المعمارية التنظيمية - لتقديم رؤية وخطة مفصلة تحدد مستوى ومجال تطبيق الميدان الأمني للدراسة. ويجب أن تحدد خارطة الطريق جميع المكونات ذات الصلة (الهيكل والعمليات) وعلاقاتها البينية والمنظمات المشاركة وأدوارها. ويتعين التمييز بين الأنظمة/الشبكات الناشئة والأنظمة/الشبكات القائمة.

ج) متابعة خارطة معايير أمن تكنولوجيا المعلومات والاتصالات وتحديثها.

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

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

و ) مواصلة إعداد تقرير تقني عن الاستخدام الناجح للمعايير الأمنية وتحديثه.

ز ) تقديم التوجيهات 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، على سبيل المثال، نماذج أو أدوات أو إجراءات أو مقاييس أداء).

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.

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.

ص) إعداد مجموعة شاملة من وثائق استراتيجية التقييس الأمني، بما في ذلك وثائق المعمارية، لدعم تقييس الحلول الأمنية بالتعاون مع المنظمات الأخرى المعنية بوضع المعايير ولجان دراسات قطاع تقييس الاتصالات الأخرى.

ويرد بيان محدّث لحالة سير العمل في إطار هذه المسألة في برنامج عمل لجنة الدراسات 17 في الموقع:
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

# 4 الروابط

خطوط عمل القمة العالمية لمجتمع المعلومات:

جيم5.

أهداف التنمية المستدامة:

8 (العمل اللائق والنمو الاقتصادي)،
9 (الصناعة والابتكار والبنية التحتية)،
17 (عقد الشراكات لتحقيق الأهداف).

التوصيات:

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

المسائل:

المسائل 2/17 و3/17 و4/17 و6/17 و7/17 و8/17 و10/17 و11/17 و13/17 و14/17 و15/17 لقطاع تقييس الاتصالات.

لجان الدراسات:

لجنتا دراسات قطاع تنمية الاتصالات؛ ولجان دراسات قطاع الاتصالات الراديوية؛ ولجان الدراسات 2 و3 و5 و9 و11 و13 و15 و16 و20 لقطاع تقييس الاتصالات؛ والفريق 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 مهندسي الكهرباء والإلكترونيات (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)؛ ومنظمة تقدم معايير المعلومات المهيكلة (OASIS)؛ مشروع الشراكة لتكنولوجيات الجيل الثالث (3GPP)؛ المشروع الثاني لشراكة الجيل الثالث (3GPP2) وبرنامج التقييس التابع لجماعة آسيا والمحيط الهادئ للاتصالات (ASTAP).

هيئات أخرى:

الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA)؛ المعهد الوطني للمعايير والتكنولوجيا (NIST)؛ مشروع الشراكة العالمية (one M2M)؛ المنتدى الإقليمي لتبادل أمن المعلومات في آسيا (RAISE).

المسألة 2/17

معمارية الأمن وأمن الشبكات

(استمرار للمسألة 2/17)

# 1 المسوغات

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 الصادرة عن قطاع تقييس الاتصالات 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)، والجوانب الأمنية للتوصيل الشبكي ال‍معرَّف بالبرم‍جيات (SDN)/التمثيل الافتراضي لوظائف الشبكة (NFV)، وتقسيم وظائف الشبكة (NS)، وسلسلة وظائف الخدمة (SFC)، وحوسبة الحافة متعددة النفاذ (MEC)، والتطور طويل الأمد/تطور معمارية النظام (LTE/SAE)، وشبكة الاتصالات IMT-2020/5G وما بعدها، وإطار الأمن المشترك ومعمارية الأمن المشتركة للخدمات/التطبيقات، وأسس الذكاء الاصطناعي (AI)/تعلُّم الآلة (ML) في دعم بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، وإرشادات التنفيذ التقني للأنظمة التي تقدم الاتصالات من طرف إلى طرف والشبكات القائمة على بروتوكول الإنترنت) والخدمات المتصلة بها. وينعكس هذا الجهد في التوصيتين X.1035 وX.1036 اللتين تبينان تفاصيل بروتوكولات تبادل المفاتيح المستيقنة بكلمة السر وتوزيع السياسات وإنفاذها، وفي التوصية X.1037 التي تقدم مبادئ توجيهية لأمن الإصدار السادس من بروتوكول الإنترنت (IPv6) والتوصيات X.1038 وX.1042 وX.1043 وX.1044 التي تقدم متطلبات الأمن وما إلى ذلك للتوصيل الشبكي ال‍معرَّف بالبرمجيات (SDN) والتمثيل الافتراضي لوظائف الشبكة (NFV)، والتوصية X.1045 التي تقدم خدمات أمن مخصصة بناءً على سلسلة وظائف الخدمة (SFC).

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 لا تقتصر على تكنولوجيا معينة من أجل حماية طائفة عريضة من الخدمات والتطبيقات. ومن أجل تحقيق هذه الحلول في بيئة متعددة البائعين، ينبغي أن يصمم أمن الشبكات ويُستمثل وفقاً لمعماريات وتكنولوجيات أمن معيارية. وبالنظر إلى تهديدات الأمن التي تتعرض لها بيئة الاتصالات وأوجه التقدم الراهنة في تدابير الأمن المضادة لمواجهة هذه التهديدات، 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 والتطبيقات الناشئة.

وتشمل التوصيات والإضافات التي تندرج في إطار مسؤولية هذه المسألة ما يلي اعتباراً من 7 يناير 2022: 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.1011 وX.1031 و X.1032و X.1033وX.1034 وX.1035 وX.1036 وX.1037 وX.1038 وX.1039 وX.1040 وX.1041 وX.1042 وX.1043 وX.1044 وX.1045 وX.1046 وX.1047 وX.1811 والإضافات X.Suppl.2 و X.Suppl.3و X.Suppl.15و X.Suppl.16وX.Suppl.23 وX.Suppl.30.

النصوص قيد الإعداد اعتباراً من 7 يناير 2022: X.5GSec-ecs و X.5GSec-guideو X.5Gsec-messageو X.5Gsec‑netec وX.5Gsec-ssl و X.5Gsec-t (X.1812) و X.5Gsec-vsو TR.zt-acpوXSTP-5Gsec-RM.

# 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؟

هـ ) 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 7/17؟

و ) ما هي معمارية الأمن الجديدة والتوصيات الإطارية المطلوبة لتقديم 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 تقديم حلول أمنية؟

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

ل) ما هي أسس الذكاء الاصطناعي/تعلُّم الآلة (AI/ML) في دعم بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات؟

م ) ما هي التهديدات والتحديات الأمنية الجديدة التي أدخلتها تكنولوجيات الشبكات الناشئة (من قبيل SDN، وNFV، وتقسيم وظائف الشبكة وSFC وMEC LTE/SAE وشبكة الاتصالات IMT-2020/5G وما بعدها، إلى آخر ذلك)؟

ن) ما هي متطلبات الأمن لشبكة الاتصالات IMT-2020/5G وما بعدها وكيف يمكن للجنة الدراسات 17 معالجتها؟

س) ما هي آليات الأمن المشترَكة لتكنولوجيات الشبكات الناشئة؟

# 3 المهام

تشمل المهام البنود التالية دون أن تقتصر عليها:

 أ ) وضع مجموعة شاملة من معماريات الأمن والتوصيات الإطارية لتقديم 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) دراسات ووضع توصيات بشأن أسس الذكاء الاصطناعي/تعلُّم الآلة دعماً لبناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات.

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

هـ ) دراسات ووضع توصيات بشأن أمن الشبكة المشترَك.

و ) دراسة متطلبات الأمن لشبكة الاتصالات IMT-2020/5G وما بعدها، وتنسيق الأعمال ذات الصلة في مختلف مسائل لجنة الدراسات 17، والقيام بدور جهة الاتصال الوحيدة بشأن الجانب الأمني لشبكة الاتصالات IMT‑2020/5G وما بعدها في لجنة الدراسات 17، وقيادة البحوث ووضع المعايير المتعلقة بالجوانب الأمنية لشبكة الاتصالات IMT-2020/5G وما بعدها.

ويرد بيان محدّث لحالة سير العمل في إطار هذه المسألة في برنامج عمل لجنة الدراسات 17 في الموقع:
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

# 4 الروابط

خطوط عمل القمة العالمية لمجتمع المعلومات:

جيم5.

أهداف التنمية المستدامة:

8 (العمل اللائق والنمو الاقتصادي)،
9 (الصناعة والابتكار والبنية التحتية)،
11 (المدن والمجتمعات المستدامة).

التوصيات:

السلسلة X وغيرها مما يتصل بالأمن.

المسائل:

المسائل 1/17 و3/17 و4/17 و6/17 و7/17 و8/17 و10/17 و11/17 و13/17 و14/17 و15/17 لقطاع تقييس الاتصالات.

لجان الدراسات:

لجنة الدراسات 2 لقطاع تنمية الاتصالات؛ فرقة العمل 6B لقطاع الاتصالات الراديوية؛ لجان الدراسات 2 و9 و11 و13 و15 و16 لقطاع تقييس الاتصالات ونشاط التنسيق المشترك المعني بالاتصالات المتنقلة الدولية-2020 (JCA-IMT2020).

هيئات التقييس:

تحالف حلول صناعة الاتصالات (ATIS)؛ المعهد الأوروبي لتقييس الاتصالات (ETSI)؛ رابطة النظام العالمي للاتصالات المتنقلة (GSMA)؛ 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 TC 12)؛ فريق مهام هندسة الإنترنت (IETF)؛ مشروع شراكة الجيل الثالث (3GPP).

المسألة 3/17

إدارة أمن معلومات الاتصالات وخدمات الأمن

(استمرار للمسألة 3/17)

# 1 المسوغات

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 لتوفير مدونة قواعد ممارسات بشأن ضوابط أمن المعلومات من أجل منظمات الاتصالات.

واستناداً إلى مدونة قواعد الممارسات، طُورت أيضاً مجالات إدارة مفصلة ومحددة، بما فيها المخاطر والأصول والحوكمة وإطار الإدارة والحوادث إلى جانب تقديم أفضل الممارسات كإضافة. 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.

وينبغي، بالتوازي مع وضع التوصيات لمجالات الإدارة المفصلة والمحددة استناداً إلى التوصية ITU‑T X.1051، النظر في المجالات الجديدة لخدمات أمن الاتصالات/تكنولوجيا المعلومات والاتصالات، من قبيل خدمات مركز الدفاع السيبراني (CDC) بما في ذلك خدمات مركز عمليات الأمن (SOC)، وخدمات الأمن المدارة (MSS)، وخدمات أفرقة الاستجابة للحوادث الحاسوبية (CIRT)، وإدارة دورة الحياة لضوابط الأمن والإدارة الفعالة للمخاطر، وإدارة المعلومات التي تحدد الهوية الشخصية التي تتطلب تدابير مضادة طارئة وعالمية. ولا تقتصر هذه المجالات على أمن المعلومات بل تغطي أيضاً جوانباً في الأمن السيبراني. لذلك ينبغي أن تركز الدراسات بصفة خاصة على جوانب الإدارة في المجالات الجديدة المذكورة أعلاه في أمن المعلومات والأمن السيبراني.

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 إنها 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 والإضافات التي تندرج في إطار مسؤولية المسألة اعتباراً من 7 يناير 2022 هي: E.409 (بالاشتراك مع لجنة الدراسات 2) وX.1051 و X.1052 و X.1053وX.1054 وX.1055 و X.1056وX.1057 وX.1058 و X.1059وX.1060 وX.1061 والإضافات X.Suppl.13 وX.Suppl.27 وX.Suppl.32 وX.Suppl.34 وX.Suppl.36.

النصوص قيد الإعداد اعتباراً من 7 يناير 2022: X.1051rev2.

# 2 المسألة

تتناول الدراسة البنود التالية دون أن تقتصر عليها:

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

ب) كيف ينبغي أن يتحدد ويدار قياس إدارة الأمن في الاتصالات؟

ج) كيف ينبغي إجراء تقابل بين أهداف التحكم والضوابط وإدماجها في الإدارة التنظيمية والجوانب التشغيلية في منظمات الاتصالات؟

د ) كيف ينبغي تطبيق المفاهيم والمبادئ الخاصة بإدارة أمن المعلومات، والتي يمكن من خلالها للمنظمات تقييم وتوجيه ومراقبة، والإبلاغ عن، الأنشطة المتعلقة بأمن المعلومات داخل المنظمة؟

هـ ) كيف ينبغي اعتماد خيار معالجة المخاطر لإدارة تأثير حادث أمني؟

و ) كيف ينبغي تطبيق أفضل الممارسات التي تقدم التوجيهات في خدمات الأمن، من قبيل خدمات مركز الدفاع السيبراني (CDC) بما في ذلك خدمات مركز عمليات الأمن (SOC)، وخدمات الأمن المدارة (MSS)، وخدمات أفرقة الاستجابة للحوادث الحاسوبية (CIRT)؟

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

ح) كيف ينبغي تنفيذ وتفعيل إدارة المعلومات المحددة لهوية الأشخاص؟

ط) ما هي التحسينات المطلوب إدخالها على التوصيات القائمة قيد المراجعة أو التوصيات الجديدة قيد الإعداد والتي ينبغي اعتمادها للحد من الأثر الناشئ عن تغير المناخ (من قبيل وفورات الطاقة والحد من انبعاثات غازات الاحتباس الحراري وتنفيذ أنظمة المراقبة) بصورة مباشرة أو غير مباشرة في صناعة الاتصالات/تكنولوجيا المعلومات والاتصالات أو في 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 إطار/مبادئ توجيهية لخدمات الأمن، من قبيل خدمات مركز الدفاع السيبراني (CDC) بما في ذلك خدمات مركز عمليات الأمن (SOC)، وخدمات الأمن المدارة (MSS)، وخدمات أفرقة الاستجابة للحوادث الحاسوبية (CIRT).

د ) دراسة ووضع مبادئ توجيهية لإدارة دورة حياة الضوابط الأمنية.

هـ ) دراسة ووضع مبادئ توجيهية للإدارة الفعالة للمخاطر، مثل معالجة المخاطر بالحصول على التأمين السيبراني للمخاطر.

و ) دراسة ووضع مبادئ توجيهية بشأن حماية المعلومات المحددة لهوية الأشخاص.

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.

ويرد بيان محدّث لحالة سير العمل في إطار هذه المسألة في برنامج عمل لجنة الدراسات 17 في الموقع:
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

# 4 الروابط

خطوط عمل القمة العالمية لمجتمع المعلومات:

جيم5.

أهداف التنمية المستدامة:

8 (العمل اللائق والنمو الاقتصادي)،
9 (الصناعة والابتكار والبنية التحتية).

التوصيات:

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

المسائل:

المسائل 1/17 و2/17 و4/17 و6/17 و7/17 و8/17 و10/17 و11/17 و13/17 و14/17 و15/17 و14/15 لقطاع تقييس الاتصالات.

لجان الدراسات:

لجنتا دراسات قطاع تنمية الاتصالات؛ ولجان دراسات قطاع الاتصالات الراديوية؛ ولجان الدراسات 2 و9 و11 و13 و15 و16 و20 لقطاع تقييس الاتصالات.

هيئات التقييس:

برنامج التقييس التابع لجماعة آسيا والمحيط الهادئ للاتصالات (ASTAP)؛ المعهد الأوروبي لمعايير الاتصالات (ETSI)؛ اللجنة الخاصة 27 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SC 27)؛ اللجنة الخاصة 40 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1 SC40)، اللجنة التقنية 68 التابعة للمنظمة الدولية للتوحيد القياسي (ISO/TC 68)، اللجنة التقنية 215 التابعة للمنظمة الدولية للتوحيد القياسي (ISO/TC 215)؛ اللجنة التقنية 307 التابعة للمنظمة الدولية للتوحيد القياسي (ISO/TC 307)، المعهد الوطني للمعايي‍ر والتكنولوجيا (NIST)؛ لجنة تكنولوجيا الاتصالات (TTC)؛ مشروع شراكة الجيل الثالث (3GPP)؛ ومنتدى أفرقة الاستجابة لحوادث الأمن (FIRST).

المسألة 4/17

الأمن السيبراني ومكافحة الرسائل الاقتحامية

(استمرار للمسألة 4/17)

# 1 المسوغات

يلاحظ أن مشهد الاتصالات في حالة تغير دائب يصحبه في ذلك ما يرتبط به من أمن الاتصالات/تكنولوجيا المعلومات والاتصالات. في هذه البيئة السيبرانية، تستفحل التهديدات والهجمات على الاتصالات/تكنولوجيا المعلومات والاتصالات باستمرار لتصبح أكثر تعقيداً وأكثر استهدافاً وتسبب مجموعة معقدة من المشاكل للمستخدمين ومقدمي الخدمات والمشغلين والشبكات. وتمس الحاجة لتطوير أطر ومتطلبات الأمن السيبراني – أي مجموعة من التوصيات تتضمن أفضل الممارسات لمساعدة المنظمات في إدارة مخاطر الأمن السيبراني.

وتتكون أطر ومتطلبات الأمن السيبراني ضد التهديدات والهجمات من مجموعة من المكونات، ينبغي أن تتكون من التعرف والحماية والكشف والتصدي والتعافي. وتحتاج مواجهة الهجمات السيبرانية بالوسائل التقنية متطلبات شمولية من أجل: تخفيف المخاطر، وكشف الحوادث والتصدي لها مبكراً، والتعافي من آثارها؛ وتبادل معلومات الأمن السيبراني مثل تقنيات تبادل معلومات الأمن السيبراني (CYBEX) ولغة التعبير المهيكل عن معلومات التهديدات (STIX)؛ وتأمين البروتوكولات والبنى التحتية والتطبيقات التي تُستخدم كجزء أساسي من اتصالاتنا اليومية.

ويطبَّق الذكاء الاصطناعي وتعلُّم الآلة على نطاق أوسع عبر الصناعات والتطبيقات أكثر من أي وقت مضى. وينبغي أن تحسِّن الوسائل التقنية المفعَّلة بالذكاء الاصطناعي وتعلُّم الآلة جودة وكفاءة الأنشطة التقنية ضد التهديدات والهجمات. وخدمات الأمن المدارة (MSS) هي خدمات عُهد بها إلى مقدم خدمة خارجي. وهناك جانبان للخدمات الأمنية المدارة: التقني والإداري.

وتتضمن تكنولوجيات الأمن السيبراني دعماً تقنياً لخدمات الأمن المُدارة، وكشف النقطة الطرفية والاستجابة لها، ومنع التسلل/كشفه، وتحديد مصدر المهاجمين من أجل حماية الخدمات والمعلومات الشخصية، بما في ذلك المعلومات المحددة لهوية الأشخاص (PII)، وتوفير ضمان المعلومات (IA) فيما بين الكيانات المتفاعلة.

ويعد تبادل معلومات الأمن السيبراني باستخدام تقنيات تبادل معلومات الأمن السيبراني (CYBEX) والمعلومات الاستخبارية عن التهديدات السيبرانية ضرورياً لحماية البنية التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات ولتعزيز الأمن السيبراني لمقدمي الاتصالات/تكنولوجيا المعلومات والاتصالات.

بالإضافة إلى ذلك، تتطلب الوتيرة الشديدة لتطور التهديدات السيبرانية استعراض الجوانب التقنية لدعم إجراءات الأمن السيبراني وسياساته وأطره التقنية. وهناك تحدٍ يتمثل في تحقيق الحد الأدنى من التنسيق لأن الأمن السيبراني يتطلب التعاون بين جميع أصحاب المصلحة.

وفي مجال تحديات الأمن السيبراني أصبحت الرسائل الاقتحامية مشكلة واسعة الانتشار تتسبب في خسارة محتملة في إيرادات مقدمي خدمات الإنترنت ومشغلي خدمات الاتصالات الثابتة والمتنقلة ومستعملي خدمات الأعمال في شتى بقاع العالم. وعلاوةً على ذلك، تتسبب الرسائل الاقتحامية بمشاكل 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) 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 الممارسات ونشر المعلومات عن طريق ورش العمل، والدورات التدريبية المشتركة، وما إلى ذلك؛ كما تكلف لجنة الدراسات 17 بأن ترفع تقارير منتظمة إلى الفريق الاستشاري لتقييس الاتصالات عن التقدم المحرز في تنفيذ هذا القرار.

ومع التوسع السريع للإنترنت المتنقلة وتقارب تكنولوجيات المعلومات والاتصالات، أصبحت تهديدات الرسائل الاقتحامية أكثر صعوبة بسمات جديدة. وتطورت المكونات الرئيسية للرسائل الاقتحامية كثيراً من الإعلانات والاحتيالات التقليدية إلى البرمجيات الخبيثة المتقاربة مثل برمجيات طلب الفدية والهجمات المستهدفة. وكذلك فإن الجيل الجديد من الرسائل الاقتحامية (SPAM) مع كونه غير مرغوب ويضايق مستهلكي خدمات تكنولوجيا المعلومات والاتصالات، فإنه يلحق أضراراً أخطر من الأضرار التقليدية. وكثيراً ما يستخدم الهجوم المستهدف التصيد الاحتيالي المركَّز، وهو نوع من الهندسة الاجتماعية، للنفاذ إلى الشبكات من خلال وسائل مشروعة مثل البريد الإلكتروني. وبرمجيات طلب الفدية هي نوع من البرمجيات الخبيثة التي تهدد بنشر بيانات الضحية أو تمنع النفاذ إليها تماماً ما لم تُدفع فدية. ويمكن أن تنتشر بعض البرمجيات الخبيثة، وخاصة معظم برمجيات طلب الفدية، من خلال مرفقات البريد الإلكتروني الضارة والمواقع الإلكترونية المخترقة. ومع تطور الذكاء الاصطناعي/تكنولوجيا تعلُّم الآلة (AI/ML)، يمكن بدء بعض الاتصالات بواسطة الآلات وليس البشر، مثل المكالمات الروبوتية والدردشة الروبوتية والرسائل النصية التلقائية وما إلى ذلك. ويمكن لخوارزميات الذكاء الاصطناعي/تعلُّم الآلة أيضاً الاستفادة من المعلومات الشخصية بشكل أدق للعثور على المستلمين المستهدفين للتوجه إليهم برسائل التسويق التجاري الاقتحامية على نطاق واسع أو حتى برسائل اقتحامية احتيالية.

ومع الانتشار الواسع للاتصالات IMT-2020 وإنترنت الأشياء وتكنولوجيات الاتصالات/تكنولوجيا المعلومات والاتصالات الأخرى، بدأت الرسائل الاقتحامية (SPAM) تؤثر تدريجياً على الأنظمة الصناعية.

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 والتقارير التقنية التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 7 يناير 2022 ما يلي: X.1205 وX.1206 وX.1207 وX.1208 وX.1209 وX.1210 وX.1211 وX.1212 وX.1213 وX.1214 وX.1215 وX.1216 وX.1217 وX.1218 وX.1231 وX.1232 وX.1233 وX.1234 وX.1235 وX.1240 وX.1241 وX.1242 وX.1243 وX.1244 وX.1245 وX.1246 وX.1247 وX.1248 وX.1249 وX.1303 وX.1303مكرر وX.1500 وX.1500.1 وX.1520 وX.1521 وX.1524 وX.1525 وX.1526 وX.1528 وX.1528.1 وX.1528.2 وX.1528.3 وX.1528.4 وX.1541 وX.1542 وX.1544 وX.1546 وX.1550 وX.1570 وX.1580 وX.1581 وX.1582، والإضافات X.Suppl.6 وX.Suppl.8 وX.Suppl.9 وX.Suppl.10 وX.Suppl.11 وX.Suppl.12 وX.Suppl.14 وX.Suppl.18 وX.Suppl.20 وX.Suppl.25 وX.Suppl.29، والتقرير التقني TR.usm.

والنصوص قيد الإعداد اعتباراً من 7 يناير 2022 هي: X.1246Amd.1 و X.1247Amd.1و X.arc-evو X.ics-schemaو X.tsfpp وX.Sup-cs-ml.

# 2 المسألة

تشمل بنود الدراسة التي يتعين النظر فيها في سياق شبكات وأنظمة الاتصالات/تكنولوجيا المعلومات والاتصالات ما يلي، على سبيل المثال لا الحصر:

 أ ) كيف ينبغي لمقدمي خدمات الاتصالات/تكنولوجيا المعلومات والاتصالات تأمين بنيتهم التحتية والحفاظ على عمليات مأمونة واستخدام آليات ضمان الأمن؟

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 تناقل المعلومات عن الثغرات الأمنية والضعف وتدابير الهجوم بكفاءة من أجل المساعدة في عمليات دورة حياة الثغرات الأمنية؟

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

هـ ) ما هي المتطلبات والحلول اللازمة من حيث المساءلة والاستجابة للحوادث وخدمات الأمن المُدارة وإسناد الهجمات السيبرانية ورصد التهديدات والإبلاغ عن المخاطر في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات؟

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

ز ) كيف يمكن استخدام الذكاء الاصطناعي وتعلُّم الآلة لتحديد التهديدات ونقاط الضعف الجديدة وتحليلها بسرعة؟

ح) كيف ينبغي لمقدمي خدمات الاتصالات/تكنولوجيا المعلومات والاتصالات استخدام المعلومات الاستخبارية عن التهديدات لتعزيز أنشطتهم الأمنية؟

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

ي) ما هي مجموعة مكونات إطار الأمن السيبراني التي يمكن لمنظمة استخدامها لمواجهة المخاطر؟

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

ل) ما نوع التقارير التقنية والتوصيات التي يمكن وضعها لدعم إجراءات الأمن السيبراني والسياسات والأطر التقنية؟

م ) كيف نفهم ونعرف الرسائل الاقتحامية؟

ن) ما هي الأشكال الجديدة للرسائل الاقتحامية في الشبكات القائمة وشبكات المستقبل؟

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

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

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

ص) كيف يمكن تحديد مسارات ومصادر وأحجام الرسائل الاقتحامية لمواجهة ومكافحة مثل هذه الرسائل الاقتحامية؟

ق) كيف يمكن تنفيذ أمن المراسلات؟

ر ) كيف يمكن منع توزيع البرمجيات الخبيثة والبرمجيات الضارة عبر البريد الإلكتروني؟

ش) كيف يمكن تحديد مسارات ومصادر وأحجام الرسائل الاقتحامية وتقدير حجم الاستثمار في المرافق والوسائل التقنية الأخرى لمواجهة ومكافحة هذه الرسائل الاقتحامية؟

ت) كيف يمكن منع هجوم مستهدف باستخدام التصيد الاحتيالي المركَّز؟

ث) كيف يمكن منع برمجيات طلب الفدية التي توزَّع عبر البريد الإلكتروني؟

خ) كيف يمكن تحديد ومنع الرسائل الاقتحامية التي تتخذ شكل اتصالات الذكاء الاصطناعي (AI)/تكنولوجيا تعلُّم الآلة (ML)؟

ذ ) كيف تحمى المعلومات الشخصية من خلال اعتماد تكنولوجيا الذكاء الاصطناعي/تعلم الآلة لتجنب انتشار الرسائل الاقتحامية؟

ض) ما هي الأعمال التقنية المضطلع بها فعلاً في إطار فريق مهام هندسة الإنترنت (IETF) ومشروع شراكة الجيل الثالث (3GPP) ورابطة 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؟

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

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

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

د د ) ما هي أفضل الممارسات لمكافحة الرسائل الاقتحامية؟

# 3 المهام

تشمل المهام التي يتعين النظر فيها في سياق شبكات وأنظمة الاتصالات/تكنولوجيا المعلومات والاتصالات ما يلي، على سبيل المثال لا الحصر:

 أ ) التعاون مع لجان الدراسات لقطاع تقييس الاتصالات والمعهد الأوروبي لمعايير الاتصالات (ETSI) والمنتدى العالمي لأفرقة الاستجابة للطوارئ وأمن المعلومات (FIRST) وفريق مهام هندسة الإنترنت (IETF) ومعهد مهندسي الكهرباء والإلكترونيات (IEEE) واللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1) ومنظمة تقدم معايير المعلومات المهيكلة (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 مقدمي الاتصالات/تكنولوجيا المعلومات والاتصالات بتأمين البنى التحتية لديهم والحفاظ على أمن العمليات وتبادل معلومات الأمن السيبراني.

ج) وضع مجموعة من التوصيات لتقديم حلول أمنية بشأن المساءلة والضمان والتصدي للحوادث والتعافي منها في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات، بما في ذلك الجوانب التقنية لخدمات الأمن المدارة.

د ) دراسة وتوصيف التقنيات والقدرات الأمنية لمقدمي الخدمات لغرض تنسيق وتبادل المعلومات بشأن مواطن الضعف والمنصات والهجمات السيبرانية.

هـ ) دراسة وتوصيف إطار الأمن السيبراني الذي يتكون من مجموعة من المكونات التي ينبغي أن تشمل التحديد والحماية والكشف والتصدي والتعافي.

و ) توصيف كيفية استخدام الذكاء الاصطناعي وتعلُّم الآلة لتحديد التهديدات ونقاط الضعف الجديدة وتحليلها بسرعة.

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

ح) وضع مبادئ توجيهية وأساليب تقنية لحماية المعلومات الشخصية وكذلك لحماية المعلومات المحددة لهوية الأشخاص (PII) باستخدام تقنيات CYBEX وSTIX وTAXII والأدوات الأمنية ذات الصلة.

ط) دراسة ووضع إرشادات تقنية لدعم إدارة التهديدات من حيث تحديد مصدر المهاجمين السيبرانيين.

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

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

ل) التعاون مع منظمات وضع المعايير الأخرى (مثل OASIS لاعتماد تقنيات STIX وTAXII في وثائق الاتحاد الدولي للاتصالات).

م ) العمل على التوصيات والتقارير التقنية بشأن كيفية مواجهة تحديات الأمن السيبراني.

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

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

ع) تحديد مسارات ومصادر وأحجام الرسائل الاقتحامية وتقدير حجم الاستثمار في المرافق والوسائل التقنية الأخرى لمواجهة ومكافحة هذه الرسائل الاقتحامية.

ف) وضع قائمة شاملة ومحدَّثة بموارد التدابير التقنية القائمة لمكافحة الرسائل الاقتحامية في شبكة الاتصالات، سواء المستخدمة أم قيد التطوير.

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

ق) وضع مجموعة من التدابير التقنية لدعم أمن المراسلات.

ر ) وضع توصيات جديدة لمنع البرمجيات الخبيثة والبرمجيات الضارة الموزعة عبر البريد الإلكتروني.

ش) وضع مجموعة من الحلول لمنع الهجمات المستهدفة باستخدام التصيد الاحتيالي المركَّز عبر البريد الإلكتروني.

ت) وضع توصيات جديدة لمنع انتشار برمجيات طلب الفدية التي توزَّع عبر البريد الإلكتروني.

ث) وضع متطلبات عامة ومحددة لتبادل المعلومات بشأن مكافحة الرسائل الاقتحامية.

خ) تقرير ما إذا كان وضع توصيات جديدة أو تعزيز توصيات قائمة، بما في ذلك أساليب مكافحة إيصال البريد الإلكتروني غير المطلوب والبرمجيات الخبيثة وغير ذلك من المحتويات المؤذية، ومكافحة معدات الشبكة المخترقة، مثل الشبكات الروبوتية، من شأنه أن يفيد الجهود المبذولة لمكافحة الرسائل الاقتحامية مكافحة فعّالة بقدر ما تتصل بثبات شبكة الاتصالات ومتانتها.

ذ ) وضع مجموعة من الحلول أو التوصيات الجديدة لمواجهة الرسائل الاقتحامية التي تتخذ شكل اتصالات الذكاء الاصطناعي/تعلُّم الآلة.

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

ويرد بيان محدّث لحالة سير العمل في إطار هذه المسألة في برنامج عمل لجنة الدراسات 17 في الموقع:
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

# 4 الروابط

خطوط عمل القمة العالمية لمجتمع المعلومات:

جيم5.

أهداف التنمية المستدامة:

8 (العمل اللائق والنمة الاقتصادي)،
9 (الصناعة والابتكار والبنية التحتية).

التوصيات:

سلسلة التوصيات X والتوصيات الأخرى ذات الصلة بالأمن.

المسائل:

1/17 و2/17 و3/17 و6/17 و7/17 و8/17 و10/17 و11/17 و13/17 و14/17 و15/17 لقطاع تقييس الاتصالات.

لجان الدراسات:

لجنتا الدراسات 1 و2 لقطاع تنمية الاتصالات؛ لجان الدراسات 2 و9 و11 و13 و16 و20 لقطاع تقييس الاتصالات.

هيئات التقييس:

المعهد الأوروبي لتقييس الاتصالات (ETSI)؛ معهد مهندسي الكهرباء والإلكترونيات (IEEE)؛ فريق مهام هندسة الإنترنت (IETF)؛ اللجنة التقنية 57 التابعة للجنة الكهرتقنية الدولية (IEC TC 57)؛ اللجنة التقنية 292 التابعة للجنة الكهرتقنية الدولية (IEC TC 292)؛ 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)؛ ومنظمة تقدم معايير المعلومات المهيكلة (OASIS)؛ الاتحاد المفتوح للاتصالات المتنقلة (OMA)؛ فريق إدارة الأشياء (OMG)؛ مشروع شراكة الجيل الثالث (3GPP)؛ المشروع الثاني لشراكة الجيل الثالث (3GPP2) وفريق الحوسبة الموثوقة (TCG).

هيئات أخرى:

فريق العمل المعني بمكافحة التصيد (APWG)؛ فريق مواجهة الطوارئ الحاسوبية/مركز التنسيق (CERT/CC)؛ وخدمات أفرقة الاستجابة للحوادث الحاسوبية (CIRT)؛ الوكالة الأوروبية لأمن الشبكات والمعلومات (ENISA)؛ 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).

المسألة 6/17

الأمن لخدمات الاتصالات وإنترنت الأشياء

 (استمرار للمسألة 6/17)

# 1 المسوغات

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 أجهزة الاستشعار 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. وتصف التوصيتان ITU-T X.1331 وX.1332 والإضافة ITU-T X.Suppl.26 الجوانب الأمنية للشبكة الكهربائية الذكية. وتقدم التوصيات ITU-T X.1361 وX.1362 وX.1363 وX.1364 وX.1365 متطلبات وآليات وأطر أمن إنترنت الأشياء. ويحتاج الأمر إلى مواصلة الجهود من أجل الحفاظ على توصيات وإضافات الأمن هذه وتعزيزها لكي تلبي احتياجات التكنولوجيات والخدمات الجديدة.

وتشير عبارة "خدمات وشبكات الاتصالات وإنترنت الأشياء" 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 إنترنت الأشياء (IoT) والمدن الذكية (بما فيها أنظمة الاتصالات من آلة إلى آلة (M2M) وتعرف الهوية بواسطة الترددات الراديوية (RFID) واتصالات المجال القريب (NFC) وشبكة أجهزة الاستشعار) والشبكة المنزلية وأنظمة التحكم الصناعي (مثل المصنع الذكي)، والشبكة الكهربائية الذكية، ووحدة هوية المشترك المدمجة (eSIM) والهواتف الذكية، وشبكات تلفزيون بروتوكول الإنترنت وغيرها، بأهمية حاسمة في مواصلة تطوير الصناعة وشركات تشغيل الشبكات ومقدمي الخدمات.

وتقييس أفضل الحلول الأمنية الشاملة أمر حيوي لمشغلي الشبكات ومقدمي الخدمات الذين يعملون في بيئة اتصالات دولية متعددة البائعين. وبالنظر إلى بعض الخصائص التي تنفرد بها بيئة إنترنت الأشياء (مثل محدودية القدرة الحاسوبية وحجم الذاكرة في الأجهزة المتنقلة الصغيرة، ودورة الحياة الطويلة، وأنظمة تشغيل وبرمجيات مكيفة خصيصاً لها)، فإن تقديم الأمن وحماية المعلومات المحددة لهوية الأشخاص مهمة عسيرة حقاً وتتطلب الاهتمام والدراسة بصورة خاصة.

وتشمل التوصيات والإضافات التي تندرج في إطار مسؤوليات هذه المسألة اعتباراً من 7 يناير 2022 ما يلي: X.1101 وX.1111 وX.1112 وX.1113 وX.1114 وX.1121 وX.1122 وX.1123 وX.1124 وX.1125 وX.1126 وX.1127 وX.1171 وX.1191 وX.1192 وX.1193 وX.1194 وX.1195 وX.1196 وX.1197 وX.1198 وX.1311 وX.1312 وX.1313 وX.1314 وX.1331 وX.1332 وX.1333 وX.1361 وX.1362 وX.1363 وX.1364 وX.1365 وX.1366 وX.1367 وX.1368 وX.1369 وX.1453 والإضافات X.Suppl.19 وX.Suppl.24 وX.Suppl.26.

والنصوص قيد الإعداد اعتباراً من 7 يناير 2022 هي: X.iotsec-4 و X.ra-iotو X.sc-iotو X.ztd-iotوTR.ibc-cd.

# 2 المسألة

تتناول الدراسة البنود التالية دون أن تقتصر عليها:

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

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

ج) ما هي التكنولوجيات الأمنية لدعم خدمات الاتصالات وإنترنت الأشياء؟

د ) كيف ينبغي الحفاظ على التوصيلية المأمونة في خدمات الاتصالات وإنترنت الأشياء وصيانتها؟

هـ ) كيف تنبغي دراسة وتطوير تكنولوجيات الأمن التي تستخدم تكنولوجيات الذكاء الاصطناعي/تعلُّم الآلة من أجل خدمات الاتصالات وإنترنت الأشياء؟

و ) ما هي تقنيات وآليات وبروتوكولات الأمن اللازمة لخدمات الاتصالات الجديدة وإنترنت الأشياء، ولا سيما الخدمات الجديدة لحماية المحتوى الرقمي؟

ز ) ما هي الحلول الأمنية العالمية لخدمات الاتصالات وإنترنت الأشياء (بما في ذلك مثلاً خدمات للمدن الذكية والشبكة الكهربائية الذكية وأنظمة التحكم الصناعي (مثل المصنع الذكي) القائمة على شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات)؟

ح) ما هي أفضل الممارسات أو المبادئ التوجيهية لخدمات الاتصالات وإنترنت الأشياء المأمونة؟

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

ي) ما هي الآليات اللازمة لحماية المعلومات المحددة لهوية الأشخاص (PII) وإدارتها في خدمات الاتصالات وإنترنت الأشياء 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 & 41)، بوضع مجموعة من التوصيات لتقديم حلول أمنية شاملة لخدمات الاتصالات وإنترنت الأشياء المأمونة.

ب) مراجعة التوصيات/المعايير الحالية لقطاع تقييس الاتصالات والمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC) وهيئات التقييس الأخرى في مجال الشبكة المنزلية والشبكة الكهربائية الذكية وأمن الهواتف الذكية وإنترنت الأشياء (IoT) وشبكة أجهزة الاستشعار الشمولية، لغرض تحديد خدمات مأمونة للاتصالات.

ج) مواصلة الدراسة لغرض تحديد الجوانب الأمنية لخدمات الاتصالات وإنترنت الأشياء في بيئة دولية متعددة البائعين، وبالنسبة لخدمات جديدة (بالنسبة مثلاً للمدن الذكية والشبكة الكهربائية الذكية وأنظمة التحكم الصناعي (مثل المصنع الذكي) التي تستند إلى شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات).

د ) دراسة وتحديد المسائل والتهديدات الأمنية في مجال خدمات الاتصالات وإنترنت الأشياء المأمونة.

هـ ) دراسة وتطوير آليات أمنية لخدمات الاتصالات وإنترنت الأشياء المأمونة.

و ) دراسة وتطوير آليات التوصيلية البينية لخدمات الاتصالات وإنترنت الأشياء المأمونة في بيئة اتصالات تضم باعة فرادى أو متعددين.

ز ) دراسة وتحديد الإشكالات والتهديدات التي تعترض حماية المعلومات المحددة لهوية الأشخاص في مجال خدمات الاتصالات وإنترنت الأشياء المأمونة.

ح) دراسة ووضع الآليات اللازمة لحماية المعلومات المحددة لهوية الأشخاص وإدارتها في خدمات الاتصالات وإنترنت الأشياء المأمونة.

ط) دراسة وتطوير تكنولوجيات الأمن باستخدام تكنولوجيات الذكاء الاصطناعي/تعلُّم الآلة لخدمات الاتصالات وإنترنت الأشياء المأمونة.

ويرد بيان محدّث لحالة سير العمل في إطار هذه المسألة في برنامج عمل لجنة الدراسات 17 في الموقع:
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

# 4 الروابط

خطوط عمل القمة العالمية لمجتمع المعلومات:

جيم5.

أهداف التنمية المستدامة:

8 (العمل اللائق والنمو الاقتصادي)،
9 (الصناعة والابتكار والبنية التحتية)،
11 (المدن والمجتمعات المستدامة).

التوصيات:

سلسلة التوصيات X والتوصيات الأخرى ذات الصلة بالأمن.

المسائل:

المسائل 1/17 و2/17 و3/17 و4/17 و7/17 و8/17 و10/17 و11/17 و13/17 و14/17 و15/17 لقطاع تقييس الاتصالات

لجان الدراسات:

لجان دراسات قطاع الاتصالات الراديوية؛ ولجان الدراسات 9 و11 و13 و15 و16 و20 لقطاع تقييس الاتصالات، ونشاط التنسيق المشترك بشأن إنترنت الأشياء (JCA-IoT) والمدن والمجتمعات الذكية (SC&C).

هيئات التقييس:

فريق مهام هندسة الإنترنت (IETF)؛ فريق تقييم الأنظمة 6 لدى اللجنة الكهرتقنية الدولية (IEC SEG) (الشبكة الكهربائية الصغرية)، فريق العمل 3 واللجنتان التقنيتان 57 و65 لدى هيئة إدارة التقييس في اللجنة الكهرتقنية الدولية (IEC SMB WG3 & TCs 57 and 65)، اللجان الخاصة 6 و25 و27 و31 و41 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SCs 6, 25, 27, 31 and 41)؛ 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) رابطة النظام العالمي للاتصالات المتنقلة (GSMA)؛ 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).

المسألة 7/17

خدمات التطبيقات المأمونة

(استمرار للمسألة 7/17)

# 1 المسوغات

توفر التوصيات X.1141 وX.1142 وX.1143 وX.1144 وX.1145 وX.1146 وX.1147 لقطاع تقييس الاتصالات مجموعة من التوصيات التي تتناول تأشيرات الأمن من أجل الاستيقان/الإجازة ومعماريات الأمن لخدمات رسائل الشبكات. وتحدد التوصيات ITU‑T X.1151 وX.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 خدمات تكنولوجيا الاتصال بين النظراء (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 وخدمات تكنولوجيا الاتصال بين النظراء وخدمات الطرف الثالث الموثوق به، بأهمية حاسمة للمضي في تطوير صناعة الاتصالات. وتؤدي بروتوكولات تطبيقات الأمن دوراً مهماً جداً في تقديم خدمات التطبيقات المأمونة. ويشكل تقييس أفضل الحلول الأمنية الشاملة أمراً حيوياً للصناعة ومشغلي الشبكات الذين يعملون في بيئة دولية متعددة الموردين. ويلزم أيضاً دراسة وتطوير أنواع أخرى من خدمات المنصات والتطبيقات المأمونة مثل خدمات الختم الزمني وخدمات الموثق العمومي المأمونة وخدمات التكنولوجيا المالية (الصيرفة المفتوحة، والإقراض من نظير إلى نظير، والتحويلات، والمحفظة المتنقلة، والتأمين) المأمونة والخدمات المتاحة بحرية على الإنترنت (OTT) المأمونة، والتوأم الرقمي، 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.

ونظراً لأن الاتصالات وتكنولوجيا المعلومات والاتصالات تطور خدمات التطبيقات، فإنها تواجه أفقين جديدين يحتاجان إلى الدراسة: تولد التطبيقات وتعالج المزيد والمزيد من البيانات، ولدعمها، أصبح الذكاء الاصطناعي مطلوباً الآن. وتحتاج خدمات التطبيقات المأمونة إلى التوسع لتشمل البحث المكثف والسوق المطلوبين لدراسة مجموعة الجوانب التشغيلية والتقنية لحماية البيانات التي تعتمد على العمل القائم في خدمات تحليلات البيانات.

وفيما يتعلق بالذكاء الاصطناعي، يواجه مقدمو الخدمات العديد من التحديات، لا سيما اختيار وإدخال ودمج العشرات، إن لم يكن المئات، من مكونات الذكاء الاصطناعي من المصادر المفتوحة ودوائر الصناعة التي يحتاجون إلى تجميعها في عوامل شكلية متنوعة (تطبيقات الذكاء الاصطناعي المتكاملة، والذكاء الاصطناعي كمنصات أعم، والذكاء الاصطناعي كمنصة وكخدمة، وما إلى ذلك) على بنى تحتية متنوعة (في مكان العمل، حيز سحابي خاص، حيز سحابي مختلط، حيز سحابي عمومي). وكما هو الحال عندما بدأت البيانات الضخمة، أدى ذلك إلى ظهور مشاكل جديدة تتعلق بإمكانية التشغيل البيني الأمني، ناهيك عن ضمان السرية والسلامة والتيسر لبيانات مدخلات التدريب إلى الذكاء الاصطناعي وبيانات مخرجات الذكاء الاصطناعي. ويشكل كل ذلك معتركاً جديداً للذكاء الاصطناعي تدعو الحاجة إلى دراسته وتطويره. ومرة أخرى يمكن أن يعتمد ذلك على العمل الأولي القائم في خدمات تحليلات البيانات.

وتشمل التوصيات التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 7 يناير 2022 ما يلي: X.1141 وX.1142 وX.1143 وX.1144 وX.1145 وX.1146 وX.1147 وX.1148 وX.1149 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 وX.1450 وX.1451 وX.1452 وX.1470 والإضافات X.Suppl.17 وX.Suppl.21 وX.Suppl.22.

النصوص قيد الإعداد اعتباراً من 7 يناير 2022: X.1144rev و X.guide-cdd و X.rddaو X.saf-dfsو X.scpaو X.sec-grp-mov وX.sg-dtn و X.slesو X.smdtscو X.smsrcو X.videو X.websec-7وTR.cta.

# 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؟

هـ ) ما هي التقنيات أو البروتوكولات الأمنية اللازمة لخدمات التطبيقات المأمونة الناشئة، بما في ذلك منصة الخدمة، وخدمات التكنولوجيا المالية، والخدمات المتاحة بحرية على الإنترنت (OTT)؟

و ) ما هي الحلول الأمنية العالمية لخدمات التطبيقات المأمونة وتطبيقاتها؟

ز ) كيف تحدَد استراتيجية لحماية البيانات التشغيلية والتقنية لخدمات التطبيقات؟

ح) كيف تحدَد استراتيجية لحماية معترك الذكاء الاصطناعي؟

# 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 لتقديم حلول أمنية شاملة لخدمات التطبيقات المأمونة.

ب) مراجعة التوصيات/المعايير القائمة لدى قطاع تقييس الاتصالات والمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية في مجال خدمات التطبيقات المأمونة.

ج) المضي في الدراسة لتحديد الجوانب الأمنية لخدمات التطبيقات المأمونة وللخدمات الجديدة الناشئة مثل خدمات التكنولوجيا المالية، والخدمات المتاحة بحرية على الإنترنت (OTT).

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

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

و ) دراسة ووضع الاستراتيجيات والتوصيات للجوانب التشغيلية والتقنية لحماية البيانات في خدمات التطبيقات.

ز ) دراسة ووضع الاستراتيجيات والتوصيات لحماية معترك الذكاء الاصطناعي.

ويرد بيان محدّث لحالة سير العمل في إطار هذه المسألة في برنامج عمل لجنة الدراسات 17 في الموقع:
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

# 4 الروابط

خطوط عمل القمة العالمية لمجتمع المعلومات

جيم5.

أهداف التنمية المستدامة

8 (العمل اللائق والنمو الاقتصادي)،
9 (الصناعة والابتكار والبنية التحتية)،
11 (المدن والمجتمعات المستدامة).

التوصيات

سلسلة التوصيات X.800 والتوصيات الأخرى ذات الصلة بالأمن.

المسائل

المسائل 1/17 و2/17 و3/17 و4/17 و6/17 و8/17 و10/17 و11/17 و14/17 و15/17 و7/13 و13/17 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 لمعايير الاتصالات (ETSI)؛ رابطة 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)؛ اللجنة الخاصة 42 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SC 42)؛ المنظمة الدولية للتوحيد القياسي/اللجنة التقنية 68 (ISO/TC 68)؛ المنظمة الدولية للتوحيد القياسي/اللجنة التقنية 307 (ISO/TC 307)؛ مبادرة قنطرةKantara ؛ ومنظمة تقدم معايير المعلومات المهيكلة (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).

المسألة 8/17

أمن البنية التحتية للحوسبة السحابية والبيانات الضخمة

(استمرار للمسألة 8/17)

# 1 المسوغات

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. ويعرَّف نموذج الحوسبة السحابية بخمس 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...) مع المرونة في التوسع في أنماط تقديم الخدمات (أساسية ومناطقية وطرفية و...). 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. ويتيح إدخال حوسبة الحافة توزيع القدرات السحابية على حافة الشبكة. ويستحدث ذلك تطبيقات خدمة سحابية ذات كمون حتمي منخفض واعتمادية عالية. ومع ذلك، تثير الأنظمة المفتوحة وتقاسم الموارد والعمل البيني المتأصل في الحيز السحابي والحافة، 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 مفعلاً رئيسياً لمجمل سوق الحوسبة السحابية ونظامها الإيكولوجي، خاصةً عندما تقدم حوسبة الحافة مزيداً من التوزيع المحلي للموارد السحابية. ويؤدي ذلك إلى علاقات أكثر تعقيداً بين تطبيقات الحافة والتطبيقات الإقليمية والأساسية للخدمة السحابية.

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).

وتُعتبر البيانات الضخمة كتكنولوجيات مجموعة الأدوات والبيانات والتحليلات المستخدمة في معالجة كمية كبيرة من البيانات. علاوةً على ذلك، ومع نمو البيانات أضعافاً مضاعفة لتصبح من الأصول الرئيسية لشبكات الاتصالات/تكنولوجيا المعلومات والاتصالات، تحلَل مجموعات البيانات الضخمة بدعم من الحوسبة السحابية لكشف أنماط وعلاقات كان من شأنها أن تظل خافية لولا ذلك الدعم. وتتحقق العمليات الأساسية للبيانات الضخمة مثل جمع البيانات وتخزينها وتحليلها وإدارتها وتمثيلها المرئي على أساس الحوسبة السحابية، والتي بدونها لا يمكن نقل البيانات الضخمة وتحليلها بسرعة باستخدام التكنولوجيات التقليدية (مثل البيانات الضخمة كخدمة). 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 8/17 مع المسائل ذات الصلة مثل 2/17 و3/17 و4/17 و7/17 و10/17 و11/17 لوضع توصيات بشأن أمن الحوسبة السحابية.

التوصيات والتقارير التقنية التي تندرج ضمن مسؤولية هذه المسألة اعتباراً من 7 يناير 2022: X.1601 وX.1602 وX.1603 وX.1604 وX.1605 وX.1606 وX.1631 وX.1641 وX.1642 وX.1643 وX.1750 وX.1751 وX.1752 والتقرير التقني TR.XAASL.

النصوص قيد الإعداد اعتباراً من 7 يناير 2022 هي: X.BaaS-sec و X.gecdsو X.nssa-ccو[X.sa-ec](https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16951) و X.sgcnpو X.sgdc وX.sgmc وX.sr-cphr.

# 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 الرئيسيين في دوائر صناعة الاتصالات لتعزيز أمن النظام الإيكولوجي للحوسبة السحابية بأكمله، بما في ذلك أمن الحوسبة السحابية، وأمن حوسبة الحافة، وأمن العمل البيني، وما إلى ذلك؟

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 هي التوصيات الجديدة التي ينبغي وضعها بشأن الحلول الأمنية أو أفضل الممارسات أو المبادئ التوجيهية لأمن منصة البيانات الضخمة وبنيتها التحتية؟

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

و ) 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.

هـ ) وضع توصيات لتحديد آليات الضمان وتكنولوجيات التدقيق وتقييم المخاطر وذلك بهدف التوصل إلى إقامة علاقات ثقة داخل النظام الإيكولوجي للحوسبة السحابية.

و ) دراسة ووضع توصيات لأمن منصة البيانات الضخمة وبنيتها التحتية تكون متوائمة مع البنية المرجعية التي وصَّفتها لجنة الدراسات 13 بقطاع تقييس الاتصالات.

ز ) الاضطلاع بجميع الأنشطة المتعلقة بأمن الحوسبة السحابية ومنصة البيانات الضخمة وبنيتها التحتية في إطار لجنة الدراسات 17.

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

ويرد بيان محدّث لحالة سير العمل في إطار هذه المسألة في برنامج عمل لجنة الدراسات 17 في الموقع:
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

# 4 الروابط

خطوط عمل القمة العالمية لمجتمع المعلومات

جيم5.

أهداف التنمية المستدامة

8 (العمل اللائق والنمو الاقتصادي)،
9 (الصناعة والابتكار والبنية التحتية)،
11 (المدن والمجتمعات المستدامة).

التوصيات:

توصيات السلسلة Y بشأن الحوسبة السحابية.

المسائل:

المسائل 1/17 و2/17 و3/17 و4/17 و7/17 و10/17 و11/17 و15/17 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)؛ ومنظمة تقدم معايير المعلومات المهيكلة (OASIS)؛ وغيرها من الهيئات المعنية التي يجري تحديدها.

هيئات أخرى:

التحالف المعني بأمن الحوسبة السحابية (CSA)؛ فريق المهام المعني بالإدارة الموزعة (DMTF).

المسألة 10/17

معمارية وآليات إدارة الهوية والقياسات البيومترية عن بُعد

(استمرار للمسألة 10/17)

# 1 المسوغات

تكتسب القياسات البيومترية قبولاً في التطبيقات التي تقوم، على سبيل المثال لا الحصر، بالتحقق من الهوية مثل التجارة الإلكترونية والطب عن بُعد والصحة الإلكترونية. فلقد شكلت أنظمة تطبيق القياسات البيومترية تحديات شتى تتعلق بحماية البيانات التشغيلية والتقنية والموثوقية وأمن البيانات البيومترية في تطبيقات السلامة البيولوجية والأمن البيولوجي.

ويزداد التعقيد والحاجة إلى الاستيقان البيومتري في جانب المخدِّم أكثر عند اعتماد الاستيقان البيومتري في بيئة شبكة مفتوحة. وتتطلب تطبيقات الاتصالات (مثل القياسات البيومترية عن بُعد) التي تستخدم المطاريف المتنقلة وخدمات الإنترنت أساليب الاستيقان لتقديم مستوى عالٍ من الأمن وسهولة الاستخدام. وتقتضي الضرورة تحديد متطلبات استخدام بيانات القياسات البيومترية عن بُعد بطريقة سالمة ومأمونة مع حماية تشغيلية معززة وحماية معززة للبيانات.

وإدارة الهوية (IdM) هي إدارة دورة الحياة واستخدام (بمعنى استحداث وحفظ واستخدام وإلغاء) بيانات الاعتماد ومعرّفات الهوية والنعوت والأنماط التي تعرف بها الكيانات (مثل مقدمي الخدمات والمستعملين النهائيين والمنظمات وأجهزة الشبكات والتطبيقات والخدمات) بمستوى مناسب من الثقة. ووفقاً للسياق، يمكن لكيان وحيد أن يتخذ هويات متعددة بمتطلبات أمنية متباينة وفي مواقع متعددة. وحسب نموذج الهوية، يمكن أن تكون السيطرة على الهويات مركزية أو لامركزية أو مزيجاً من الاثنتين. وفي الشبكات العمومية، تدعم إدارة الهوية تبادل المعلومات الموثوق بين الكيانات المجازة. ويعتمد التبادل على تأكيد الهويات عبر الأنظمة الموزعة من مقدمي خدمة متعددين. ويمكن أن يعتمد التبادل أيضاً على بيئات الخدمة المختلفة مثل الخدمة السحابية والجيل الخامس (5G). وتحسِّن إدارة الهوية أيضاً حماية المعلومات الخاصة ويمكنها، استناداً إلى نموذج الثقة، ضمان نشر المعلومات المجازة حصراً.

وتشكل إدارة الهوية عنصراً رئيسياً من عناصر شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات وخدماتها ومنتجاتها لأنها تدعم إنشاء ودعم الاتصالات الموثوق بها. وإلى جانب إجراء الاستيقان على هوية كيان معين، فإنها تتيح أيضاً إجازة النفاذ بناءً على امتيازات، وهي تدعم أيضاً تغيير الامتيازات عندما يغيِّر دور الكيان التفويض وغير ذلك من الخدمات القائمة على الهوية.

وإدارة الهوية هي أحد العناصر الحاسمة في إدارة أمن الشبكات لأنها تحسن الضمان للنفاذ المتجول وحسب الطلب إلى الشبكات والخدمات التي يتوقعها 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. ونظراً لأن إدارة الهوية تعمل بطريقة متبادلة، فإن هذا المستوى المتزايد من الثقة ينطبق بالتساوي على كل من المستخدم النهائي ومقدم الخدمة.

وستكون هناك مواصفات وحلول وطنية/إقليمية محددة بشأن إدارة الهوية، وستواصل هذه المواصفات والحلول تطورها. ومن المهم وضع أساس يقوم عليه تنفيذ الحلول المنسقة. وبالإضافة إلى دراسة القياسات البيومترية عن بُعد، فإن هذه 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 الأخرى لوضع المعايير (SDO). ومن المسلم به أن هناك مسائل أخرى ستشارك في جوانب محددة من عملية إدارة الهوية، أي البروتوكولات والمتطلبات ومعرفات أجهزة الشبكات.

وتشمل التوصيات التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 7 يناير 2022 ما يلي: X.1080.0 وX.1080.1 وX.1080.2 وX.1081 وX.1082 وX.1083 وX.1084 وX.1085 وX.1086 وX.1087 وX.1088 وX.1089 وX.1090 وX.1091 وX.1092 وX.1093 وX.1094 وX.1250 وX.1251 وX.1252 وX.1253 وX.1254 وX.1255 وX.1256 وX.1257 وX.1258 وX.1261 (بالاشتراك مع لجنة الدراسات 2) وX.1275 وX.1276 وX.1277 وX.1278 وX.1279 والإضافات X.Suppl.7 وX.Suppl.35.

النصوص قيد الإعداد اعتباراً من 7 يناير 2022 هي: X.1250rev و X.gpwdو X.oob-saو X.pet\_authوX.srdidm و.X.tec‑idms

# 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 البيومتري في شبكة على درجة عالية من الخصائص الوظيفية؟

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

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

هـ ) كيف يمكن تحسين التعرف على هوية المستعملين واستيقانها في جوانب السلامة والأمن عن طريق استعمال نماذج قابلة للتشغيل البيني لطرائق القياس البيومتري عن بُعد؟

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

ز ) كيف ينبغي تطوير أنظمة وعمليات بيومترية لتكون متوافقة مع المتطلبات الوظيفية كي يستيقن الكيان الحيوانات الأليفة باستخدام القياسات البيومترية عن بُعد؟

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

ط) ما هو النموذج الملائم لإدارة الهوية الذي يتمتع بالاستقلال عن تكنولوجيات الشبكات ويدعم المشاركة المتمحورة حول المستعملين والهوية القائمة على الخدمة السحابية ونماذج الهوية اللامركزية ويدعم التبادل المأمون لمعلومات إدارة الهوية بين الكيانات المعنية (مثل المستعملين والأطراف المعوِّلة ومقدمي الهوية) على أساس الموافقة والسياسات ذات الصلة؟

ي) ما هي العناصر التي تشكل إطاراً تنوعياً لإدارة الهوية وللمتطلبات المتعلقة بها؟

ك) ما هي المتطلبات المحدد لإدارة الهوية من جانب مقدمي الخدمات؟

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

م ) ما هي القضايا التي تجب مراعاتها لدعم الهوية في تكنولوجيا السجلات الموزعة بما في ذلك المحفظة والمعرفات اللامركزية وبيانات الاعتماد التي يمكن التحقق منها؟

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

س) ما هي متطلبات وآليات حماية المعلومات المحددة لهوية الأشخاص (PII) والكشف عنها؟

ع) كيف يمكن للكيان أن يتحكم في علاقته عندما يشارك في علاقات وتفاعلات قائمة على الهوية؟

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

ص) ما هي القدرات في مجال إدارة الهوية التي يمكن استخدامها ضد الهجمات السيبرانية؟

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

ر) كيف يمكن إجراء الاستيقان بدون أسرار مشتركة؟

ش) هل يمكن إجراء الاستيقان القائم على البنية التحتية للمفاتيح العمومية بطريقة مأمونة وقابلة للتشغيل البيني؟

ت) هل يمكن استخدام القياسات البيومترية كجزء من طبقة استيقان وثقة قوية لتمكين التفاعلات الموثوقة عبر شبكة ما؟

ث) ما هي المتطلبات الفريدة لنظام إدارة الهوية المستند إلى المستهلك من حيث فحص الهوية واستعادة الحساب دون الاعتماد على كلمات المرور؟

خ) كيف يمكن استخدام الثقة والعلاقة لتعزيز استعادة الحساب وأمن المستخدمين وتجربتهم عند التعامل مع الأطراف المعولة؟

# 3 المهام

تشمل المهام البنود التالية دون أن تقتصر عليها:

 أ ) تحسين ومراجعة التوصيات الراهنة بشأن الاستيقان بالقياسات البيومترية.

ب) استعراض أوجه التشابه والتباين بين التوصيات القائمة المتعلقة بالقياسات البيومترية عن بُعد 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 البيومترية عن بُعد يستعمل المعماريات والأطر بما فيها تلك الموضوعة في إطار المسألة 2/17.

د ) دراسة ووضع المتطلبات المتعلقة بتقييم الأمن وتقنيات حماية البيانات التشغيلية والتقنية بالنسبة لأي من تطبيقات القياسات البيومترية عن بُعد.

هـ ) دراسة ووضع المتطلبات المتعلقة بتطبيقات القياسات البيومترية عن بُعد في الاتصالات في الشبكات التي تتمتع بدرجة عالية من الخصائص الوظيفية.

و ) دراسة ووضع الأطر المتكاملة والمتطلبات اللازمة لتطبيقات القياسات البيومترية عن بُعد من أجل بيئات الحوسبة السحابية وتخزين البيانات.

ز ) دراسة ووضع المتطلبات اللازمة للاستيقان بالقياسات البيومترية عن بُعد من أجل إطار الهوية الموثوق بها.

ح) دراسة ووضع المتطلبات اللازمة لوضع بروتوكولات عامة ملائمة توفر السلامة والأمن وحماية البيانات التشغيلية والتقنية، والموافقة "على معاملة بيانات القياسات البيومترية" في أي من تطبيقات القياسات البيومترية عن بُعد، مثل الصحة الإلكترونية والطب عن بُعد والتجارة الإلكترونية والصيرفة على الإنترنت والدفع الإلكتروني والمراقبة الفيديوية.

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

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

ك) دراسة ووضع خدمات يستيقن بها الكيان الحيوانات الأليفة على أساس القياسات البيومترية عن بُعد.

ل) تحديد إطار لإدارة الهوية يدعم خصائص الاكتشاف، والسياسة ونموذج الثقة، والاستيقان والترخيص، والتأكيدات، والإدارة الموثوقة لدورة الحياة وهي المتطلبات التي تقتضيها إدارة الهوية.

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

ن) تحديد المتطلبات (واقتراح الآليات) لتأكيد الهوية وتحديد مختلف طرائق تأكيد الهوية التي يمكن اعتمادها في شبكات شتى، والربط البيني فيما بينها. وفي هذا السياق، يشمل تأكيد الهوية أنماط الهوية والسمعة.

س) تحديد الأسطح البينية اللازمة لقابلية التشغيل البيني بين أنظمة إدارة الهوية.

ع) تحديد المتطلبات (واقتراح الآليات) لحماية المعلومات المحددة لهوية شخص (PII) والكشف عنها.

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

ص) الاحتفاظ بقائمة حديثة لمصطلحات وتعريفات إدارة الهوية وتنسيقها.

ق) دراسة وتحديد المخاطر الأمنية المتعلقة بإدارة الهوية.

ر ) دراسة ووضع أنظمة إدارة الهوية اللامركزية مع دعم تحكم المستخدمين في هوياتهم.

ش) دعم أنظمة إدارة الهوية الموثوقة التي يمكن أن تتحد عبر الأنظمة والخدمات والأجهزة وإنترنت الأشياء والتطبيقات.

ت) دعم نظام إدارة الهوية الذي يقدم إدارة الهوية كخدمة للوكلاء السحابيين وشبكات الجيل الخامس والأجهزة المتنقلة.

ث) تحديد المتطلبات واقتراح الآليات لتأكيد الهوية في الاستيقان والاتحاد. ووضع معايير التقابل/العمل المتبادل بين مختلف طرائق ضمان الهوية التي يمكن اعتمادها في شبكات شتى. وفي هذا السياق، يشمل ضمان الهوية أنماط الهوية والسمعة.

ويرد بيان محدّث لحالة سير العمل في إطار هذه المسألة في برنامج عمل لجنة الدراسات 17 في الموقع:
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

# 4 الروابط

خطوط عمل القمة العالمية لمجتمع المعلومات:

جيم5.

أهداف التنمية المستدامة:

8 (العمل اللائق والنمو الاقتصادي)،
9 (الصناعة والابتكار والبنية التحتية).

التوصيات:

السلسلة X والسلسلة Y

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

المسائل:

1/17 و2/17 و3/17 و4/17 و6/17 و7/17 و8/17 و11/17 و15/17 و7/13 و14/15 لقطاع تقييس الاتصالات.

لجان الدراسات:

لجنتا الدراسات 1 و2 لقطاع تنمية الاتصالات؛ ولجنة الدراسات 7 لقطاع الاتصالات الراديوية؛ ولجان الدراسات 2 و5 و9 و11 و13 و15 و16 و20 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 مهندسي الكهرباء والإلكترونيات (IEEE)؛ فريق مهام هندسة الإنترنت (IETF)؛ اللجان الخاصة 6 و17 و27 و37 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SCs 6, 17, 27 and 37)؛ المنظمة الدولية للتوحيد القياسي/اللجان التقنية 12 و68 و215 و307 (ISO/TCs 12, 68, 215 and 307)؛ المنظمة الدولية للتوحيد القياسي/اللجنة التقنية 12/فريق العمل المشترك 20 (ISO/TC 12/JWG 20)؛ المعهد الأوروبي لمعايير الاتصالات (ETSI)؛ ومنظمة تقدم معايير المعلومات المهيكلة (OASIS)؛ مبادرة قنطرة Kantara؛ مشروع شراكة الجيل الثالث (3GPP)؛ المشروع الثاني لشراكة الجيل الثالث (3GPP2).

هيئات أخرى:

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

المسألة 11/17

التكنولوجيات العامة (مثل الدليل، البنية التحتية للمفاتيح العمومية (PKI)،
اللغات الشكلية، معرفات الكائنات) لدعم التطبيقات المأمونة

(استمرار للمسألة 11/17)

# 1 المسوغات

تدعم هذه المسألة مواصلة وضع مجموعة متنوعة 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

- الاتصالات المأمونة (X.510)

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

- قواعد التركيب المجردة رقم واحد (ASN.1)

- معرّفات الكائنات وسلطات تسجيلها

- الإصدار 3 من ترميز الاختبار وضبط الاختبار (TTCN-3)

- صيانة اللغات الشكلية:

• لغة التوصيف والوصف (SDL)

• تصميم ملف تعريف لغة النمذجة الموحدة (UML)

• مخطط تتابع الرسائل (MSC)

• ترميز متطلبات المستخدم (URN)

• CHILL، لغة البرمجة بقطاع تقييس الاتصالات

- الحفاظ على التوصيل البيني للأنظمة المفتوحة (OSI) وعلى المعالجة المفتوحة الموزعة (ODP).

## 1.1 مسوغات 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 التوصية X.500. وقد شملت التوصية ITU-T X.500 قدرات للعمل البيني مع البروتوكول LDAP. وتشكل حلول التوصية ITU‑T X.500 والبروتوكول LDAP جزءاً هاماً من إدارة الهوية (IdM).

وتتسم التوصية ITU-T X.509 بأهمية خاصة، كما تستخدم شهادات المفاتيح العمومية على نطاق واسع.

فبالإضافة إلى كونها جزءاً رئيسياً من الأعمال الإلكترونية، والصيرفة الإلكترونية، والصحة الإلكترونية، فإنها تُستخدم الآن أيضاً في شبكات أخرى كبيرة تتميز بالاتصالات من آلة إلى آلة وكيانات مقيدة مثل إنترنت الأشياء (IoT) والشبكات الكهربائية الذكية (smart grid).

وشهادات المفاتيح العمومية هي أيضاً للعديد من مواصفات فريق مهام هندسة الإنترنت (IETF)، من قبيل أمن طبقة النقل (TLS).

وتوفر شهادات النعوت طريقة مأمونة لنقل الامتيازات الهامة للتحكم في النفاذ. وتقوم مواصفات OASIS SAML على أساس شهادات نعوت التوصية X.509. وتُستخدم شهادات النعوت أيضاً في أنظمة القدرة. وشهادات النعوت مفيدة بصفة خاصة عندما تنسب الامتيازات من جانب سلطات أخرى غير السلطات التي تصدر شهادات المفاتيح العمومية.

وتحتاج التوصية ITU-T X.509، بالتعاون مع مجموعات أخرى، إلى أن تتطور ويحافظ عليها لكي تعبر عن الخبرات المكتسبة في مجال البنية التحتية للمفاتيح العمومية (PKI) وفي مجال البنية التحتية لإدارة الامتيازات (PMI) وتستفيد منها. وتدعو الحاجة لتعزيز التوصية X.509 كي تتناول المتطلبات الجديدة كالاتصالات من آلة إلى آلة وأمن الشبكة الكهربائية الذكية وأمن إنترنت الأشياء والخوارزميات المأمونة كمومياً وتكنولوجيا السجلات الموزعة. ويجري تطوير آلية لامركزية للبنية التحتية للمفاتيح العمومية تستخدم سلاسل الكتل.

وتشمل التوصيات التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 7 يناير 2022 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.510 وX.511 وX.518 وX.519 وX.520 وX.521 وX.525 وX.530 وX.1341.

النصوص قيد الإعداد اعتباراً من 7 يناير 2022 هي: X.510 Amd.1، X.pki-em.

## 2.1 مسوغات العمل بشأن قواعد التركيب المجردة رقم واحد (ASN.1)

ستوضع، حسب الحاجة، توصيات إضافية بما يتوافق مع أوجه التقدم في التكنولوجيا، ومتطلبات إضافية من مستعملي قواعد التركيب المجردة رقم واحد (ASN.1)، وقواعد تشفيرها.

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 المتبقية.

وهناك حاجة متواصلة إلى توفير المشورة والمساعدة إلى لجان الدراسات الأخرى، ومنظمات وضع المعايير (SDO) الخارجية، والبلدان، بشأن المسائل المتصلة بقواعد التركيب المجردة رقم واحد.

وتشمل التوصيات التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 7 يناير 2022 ما يلي: X.680 وX.681 وX.682 وX.683 وX.690 وX.691 وX.692 وX.693 وX.694 وX.695 وX.696 وX.697 وX.891 وX.892 وX.893 وX.894.

النصوص قيد الإعداد اعتباراً من 7 يناير 2022: لا توجد.

## 3.1 مسوغات العمل بشأن معرّفات الكائنات وسلطات تسجيلها

أثبتت معرّفات الكائنات(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 الكائنات الدولية، على نحو يسمح بتحديد الأقواس المعرفة ببطاقات Unicode موحدة الترميز، أيضاً الطلب من أجل مختلف التطبيقات، ومن المحتمل أن يسفر عن متطلبات تلتمس زيادة تطويرها وتوسيعها وتوزيعاتها.

وهناك حاجة متواصلة إلى توفير المشورة والمساعدة إلى لجان الدراسات الأخرى والمنظمات الخارجية لوضع المعايير (SDO) والبلدان، بشأن إدارة أماكن أسماء معرفات الكائنات. ومن المتوقع أن تزداد الحاجة إلى المساعدة والمشورة مع إدخال نظام معرفات الكائنات الدولية وزيادة استخدام هيئات التسجيل القطرية من جانب البلدان النامية. ولذلك فإن هناك حاجة متواصلة إلى "مشروع معرفات الكائنات" 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 الكائنات.

وتشمل التوصيات والورقات التقنية التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 7 يناير 2022 ما يلي: X.660 وX.662 وX.665 وX.666 وX.667 وX.668 وX.669 وX.670 وX.671 وX.672 وX.674 وX.675 وX.676 وX.677 والورقة التقنية XSTP-OID-ORS.

النصوص قيد الإعداد اعتباراً من 7 يناير 2022 هي: X.672rev.

## 4.1 مسوغات العمل بشأن الإصدار 3 من ترميز الاختبار وضبط الاختبار (TTCN-3)

يمكّن الإصدار 3 من ترميز الاختبار وضبط الاختبار (TTCN-3) من إجراء اختبارات لتوصيف الخواص الوظيفية وقابلية التشغيل البيني للأنظمة وكتابة مجموعات الاختبار العامة. 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.

وتشمل التوصيات التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 7 يناير 2022 ما يلي: X.292 وZ.161 وZ.161.1 وZ.161.2 وZ.161.3 وZ.161.4 وZ.161.5 وX.161.6 وZ.161.7 وZ.162 وZ.163 وZ.164 وZ.165 وZ.165.1 وZ.166 وZ.167 وZ.168 وZ.169 وZ.170 وZ.171.

النصوص قيد الإعداد اعتباراً من 7 يناير 2022 هي: لا توجد.

## 5.1 مسوغات العمل بشأن صيانة اللغات الشكلية

لا يتوقع المزيد من التطوير للغات الشكلية التالية:

- لغة التوصيف والوصف (SDL)

- ملف تعريف لغة النمذجة الموحدة (UML)

- مخطط تتابع الرسائل (MSC)

- ترميز متطلبات المستخدم (URN)

- CHILL، لغة البرمجة بقطاع تقييس الاتصالات

ولكن هناك حاجة إلى صيانة مستمرة.

وتشمل التوصيات والإضافات وأدلة المنفِّذ التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 7 يناير 2022 ما يلي: Z.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.200 وZ.450 والإضافة Z.Suppl.1 ودليل المنفَّذ Z.Imp100.

## 6.1 مسوغات العمل بشأن الحفاظ على التوصيل البيني للأنظمة المفتوحة (OSI)

وقد تم الانتهاء من الأعمال المتعلقة بالتوصيات الأساسية من أجل 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.

وتشمل التوصيات وأدلة المنفذ التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 7 يناير 2022 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 ودليل المنفِّذ X.ImpOSI.

## 7.1 سوغات العمل بشأن الحفاظ على المعالجة المفتوحة الموزعة (ODP)

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

وتشمل التوصيات التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 7 يناير 2022 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؟

هـ ) ما هي قواعد التشفير الأخرى للتوصية ITU‑T X.500، مثل لغة الوسم القابلة للتوسيع (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 القياسات البيومترية والاستيقان والتحكم في النفاذ والتجارة الإلكترونية؟

ح) ما هي التغييرات التي يلزم إدخالها على التوصيتين ITU‑T X.509 وITU-T X.510 لدعم الخوارزميات المأمونة كمومياً وتكنولوجيا السجلات الموزعة؟

وسيتم القيام بهذا العمل بالتعاون مع اللجنة الخاصة 6 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SC 6) فيما تقوم به من أعمال بشأن توسيع نطاق استعمال المعيار 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)

 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 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 في طليعة الأعمال المضطلع بها في مجال تقديم الترميزات لتعريف البروتوكولات؟

وسينفَّذ هذا العمل بالتعاون مع اللجنة الخاصة 6 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SC 6).

## 3.2 دراسة البنود المتصلة بالأعمال في مجال معرّفات الكائنات وهيئات تسجيلها

 أ ) ما هو نشاط التعليم اللازم لدعم استعمال معرفات الكائنات في بيئات متنوعة؟

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

ج) 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 معرفات الكائنات في طليعة الأعمال المضطلع بها في مجال وضع التسميات الواضحة؟

وسينفَّذ هذا العمل بالتعاون مع اللجنة الخاصة 6 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SC 6).

## 4.2 دراسة البنود المتعلقة بالعمل على الإصدار 3 من ترميز الاختبار وضبط الاختبار (TTCN-3)

ما هي التحسينات المطلوبة للإصدار 3 من ترميز الاختبار وضبط الاختبار (TTCN-3) لتلبية احتياجات التطبيقات المستقبلية؟

وسينفَّذ هذا العمل بالتعاون مع اللجنة التقنية المعنية بنظام نقل الرسائل لدى المعهد الأوروبي لمعايير الاتصالات (ETSI TC MTS).

## 5.2 صيانة اللغات الشكلية

مواصلة صيانة التوصيات المتعلقة بلغة التوصيف والوصف (SDL) وملف تعريف لغة النمذجة الموحدة (UML) ومخطط تتابع الرسائل (MSC) وترميز متطلبات المستخدم (URN) ولغة البرمجة CHILL.

## 6.2 صيانة التوصيل البيني للأنظمة المفتوحة (OSI)

مواصلة صيانة توصيات معمارية التوصيل البيني للأنظمة المفتوحة وفرادى الطبقات لتوفير أي تحسينات لازمة وتقويم أي أوجه قصور مبلغ عنها؛ ومواصلة صيانة التوصيات المتعلقة بخدمة وأنظمة معالجة الرسائل والنقل الموثوق به والعمليات عن بُعد والالتزام والتوافق والاستعادة ومعالجة المعامَلات، وذلك لغرض أي تحسينات لازمة وتقويم أي أوجه قصور 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 1 للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1) ولجانها الفرعية.

## 7.2  الحفاظ على المعالجة المفتوحة الموزعة (ODP)

مواصلة رعاية التوصيات المعنية بالمعالجة المفتوحة الموزعة.

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

وسيجري الاضطلاع بهذا العمل بالتعاون مع فريق العمل 19 التابع للجنة الخاصة 7 لدى اللجنة التقنية المشتركة 1 للمنظمة 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 للتوصيات ITU-T X.509 وX.510 وX.pki-em لدعم المتطلبات الجديدة مثل الإجراءات التلقائية لإنشاء وصيانة البنية التحتية للمفاتيح العمومية.

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

 أ ) تحديث سلاسل التوصيات X.680 وX.690 وX.890 خلال فترة الدراسة استجابة لاحتياجات المستعملين، وإصدار طبعات جديدة عند الاقتضاء.

ب) 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 الوسم القابلة للتوسيع (XML) المعرفة في توصيات قطاع تقييس الاتصالات (سواء الموجودة منها أو التي قيد الإعداد)، ولا سيما في حالات النطاق العريض المنخفض.

ج) المراقبة والمساعدة في عملية نشر التوصيات/المعايير الدولية والتصويبات التقنية الموافق عليها.

د ) البت في كل تقارير العيوب والتقدم في التصويبات التقنية حسب الضرورة.

هـ ) التأكد من معالجة جميع بيانات الاتصال المتعلقة بأعمال ترميز قواعد التركيب المجردة رقم 1 (ASN.1) على نحو مناسب مع حسن التوقيت.

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

## 3.3 المهام المتصلة بالأعمال في معرفات الكائنات وهيئات تسجيلها

 أ ) تحديث سلسلتي التوصيات ITU‑T X.660 وX.670 خلال فترة الدراسة استجابة لاحتياجات المستعملين، وإصدار طبعات جديدة عند الاقتضاء.

ب) المراقبة والمساعدة في عملية نشر التوصيات/المعايير الدولية والتصويبات التقنية الموافق عليها.

ج) البت في كل تقارير العيوب والتقدم في التصويبات التقنية حسب الضرورة.

د ) التأكد من معالجة جميع بيانات الاتصال المتعلقة بمعرفات الكائنات على نحو مناسب مع حسن التوقيت.

هـ ) وضع أي برمجيات تعليم أو صفحات ويب إضافية من المحتمل أن تساعد مستعملي معرفات الكائنات.

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

ز ) استعراض ترشيحات هيئات التسجيل لكل نوع من الأسماء المشمولة بالتوصية ITU-T X.660 | ISO/IEC 9834‑1، والاقتراح على لجنة الدراسات 17 المنظمة الكفيلة بتعيين اللجنة ISO/IEC/JTC 1/SC 6 وإبلاغها باستخدام بيان الاتصال للترشيح المحتفظ به.

ح) القيام، في إطار مسؤولية رئيس مشروع معرفات الكائنات بما يلي:

• توفير المشورة العامة للمستعملين بشأن معرفات الكائنات؛

• تعزيز استعمال قواعد التركيب المجردة رقم واحد (ASN.1) داخل لجان الدراسات الأخرى والمنظمات الخارجية الأخرى لوضع المعايير (SDO)؛

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

## 4.3 المهام المتصلة بالأعمال في ترميز الاختبار وضبط الاختبار (TTCN)

 أ ) إدارة التوصيات المندرجة في إطار مسؤولية هذه المسألة؛

ب) تعزيز استخدام ترميز الاختبار وضبط الاختبار (TTCN) ضمن لجان الدراسات الأخرى والمنظمات الخارجية الأخرى لوضع المعايير.

## 5.3 المهام المتصلة بالأعمال في صيانة اللغات الشكلية

إعداد تصحيحات أو تحسينات، حسب الحاجة، للتوصيات المتعلقة بلغة التوصيف والوصف (SDL) وملف تعريف لغة النمذجة الموحدة (UML) ومخطط تتابع الرسائل (MSC) وترميز متطلبات المستخدم (URN) ولغة البرمجة CHILL. وصيانة دليل منفذي لغة التوصيف والوصف (SDL).

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

وضع التصويبات أو إدخال التحسينات على التوصيات المتعلقة بالتوصيل البيني للأنظمة المفتوحة، حسب الحاجة، استناداً إلى المساهمات الواردة والبت في أي عيوب مبلغ عنها؛ صيانة الدليل الإرشادي للمنفِّذين في مجال التوصيل البيني للأنظمة المفتوحة.

## 7.3 المهام المتصلة بالأعمال في مجال الحفاظ على المعالجة المفتوحة الموزعة (ODP)

وضع التصويبات أو إدخال التحسينات على التوصيات المتعلقة بالمعالجة المفتوحة الموزعة، حسب الحاجة، استناداً إلى المساهمات الواردة والبت في أي عيوب مبلغ عنها.

ويرد بيان محدّث لحالة سير العمل في إطار هذه المسألة في برنامج عمل لجنة الدراسات 17 في الموقع:
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

# 4 الروابط

خطوط عمل القمة العالمية لمجتمع المعلومات:

جيم5.

أهداف التنمية المستدامة:

8 (العمل اللائق والنمو الاقتصادي)،
9 (الصناعة والابتكار والبنية التحتية).

التوصيات:

السلاسل H.200 وH.323 وH.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 والمسألة 14/17 المتعلقة بالبنية التحتية للمفاتيح العمومية الموزعة.

لجان الدراسات:

لجان الدراسات 2 و9 و11 و13 و15 و16 و20 لقطاع تقييس الاتصالات وجميع لجان الدراسات التي تستخدم الدليل أو ASN.1 أو معرفات الكائنات أو اختبار المطابقة وقابلية التشغيل البيني أو التي تحتاج إليها.

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 (ISO TCs 68, 204)؛ ومنظمة تقدم معايير المعلومات المهيكلة (OASIS)؛ فريق إدارة الأشياء (OMG)؛ اتحاد شبكة الويب العالمية (W3C)؛ اللجنة التقنية المعنية بنظام نقل الرسائل لدى المعهد الأوروبي لمعايير الاتصالات (ETSI) (TC MTS)؛ اللجنة التقنية المشتركة 1 لدى المنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1) ولجانها الفرعية التي تستخدم لغات تصميم نظام الاتحاد الدولي للاتصالات.

هيئات أخرى:

الاتحاد البريدي العالمي (UPU)؛ جمعية منتدى لغة التوصيف والوصف (SDL).

مشروع المسألة 13/17

أمن نظام النقل الذكي

(استمرار للمسألة 13/17)

# 1 المسوغات

يقدم نظام النقل الذكي (ITS) بما في ذلك نظام القيادة المستقلة أنواعاً مختلفة من التطبيقات من أجل زيادة السلامة على الطرق وتقليل الوطأة البيئية للنقل وتعزيز إدارة حركة المرور وتحقيق فوائد قطاع النقل القصوى لعموم المستخدمين وللمستخدمين التجاريين.

وتتضمن أنظمة النقل الذكية أنواعاً مختلفة من الاتصالات في المركبات (من مركبة إلى جهاز متجول على سبيل المثال)، وبين المركبات (من مركبة إلى مركبة (V2V) على سبيل المثال)، وبين المركبات والمواقع الثابتة (من مركبة إلى بنية تحتية (V2I) على سبيل المثال)، أي اتصالات من مركبة إلى كل شيء (V2X). وتُستخدم تكنولوجيا المعلومات والاتصالات (ICT) لتنفيذ أنظمة النقل الذكية بما في ذلك أنظمة النقل البري والسكك الحديدية والنقل المائي والجوي، بما في ذلك أنظمة الملاحة.

ويتكون نظام القيادة المؤتمت والمساعَد من مكونات مختلفة للأنظمة حيث يجري التنبه واتخاذ القرار وتشغيل السيارة عن طريق الإلكترونيات والآلات بدلاً من السائق البشري، وكإدخال للأتمتة في حركة المرور على الطرق.

وفي أنظمة النقل الذكية (ITS) بما في ذلك بيئة نظام القيادة المستقلة والمُساعَدة، يمكن نشر نقاط الضعف في السيارة إلى المركبات الأخرى نظراً لأن المركبات موصولة ببعضها البعض. وبالتالي، تنبغي إدارة نقاط الضعف في أنظمة اتصالات V2X في السيارة والتعامل معها بغية عدم التأثير على الكثير من المركبات الأخرى.

وأصبحت الأجهزة الكهربائية داخل مركبة، مثل وحدات التحكم الإلكترونية (ECU) وأجهزة تحصيل الرسوم الكهربائية (ETC)، أكثر تطوراً. ونتيجة لذلك، تحتاج وحدات البرمجيات داخل تلك الكيانات إلى التحديث بشكل مناسب لتحسين الأداء والأمن.

وتقدم التوصية ITU-T X.1373 التي ووفق عليها في مارس 2017 قدرات تحديث البرمجيات المأمونة لأجهزة اتصالات أنظمة النقل الذكية. والتوصية X.1373 قيد المراجعة حالياً.

ويعد تقييس أفضل الحلول الأمنية الشاملة أمراً حيوياً لبيئة أنظمة النقل الذكية. ونظراً لبعض الخصائص المحددة لاتصالات المركبات، ينطوي تحقيق الأمن بشكل خاص على مهام صعبة تستحق الدراسة.

وتشمل التوصيات التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 7 يناير 2022 ما يلي: X.1371، X.1372، X.1373 وX.1374 وX.1375 وX.1376.

النصوص قيد الإعداد اعتباراً من 7 يناير 2022 هي: X.1373rev و X.edrsecو X.eivnsecو X.evtol-secو X.fstiscvوX.idse وX.ipscv و X.itssec-5و X.rsu-secوX.srcd.

# 2 المسألة

تتناول الدراسة البنود التالية دون أن تقتصر عليها:

 أ ) كيف ينبغي تحديد وتعريف الجوانب الأمنية (من قبيل معمارية الأمن والأنظمة الفرعية) في بيئة أنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة؟

ب) كيف ينبغي تحديد التهديدات ونقاط الضعف في خدمات وشبكات أنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة والتعامل معها؟

ج) ما هي متطلبات الأمن (كتلك الخاصة بتحديد الهوية والاستيقان) للتخفيف من التهديدات في بيئة أنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة؟

د ) ما هي تقنيات الأمن اللازمة لدعم خدمات وشبكات أنظمة النقل الذكية؟

هـ ) كيف ينبغي الحفاظ على التوصيلية البينية المأمونة وصيانتها بين الكيانات في بيئة أنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة؟

و ) ما هي التقنيات والآليات والبروتوكولات الأمنية اللازمة لخدمات وشبكات أنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة؟

ز ) ما هي الحلول الأمنية المقبولة عالمياً لخدمات وشبكات أنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة والتي تستند إلى شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات؟

ح) ما هي أفضل الممارسات أو المبادئ التوجيهية لأمن أنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة؟

ط) كيف يمكن استخدام تكنولوجيات الذكاء الاصطناعي/تعلم الآلة لتقديم الأمن والثقة في أنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة؟

ي) ما هي الآليات اللازمة لحماية المعلومات المحددة لهوية الأشخاص (PII) وإدارتها في خدمات أنظمة النقل الذكية؟

# 3 المهام

تشمل المهام البنود التالية دون أن تقتصر عليها:

 أ ) إعداد مجموعة من التوصيات التي تقدم حلولاً أمنية شاملة لأنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة.

ب) مواصلة الدراسة لتحديد الجوانب الأمنية لخدمات وشبكات أنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة والتي تستند إلى شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات.

ج) دراسة وتحديد القضايا والتهديدات الأمنية في أنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة.

د ) دراسة وتحديد المتطلبات وحالات الاستخدام لخدمات وشبكات أنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة.

هـ ) دراسة ووضع آليات وبروتوكولات وتكنولوجيات الأمن لأنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة.

و ) دراسة ووضع بيانات وصفية أمنية ومخطط تراتبي للاستيقان ولآلية تخص خدمات وتطبيقات أنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة.

ز ) دراسة ووضع تطبيقات خوارزميات التجفير وفك التجفير الفعالة لعقد الشبكة سريعة الحركة وطوبولوجيات الشبكة المتغيرة دينامياً.

ح) دراسة ووضع تكنولوجيات تسجيل بيانات الأحداث في سياق أنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة.

ط) دراسة ووضع آليات التوصيلية البينية المأمونة لأنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة في بيئة اتصالات.

ي) دراسة وتحديد قضايا المعلومات المحددة لهوية الأشخاص (PII) والتهديدات التي تتعرض لها في أنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة.

ك) دراسة ووضع آليات حماية وإدارة المعلومات المحددة لهوية الأشخاص في أنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة.

ل) دراسة ووضع أنظمة النقل الذكية وأنظمة القيادة المستقلة والمُساعَدة المأمونة على أساس تكنولوجيات الذكاء الاصطناعي/تعلم الآلة.

م ) دراسة ووضع مشاريع التوصيات القائمة X.1373rev، وX.itssec-5، وX.srcd، وX.edrsec، وX.eivnsec، وX.fstiscv وX.ipscv وX.rsu-sec وX.evtol-sec.

ن) التعاون مع منظمات وضع المعايير ذات الصلة لوضع توصيات بشكل مشترك.

ويرد بيان محدّث لحالة سير العمل في إطار هذه المسألة في برنامج عمل لجنة الدراسات 17 في الموقع:
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

# 4 الروابط

خطوط عمل القمة العالمية لمجتمع المعلومات:

جيم5.

أهداف التنمية المستدامة:

8 (العمل اللائق والنمو الاقتصادي)،
9 (الصناعة والابتكار والبنية التحتية)،
11 (المدن والمجتمعات المستدامة).

التوصيات:

سلسلة التوصيات X وغيرها من التوصيات المتعلقة بالأمن.

المسائل:

المسائل 1/17 و2/17 و3/17 و4/17 و6/17 و7/17 و8/17 و10/17 و11/17 و15/17.

لجان الدراسات والأفرقة المتخصصة:

لجان الدراسات 11 و13 و16 و20 لقطاع تقييس الاتصالات؛ فرقة العمل 5A لقطاع الاتصالات الراديوية؛ التعاون بشأن معايير الاتصالات لأنظمة النقل الذكية (CITS)؛ الفريق المتخصص التابع لقطاع تقييس الاتصالات المعني بالوسائط المتعددة في المركبات (ITU-T FG-VM).

هيئات التقييس:

اللجنتان التقنيتان 22 و204 لدى المنظمة الدولية للتوحيد القياسي؛ اللجنتان الخاصتان 6 و27 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SCs 6 and 27)؛ فريق العمل المعني بنظام النقل الذكي لدى فريق مهام هندسة الإنترنت (IETF)؛ فريق العمل 802.11 وفريق العمل 1609 لدى معهد مهندسي الكهرباء والإلكترونيات (IEEE)؛ الجمعية الدولية لمهندسي السيارات (SAE International) (من قبيل لجنة هندسة أنظمة الأمن السيبراني للمركبة، ولجنة توجيه المركبات الموصولة، ولجنة المعايير التقنية DSRC)؛ اللجنة التقنية المعنية بنظام النقل الذكي لدى المعهد الأوروبي لمعايير الاتصالات (ETSI)؛ فريق العمل المعني بالسيارات لدى اتحاد شبكة الويب العالمية (W3C).

هيئات أخرى:

رابطة النظام العالمي للاتصالات المتنقلة (GSMA)؛

تحالف حلول صناعة الاتصالات (ATIS)؛ رابطة تقييس الاتصالات الصينية (CCSA)؛ رابطة صناعة الاتصالات (TIA)؛ رابطة تكنولوجيا الاتصالات (TTA)؛ لجنة تكنولوجيا الاتصالات (TTC)؛ فرقة العمل رقم 29 لدى اللجنة الاقتصادية لأوروبا التابعة للأمم المتحدة والهيئات الفرعية (كفريق المهام المعني بالأمن السيبراني (TFCS))؛ نظام Linux من درجة السيارات (AGL).

المسألة 14/17

أمن تكنولوجيا السجلات الموزعة (DLT)

(استمرار للمسألة 14/17)

# 1 المسوغات

تعد تكنولوجيا السجلات الموزعة (DLT)، وأبرز تطبيق لها هو سلسلة الكتل، نوعاً جديداً من السجلات المأمونة التي تُتداول وتُستنسخ وتتزامن بشكل موزع. وتتحكم أطراف متعددة في البيانات الموجودة في السجلات الموزعة.

وباعتبارها تكنولوجيا قاعدة بيانات موزعة محددة، تقاوم تكنولوجيا السجلات الموزعة بطبيعتها تعديل البيانات - بمجرد تسجيلها، ولا يمكن تغيير البيانات الموجودة في كتلة بأثر رجعي. وباتت هذه الميزة البارزة لتكنولوجيا السجلات الموزعة معروفة جيداً بعد نجاح تطبيقاتها المبكرة في العملات الرقمية المجفَّرة المعروفة باسم عملة البتات (Bitcoin).

وأصبحت تكنولوجيا السجلات الموزعة إحدى التكنولوجيات المحدِثة لتحولات ذات إمكانات كبيرة كفيلة بتغيير اقتصادنا وثقافتنا ومجتمعنا. وتمكن تكنولوجيا السجلات الموزعة التطبيقات المالية/غير المالية اللامركزية المبتكرة التي تُغني عن وسطاء من أطراف ثالثة. وستقدم تكنولوجيا السجلات الموزعة بنية تحتية جديدة لإدارة البيانات من شأنها تسريع ثورة الخدمات في صناعات (كالصيرفة والتمويل، والحكومة، والرعاية الصحية، والخدمات اللوجستية الفائقة) قائمة على الاتصالات.

وستؤثر تكنولوجيات السجلات الموزعة تأثيراً عميقاً على مستخدمي الاتصالات وعلى الصناعات بما في ذلك مقدمو خدمات الاتصالات.

وهناك حاجة لتحديد أدوار ومسؤوليات مستخدمي ومشغلي الاتصالات ومقدمي الخدمات فيما يتعلق بجوانب الأمن في بيئة تكنولوجيا السجلات الموزعة.

ويعد تقييس أفضل الحلول الأمنية الشاملة أمراً حيوياً لتكنولوجيا السجلات الموزعة التي تضم عدداً كبيراً من حالات الاستخدام في جميع القطاعات بما في ذلك صناعة الاتصالات. ونظراً لبعض الخصائص المحددة لتكنولوجيا السجلات الموزعة، ينطوي تقديم الأمن بشكل خاص على مهام صعبة تستحق الدراسة.

وتشمل التوصيات التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 7 يناير 2022 ما يلي: X.1400 وX.1401 وX1402 وX.1403 وX.1404 وX.1405 وX.1406 وX.1407 وX.1408.

النصوص قيد الإعداد اعتباراً من 7 يناير 2022 هي: X.sa-dsm و X.sc-dltو X.srscm-dltو X.ss-dlt وTR.qs-dlt.

# 2 المسألة

تتناول الدراسة البنود التالية دون أن تقتصر عليها:

 أ ) كيف ينبغي تحديد وتعريف الجوانب الأمنية (مثل المعمارية والأنظمة الفرعية) باء على الأسس (المصطلحات والتعاريف والمفاهيم والتصنيف وحالات الاستخدام) في بيئة تكنولوجيا السجلات الموزعة (DLT)؟

ب) كيف ينبغي التعامل مع التهديدات ونقاط الضعف في التطبيقات والخدمات القائمة على تكنولوجيا السجلات الموزعة؟

ج) ما هي المتطلبات الأمنية للتخفيف من التهديدات في بيئة تكنولوجيا السجلات الموزعة؟

د ) ما هي تكنولوجيات الأمن اللازمة لدعم التطبيقات والخدمات القائمة على تكنولوجيا السجلات الموزعة؟

هـ ) كيف ينبغي الحفاظ على التوصيلية البينية المأمونة وصيانتها بين الكيانات في بيئة تكنولوجيا السجلات الموزعة؟

و ) ما هي تقنيات وآليات وبروتوكولات الأمن اللازمة للتطبيقات والخدمات القائمة على تكنولوجيا السجلات الموزعة؟

ز ) ما هي الحلول الأمنية المقبولة عالمياً للتطبيقات والخدمات القائمة على تكنولوجيا السجلات الموزعة، والتي تستند إلى شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات؟

ح) ما هي أفضل الممارسات أو المبادئ التوجيهية لأمن التطبيقات والخدمات القائمة على تكنولوجيا السجلات الموزعة

ط) ما هي حماية المعلومات المحددة لهوية الأشخاص (PII) وإدارة أمن المعلومات اللازمتان للتطبيقات والخدمات القائمة على تكنولوجيا السجلات الموزعة؟

ي) كيف يمكن استخدام تكنولوجيا السجلات الموزعة لدعم الأمن؟

ك) كيف يمكن تقدير أمن تكنولوجيا السجلات الموزعة وتقييمه وضمانه؟

ل) من هم أصحاب المصلحة الذين ينبغي للجنة الدراسات 17 أن تتعاون معهم؟

# 3 المهام

تشمل المهام البنود التالية دون أن تقتصر عليها:

 أ ) إجراء تحليل للثغرات القائمة في العمل الجاري المتعلق بالأمن في المؤسسات الأخرى لتكنولوجيات السجلات الموزعة.

ب) مواصلة الدراسة لتحديد الجوانب الأمنية للتطبيقات والخدمات القائمة على تكنولوجيا السجلات الموزعة، والتي تستند إلى شبكات الاتصالات/تكنولوجيا المعلومات والاتصالات.

ج) دراسة الأسس مثل المصطلحات والتعاريف والمفاهيم والتصنيف وحالات الاستخدام التي تتعلق بالأمن وحماية المعلومات المحددة لهوية الأشخاص في شبكات تكنولوجيا السجلات الموزعة.

د ) دراسة وتحديد القضايا والتهديدات الأمنية في التطبيقات والخدمات القائمة على تكنولوجيا السجلات الموزعة.

هـ ) دراسة ووضع آليات وبروتوكولات وتكنولوجيات الأمن للتطبيقات والخدمات القائمة على تكنولوجيا السجلات الموزعة.

و ) دراسة ووضع آليات التوصيلية البينية المأمونة للتطبيقات والخدمات القائمة على تكنولوجيا السجلات الموزعة.

ز ) دراسة وتحديد قضايا حماية المعلومات المحددة لهوية الأشخاص والتهديدات التي تتعرض لها في التطبيقات والخدمات القائمة على تكنولوجيا السجلات الموزعة.

ح) دراسة ووضع نظام إدارة معلومات للجهات التي تقدم التطبيقات والخدمات القائمة على تكنولوجيا السجلات الموزعة.

ط) دراسة ووضع إرشادات بشأن استخدام تكنولوجيا السجلات الموزعة لدعم الأمن.

ي) دراسة ووضع الإرشادات الخاصة بالتقييم والتقدير والضمان في مجال أمن تكنولوجيات السجلات الموزعة.

ك) وضع مجموعة من التوصيات لتقديم حلول أمنية شاملة للتطبيقات والخدمات القائمة على تكنولوجيات السجلات الموزعة.

ويرد بيان محدّث لحالة سير العمل في إطار هذه المسألة في برنامج عمل لجنة الدراسات 17 في الموقع:
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

# 4 الروابط

خطوط عمل القمة العالمية لمجتمع المعلومات:

جيم5.

أهداف التنمية المستدامة:

8 (العمل اللائق والنمو الاقتصادي)،
9 (الصناعة والابتكار والبنية التحتية)،
11 (المدن والمجتمعات المستدامة).

التوصيات:

سلسلة التوصيات X وغيرها من التوصيات المتعلقة بالأمن.

المسائل:

المسألة 1/17 و2/17 و3/17 و4/17 و6/17 و7/17 و8/17 و10/17 و11/17 و13/17 و15/17.

لجان الدراسات:

لجان الدراسات 5 و11 و13 و16 و20 لقطاع تقييس الاتصالات.

هيئات التقييس:

اللجنة التقنية 307 لدى المنظمة الدولية للتوحيد القياسي؛ اللجنة الخاصة 27 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SC 27).

هيئات أخرى:

رابطة النظام العالمي للاتصالات المتنقلة (GSMA)؛ اتحاد شبكة الويب العالمية (W3C)؛ معهد مهندسي الكهرباء والإلكترونيات (IEEE)؛ اللجنة الاقتصادية لأوروبا التابعة للأمم المتحدة (UNECE)؛ المبادرة العالمية للشمول المالي (FIGI)؛ تحالف حلول صناعة الاتصالات (ATIS)؛ رابطة تقييس الاتصالات الصينية (CCSA)؛ رابطة صناعة الاتصالات (TIA)؛ رابطة تكنولوجيا الاتصالات (TTA)؛ لجنة تكنولوجيا الاتصالات (TTC).

المسألة 15/17

الأمن من أجل/من خلال التكنولوجيات الناشئة
بما في ذلك الأمن القائم على التكنولوجيا الكمومية

(استمرار للمسألة 15/17)

# 1 المسوغات

تدرك لجنة الدراسات 17 الطبيعة الدينامية للدراسات الأمنية التي تعتمد إلى حد كبير على كل من سباق التسلح بين المهاجم والمدافعين وتداعيات الابتكارات التي يستخدمها كلا الجانبين. وينتج عن ذلك وتيرة متسارعة لتكنولوجيات الأمن الناشئة التي يتطلب بعضها تقييساً عالمياً.

ونظراً لاستحالة توقع ماهية وتوقيت المجالات الأمنية الناشئة بحكم طبيعتها، قامت لجنة الدراسات 17 استباقياً بإنشاء وتشغيل آلية حضانة (TP.inno) توفر مرونة محكمة في دراسة المجالات الأمنية الناشئة من أجل تأمين خدمات وتطبيقات جديدة قائمة على الاتصالات/تكنولوجيا المعلومات والاتصالات.

وتمكّن آلية الحضانة لجنة الدراسات 17 من تقديم بنود عمل جديدة بكفاءة في المجالات الناشئة وتشجع النصوص غير المعيارية (الأوراق التقنية والتقارير التقنية) كأفضل ممارسة مثبتة لإفساح الوقت أمام مجتمع لجنة الدراسات 17 للتعرف على هذه المجالات الناشئة الجديدة وأمام القادمين الجدد للتعرف على إجراءات وبيئة لجنة الدراسات 17 وقطاع تقييس الاتصالات. وعند إعداد بنود العمل الجديدة، تكشف طبيعة تكنولوجيا الأمن الناشئة أحياناً أنها أقرب إلى مسألة قائمة وإمكانية نقل بند العمل هذا لتحقيق أقصى ما يمكن من تماسك وكفاءة وجودة في عمل لجنة الدراسات 17.

بالإضافة إلى ذلك، تتيح آلية الحضانة هذه تحديد الاتجاهات في تكنولوجيات الأمن الناشئة الجاري تطويرها في هذا المسألة. وبعض التكنولوجيات الناشئة تأتي مما يلي:

- حداثة عهد الموضوع نفسه، كالأمن المستند إلى التكنولوجيا الكمومية، أو الحوسبة المأمونة متعددة الأطراف، أو التشابه بين الأشكال، أو الأمن الذي يمكن تحديده للروبوتات، وما إلى ذلك.

- موضوع ليس مستجداً ولكنه في أول عهده بالتقييس العالمي، كتحليل البرمجيات الخبيثة، ومنع فقدان البيانات، وما إلى ذلك.

- ثغرات في المعمارية الأمنية التشغيلية لا تتعلق بأي مسألة، كمنتجات الأمن نفسها، وإشكالات كثافة الدمج والتكوين التي تعرض حلولاً جديدة ناشئة لموضوعات مشتركة، ومخططات بيانات أمنية، وما إلى ذلك.

ويتمثل أحد المجالات الناشئة التي تبينت أثناء آلية الحضانة في الأمن القائم على التكنولوجيا الكمومية. لأن ظهور الحواسيب الكمومية الضخمة ينطوي على إمكانية حدوث تحولات كبيرة في أنظمة الاتصالات التقليدية القائمة على تكنولوجيا المعلومات والاتصالات، ويشكل أيضاً مخاطر كبيرة على الأمن.

وفي الواقع، يعتمد أمن التجفير الحالي على مشكلتين حاسوبيتين صعبتين: مشكلة لوغاريتمية منفصلة ومشكلة عوامل العدد الصحيح. ويصعب حلهما في وقت معقول بالنظر إلى المعماريات الحالية للحواسيب الحالية المتاحة اليوم وعلى المدى المتوسط. ولكن يعد تجفير المفاتيح العمومية باستخدام المفاتيح غير المتناظرة حجر الزاوية في الاستيقان عبر الشبكات العمومية. ونظراً لأن الحواسيب الكمومية يمكنها، بطبيعتها، حل مشاكل عوامل العدد الصحيح واللوغاريتم المنفصل بسرعة معقولة، فهي قادرة، من خلال تأثيراتها، على كسر الأسس التي يُبنى عليها التجفير حالياً، مما يهدد حجر الزاوية الوجودي للحياة السيبرانية والرقمنة اليوم.

ويتيح التوزيع الكمومي للمفاتيح (QKD) لطرفين إنتاج مفتاح سري عشوائي مشترك معروف لهما فقط ويمكن استخدامه لتجفير وفك تجفير الرسائل باستخدام خوارزميات التجفير التقليدية. فللتوزيع الكمومي للمفاتيح حدان يتسببان بإشكالات للشبكة من حيث الطوبولوجيا والتكامل: أ) فهو يعمل من نقطة إلى نقطة (p-t-p) ولا يمكن تطبيقه إلا على طرفين، A وB وب) هو مقيد بالمسافة على الشبكات الأرضية. وللتغلب على هذين التقييدين، أُدخل مفهوم شبكات QKD في الصناعة وهو يتكون من (1) مجموعة من العقد الموصولة ببعضها البعض من خلال أنظمة QKD التي تعمل من نقطة إلى نقطة (p-t-p)، و(2) نظام إدارة مشترك بين، ودمج في، كل من عقد QKD. والغرض من نظام الإدارة هذا هو توزيع المفاتيح السرية بين عقدتين أو أكثر داخل شبكة QKD نفسها والتي قد لا تكون موصولة بشكل مباشر. وأنظمة QKD التجارية مستقرة وناضجة بما يكفي حالياً لبدء التخطيط لشبكات QKD واسعة النطاق. وهناك عدة مبادرات من قبل الشركات/المؤسسات لتطوير شبكات QKD، ولكن لا يوجد معيار مقبول على نطاق واسع لما يشكل نظام QKD.

بالإضافة إلى ذلك، تعد الأرقام العشوائية عنصراً رئيسياً في الهندسة بتطبيقات مهمة في التجفير. والعشوائية المتأصلة في جوهر الميكانيكا الكمومية تجعل الأنظمة الكمومية مصدراً مثالياً للإنتروبيا. ويعد توليد الأرقام العشوائية الكمومية من أكثر التكنولوجيات الكمومية نضجاً بفضل كثرة اساليب الإنشاء البديلة.

وخلاصة القول، يضمن الأمن المعتمد على التكنولوجيا الكمومية اتصالاً عصياً على هجمات الحواسيب الكمومية. ويتطلب تنفيذ الأمن المستند إلى التكنولوجيا الكمومية العديد من العناصر الرئيسية بما في ذلك التوزيع الكمومي للمفاتيح ومولد الأرقام العشوائية الكمومية (QRNG). وبالإضافة إلى ذلك، فإن قابلية التشغيل البيني في العناصر والوظائف الرئيسية للتوزيع الكمومي للمفاتيح ومولد الأرقام العشوائية الكمومية تكتسي أهمية عند استخدامها على نطاق واسع في شبكات الاتصالات الحقيقية.

وفي المقابل، هناك حاجة ماسة لقيام لجنة الدراسات 17 بدراسة الأمن القائم على التكنولوجيا الكمومية والمقاوم للهجمات الكمومية.

وتشمل التوصيات والورقات/التقارير التقنية التي تندرج في إطار مسؤولية هذه المسألة اعتباراً من 7 يناير 2022 ما يلي: X.1702 وX.1710 وX.1712 وX.1714 وX.1770 والورقات التقنية TP.inno وTP.sgstruct وTR.sec-qkd.

النصوص قيد الإعداد اعتباراً من 7 يناير 2022 هي: تصويب التوصية X.1712 و X.icd-schemasوX.sec\_QKDN\_AA وX.sec\_QKDN\_CM و X.sec\_QKDN\_intrqو X.sec-QKDN-tnو TR.hybsec-qkdnو TR.sec-ai وTR.sgfdm.

# 2 المسألة

تتناول الدراسة البنود التالية دون أن تقتصر عليها:

 أ ) ما هي تكنولوجيات الأمن الناشئة الجديدة؟

ب) ما هي فئات تكنولوجيات الأمن الناشئة الجديدة؟

ج) كيف يمكن تطوير تكنولوجيات الأمن الناشئة بما يضمن السلامة؟

د ) ما هي أكثر الآليات فعالية لتنفيذ آلية الحضانة؟

هـ ) ما هي التأثيرات والتحديات التي تواجهها الاتصالات التقليدية جراء ظهور الحواسيب الكمومية الضخمة؟

و ) ما هي العناصر الأساسية لبناء الأمن القائم على التكنولوجيا الكمومية؟

ز ) ما هي استراتيجية الانتقال لبناء الأمن القائم على التكنولوجيا الكمومية ؟

ح) كيف ينبغي التعامل مع التهديدات ونقاط الضعف في الأمن القائم على التكنولوجيا الكمومية؟

ط) ما هي متطلبات الأمن للتخفيف من التهديدات في الأمن القائم على التكنولوجيا الكمومية؟

ي) ما هي تكنولوجيات الأمن اللازمة لدعم الأمن القائم على التكنولوجيا الكمومية؟

ك) كيف ينبغي الحفاظ على التوصيلية البينية المأمونة وصيانتها بين الكيانات في الأمن القائم على التكنولوجيا الكمومية؟

ل) ما هي متطلبات وتقنيات وآليات وبروتوكولات الأمن اللازمة للأمن القائم على التكنولوجيا الكمومية؟

م ) ما هي الحلول الأمنية المقبولة عالمياً للأمن القائم على التكنولوجيا الكمومية، والتي تستند إلى اتصالات الاتصالات/تكنولوجيا المعلومات والاتصالات؟

ن) ما هي أفضل الممارسات أو المبادئ التوجيهية للأمن في مجال الأمن القائم على التكنولوجيا الكمومية؟

# 3 المهام

تشمل المهام البنود التالية دون أن تقتصر عليها:

 أ ) تحديد تكنولوجيات الأمن الناشئة الجديدة.

ب) تحديد فئات جديدة من تكنولوجيات الأمن الناشئة لتوطيد استراتيجية المسألة M.

ج) إمكانية إعادة توزيع بند العمل الجديد لمسألة أخرى إذا اتضح عند إعداده تطابقه مع مسألة موجودة.

د ) دمج آلية الحضانة لمعالجة المجالات الناشئة الجديدة في لجنة الدراسات 17 لقطاع تقييس الاتصالات.

هـ ) وضع مجموعة من التوصيات التقنية التي تقدم حلولاً أمنية شاملة لتأسيس الأمن القائم على التكنولوجيا الكمومية.

و ) دراسة لتحديد الجوانب الأمنية للأمن القائم على التكنولوجيا الكمومية الذي يقوم على البنية التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات.

ز ) دراسة وتحديد القضايا والتهديدات الأمنية في الأمن القائم على التكنولوجيا الكمومية.

ح) دراسة ووضع المتطلبات والآليات والبروتوكولات والتكنولوجيات الأمنية للأمن القائم على التكنولوجيا الكمومية.

ط) دراسة ووضع آليات التوصيلية البينية المأمونة للأمن القائم على التكنولوجيا الكمومية.

ي) دراسة ووضع نظام إدارة المعلومات للجهات التي تقدم الأمن القائم على التكنولوجيا الكمومية.

ويرد بيان محدّث لحالة سير العمل في إطار هذه المسألة في برنامج عمل لجنة الدراسات 17 في الموقع:
<https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17>.

# 4 الروابط

خطوط عمل القمة العالمية لمجتمع المعلومات:

جيم5.

أهداف التنمية المستدامة:

8 (العمل اللائق والنمو الاقتصادي)،
9 (الصناعة والابتكار والبنية التحتية)،
11 (المدن والمجتمعات المستدامة).

التوصيات:

سلسلة التوصيات X وغيرها من التوصيات المتعلقة بالأمن.

المسائل:

المسائل 1/17 و2/17 و3/17 و4/17 و6/17 و7/17 و8/17 و10/17 و11/17 و13/17 و14/17.

لجان الدراسات:

لجان الدراسات 2 و3 و5 و9 و11 و12 و13 و15 و16 و20 لقطاع تقييس الاتصالات.

هيئات التقييس:

اللجنة التقنية المعنية بالأمن السيبراني لدى المعهد الأوروبي لتقييس الاتصالات (ETSI)؛ فريق المواصفات الصناعية المعني بالتوزيع الكمومي للمفاتيح لدى المعهد الأوروبي لمعايير الاتصالات (ISG-QKD)؛ اللجنة الخاصة 27 لدى اللجنة التقنية المشتركة 1 التابعة للمنظمة الدولية للتوحيد القياسي/اللجنة الكهرتقنية الدولية (ISO/IEC JTC 1/SC 27)؛ منظمة تقدم معايير المعلومات المهيكلة (OASIS)؛ فريق مهام هندسة الإنترنت (IETF).

هيئات أخرى:

رابطة النظام العالمي للاتصالات المتنقلة (GSMA)؛ تحالف حلول صناعة الاتصالات (ATIS)؛ رابطة تقييس الاتصالات الصينية (CCSA)؛ رابطة صناعة الاتصالات (TIA)؛ رابطة تكنولوجيا الاتصالات (TTA)؛ لجنة تكنولوجيا الاتصالات (TTC).

ــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــــ