التوصية

ITU-T X.1454 (09/2023)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تطبيقات وخدمات آمنة (2) – أمن التطبيقات (2)

التدابير الأمنية المتعلقة بخدمات المكاتب الذكية القائمة على الموقع

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199-X.1
التوصيل البيني للأنظمة المفتوحة	X.299-X.200
التشغيل البيني للشبكات	X.399-X.300
أنظمة معالجة الرسائل	X.499-X.400
الدليل	X.599-X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699-X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799-X.700
الأمن	X.849-X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899-X.850
المعالجة الموزعة المفتوحة	X.999-X.900
أمن المعلومات والشبكات	X.1099-X.1000
تطبيقات وخدمات آمنة (1)	X.1199-X.1100
الأمن السيبراني	X.1299-X.1200
تطبيقات وخدمات آمنة (2)	X.1499-X.1300
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319-X.1310
أمن شبكة الكهرباء الذكية	X.1339-X.1330
البريد المعتمد	X.1349-X.1340
أمن إنترنت الأشياء (IoT)	X.1369-X.1350
أمن أنظمة النقل الذكية (ITS)	X.1399-X.1370
أمن سجل الحسابات الموزع	X.1429-X.1400
أمن التطبيقات (2)	**X.1459-X.1450**
أمن شبكة الويب (2)	X.1489-X.1470
تبادل معلومات الأمن السيبراني	X.1599-X.1500
أمن الحوسبة السحابية	X.1699-X.1600
الاتصالات الكمومية	X.1729-X.1700
أمن البيانات	X.1799-X.1750
أمن شبكات الاتصالات المتنقلة الدولية–2020	X.1819-X.1800

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

التوصية ITU-T X.1454

التدابير الأمنية المتعلقة بخدمات المكاتب الذكية القائمة على الموقع

ملخص

تهدف خدمات المكاتب الذكية التي تجمع بين تطبيقات ذكية متعددة إلى تحسين جودة الأعمال القائمة على المكاتب وتعزيز إدارة الكفاءة. ونظراً إلى أن تكنولوجيا المعلومات والاتصالات (ICT) تُستعمل كأساس للتكنولوجيات في خدمات المكاتب الذكية، يؤدي مشغل الاتصالات دوراً هاماً ضمن أصحاب المصلحة في إطار خدمات المكاتب الذكية.

وتشمل خدمات المكاتب الذكية النمطية مواقف السيارات الذكية والقيادة الذكية ومتاجر البيع بالتجزئة الذكية والمكاتب الذكية والإدارة الذكية لقاعات الاجتماعات والإدارة الذكية للمياه والإدارة الذكية لاستهلاك الطاقة، وغير ذلك. ومن بين هذه الخدمات المكتبية الذكية النمطية، تشكل بيانات الموقع التي يقدمها المشغل أحد العناصر الرئيسية في معظم عمليات تنفيذ خدمات المكاتب الذكية.

وبغية ضمان أمن خدمات المكاتب الذكية القائمة على الموقع، يتعين تحليل التهديدات الأمنية والمتطلبات الأمنية ذات الصلة الخاصة بالخدمات القائمة على الموقع، ووضع التدابير الأمنية الشاملة.

وتحلل التوصية ITU-T X.1454 سيناريوهات التطبيق النمطية لخدمات المكتب الذكية القائمة على الموقع، وتحدد التهديدات والمتطلبات الأمنية المرتبطة بها وتضع تدابير أمنية للمشغل وأصحاب المصلحة الرئيسيين في المكتب الذكي لحماية الخدمات القائمة على الموقع.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1454	2023-09-08	17	11.1002/1000/15111

مصطلحات أساسية

الموقع، التدابير الأمنية، خدمات المكاتب الذكية.

* للنفاذ إلى توصية، ترجى كتابة العنوان https://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد.

تمهيد

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

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

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

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

ملاحظة

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

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

حقوق الملكية الفكرية

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

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات/حقوق تأليف ونشر برمجيات يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قواعد البيانات ذات الصلة لقطاع تقييس الاتصالات (ITU-T) في موقع قطاع تقييس الاتصالات http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1454

التدابير الأمنية المتعلقة بخدمات المكاتب الذكية القائمة على الموقع

1 مجال التطبيق

تحلل هذه التوصية سيناريوهات التطبيق النمطية لخدمات المكاتب الذكية القائمة على الموقع، وتحدد التهديدات والمتطلبات الأمنية الخاصة بالخدمات القائمة على الموقع، وبالتالي تضع التدابير الأمنية للمشغل وأصحاب المصلحة الرئيسيين في المكاتب الذكية لحماية الخدمات القائمة على الموقع.

2 المراجع

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

لا توجد.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

لا توجد.

2.3 المصطلحات المعرّفة في هذه التوصية

تعرّف هذه التوصية المصطلح التالي:

1.2.3 خدمة المكتب الذكي (Smart office service): خدمة تضم العديد من التطبيقات الذكية (مثل مواقف السيارات الذكية والإدارة الذكية للمياه ومتاجر البيع بالتجزئة الذكية) التي تهدف إلى خدمة الأعمال القائمة على المكاتب ودعمها وتحسين جودتها وكفاءة إدارتها وتهيئة بيئة مكتبية مناسبة للناس.

4 الاختصارات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

DDoS رفض الخدمة الموزع (*Distributed Denial of Service*)

GNSS النظام العالمي للملاحة الساتلية (*Global Navigation Satellite System*)

ICT تكنولوجيا المعلومات والاتصالات (*Information and Communication Technology*)

RNSS خدمة الملاحة الراديوية الساتلية (*Radio Navigation Satellite System*)

SEM المراقبة البيئية الذكية (*Smart Environmental Monitoring*)

UWB نطاق عريض جداً (*Ultra-Wide Band*)

WiFi دقة لاسلكية (*Wireless Fidelity*)

5 اصطلاحات

تدل الكلمة الرئيسية "**يلزم**" على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم المطابقة مع هذه الوثيقة.

6 نظرة عامة على خدمات المكاتب الذكية القائمة على الموقع

وفقاً لرؤية المدن الذكية المستدامة التي تستعمل تكنولوجيات المعلومات والاتصالات (ICT) وغيرها من الوسائل لتحسين نوعية الحياة وكفاءة العمليات والخدمات الحضرية والقدرة على المنافسة، تصبح خدمة المكاتب الذكية تطبيقاً نموذجياً في مدينة ذكية مستدامة.

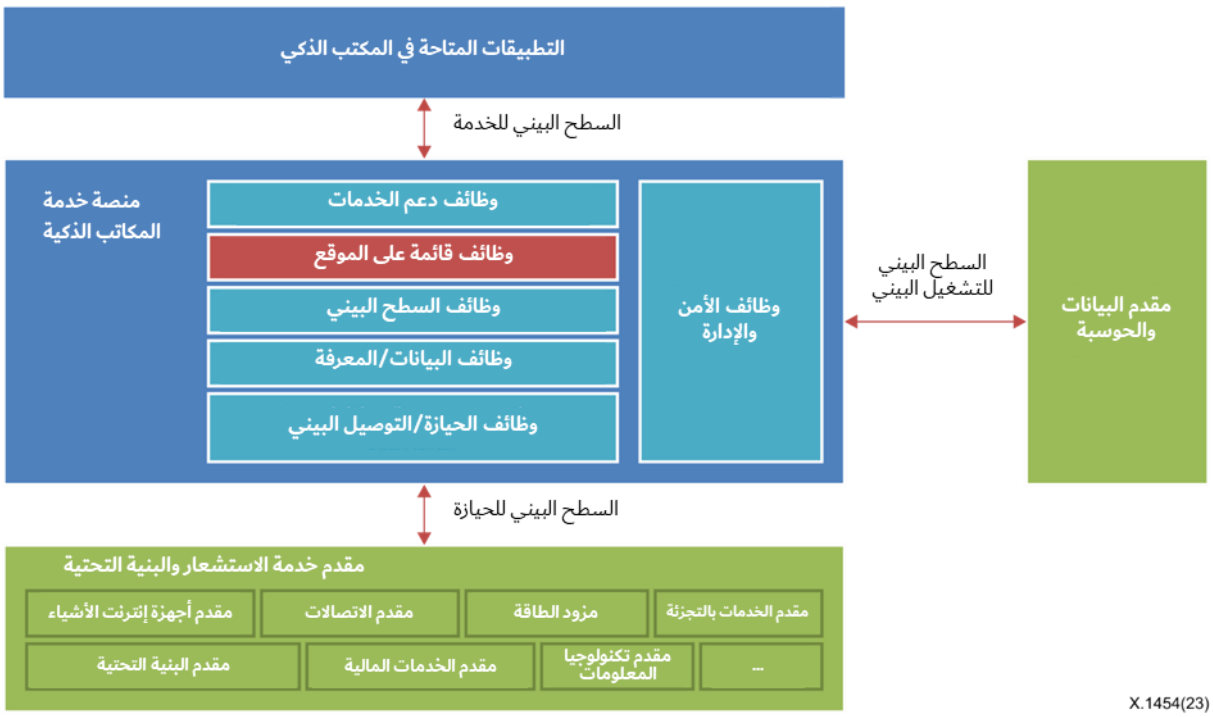
وتهدف خدمة المكاتب الذكية التي تجمع بين تطبيقات ذكية متعددة (مثل مواقف السيارات الذكية والإدارة الذكية للمياه ومتاجر البيع بالتجزئة الذكية) إلى تحسين نوعية عروض الأعمال التجارية القائمة على المكاتب وكفاءة إدارتها.

ونظراً لأن خدمات المكاتب الذكية تجمع بين تطبيقات ذكية متعددة، فإن أصحاب المصلحة الرئيسيين متنوعون. وبما أن تكنولوجيات المعلومات والاتصالات تستخدم كأساس لتكنولوجيات في خدمات المكاتب الذكية من بين خدمات المكاتب الذكية النمطية، تشكل بيانات الموقع التي يقدمها المشغل أحد العناصر الرئيسية في معظم تنفيذ هذه الخدمات.

وأصحاب المصلحة الرئيسيون في أنظمة المكاتب الذكية القائمة على الموقع هم:

- مقدم خدمة المكاتب الذكية؛
- مقدم البيانات والحوسبة؛
- مقدم خدمات الاستشعار والبنية التحتية؛
- المستعمل.

ملاحظة: يمكن أن يكون أصحاب المصلحة الرئيسيون هؤلاء، مقدمو خدمات المكاتب الذكية ومقدمو خدمات البيانات والحوسبة ومقدمو خدمات الاستشعار والبنية التحتية، في أنظمة المكاتب الذكية القائمة على الموقع، من مقدمي الخدمات المنفصلين أو من مقدمي الخدمات المتكاملة.



الشكل 1 – نظرة عامة على نظام المكاتب الذكية القائمة على الموقع

يوفر نظام المكتب الذكي القائم على الموقع الوظائف التالية:

- **وظائف الحيازة/التوصيل البيني:** توفر هذه الوظائف آليات التقاط البيانات من المصادر المختلفة لأنظمة الجمع.
- **وظائف البيانات/المعرفة:** تدعم هذه الوظائف معالجة البيانات وإضافة قيمة وتحويل المعلومات إلى معرفة.
- **وظائف السطح البيني:** تتيح هذه الوظائف من النفاذ إلى المعلومات على مختلف المستويات.
- **وظائف قائمة على الموقع:** توفر هذه الوظائف بيانات الموقع من نظام المشغل.
- **وظائف دعم الخدمات:** تتيح هذه الوظائف تنسيق جميع الخدمات الممكنة التي ينطوي عليها كل إجراء يوفر الدعم لوظائف التشغيل البيني.
- **وظائف الأمن والإدارة:** توفر وظائف أفقية مثل عمليات المراجعة والمراقبة والأمن.

وتتيح السطوح البينية الاتصال بين الوظائف:

- **السطح البيني للحيازة:** تتيح هذه الواجهة إمكانية جمع المعلومات من العناصر الخارجية.
- **السطح البيني للتشغيل البيني:** يتيح هذا السطح البيني التواصل مع مقدمي البيانات الخارجيين وأنظمة الحوسبة التابعة لجهات خارجية.
- **السطح البيني للخدمة:** يتيح هذا السطح البيني النفاذ من تطبيق إلى تطبيق لدعم الوظائف التي توفرها منصة الخدمات المكتبية الذكية.

7 سيناريوهات التطبيق النمطية لخدمات المكتب الذكية القائمة على الموقع

1.7 مواقف السيارات الذكية

توفر مواقف السيارات الذكية تكاملاً فعالاً لموارد مواقف السيارات في مواقف السيارات المكتبية وتنسق مرافق وقوف السيارات إلى جانب أنظمة أخرى (مثل نظام الدفع الخارجي، نظام مواقف السيارات القائم على الويب/التطبيق).

وقد تشمل مواقف السيارات الذكية الخدمات النمطية مثل توجيهات رَكْن السيارات وحجز أماكن رَكْن السيارات والبحث عند قيادة السيارات بالاتجاه الخلفي والتحكم التلقائي في الوصول إلى السيارات وخدمة الدفع الذاتية. وفيما يلي وظائف وقوف السيارات الذكية القائمة على الموقع:

- **توجيه رَكْن السيارات:** تدعم معلومات الموقع المتعلقة بأماكن وقوف السيارات غير المشغولة نشر معلومات عن وقوف السيارات.
- **حجز أماكن رَكْن السيارات:** يمكن أن تساعد معلومات الموقع في البحث عن معلومات حول الأماكن المتاحة لركن السيارات وحجز أماكن ركن السيارات مقدماً.
- **البحث بالاتجاه العكسي عن مكان ركن السيارة:** يمكن أن تساعد معلومات الموقع مستخدمي السيارة على تحديد مكان رَكْن سيارتهم في حالة نسيان مكان ركنها.

2.7 المراقبة البيئية الذكية

يمكن للمراقبة البيئية الذكية (SEM) أن تدرك الوضع البيئي الحالي باعتبارها تطبيقاً للمراقبة الذاتية والمراقبة البيئية ذاتية الحماية.

وقد تشمل المراقبة البيئة الذكية كيانات وظيفية لمنصات المراقبة البيئية الذكية وأجهزة المراقبة البيئية الذكية وشبكتها، وفيما يلي وظائف مراقبة البيئة الذكية القائمة على الموقع:

- **إدارة إعداد القياس:** يمثل موقع الجهاز المعلومات اللازمة لإعدادات القياس إلى جانب العوامل البيئية.
- **عرض البيانات:** البيانات غير المعالجة في كل موقع معيّن (لجهاز أو أكثر من أجهزة المراقبة البيئية الذكية) هي المعلومات الاختيارية لعرض الجودة البيئية.

3.7 التسليم الذكي

يستفيد التسليم الذكي من السيارة بدون سائق وتطبيق الروبوت في سيناريو المكتب الذكي، وبإمكانه تسليم الحزم والملفات واللوازم المكتبية وغيرها تلقائياً.

وفيما يلي وظائف التسليم الذكي القائم على الموقع:

- مساعدة القيادة الذاتية من خلال توفير القدرة على تحديد الموقع بدقة في حدود السنتميتر.
- تعزيز كفاءة الإرسال لدى السيارة/الروبوت من خلال تقابل ترتيب التسليم مع موقع الجهاز.
- استمثال مسار التسليم ومراقبة عملية التسليم من خلال تتبع موقع ومسار السيارة/الروبوت في الوقت الفعلي.

8 التهديدات الأمنية لخدمة المكاتب الذكية القائمة على الموقع

1.8 التهديدات الأمنية بالنسبة للبيانات

1.1.8 التنصت على بيانات الموقع

يمكن أن تستند بيانات الموقع في خدمات المكاتب الذكية إلى الشبكة اللاسلكية المفتوحة، فقد يتنصت مهاجم ما على بيانات الموقع عن طريق مراقبة القناة اللاسلكية.

2.1.8 التلاعب ببيانات الموقع

يمكن لأي مهاجم أن يقوم بالتقاط رزمة البيانات ضمن بيانات الموقع المرسلة من الشبكة، وتعديل/تزييف بيانات الموقع لشن المزيد من الهجمات. وفي بعض السيناريوهات، قد تتسبب بيانات الموقع المعدّلة/المزيفة في مشاكل تتعلق بالسلامة، مثل مواقف السيارات الذكية والقيادة الذكية والإنقاذ في حالات الطوارئ.

3.1.8 اعتراض الإبلاغ عن بيانات الموقع

يمكن لأي مهاجم أن يستولي على أجهزة إنترنت الأشياء أو يتلاعب بها من خلال رفض الإبلاغ عن بيانات موقع أجهزة إنترنت الأشياء إلى الشبكة أو منصة خدمة المكاتب الذكية.

4.1.8 استدعاء بيانات الموقع غير المصرح به

دون آلية استيقان بين التطبيقات ومنصة خدمة المكاتب الذكية، يمكن للمهاجم أن يقوم باستدعاء بيانات الموقع بشكل غير مصرح به.

5.1.8 عدم توافر البيانات

يمكن أن يؤدي نسق البيانات غير الموحد إلى عدم توفر التطبيق في المكتب الذكي، مثل نسق بيانات الموقع داخل المباني غير الموحد (بما في ذلك البيانات المتعلقة بالطابق أو القاعة أو المكتب)، وقد يربك قدرة الروبوت عند قيامه بتسليم الرزمة إلى المتلقي.

6.1.8 الإفصاح عن المعلومات السلوكية

قد يحدث هذا التهديد عند التلاعب بمنصة مكتب ذكي أو عندما ينتحل مهاجم ما شخصية كيان قانوني لديه فرصة الحصول على معلومات بشأن سلوك المستعملين (مثل تفضيلات خطة المسير) لأغراض خبيثة، مثل إعادة بيعها بربح.

7.1.8 تحديد الموقع دون موافقة المستعمل

يحدث هذا التهديد عندما يقوم كيان وظيفة تحديد الموقع بجمع بيانات موقع المستعمل وتحليل البيانات ذات الصلة دون موافقة المستعمل، بما في ذلك فيما يتعلق بنطاق التطبيق والنية والطريقة واستخدام النتائج.

2.8 التهديدات الأمنية بالنسبة للجهاز

1.2.8 ضعف الأجهزة والبرامج

من الممكن إدراج مواطن الضعف والتهديدات الأمنية في عملية تطوير أجهزة تحديد المواقع. فعلى سبيل المثال، قد لا تكون منافذ تصحيح الأخطاء محمية بشكل صحيح، وقد تستخدم خوارزميات تجفير ضعيفة وقد يحدث تعثر في تطبيق تحديثات العتاد والبرمجيات وعدم التحقق من السلامة في الوقت المناسب.

2.2.8 التلاعب بجهاز تحديد المواقع

يمكن أن يتلاعب المهاجم بجهاز تحديد الموقع عن طريق التلاعب بأنظمة الاستشعار والبنية التحتية، مما يؤدي إلى نتيجة غير دقيقة لتحديد الموقع.

3.8 التهديدات الأمنية بالنسبة للسطوح البينية

1.3.8 السطح البيني للحيازة

يتعرض السطح البيني بين مقدم خدمات الاستشعار والبنية التحتية ومنصة خدمة المكاتب الذكية للتهديدات التالية:

- **استشفاف البيانات**: دون آليات الاستيقان والتخويل بين منصة خدمة المكاتب الذكية ومقدم خدمات الاستشعار والبنية التحتية، يمكن لمهاجم ما أن ينتحل شخصية منصة خدمة المكاتب الذكية لجمع بيانات الاستشعار والبنية التحتية.
- **رفض الخدمة**: قد يطلق أي مهاجم هجمات رفض الخدمة الموزعة (DDoS) عن طريق تغيير سياسة جمع البيانات (مثلاً جمع بيانات الاستشعار والبنية التحتية في وقت قصير جداً).
- **تسرب المعلومات**: ترسل الأجهزة المتنقلة بيانات الخدمة بشكل دوري، وخاصة بيانات الموقع عبر السطح البيني لحيازة البيانات إلى منصة خدمة المكاتب الذكية، ويمكن أن يلاحظ أي مهاجم الروتين اليومي للمستعمل إذا تمكن من استشفاف بيانات الخدمة والموقع.

2.3.8 السطح البيني للتشغيل البيني

يتعرض السطح البيني بين منصة خدمة المكاتب الذكية ومقدم البيانات/الحوسبة للتهديدات التالية:

- **النفاذ غير المصرح به إلى البيانات**: بدون آليات الاستيقان والتخويل بين منصة خدمة المكاتب الذكية ومقدم البيانات/الحوسبة، يستطيع المهاجم التلاعب بالسطح البيني للتشغيل البيني للنفاذ إلى بيانات الخدمة وبيانات الموقع وبيانات الملف الشخصي.
- **تزييف البيانات**: بدون آليات الاستيقان والتخويل بين منصة خدمة المكاتب الذكية ومقدم البيانات/الحوسبة، يستطيع المهاجم التلاعب بالسطح البيني للتشغيل البيني لتزييف بيانات الخدمة وبيانات الموقع وبيانات الملف الشخصي، وقد يؤدي هذا التهديد إلى تسرب المعلومات وتشغيل المنصة بشكل غير سليم والفوترة غير الصحيحة لمقدم البيانات/الحوسبة.

3.3.8 السطح البيني للخدمة

يتعرض السطح البيني بين منصة خدمة المكاتب الذكية والتطبيقات في المكاتب الذكية للتهديدات التالية:

- **النفاذ غير المصرح به إلى البيانات**: بدون آليات الاستيقان والتخويل بين منصة خدمة المكاتب الذكية والتطبيقات في المكاتب الذكية، يستطيع أي مهاجم التلاعب بالسطح البيني للخدمة للنفاذ إلى بيانات الخدمة، وبيانات الموقع وبيانات الملف الشخصي.

- **تزييف البيانات**: بدون آليات الاستيقان والتخويل بين منصة خدمة المكاتب الذكية والتطبيقات في المكاتب الذكية، يستطيع المهاجم التلاعب بالسطح البيني للخدمة لتزييف بيانات الخدمة وبيانات الموقع وبيانات الملف الشخصي، وقد يؤدي هذا التهديد إلى فوترة غير صحيحة للعملاء.

4.8 التهديدات الأمنية بالنسبة للمنصة

1.4.8 ضعف التكنولوجيات الهجينة لتحديد الموقع

قد تحتاج وظيفة تحديد الموقع كواحدة من كيانات الوظائف الأساسية في طبقة المنصة إلى تجميع التكنولوجيات الهجينة لتحديد الموقع القائمة على أنظمة لاسلكية متعددة، مثل النظام العالمي للملاحة الساتلية وخدمة الملاحة الراديوية الساتلية وتقنية البلوتوث وتكنولوجيا Wi-Fi والشبكة الخلوية والنطاق العريض جداً (UWB). وينطوي تنفيذ تكنولوجيات تحديد الموقع الهجينة هذه على استخراج المعلومات وحساب تحديد المواقع وترشيح نقاط الضعف في عملية التجميع وقد تؤدي الخوارزمية إلى الحصول على نتيجة غير دقيقة لتحديد الموقع.

2.4.8 عرض القدرات

تعرض منصة المكاتب الذكية الموقع وقدرات الخدمات الأخرى على التطبيقات الذكية، وقد يقوم كيان غير مخوَّل بإدراج أو تغيير أو حذف امتياز استعمال القدرات. ويمكن أن يكون الكيان غير المخوَّل شخصاً أو برنامجاً أو جهازاً. وتحدث هذه الهجمات عندما يضيف المهاجم بيانات إلى توصيل موجود باستخدام قدرة الخدمة باختطاف التوصيل أو عندما يرسل بيانات التشكيل بطريقة خبيثة. ويمكن أن يؤدي ذلك إلى هجوم رفض الخدمة والنفاذ إلى بيانات الخدمة.

5.8 التهديدات الأمنية بالنسبة للتطبيق الذكي

1.5.8 الاستعمال غير المرخص به

يحدث هذا التهديد عندما يكتسب تطبيق ذكي غير مصرح به قدرات الخدمة التي تقدمها منصة المكاتب الذكية عن طريق التنكر في صفة كيان مخوَّل.

2.5.8 حصان طروادة وحقن الفيروسات

يحدث هذا التهديد عندما ينتحل المهاجم صفة تطبيق ذكي قانوني ويحقن حصان طروادة أو فيروساً في التطبيق الذكي، ويضر ذلك بمنصة المكتب الذكي بل ويشن هجمات أخرى عليها.

6.8 علاقة التهديدات الأمنية بأصحاب المصلحة الرئيسيين

يبين الجدول 1 العلاقة بين التهديدات الأمنية وأصحاب المصلحة الرئيسيين في خدمات المكاتب الذكية القائمة على الموقع.

وفي الجدول 1، يشير الحرف "Y" (نعم) في كل خلية إلى ارتباط صاحب المصلحة الرئيسي بتهديد أمني معيّن.

الجدول 1 – علاقة التهديدات الأمنية بالكيانات

صاحب المصلحة الرئيسي / التهديدات	مقدم خدمة المكاتب الذكية	مقدم البيانات والحوسبة	مقدم خدمات الاستشعار والبنية التحتية	المستعمل
التنصت على بيانات الموقع	Y		Y	Y
التلاعب ببيانات الموقع	Y		Y	Y
اعتراض الإبلاغ عن بيانات الموقع	Y		Y	Y
استدعاء بيانات الموقع غير المصرح به	Y		Y	Y
عدم توفر البيانات	Y	Y		Y
الإفصاح عن المعلومات السلوكية	Y	Y	Y	Y
تحديد الموقع دون موافقة المستعمل	Y		Y	Y
استشفاف البيانات	Y		Y	Y
رفض الخدمة	Y		Y	Y
تسرب المعلومات	Y		Y	Y
نفاذ غير مصرح به إلى البيانات	Y	Y	Y	Y
تزييف البيانات	Y	Y	Y	Y
ضعف التكنولوجيات الهجينة لتحديد الموقع			Y	
عرض القدرات	Y			
ضعف الأجهزة والبرامج			Y	
التلاعب بجهاز تحديد الموقع			Y	
استخدام غير مصرح به	Y			
حصان طروادة وحقن الفيروسات	Y			

9 المتطلبات الأمنية لخدمة المكاتب الذكية القائمة على الموقع

1.9 المتطلبات الأمنية المتعلقة بالبيانات

- R-01: يلزم أن يقوم مقدم خدمة المكتب الذكي، ومقدم خدمات البيانات والحوسبة، ومقدم خدمات الاستشعار والبنية التحتية بتوفير وظيفة لضمان سرية البيانات، وخاصة بيانات الموقع.
- R-02: يلزم أن يقوم مقدم خدمة المكتب الذكي، ومقدم خدمات البيانات والحوسبة، ومقدم خدمات الاستشعار والبنية التحتية بتوفير وظيفة لضمان سلامة البيانات، وخاصة بيانات الموقع.
- R-03: يجب على مقدم خدمة المكتب الذكي، ومقدم خدمات البيانات والحوسبة، ومقدم خدمات الاستشعار والبنية التحتية التأكد من السماح للمستعملين المخولين أو الأجهزة المصرح لها فقط بالنفاذ إلى البيانات، وخاصة بيانات الموقع.
- R-04: يجب على مقدم خدمة المكتب الذكي، ومقدم خدمات البيانات والحوسبة، ومقدم خدمات الاستشعار والبنية التحتية التحقق من هويات الكيانات ومنع المهاجمين من محاولة التنكر ككيان معتمد.
- R-05: يلزم أن يقوم مقدم خدمة المكتب الذكي بتوفير وظيفة لضمان السماح للأجهزة أو التطبيقات المرخص لها فقط بالنفاذ إلى بيئة المكتب.

- R-06: يجب على مقدم خدمة المكتب الذكي، ومقدم خدمات البيانات والحوسبة، ومقدم خدمات الاستشعار والبنية التحتية بإنشاء آلية تعاون لتوحيد نسق البيانات.
- R-07: يجب أن يُصرح لمقدم خدمة المكتب الذكي، ومقدم خدمات البيانات والحوسبة، ومقدم خدمات الاستشعار والبنية التحتية بموافقة من المستعمل بجمع البيانات الشخصية للمستعملين، وخاصة بيانات الموقع. وتتضمن موافقة المستعمل الموافقة على التذكيرات وعرض وشرح جمع البيانات الشخصية للمستعملين بشكل موجز للمستعمل.

وفيما يتعلق ببيانات خدمة المكاتب الذكية القائمة على الموقع، تُعرض المتطلبات الأمنية المستمدة من التهديدات الأمنية المقابلة في الجدول 2.

الجدول 2 – تقابل المتطلبات الأمنية للبيانات مع التهديدات الأمنية

التهديدات الأمنية	المتطلبات الأمنية
التنصت على بيانات الموقع	R-01، R-02، R-03، R-04
التلاعب ببيانات الموقع	R-03، R-04
اعتراض تقرير بيانات الموقع	R-03، R-04
استدعاء بيانات الموقع غير المصرح به	R-03، R-04، R-05
عدم توفر البيانات	R-06
الكشف عن معلومات السلوك	R-01، R-03، R-04
تحديد المواقع دون موافقة المستعمل	R-07

2.9 المتطلبات الأمنية للأجهزة

- R-08: يجب أن يقوم مقدم خدمة المكتب الذكي، ومقدم خدمات البيانات والحوسبة، ومقدم خدمات الاستشعار والبنية التحتية بتوفير عملية للاستجابة للحوادث من أجل الكشف عن البرمجيات الضارة، والنشر المسبق لآليات الأمن للاستجابة للهجوم والتصدي له في الوقت المناسب.
- R-09: يجب أن يعمل مقدم خدمات الاستشعار والبنية التحتية على ضمان عدم تمكن المهاجم من النفاذ إلى البيانات حتى وإن استُحوذ على العتاد ويشمل الوسائل التالية:
  - التحقق من استيقان وسلامة البرمجيات المثبتة على الأجهزة باستعمال التوقيعات الرقمية المولدة تجفيرياً [b-ISO/IEC 9796-3]؛
  - التحكم في الحركة المقصود إنهاؤها في جهاز ما عن طريق جدار الحماية وكشف الاقتحام والحماية منه.
- R-10: يجب أن يقوم مقدم خدمة المكتب الذكي، ومقدم خدمات البيانات والحوسبة، ومقدم خدمات الاستشعار والبنية التحتية باستخدام خوارزميات التجفير المناسبة لضمان سرية البيانات، خاصة بيانات الموقع.
- R-11: يجب أن يقوم مقدم خدمات الاستشعار والبنية التحتية بتوفير وظيفة لتحقق من هويات الكيانات ومنع أي مهاجم يحاول التنكر ككيان معتمد.

وفيما يتعلق بجهاز خدمة المكاتب الذكية القائمة على الموقع، تُعرض المتطلبات الأمنية المستمدة من التهديدات الأمنية المقابلة في الجدول 3.

الجدول 3 – تقابل المتطلبات الأمنية للأجهزة مع التهديدات الأمنية

التهديدات الأمنية	المتطلبات الأمنية
ثغرة أمنية في العتاد والبرمجيات	R-08، R-09، R-10
التلاعب بجهاز تحديد الموقع	R-09، R-11،

3.9 المتطلبات الأمنية للسطوح البينية

- R-12: يجب أن يقوم مقدم خدمة المكتب الذكي، ومقدم خدمات الاستشعار والبنية التحتية بتوفير وظيفة لضمان السماح للمستعملين المخولين أو الأجهزة المصرح لها فقط بالنفاذ إلى بيانات الاستشعار والبنية التحتية من خلال السطوح البينية.
- R-13: يجب أن يقوم مقدم خدمة المكتب الذكي، ومقدم خدمات الاستشعار والبنية التحتية بتوفير وظيفة للتحقق من هويات الكيانات ومنع أي مهاجم يحاول التنكر في صورة كيان معتمد.
- R-14: يجب أن يقوم مقدم خدمة المكتب الذكي، ومقدم خدمات الاستشعار والبنية التحتية بتوفير وظيفة لضمان سرية البيانات وخاصة بيانات الموقع.
- R-15: يجب أن يقوم مقدم خدمة المكتب الذكي، ومقدم خدمات البيانات والحوسبة بتوفير وظيفة لضمان السماح للمستعملين المصرح لهم فقط بالنفاذ إلى بيانات الخدمة وبيانات الموقع وبيانات الملفات الشخصية.
- R-16: يجب أن يقوم مقدم خدمة المكتب الذكي، ومقدم خدمات البيانات والحوسبة بتوفير وظيفة للتحقق من هويات الكيانات ومنع أي مهاجم يحاول التنكر في صورة كيان معتمد.
- R-17: يجب أن يقوم مقدم خدمة المكتب الذكي، ومقدم خدمات البيانات والحوسبة بتوفير وظيفة لضمان سلامة بيانات الخدمة وبيانات الموقع وبيانات الملفات الشخصية.

وفيما يتعلق بالسطوح البينية لخدمة المكاتب الذكية القائمة على الموقع، تُعرض المتطلبات الأمنية المستمدة من التهديدات الأمنية المقابلة في الجدول 4.

الجدول 4 – تقابل المتطلبات الأمنية للسطوح البينية مع التهديدات الأمنية

التهديدات الأمنية	المتطلبات الأمنية
استشفاف البيانات	R-12، R-13
رفض الخدمة	R-13
تسرب المعلومات	R-13، R-14
نفاذ غير مصرح به إلى البيانات	R-15، R-16
تزييف البيانات	R-17

4.9 المتطلبات الأمنية للمنصة

- R-18: يجب أن يقوم مقدم خدمات الاستشعار والبنية التحتية بتوفير وظيفة للتحقق من دقة وسلامة خوارزمية (خوارزميات) تحديد الموقع المختلطة.
- R-19: يجب أن يقوم مقدم خدمة المكتب الذكي بتوفير وظيفة لضمان السماح للأجهزة أو التطبيقات المصرح لها فقط بالنفاذ إلى خدمة المكاتب الذكية القائمة على الموقع.
- R-20: يجب أن يقوم مقدم خدمة المكتب الذكي بتوفير وظيفة للتحقق من هويات الكيانات ومنع أي مهاجم يحاول التنكر في صورة كيان معتمد.

وفيما يتعلق بمصة خدمة المكاتب الذكية القائمة على الموقع، تُعرض المتطلبات الأمنية المستمدة من التهديدات الأمنية المقابلة في الجدول 5.

الجدول 5 – تقابل المتطلبات الأمنية للمنصة مع التهديدات الأمنية

التهديدات الأمنية	المتطلبات الأمنية
ثغرة أمنية في خوارزميات تحديد الموقع المختلطة	R-18
عرض القدرات	R-19، R-20

5.9 المتطلبات الأمنية للتطبيق الذكي

- R-21: يجب أن يقوم مقدم خدمة المكتب الذكي بتوفير وظيفة لضمان السماح للمستعملين المخولين أو الأجهزة المرخص لها فقط بالنفاذ إلى البيانات، وخاصة بيانات الموقع.
- R-22: يجب أن يقوم مقدم خدمة المكتب الذكي بتوفير وظيفة لضمان السماح للأجهزة أو التطبيقات المصرح لها فقط بالنفاذ إلى خدمة المكتب الذكي.
- R-23: يجب أن يقوم مقدم خدمة المكتب الذكي بتوفير وظيفة لضمان السماح للمستعملين المخولين أو الأجهزة المرخص لها فقط بالنفاذ إلى خدمة المكاتب الذكية القائمة على الموقع.
- R-24: يجب ان يقوم مقدم خدمة المكتب الذكي بتوفير وظيفة لتأسيس عملية للاستجابة للحوادث من أجل الكشف عن البرمجيات الضارة، والنشر المسبق لآليات الأمن للاستجابة للهجوم والتصدي له في الوقت المناسب.

وفيما يتعلق بالتطبيق الذكي لخدمة المكاتب الذكية القائمة على الموقع، تُعرض المتطلبات الأمنية المستمدة من التهديدات الأمنية المقابلة في الجدول 6.

الجدول 6 – تقابل المتطلبات الأمنية للتطبيق الذكي مع التهديدات الأمنية

التهديدات الأمنية	المتطلبات الأمنية
استعمال غير مصرح به	R-21، R-22
حصان طروادة وحقن الفيروسات	R-23، R-24

10 الوظائف الأمنية

لتحقيق المتطلبات الأمنية لخدمة المكاتب الذكية القائمة على الموقع، هناك العديد من الوظائف الأمنية التي تشمل على سبيل المثال لا الحصر ما يلي:

- تجفير البيانات وإدارة المفاتيح؛
- إدارة الهوية والتحكم في النفاذ؛
- التحقق من السلامة؛
- المراقبة الأمنية والاستجابة للحوادث الأمنية؛
- تذكير المستعملين.

1.10 تجفير البيانات وإدارة المفاتيح

يعتبر التجفير وإدارة المفاتيح الآليات الرئيسية لحماية سرية البيانات في خدمات المكاتب الذكية. ويوفر التجفير نهجاً لحماية الموارد، في حين تتيح إدارة المفاتيح التحكم في مفاتيح التجفير.

وينبغي أن يمتثل التجفير للمعايير الصناعية والحكومية ذات الصلة. ويشمل على سبيل المثال لا الحصر العناصر التالية:

- تجفير البيانات الدينامية في عمليات الخدمة؛
- تجفير البيانات السكونية في قاعدة البيانات؛
- تجفير البيانات في ملف النسخ الاحتياطي.

وتشمل إدارة المفاتيح توليد مفاتيح التجفير وتوزيعها وتقاسمها وتجديدها وإبطالها من أجل سرية البيانات واستيقانها. وتشكل الإدارة أساس أمن الخدمة الذي يتضمن على سبيل المثال لا الحصر ما يلي:

- **حماية معلومات المفاتيح:** يجب حماية معلومات المفاتيح مثلها مثل أي بيانات حساسة أخرى، بل ويجب أن يكون مستوى أمنها أعلى من مستوى أمن غيرها من البيانات.
- **النسخ الاحتياطي والاستعادة:** بما أن الحادث المحتمل قد يتسبب في فقدان مفتاح محدد وإيقاف الخدمة، لا بد من وضع حل النسخ الاحتياطي والاستعادة للمفتاح.

2.10 إدارة الهوية ومراقبة النفاذ

ينبغي توفير إدارة الهوية لكيانات خدمة المكاتب الذكية، التي يمكنها تقديم البيانات الخام للتحكم في النفاذ وتخويله وتدقيقه.

- وهي تدعم إدارة دورة حياة الهوية بأكملها، مثل السجل وإسناد الدور والإذن وتعديل الإذن والحذف. بالإضافة إلى ذلك، ينبغي أن يحظى تسجيل الهوية وتبديلها بإجراءات الموافقة من جانب الجهات الإدارية.
- وتدعم إدارة كلمة سر الكيان، التي تتضمن مجموعة من سياسات كلمة سر الكيان استناداً إلى السياسة الأمنية للعميل، من قبيل خوارزميات التجفير وطول كلمة السر وتعقيد كلمة السر ودورة تحديث كلمة السر. ويمكن أن تدعم أشكالاً مختلفة من كلمات السر، من قبيل كلمات السر البيانية وكلمات السر الصوتية وما إلى ذلك. وبالإضافة إلى ذلك، تدعم وظائف تزامن كلمة السر وإعادة تحديدها.
- ينبغي أن تشمل إدارة الهوية سياسة تسمية حساب الهوية وسياسة تطبيق حساب الهوية.

وينبغي توفير التحكم في النفاذ لإدارة نفاذ الكيان إلى خدمة المكتب الذكي، التي تستخدم هوية الكيان أو قدرة الكيان المستيقن منها لتحديد وإنفاذ امتيازات النفاذ الخاصة بالكيان. ويمكن للتحكم في النفاذ أن يرفض محاولات النفاذ غير المصرح بها أو غير السليمة وأن يبلغ عنها لتوليد إنذار أو إجراء سجل تدقيق أمني.

- بيانات الاستيقان مثل كلمات السر، وحيازتها وعرضها لاحقاً هي دليل على تخويل نفاذ الكيان؛
- يتم إنتاج وسم الأمن وفقاً لسياسة أمن المكتب؛
- وقت محاولة النفاذ؛
- مسير محاولة النفاذ؛
- مدة النفاذ؛
- الموقع المادي لمحاولة النفاذ.

3.10 التحقق من السلامة

يشمل التحقق من سلامة البيانات مستويين:

- **وحدة بيانات واحدة أو مستوى مجال واحد:** يشمل التحقق من سلامة وحدة بيانات واحدة عمليتين: واحدة لدى الكيان المرسل والأخرى لدى كيان المتلقي. فيُلحِق الكيان المرسل كمية بوحدة بيانات تتوقف على البيانات نفسها. ويولد الكيان المتلقي كمية مقابلة ويقارن نتيجتها بالكمية الواردة لتحديد ما إذا كانت البيانات قد عُدلت أثناء الإرسال.

- **تدفق وحدات البيانات أو تدفق مستوى المجال:** يتطلب التحقق من تدفق مستوى وحدة البيانات إضافة شكل من أشكال الترتيب الصريح، مثل رقم التسلسل أو خاتم التوقيت أو سلسلة التجفير.

التحقق من سلامة البيانات باستخدام آلية تُنشر مسبقاً للتحقق من نسق البيانات وآلية التوقيع الرقمي المولدة بالتجفير للتحقق من البيانات التي لم يتم العبث بها.

4.10 التحقق من سلامة البرمجيات والخوارزميات باستخدام آلية التوقيعات الرقمية المولدة تجفيرياً المراقبة الأمنية والاستجابة للحوادث الأمنية

يمكن توفير المراقبة الأمنية لمديري الخدمة لفحص عيوب الخدمة وأدائها. وتشمل المراقبة على سبيل المثال لا الحصر ما يلي:

- **مراقبة الحالة الصحية:** تشمل جمع وعرض سجلات الحوادث الأمنية والمعلومات المتعلقة بمواطن الضعف وتغيير تشكيلة الأجهزة الأمنية والأداء والحالة التشغيلية للخدمة. وتساعد المديرين على إدراك الحالة الصحية الشاملة للخدمة.
- **الكشف عن السلوك الشاذ:** يشمل تسجيل الدخول غير القانوني أو النفاذ غير القانوني أو النفاذ المنتهك لخدمات معينة والتعديلات الشاذة على جهاز مادي.
- **مراقبة الأمن المادي:** تتضمن مراقبة درجة الحرارة والرطوبة والدوائر التلفزيونية المغلقة (CCTV) وحارس المدخل ونظام الحماية من الحرائق ومكيف الهواء ونظام الإمداد بالطاقة والمراقبة.

وتتعامل الاستجابة للحوادث الأمنية مع الطلبات والاستعادة من آليات مثل وظائف التعامل مع الحدث وإدارته، وتتخذ إجراءات الاستعادة نتيجة لتطبيق مجموعة من القواعد.

5.10 تذكير المستعملين

تتيح عملية تذكير المستعملين آلية لضمان استخدام البيانات التي يتم جمعها من جهاز الاستشعار والتصريح بها من قبل مستعمل خدمات المكاتب الذكية القائمة على الموقع.

وتكمن النقطة الرئيسية في أنه بالنسبة لخدمة معينة من خدمات المكاتب الذكية القائمة على الموقع تحتاج إلى جمع البيانات الشخصية للمستعملين، تتمثل الخدمة في إرسال تذكير للمستعمل لعرضها وشرحها بإيجاز للمستعمل. يمكن تذكير المستعمل بما إذا كان تم التخطيط لجمع البيانات وما هي البيانات التي سيتم جمعها. وسيتم إبلاغه أيضاً بكيفية معالجة البيانات وتداولها.

6.10 العلاقة بين الوظائف الأمنية والمتطلبات الأمنية

يعرض الجدول 7 الوظائف الأمنية لتلبية المتطلبات الأمنية المقابلة لخدمة المكاتب الذكية القائمة على الموقع.

الجدول 7 – تقابل المتطلبات الأمنية للتطبيق الذكي مع التهديدات الأمنية

الوظائف الأمنية	المتطلبات الأمنية	
تجفير البيانات وإدارة المفاتيح	بالنسبة للبيانات: R-01	
	المتطلبات الأمنية للأجهزة	R-09، R-10، R-11
	المتطلبات الأمنية للسطوح البينية	R-14
إدارة الهوية والتحكم في النفاذ	المتطلبات الأمنية للبيانات	R-03، R-04، R-05
	المتطلبات الأمنية للسطوح البينية	R-12، R-13، R-15، R-16
	المتطلبات الأمنية للمنصة	R-19، R-20
	المتطلبات الأمنية للتطبيق الذكي	R-21، R-22، R-23

الجدول 7 – تقابل المتطلبات الأمنية للتطبيق الذكي مع التهديدات الأمنية

الوظائف الأمنية	المتطلبات الأمنية	
التحقق من السلامة	المتطلبات الأمنية للبيانات	R-02، R-06
	المتطلبات الأمنية للسطوح البينية	R-17
	المتطلبات الأمنية للمنصة	R-18
المراقبة الأمنية والاستجابة للحوادث الأمنية	المتطلبات الأمنية للأجهزة	R-08، R-09
	المتطلبات الأمنية للتطبيق الذكي	R-24
تذكير المستعملين	المتطلبات الأمنية للبيانات	R-07

بيبليوغرافيا

[b-ITU-T X.1121] Recommendation ITU-T X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

[b-ISO/IEC 9796-3] ISO/IEC 9796-3:2006, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms.*

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2024