التوصية

ITU-T X.1817 (09/2023)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن شبكات الاتصالات المتنقلة الدولية-2020

متطلبات الأمن لخدمة المراسلة في شبكة الجيل الخامس (5G)

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
أمن الفضاء السيبراني	X.1299-X.1200
تطبيقات وخدمات آمنة (2)	X.1499-X.1300
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.1817

متطلبات الأمن لخدمة المراسلة في شبكة الجيل الخامس (5G)

ملخص

تقدم التوصية ITU-T X.1817 متطلبات أمن خدمة الرسائل في شبكة الجيل الخامس (5G)، بما في ذلك متطلبات أمن النفاذ، ومتطلبات أمن الإدارة، ومتطلبات أمن التحكم لخدمة الرسائل في شبكة الجيل الخامس (5G).

التسلسل التاريخي*

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد
1.0	ITU-T X.1817	2023-09-08	17	11.1002/1000/15524

مصطلحات أساسية

خدمة الرسائل في شبكة الجيل الخامس (5G)، إطار الأمن، متطلبات الأمن.

* للنفاذ إلى التوصية، تُرجى كتابة العنوان https://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرّف 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، يُوصى 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

متطلبات الأمن لخدمة المراسلة في شبكة الجيل الخامس (5G)

1 مجال التطبيق

خدمة الرسائل في شبكة الجيل الخامس (5G) هي ترقية لخدمة الرسائل القصيرة (SMS). وهي واحدة من خدمات أعمال الاتصالات الأساسية وتشمل خدمة الرسائل القصيرة (SMS) المعرّفة في إطار مشروع شراكة الجيل الثالث (3GPP) وخدمة الاتصالات الغنية (RCS) ورابطة النظام العالمي للاتصالات المتنقلة (GSMA). وتدعم هذه الخدمة على وجه الخصوص، الرسائل بين الأشخاص أو بين التطبيقات والأشخاص، كما تدعم الوسائط المختلفة (مثل النصوص الطويلة والصور والفيديو والملفات والموضع) في الرسالة. وتَصِفُ هذه التوصية المتطلبات الأمنية التي يمكن أن تخفف من التهديدات والتحديات الأمنية لخدمة المراسلة في شبكة الجيل الخامس (5G). وتوفر هذه التوصية المتطلبات الأمنية لخدمة المراسلة 5G بما في ذلك متطلبات أمن النفاذ، ومتطلبات أمن الإدارة، ومتطلبات أمن التحكم في خدمة المراسلة 5G. كما تَصِفُ التوصية الاختلافات الوظيفية بين المتطلبات الأمنية لخدمة المراسلة 5G وتلك الخاصة بالأجيال WLAN/5G/4G/3G.

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 المراجَعة، 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.

[ETSI TS 123 040] ETSI TS 123 040 v17.2.0 (2022), *Digital cellular telecommunications system (Phase 2+) GSM; Universal Mobile Telecommunications System (UMTS); LTE; 5G; Technical realization of the Short Message Service (SMS)*.

[ETSI TS 124 229] ETSI TS 124 229 (2017), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3*.

[ETSI TS 129 109] ETSI TS 129 109 (2018), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3*.

[ISO/IEC 11770-1] ISO/IEC 11770-1:2010, *Information technology – Security techniques – Key management – Part 1: Framework*.

3 التعاريف

1.3 تعاريف معرّفة في أماكن أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 روبوت الدردشة (Chatbot) [b-GSMA RCC.71]: خدمة مؤتمتة قائمة على خدمة الاتصالات الغنية (RCS) تُقدَّم للمستعملين وتُعرَض مخرجاتها في شكل محادثة.

2.3 مصطلحات معرَّفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 مركز رسائل 5G (5G message centre): مخدم يوفر خدمة المراسلة 5G.

2.2.3 منصة الرسائل (message platform): منصة تطبيق للطرف الثالث للتوصيل بمركز الرسائل 5G.

3.2.3 معدات مستعمل (UE) الرسائل 5G (5G message user equipment): يطلق على معدات مستعمل 5G الذي يدعم تطبيق الرسائل الخاص به كلا من خدمة الرسائل القصيرة (SMS) وخدمة الاتصالات الغنية (RCS).

4.2.3 خدمة المراسلة 5G (5G messaging service): خدمة المراسلة 5G بما في ذلك خدمة الرسائل القصيرة (SMS) وخدمة الاتصالات الغنية (RCS). وتدعم خدمة المراسلة 5G، الرسائل بين الأشخاص أو بين التطبيقات والأشخاص، كما تدعم الوسائط المختلفة (مثل النصوص الطويلة والصور والفيديو والملفات والموضع) في الرسالة.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية الاختصارات والأسماء المختصرة التالية:

3GPP	مشروع شراكة الجيل الثالث (*3rd Generation Partnership Project*)
A2P	من تطبيق إلى شخص (*Application to Person*)
AKA	الاستيقان واتفاق المفاتيح (*Authentication and Key Agreement*)
GBA	معمارية التشغيل التلقائي العامة (*Generic Bootstrapping Architecture*)
GSMA	رابطة النظام العالمي للاتصالات المتنقلة (*Global System for Mobile Communications Association*)
HSS	خدمة المشترك المحلي (*Home Subscriber Service*)
HTTPS	أمن بروتوكول نقل النصوص الترابطية (*Hypertext Transfer Protocol Secure*)
IMS	نظام فرعي متعدد الوسائط لبروتوكول الإنترنت (*IP Multimedia Subsystem*)
MO	إنشاء الرسالة عند طرف الهاتف المتنقل (*Mobile Originate*)
MT	انتهاء الرسالة عند طرف الهاتف المتنقل (*Mobile Terminate*)
OTP	كلمة سر لمرة واحدة (*One-Time Password*)
P2P	من شخص إلى شخص (*Person to Person*)
RCS	خدمة اتصالات غنية (*Rich Communication Service*)
SIM	وحدة هوية المشترك (*Subscriber Identity Module*)
SIP	بروتوكول استهلال الدورة (*Session Initiation Protocol*)
SMS	خدمة الرسائل القصيرة (*Short Message Service*)
UE	معدات المستعمل (*User Equipment*)
UDM	إدارة البيانات الموحدة (*Unified Data Management*)
VoLTE	نقل الصوت باستعمال تكنولوجيا التطور طويل الأجل (*Voice over Long-Term Evolution*)
WLAN	شبكة محلية لاسلكية (*Wireless Local Area Network*)

5 الاصطلاحات

تستخدم هذه التوصية الاصطلاحين التاليين:

تشير كلمة "يلزم" إلى متطلب يجب التقيد به تماماً ولا يسمح بأي انحراف عنه في حال ادعاء الامتثال لهذه التوصية.

تشير كلمة "يُوصى" إلى متطلب يُوصى به لكنه غير إلزامي في المطلق. وبالتالي لا يتعين توفر هذا المتطلب لزعم الامتثال.

6 نظرة عامة

1.6 خدمة المراسلة 5G

تتيح خدمة المراسلة 5G، التي تتبع المواصفات العالمية لخدمة الاتصالات الغنية (RCS) لرابطة النظام العالمي للاتصالات المتنقلة، خدمات متقدمة مثل خدمة الرسائل متعددة الوسائط والدردشة الجماعية ومنصة الرسائل. وتعتمد خدمة المراسلة 5G على بوابة خدمة الرسائل القصيرة (SMS) الأصلية للمحطة الطرفية، مما يسمح للمستعملين بإرسال واستقبال النصوص والصور والصوت والفيديو وبيانات الموقع ومعلومات جهات الاتصال ومحتوى الوسائط الأخرى، بما في ذلك وظائف الخدمات التالية:

- رسائل من شخص إلى شخص (P2P)

تشير الرسائل من شخص إلى شخص (P2P) إلى الرسائل المرسلة بين المستعملين الفرديين وتدعم محتوى الوسائط التالي: النص (بما في ذلك الرموز) والصور والصوت والفيديو وبيانات الموقع وجهات الاتصال (vCard) والوثائق.

- رسائل جماعية

تشير الرسالة الجماعية إلى رسالة يرسلها مستعمل فردي إلى عدة مستعملين فرديين آخرين في نفس الوقت. ويمكن للمستعمل إدخال أرقام اتصال متعددة في وقت ما أو تحديد مستقبلين متعددين من دفتر العناوين لإرسال رسالة جماعية إلى مستقبلين متعددين. ويتلقى كل مستقبل رسالةً تتضمن المحتوى نفسه، ورقم المرسِل هو رقم هاتفه المتنقل الفعلي، ويستطيع المستقبِل الرد مباشرةً على الرسالة إلى المرسِل في رسالة من شخص إلى شخص (P2P).

- رسائل الدردشة الجماعية

رسالة دردشة جماعية هي رسالة تفاعل بين جميع المستعملين الفرديين الذين ينضمون إلى المجموعة.

- رسائل من تطبيق إلى شخص (A2P)

أي رسالة مُنشأة بمساعدة تطبيق وموجهة للمعدات المتنقلة التي يحملها شخص، تسمى رسائل من تطبيق إلى شخص (A2P). وتمكّن هذه الرسائل العلامات التجارية للشركات من التواصل مع المستعملين من خلال روبوت الدردشة. ويمكن للمستعملين إرسال رسائل خدمة الاتصالات الغنية إلى روبوت الدردشة التي تشمل النصوص (بما في ذلك الرموز) والصور والصوت والفيديو وبيانات الموقع وجهات الاتصال (vCard) والوثائق. ويمكن لروبوتات الدردشة إرسال رسائل من طرف إلى طرف أو من طرف إلى عدة أطراف وإرسال رسائل غنية تشمل النصوص (بما في ذلك الرموز) والصور والصوت والفيديو وبيانات الموقع وجهات الاتصال (vCard) والوثائق. ويمكن لروبوت الدردشة أن يرسل "بطاقات غنية" توفر "قائمة رقاقات مقترحة" تتألف من "أجوبة وإجراءات مقترحة".

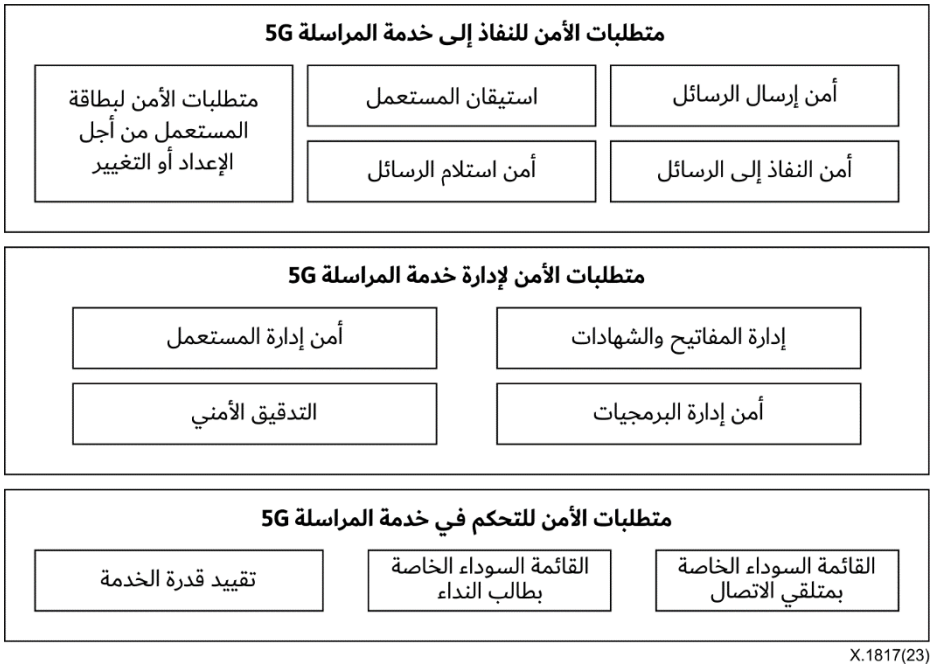
2.6 معمارية متطلبات الأمن لخدمة المراسلة 5G

يبين الشكل 1 معمارية متطلبات الأمن لخدمة المراسلة 5G، التي تتألف من متطلبات أمن مستوي المستعمل، ومتطلبات أمن مستوي الإدارة، ومتطلبات أمن مستوي التحكم في خدمة المراسلة 5G.

وتشمل متطلبات أمن مستوي المستعمل لخدمة المراسلة 5G متطلبات أمن بطاقة المستعمل من أجل الإعداد أو التغيير واستيقان المستعمل وأمن استقبال الرسائل وإرسالها والنفاذ إليها.

وتشمل متطلبات أمن مستوي الإدارة لخدمة المراسلة 5G أمن إدارة المستعمل وإدارة المفاتيح والشهادات والتدقيق الأمني وأمن إدارة البرمجيات.

وتشمل متطلبات أمن مستوي التحكم في خدمة المراسلة 5G تقييد قدرة الخدمة والتحكم في القائمة السوداء لطالب النداء والتحكم في القائمة السوداء لمتلقي الاتصال.



الشكل 1 – معمارية متطلبات الأمن لخدمة المراسلة 5G

3.6 الاختلافات الوظيفية بين المتطلبات الأمنية لخدمة المراسلة 5G وتلك الخاصة بالأجيال WLAN/5G/3G/4G

يكمن الفرق بين خدمة المراسلة 5G وخدمة الرسائل SMS التقليدية في أن الرسائل القصيرة التقليدية لا يمكنها إرسال سوى النصوص فقط، في حين أن خدمة الرسائل 5G يمكنها إرسال مجموعة متنوعة من أنواع الوسائط، تشمل النصوص (بما في ذلك الرموز) والصور المصغرة والصور والصوت والفيديو وبيانات المواقع وجهات الاتصال والوثائق.

وعند استعمال خدمات المراسلة 5G، يمكن للأجهزة الطرفية النفاذ إلى وحدات الوظائف من خلال الشبكة 3G أو 4G أو 5G أو الشبكة المحلية اللاسلكية (WLAN). وبعد استكمال النفاذ إلى الشبكة، تحصل الأجهزة الطرفية أولاً على معلمات الخدمة من مخدم التشكيل، ثم تبدأ عملية تسجيل بروتوكول استهلال الدورة (SIP) إلى نقطة النفاذ. وبعد التسجيل الناجح، يمكنها إرسال رسائل 5G واستقبالها، بما في ذلك الرسائل الشخصية ورسائل الصناعة.

وتوفر معمارية متطلبات أمن الرسائل 5G الموضحة في الفقرة 2.6 معمارية الحماية الأمنية للرسائل 5G. وتُؤمن الحماية لخدمات المراسلة 5G بغض النظر عن أسلوب الشبكة التي يتم من خلاله النفاذ إلى الأجهزة الطرفية.

7 متطلبات الأمن للنفاذ إلى خدمة المراسلة 5G

1.7 متطلبات الأمن لبطاقة المستعمل من أجل الإعداد أو التغيير

بالنسبة إلى مستعملي خدمة نقل الصوت عبر تكنولوجيا التطور طويل الأجل (VoLTE) وخدمة المراسلة 5G الذين يُطلب منهم تغيير بطاقة وحدة هوية المشترك (SIM) الخاصة بهم بسبب فقدان/سرقة بطاقة SIM بشكل غير قابل للاسترداد، يُوصى بأن يقوم مركز الرسائل 5G بتجديد/تحديث المعلومات ذات الصلة بحيث يتمكن المستعملون من استعمال خدمة المراسلة 5G بسلاسة بعد تغيير بطاقات SIM.

2.7 استيقان المستعمل

من المطلوب أن يستوفي استيقانُ المستعمل بين مرسِل الرسالة ومتلقيها متطلباتِ الاستيقان، وعدم فتح منصة الخدمة لخدمة المراسلة 5G إلا للمستعملين المستيقَن منهم.

1.2.7 استيقان المستعمل الشخصي

تتضمن الرسائل 5G مجموعةً متنوعةً من أساليب تنفيذ الخدمة، تقابل مجموعةً متنوعةً من آليات استيقان المستعمل. ويعرض الجدول 1 أنواع خدمات الرسائل 5G ومتطلبات استيقان الأمن ذات الصلة.

الجدول 1 – متطلبات استيقان أمن خدمات المراسلة 5G

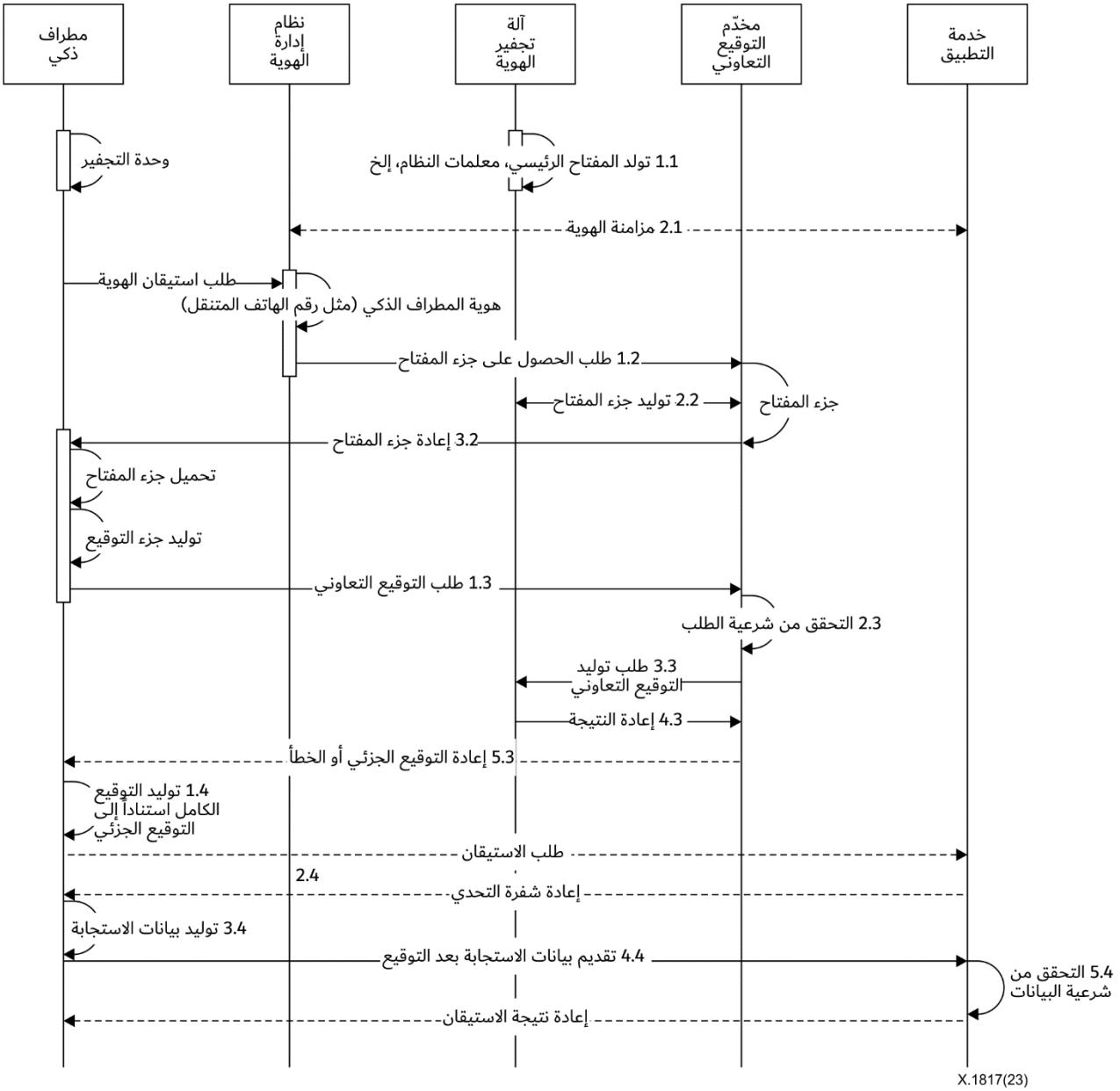
خدمة المراسلة 5G	متطلبات استيقان الأمن
المراسلة 5G (مختلف تفاعلات المراسلة الآنية، بما في ذلك المراسلة P2P والدردشة الجماعية ومراسلات روبوت الدردشة وغيرها من الإشارات والوسائط ذات الصلة)	USIM IMS AKA (يدعم تسجيل بروتوكول استهلال الدورة اتفاق المفاتيح المستيقنة)
المراسلة 5G (تخزين الرسائل، بما في ذلك تحميل وتنزيل محتوى الوسائط المتعددة في الرسائل)	USIM GBA_ME
اكتشاف روبوت الدردشة	
الاستعلام عن المعلومات من روبوت الدردشة	
إدارة تشكيل المطاريف	لأول مرة، استخدم استيقان إدخال رقم الهاتف المتنقل (الشبكة الخلوية) أو كلمة السر SMS لمرة واحدة (OTP) (شبكة غير خلوية) في عملية لاحقة للحصول على التشكيل، يمكن لإدارة تشكيلة المطراف أن تختار استيقان معمارية التشغيل التلقائي العامة (GBA) حسب الحاجة. ويمكنها أيضاً اختيار آلية التوقيع التعاوني من أجل الاستيقان. ويُوصى أن تمتثلَ كلمة السرّ لمرة واحدة المرسَلة في شكل رسالة نصيّة (SMS) للمواصفة التقنية [ETSI TS 123 040 v17.2.0].

ويرد وصف أساليب الاستيقان على النحو التالي:

أ) USIM IMS AKA: بالنسبة لمستعمل الرسائل 5G، أثناء تسجيل النظام الفرعي للوسائط المتعددة IP (IMS) مع مركز الرسائل 5G، يحصل مركز الرسائل 5G على متجه الاستيقان واتفاق الاستيقان والمفتاح (AKA) للمستعمل من مخدِّم المشترك المحلي (HSS)/إدارة البيانات الموحدة (UDM) لدى المستعمل من خلال السطح البيني Zh ويستكمل الاستيقان IMS AKA للمستعمل بناءً على متجه الاستيقان. ويوصى بتوافق شهادة AKA مع المعيار [ETSI TS 124 229].

ب) USIM GBA_ME: من المطلوب أن تدعم مطاريف دعم الرسائل 5G السطوح البينية GBA. ومن المطلوب أن تدعم مخدمات التطبيقات غير القائمة على بروتوكول SIP في نظام المراسلة 5G السطوح البينية GBA Zn. ويوصى بتوافق شهادة GBA مع المعيار [ETSI TS 124 229].

ج) إدارة تشكيل المطاريف: لأول مرة، استخدم استيقان إدخال رقم الهاتف المتنقل (الشبكة الخلوية) أو كلمة السر SMS لمرة واحدة (OTP) (شبكة غير خلوية) أو SMS OTP (شبكة غير خلوية) في عملية لاحقة للحصول على التشكيل. ولحماية المفاتيح من تسرب المفاتيح، يمكن استخدام آلية التوقيع التعاوني.



الشكل 2 – آلية التوقيع التعاوني لخدمة المراسلة 5G

تُستخدم آلية التوقيع التعاوني الموضحة في الشكل 2 لاستيقان الهوية في خدمة الرسائل 5G. وفيما يلي العملية الرئيسية:

1) تولِّد آلة تجفير الهوية المفتاح الرئيسي ومعلمات النظام ومكون مفتاح الهوية. ويمكن تنفيذ مزامنة الهوية بين نظام إدارة الهوية وخدمة التطبيق استناداً إلى الخوارزمية المحددة مسبقاً وفقاً للمفتاح الرئيسي ومعلمات النظام ومكون مفتاح الهوية. وتتضمن الخوارزمية المحددة مسبقاً واحدةً على الأقل من خوارزمية توليد المفاتيح وخوارزمية التوقيع وخوارزمية التحقق. وفيما يلي وصف الخطوات:

- الخطوة 1.1: تولِّد آلة تجفير الهوية المفتاح الرئيسي ومعلمات النظام ومكون مفتاح الهوية.
- الخطوة 2.1: يمكن تنفيذ مزامنة الهوية بين نظام إدارة الهوية وخدمة التطبيق استناداً إلى الخوارزمية المحددة مسبقاً وفقاً للمفتاح الرئيسي ومعلمات النظام ومكون مفتاح الهوية.

2) بعد مزامنة الهوية بين نظام إدارة الهوية وخدمة التطبيق، تُستخدم هوية المطراف الذكية لاستيقان هوية التوقيع التعاوني مع مخدم التوقيع التعاوني. ويرسل المطراف الذكي هوية المطراف الذكي (مثل رقم الهاتف المتنقل) إلى نظام إدارة الهوية. ويرسل

نظام إدارة الهوية طلب المفتاح إلى مخدم التوقيع التعاوني استناداً إلى هوية المطراف الذكي. ويعيد مخدم التوقيع التعاوني جزء المفتاح كتغذية ارتجاعية إلى المطراف الذكي استناداً إلى طلب المفتاح. وفيما يلي وصف الخطوات:

- الخطوة 1.2: يبدأ المطراف الذكي طلب استيقان الهوية ويطلب الحصول على جزء المفتاح من مخدم التوقيع التعاوني.
- الخطوة 2.2: يولّد مخدم التوقيع التعاوني جزء المفتاح.
- الخطوة 3.2: يعيد مخدم التوقيع التعاوني جزء المفتاح كتغذية ارتجاعية إلى المطراف الذكي استناداً إلى طلب المفتاح.

3) يقوم المطراف الذكي بتحميل جزء المفتاح ويولّد جزء التوقيع المقابل. ويرسل المطراف الذكي طلب التوقيع التعاوني إلى مخدم التوقيع التعاوني استناداً إلى جزء التوقيع. ويتحقق مخدم التوقيع التعاوني من شرعية طلب التوقيع التعاوني. وعند تمرير استيقان هوية التوقيع التعاوني، يقوم مخدم التوقيع التعاوني بإعادة توجيه طلب التوقيع التعاوني إلى آلة تجفير الهوية. وتولّد آلة تجفير الهوية توقيعاً جزئياً وفقاً لطلب التوقيع التعاوني، ويعيد مخدم التوقيع التعاوني التوقيع الجزئي كتغذية ارتجاعية إلى المطراف الذكي. وفيما يلي وصف الخطوات:

- الخطوة 1.3: يرسل المطراف الذكي طلب التوقيع التعاوني إلى مخدم التوقيع التعاوني بناءً على جزء التوقيع.
- الخطوة 2.3: يتحقق مخدم التوقيع التعاوني من شرعية طلب التوقيع التعاوني.
- الخطوة 3.3: عند تمرير استيقان هوية التوقيع التعاوني، يقوم مخدم التوقيع التعاوني بإعادة توجيه طلب التوقيع التعاوني إلى آلة تجفير الهوية.
- الخطوة 4.3: تولّد آلة تجفير الهوية توقيعاً جزئياً وفقاً لطلب التوقيع التعاوني، ويعيد مخدم التوقيع التعاوني التوقيع الجزئي كتغذية ارتجاعية إلى المطراف الذكي.
- الخطوة 5.3: يعيد مخدّم التوقيع التعاوني التوقيع الجزئي كتغذية ارتجاعية إلى المطراف الذكي.

4) يولّد المطراف الذكي توقيعاً كاملاً بناءً على التوقيع الجزئي. وتكون عملية استيقان هوية التوقيع المشترك مع خدمة التطبيق استناداً إلى التوقيع الكامل كما يلي. يرسل المطراف الذكي طلب استيقان إلى خدمة التطبيق استناداً إلى التوقيع الكامل. وتعيد خدمة التطبيق شفرة التحدي كتغذية ارتجاعية إلى المطراف الذكي استناداً إلى طلب الاستيقان. ويولّد المطراف الذكي بيانات استجابة وفقاً لجزء المفتاح المحلي وشفرة التحدي ويرسل بيانات الاستجابة إلى خدمة التطبيق. وبعد تلقي بيانات الاستجابة، تتحقق خدمة التطبيق من شرعية بيانات الاستجابة وتتحقق من هوية المطراف الذكي استناداً إلى التوقيع الكامل. ويُستكمل استيقان هوية التوقيع المشترك، وتعيد خدمة التطبيق نتيجة الاستيقان كتغذية ارتجاعية إلى المطراف الذكي. وفيما يلي وصف الخطوات:

- الخطوة 1.4: يولّد المطراف الذكي التوقيع الكامل بناءً على التوقيع الجزئي.
- الخطوة 2.4: يرسل المطراف الذكي طلب استيقان إلى خدمة التطبيق استناداً إلى التوقيع الكامل، وترسل خدمة التطبيق شفرة التحدي إلى المطراف الذكي.
- الخطوة 3.4: يولد المطراف الذكي بيانات استجابة وفقاً لجزء المفتاح المحلي وشفرة التحدي. وجزء المفتاح المحلي هو جزء المفتاح الذي يعيده مخدم التوقيع التعاوني كتغذية ارتجاعية.
- الخطوة 4.4: يرسل المطراف الذكي بيانات الاستجابة إلى خدمة التطبيق.
- الخطوة 5.4: تتحقق خدمة التطبيق من مشروعية بيانات الاستجابة. ويُستكمل استيقان هوية التوقيع المشترك، وتعيد خدمة التطبيق نتيجة الاستيقان كتغذية ارتجاعية إلى المطراف الذكي.

2.2.7 استيقان مخدم روبوت الدردشة

قبل توصيل روبوت الدردشة بمنصة الرسالة، يجب الاستيقان منه. ويعتمد الاستيقان توليفةً من استيقان المنصة واستيقان طبقة التطبيق. ويمكن لاستيقان المنصة أن يستخدم الاستيقان من الشهادات الرقمية القائم على بروتوكول نقل النصوص التشعبية الآمن (HTTPS)، ويمكن للاستيقان من طبقة التطبيق أن يستخدم الاستيقان القائم على اسم المستعمل وكلمة السر.

ومن الضروري أن يقدم مخدِّم روبوت الدردشة طلباً للحصول على شهادة مخدِّم من خلال هيئة إصدار شهادات قانونية (CA)، وأن يقدّم الشهادة الجذرية CA، واسم الميدان القانوني، أو عنوان بروتوكول الإنترنت لمخدِّم روبوت الدردشة، إلى منصة الرسالة لاستعراض التسجيل خلال عملية تسجيل المستعمل. وبعد الانتهاء من التسجيل، تقوم منصة الرسالة باستيقان الهوية في مخدم روبوت الدردشة أثناء عملية النفاذ إلى روبوت الدردشة. ويشمل الاستيقان التحقق من شهادة مخدم روبوت الدردشة، والاستيقان من هوية روبوت الدردشة.

3.7 أمن تلقي الرسائل

يمكن لتطبيقات المراسلة 5G أن تتعاون مع النظام المطرافي لإدراك أن تطبيقات المراسلة 5G فقط هي التي يمكنها استقبال الرسائل 5G ضماناً لعدم استخدامها بشكل ضار وعدم تسرب البيانات الخاصة لرسالة المستعمل.

4.7 أمن إرسال الرسائل

يمكن لتطبيقات المراسلة 5G أن تتعاون مع النظام المطرافي لإدراك أن تطبيقات المراسلة 5G فقط هي التي يمكنها إرسال الرسائل 5G، ولا يمكن تفويض إذن إرسال الرسائل إلى أي تطبيقات أخرى لضمان عدم استخدامها بشكل ضار.

5.7 أمن النفاذ إلى الرسائل

يمكن لتطبيقات المراسلة 5G أن تتعاون مع الأنظمة المطرافية لتقييد قدرات النفاذ المرخص إلى الرسائل 5G. ويُشترط قراءة ملف الرسالة على جانب المطراف فقط بواسطة تطبيق المراسلة 5G أو تنفيذ عمليات إدارة أخرى (مثل الحذف والنسخ الاحتياطي). ويُوصى بأن توفر الرسالة على جانب المنصة الاستعلام والقراءة (بما في ذلك البيانات المتصلة بالسجل) لمالك الرسالة وأن يُحظر نفاذ المستعملين الآخرين (بمن في ذلك المديرون) بشكل عام.

8 المتطلبات الأمنية لإدارة خدمة المراسلة 5G

1.8 أمن إدارة المستعمل

1.1.8 تقسيم الأدوار والأذونات

يقسّم أمن إدارة المستعمل منصة الخدمة إلى طبقات ومجالات وفقاً لوظائف تقسيم وحدات الخدمة والامتيازات. ويُوصى بتحديد حساب المدير طبقاً للامتيازات المختلفة التي تشمل المشرف المتميز ومدير الخدمة ومراجع الحسابات.

أ) المشرفون المتميزون: لديهم سلطة إدارية متقدمة فيما يتعلق بمنصة وظائف الخدمة مما يعني أنه يمكنهم إدارة مديري الخدمة والمدققين.

ب) مديرو الخدمة: لديهم سلطة لإدارة الخدمة وتشغيلها بشكل جزئي أو كامل. ومع ذلك، لا يمكن أن يكون لدى مديري الخدمة سلطة التدقيق أو إدارة مديري الخدمة الآخرين.

ج) المدققون: لديهم سلطة فيما يتعلق بعمليات تدقيق التسجيل وتدقيق التشغيل، ولكن لا يمكن أن تكون لديهم سلطة معالجة الخدمة.

2.1.8 مراقبة السلوك غير الطبيعي

مراقبة وتدقيق بعض السلوكيات غير الطبيعية، كتسجيل الدخول غير الطبيعي، وتسجيل الدخول في أماكن متعددة في الوقت نفسه، وإرسال رسائل تتجاوز معدل العتبة (لتصنيف الإجراء كرسائل اقتحامية). وفيما يخص هذه السلوكيات غير الطبيعية، هناك حاجة مقابلة لاتخاذ إجراءات (من قبيل إضافتها إلى القائمة السوداء، وتجميد الحساب) لتقييد هؤلاء المستخدمين ذوي السلوك غير الطبيعي.

2.8 إدارة المفاتيح والشهادات

1.2.8 إدارة المفاتيح

إدارة المفاتيح هي آلية إدارة يدير من خلالها مطراف الرسائل 5G ومنصة الخدمة مفاتيح تجفير البيانات الحساسة الخاصة بهما. ويُوصى بتوفر مجموعة من مفاتيح التجفير المختلفة لأنواع مختلفة من البيانات الحساسة التي يمكن استخدامها عندما يقوم جانب المنصة أو جانب المطراف بالتخزين المجفر للبيانات الحساسة. ويُوصى بأن تمتثل متطلبات إدارة المفاتيح للمعيار [ISO/IEC 11770-1].

ويمكن لنظام المراسلة 5G أن يصمم مفاتيح مقابلة لحماية الأشياء المختلفة، بما في ذلك أنماط المفاتيح التالية الموضحة في الجدول 2 على الأقل:

الجدول 2 – أنواع مفاتيح نظام الرسائل 5G وأنواعها

الأنواع	الوصف
مفتاح تخزين أمن البيانات	حماية البيانات الهامة المخزنة والمعلومات الحساسة.
مفتاح اتصال آمن	يتم إنشاء مفتاح معمارية التشغيل التلقائي العامة (GBA) أثناء عملية استيقان تسجيل الدخول للمطراف والمنصات المتعددة من خلال عملية المعمارية GBA (أسلوب الإنشاء المحدد) ويُوصى بأن تتوافق المتطلبات مع استيقان المعمارية GBA الوارد في المعيار [ETSI TS 129 109].
مفتاح تجفير معلومات تحديد هوية المستعمل	حماية معلومات تحديد هوية المستعمل.
مفتاح تجفير بيانات المفتاح	حماية البيانات المتعلقة بالمفاتيح.
مفتاح نقل أمن البيانات	حماية البيانات الهامة والمعلومات الحساسة عند العبور.

2.2.8 إدارة الشهادات

لتنفيذ توصيلات HTTPS آمنة، يتعين تشكيل مخدم الويب بشهادة رقمية تصادق على نوع استعمال المخدم. وفيما يتعلق بالمخدمات الواجب تشكيلها بشهادات رقمية، في حال وجود أسماء ميادين متعددة، هناك حاجة إلى طلب شهادة مخدم لكل اسم ميدان. وعندما يستخدم المخدم بروتوكول الإنترنت (IP) لتقديم الخدمات، وفي حال وجود عدة نقط، هناك حاجة إلى تقديم طلب للحصول على شهادة المخدّم لكل IP وترد أنواع الشهادات هذه في الجدول 3.

الجدول 3 – وصف تشكيل شهادة مخدم نظام الرسائل 5G

اسم المخدم	أسلوب النفاذ	نوع الشهادة
5GMC	اسم الميدان	شهادة SSL عادية (تتطلب من المطراف ضبط شهادة جذرية CA مسبقاً)
منصة الرسائل	اسم الميدان	شهادة SSL عادية (تتطلب من المطراف ضبط شهادة جذرية CA مسبقاً)
وحدة إدارة منصة الرسائل	اسم الميدان	شهادة SSL عادية
روبوت الدردشة	اسم الميدان	شهادة SSL عادية

3.8 التدقيق الأمني

السجلات هي سجلات سلوكيات المستعمل الهامة والاستخدام غير الطبيعي لموارد النظام، واستخدام أوامر المنصات الهامة في المنصة. وقد تشمل السجلات التاريخ والوقت والنوع وتحديد هوية الموضوع وتحديد هوية الكائنات ونتائج الحدث. وتشمل المحتويات التي يمكن تسجيلها في سجل أمن الخدمة، على سبيل المثال لا الحصر، سجلات عمليات وسجلات عمليات المدير وسجلات الخدمة.

أ) سجلات عمليات المستعمل: تسجل عمليات الحساب والنتائج وعمليات الخدمة والنتائج وما إلى ذلك. ويمكن أن تشمل سجلات عمليات المستعمل معلومات المستعمل وعمليات المستعمل وكائنات التشغيل ووقت التشغيل ونتائج التشغيل والنتائج غير الطبيعية وما إلى ذلك.

ب) سجلات عمليات المدير: تسجل عمليات الحساب والنتائج وعمليات الخدمة والنتائج وما إلى ذلك. ويمكن أن تشمل سجلات عمليات المدير معلومات المدير وعملياته وكائنات التشغيل ووقت التشغيل ونتائج التشغيل والنتائج غير الطبيعية وما إلى ذلك.

ج) سجلات الخدمة: يُوصى بأن تتمكن الأنظمة من تسجيل سجلات خدماتها. ويمكن للمنصة أن تخزن جميع أنواع السجلات ضمن وقت محدد للاستعلام الإلكتروني وفقاً للطلب؛ وبالنسبة إلى السجلات التي تتجاوز متطلبات زمن التخزين الإلكتروني، يمكن تحديد مدة التخزين خارج الإنترنت. وتُخزن السجلات الإلكترونية في قاعدة بيانات أو بأسلوب يحدده النظام. وتدير منصة الخدمة حقوق النفاذ ولا يمكن عرضها أو تصديرها أو تدقيقها إلا من قبل مدير معيّن (مدقق)؛ وبالنسبة إلى السجلات خارج الإنترنت، يمكن استيرادها إلى النظام أو استعمال أدوات خاصة للاستعلام والتدقيق والعمليات الأخرى. أما السجلات خارج الإنترنت التي تحتوي على بيانات حساسة فيمكن تخزينها في ملفات مجفرة بعد تصديرها.

4.8 أمن إدارة البرمجيات

1.4.8 أمن إدارة تطوير البرمجيات لخدمات المراسلة 5G

يُشترط أن تشمل مبادئ التشفير الآمنة لنظام خدمة المراسلة 5G ما يلي:

أ) التحقق من فعالية البيانات التي يُدخلها المستعمل، وترشيح الرموز الحساسة.

ب) تجفير تخزين البيانات الحساسة مثل كلمات السر.

ج) نقل البيانات الحساسة بواسطة بروتوكول HTTPS، مثل أسماء المستعملين وكلمات السر.

د) عدم النفاذ إلى موارد النظام مباشرة، مثل الملفات.

هـ) عدم استخدام واجهة أوامر في الشفرات المرتبطة بالويب.

و) استخدام وظيفة السلامة للبرامج.

2.4.8 أمن إدارة العمليات لنظام المراسلة 5G

يمكن لنظام الرسائل 5G مراقبة العمليات الهامة ومنطق معالجة الخدمة ويُصدر إنذاراً عند اكتشاف الأعطال.

9 المتطلبات الأمنية للتحكم في خدمة المراسلة 5G

1.9 قيود قدرة الخدمة

تشمل قيود قدرة الخدمة تقييد الأفراد في المجموعة، والتحكم المتمايز في وظائف المجموعة، وتقييد الدردشة الجماعية.

أ) تقييد عدد الأشخاص في المجموعة: تحتاج عمليات الإرسال الجماعي للرسائل 5G إلى تحديد الحد الأعلى لعدد عمليات الإرسال الجماعي وذلك للحد من الآثار السلبية المحتملة إلى نطاق محدود.

ب) التحكم المتمايز في وظائف المجموعة: يمكن لمنصات الخدمة أن تدعم التحكم المتمايز في عدد المستعملين المتلقين للاتصال في خدمة جماعية.

ج) تقييد الدردشات الجماعية: يمكن لمنصات الخدمة أن تدعم تقييد عدد المستعملين في الدردشة الجماعية، ويمكن تشكيل معلمات عدد مجموعة المستعملين، ويمكن لمنصات الخدمة أن تدعم تقييد طول اسم المجموعة.

2.9 القائمة السوداء لطالب النداء

فيما يتعلق بالرسائل الصادرة عن جهاز متنقل 5G، هناك حاجة إلى إضافة وظيفة التحكم في الاستيقان من القائمة السوداء لطالب النداء لمنع مخاطر القصف بالرسائل 5G. ويمكن لنظام التحكم أن ينشئ آليةً لمراقبة الدردشات الجماعية من شأنها تحليل أعمال

الرسائل الجماعية الخبيثة التي ستضاف إلى التحكم في القائمة السوداء لطالب النداء من خلال الإضافة التلقائية وعمليات الاستعراض اليدوي ووسائل أخرى. ويمكن أن يقوم التحكم في القائمة السوداء لطالب النداء بعد ذلك باعتراض أعمال الرسائل الجماعية الخبيثة والتحكم فيها.

3.9 القائمة السوداء لمتلقي الاتصال

فيما يتعلق بالرسائل المنتهية عند طرف الهاتف المتنقل 5G، هناك حاجة إلى إضافة التحكم في القائمة السوداء لطالب النداء لتقليل احتمالية شكاوى مستعملي المطاريف. ويمكن للمستعملين الشخصيين تقديم شكوى أو تحديد قائمة سوداء لمتلقي الاتصال عن طريق الاتصال بخدمة العملاء وتسجيل الدخول إلى واجهة الخدمة الذاتية والتوجه إلى مركز الخدمات ووسائل أخرى. ويمكن لنظام التحكم أو أنظمة الخدمة ذات الصلة أن تقوم بإنشاء قائمة سوداء من شأنها أن تعترض الرسائل التي يرسلها المستعملون وفقاً لمستعمل معيّن أو نوع خدمة معيّن.

بيبليوغرافيا

[b-GSMA RCC.71] GSM Association (2019), *RCS Universal Profile Service Definition Document*.

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