التـوصيــة

ITU-T X.1383 (03/2023)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تطبيقات وخدمات آمنة (2) – أمن أنظمة النقل الذكية (ITS)

المتطلبات الأمنية من أجل البيانات المصنَّفة في الاتصالات من مركبة إلى كل شيء (V2X)

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1–X.199
التوصيل البيني للأنظمة المفتوحة	X.200–X.299
التشغيل البيني للشبكات	X.300–X.399
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.700–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
آمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000–X.1029
آمن الشبكة	X.1030–X.1049
إدارة الأمن	X.1050–X.1069
الخصائص البيومترية	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
آمن البث المتعدد	X.1100–X.1109
آمن الشبكة المحلية	X.1110–X.1119
آمن الخدمات المتنقلة	X.1120–X.1139
آمن الويب	X.1140–X.1149
بروتوكولات الأمن (1)	X.1150–X.1159
الأمن بين جهتين نظيرتين	X.1160–X.1169
آمن معرفات الهوية عبر الشبكات	X.1170–X.1179
آمن التلفزيون القائم على بروتوكول الإنترنت	X.1180–X.1199
آمن الفضاء السيبراني	
الأمن السيبراني	X.1200–X.1229
مكافحة الرسائل الاقتحامية	X.1230–X.1249
إدارة الهوية	X.1250–X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300–X.1309
آمن شبكات المحاسيس واسعة الانتشار	X.1310–X.1319
آمن شبكة الكهرباء الذكية	X.1330–X.1339
البريد المعتمد	X.1340–X.1349
آمن إنترنت الأشياء (IoT)	X.1350–X.1369
آمن أنظمة النقل الذكية (ITS)	**X.1370–X.1399**
آمن سجل الحسابات الموزع	X.1400–X.1429
آمن سجل الحسابات الموزع	X.1450–X.1459
البروتوكول الأمني (2)	X.1470–X.1489
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1500–X.1519
تبادل مواطن الضعف/الحالة	X.1520–X.1539
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل السياسات	X.1550–X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560–X.1569
تعرف الهوية والاكتشاف	X.1570–X.1579
التبادل المضمون	X.1580–X.1589
الدفاع السيبراني	X.1590–X.1599
آمن الحوسبة السحابية	
نظرة عامة على آمن الحوسبة السحابية	X.1600–X.1601
تصميم آمن الحوسبة السحابية	X.1602–X.1639
أفضل الممارسات ومبادئ توجيهية بشأن آمن الحوسبة السحابية	X.1640–X.1659
تنفيذ آمن الحوسبة السحابية	X.1660–X.1679
آمن أشكال أخرى للحوسبة السحابية	X.1680–X.1699
الاتصالات الكمومية	
المصطلحات	X.1700–X.1701
مولد الأعداد العشوائية الكمومية	X.1702–X.1709
إطار آمن شبكات توزيع المفاتيح الكمومية	X.1710–X.1711
تصميم آمن شبكات توزيع المفاتيح الكمومية	X.1712–X.1719
تقنيات آمن شبكات توزيع المفاتيح الكمومية	X.1720–X.1729
آمن البيانات	
آمن البيانات الضخمة	X.1750–X.1759
حماية البيانات	X.1770–X.1789
آمن الاتصالات المتنقلة الدولية–2020	X.1800–X.1819

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

التوصية ITU-T X.1383

المتطلبات الأمنية من أجل البيانات المصنَّفة في الاتصالات من مركبة إلى كل شيء (V2X)

ملخص

يُعتبر أمن البيانات من أهم الاعتبارات المتعلقة بالاتصالات من مركبة إلى كل شيء (V2X). ولكن في بيئة محدودة الموارد، مثل بيئة الاتصالات على متن مركبة، تستهلك حماية البيانات الكثير من الموارد لأنه يجب إجراء وظائف تجفير.

وتصنّف التوصية ITU-T X.1383 البيانات المستخدمة في الاتصالات من مركبة إلى كل شيء (V2X) إلى عدة أنماط منها بيانات نعوت الأغراض، وبيانات حالة المركبة، وبيانات التصور البيئي، وبيانات التحكم في المركبة، وبيانات خدمة التطبيقات وبيانات المستعملين الشخصية، وتخصَّص ثلاثة مستويات أمنية لأنماط البيانات المصنفة. واستناداً إلى هذه الأنماط المصنّفة من البيانات ومستويات أمن البيانات المخصصة لها، تقدّم هذه التوصية متطلبات أمن البيانات المصنَّفة في الاتصالات من مركبة إلى كل شيء (V2X).

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1383	2023-03-03	17	11.1002/1000/15108

مصطلحات أساسية

البيانات المصنَّفة، أمن البيانات، الاتصالات من مركبة إلى كل شيء (V2X).

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

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 الاختراع 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 قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1383

المتطلبات الأمنية من أجل البيانات المصنَّفة في الاتصالات من مركبة إلى كل شيء (V2X)

1 مجال التطبيق

تصنّف هذه التوصية البيانات المستخدمة في الاتصالات من مركبة إلى كل شيء (V2X) إلى عدة أنماط وتحدّد المستوى الأمني لكل نمط من أنماط البيانات المصنفة. واستناداً إلى هذه الأنماط المصنّفة من البيانات في كل مستوى من المستويات الأمنية، تقدّم هذه التوصية متطلبات أمن البيانات المصنَّفة في الاتصالات من مركبة إلى كل شيء (V2X).

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 للمراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.1641] التوصية ITU-T X.1641 (2016)، *مبادئ توجيهية لأمن بيانات عملاء الخدمات السحابية*.

[ITU-T X.1603] التوصية ITU-T X.1603 (2018): *متطلبات أمن البيانات لخدمة المراقبة في الحوسبة السحابية*.

[ITU-T X.1372] التوصية ITU-T X.372 (2020)، *المبادئ التوجيهية للسلامة من أجل الاتصالات من مركبة إلى كل شيء (V2X)*.

3 التعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في مراجع أخرى:

1.1.3 إزالة حساسية البيانات (data desensitization) [b-ITU-T X.1217]: عملية إخفاء البيانات الحساسة.

2.1.3 دورة حياة البيانات (data lifecycle) [b-ITU-T X.1751]: عملية البقاء الكاملة بعد إنشاء البيانات، بما في ذلك جمع البيانات وإرسال البيانات وتخزين البيانات واستخدام البيانات (وهي تغطي تحليل البيانات وعرضها بصرياً) وتبادل البيانات وإتلاف البيانات.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

ABS نظام كبح مانع للانزلاق (*Anti-skid Braking System*)

BSM رسالة سلامة أساسية (*Basic Safety Message*)

CAM رسالة توعية تعاونية (*Cooperative Awareness Message*)

DoS رفض الخدمة (*Denial of Service*)

GDPR اللائحة العامة لحماية البيانات (*General Data Protection Regulation*)

ICV مركبة ذكية موصولة (*Intelligent Connected Vehicle*)

TLS أمن طبقة النقل (*Transport Layer Security*)

V2I من مركبة إلى بنية تحتية (*Vehicle-to-Infrastructure*)

V2D من مركبة إلى جهاز جوال (*Vehicle-to-nomadic Device*)

V2P من مركبة إلى مشاة (*Vehicle-to-Pedestrian*)

V2V من مركبة إلى مركبة (*Vehicle-to-Vehicle*)

V2X من مركبة إلى كل شيء (*Vehicle-to-Everything*)

5 الاصطلاحات

تستعمل هذه التوصية الاصطلاحات التالية:

تشير كلمة "**يُتطلب/يتعيَّن/يلزم/يجب**" إلى متطلَّب يجب التقيد به على نحو صارم ولا يجوز أي حيدان عنه إذا أريد إعلان المطابقة مع مقتضيات هذه التوصية.

وتشير كلمة "**ينبغي**" إلى متطلَّب يُوصى به لكنه ليس ملزِماً إلزاماً مطلَقاً. وبالتالي لا يتعين توفر هذا المتطلب لزعم الامتثال.

وتشير كلمة "**يجوز**" إلى متطلَّب اختياري مسموح به دون أن ينطوي على أي توصية به.

وتشير كلمة "**ينبغي عدم**" إلى متطلَّب يجب التقيّد به بصرامة، ولا يُسمح بأي انحراف عنه في حال زعم الامتثال لهذه التوصية.

6 دورة حياة البيانات في الاتصالات من مركبة إلى كل شيء (V2X)

1.6 دورة حياة البيانات

تُحدَّد دورة حياة البيانات استناداً إلى تدفق البيانات في أعمال تنظيم بيئة الاتصالات من مركبة إلى كل شيء (V2X). واستناداً إلى الوضع الفعلي للاتصالات من مركبة إلى كل شيء (V2X)، فإن دورة حياة أمن البيانات تشبه ما هو وارد في التوصية [ITU-T X.1641]، التي تتضمن المراحل التي يرد وصفها أدناه وهي جمع البيانات وإرسال البيانات وتخزين البيانات واستخدام البيانات وانتقال البيانات وإتلاف البيانات والنسخ الاحتياطي للبيانات واستعادة البيانات:

- **جمع البيانات**: عملية توليد بيانات جديدة في النظام داخل المنظمة وجمع البيانات من الخارج. وهناك شكلان من أشكال جمع البيانات في الاتصالات من مركبة إلى كل شيء (V2X)، أحدهما هو البيانات الناشئة عن مختلف عمليات أعمال الاتصالات من مركبة إلى كل شيء (V2X) والآخر هو البيانات التي يجمعها المستعملون والشركاء المعنيون والأطراف الثالثة الأخرى.
- **إرسال البيانات**: عملية تتدفق فيها البيانات من كيان إلى آخر داخل المنظمة. ويتعلق إرسال البيانات في الاتصالات من مركبة إلى كل شيء (V2X) بشكل رئيسي بتدفق البيانات بين الأنظمة والمعدات المتصلة بخدمات الاتصالات من مركبة إلى كل شيء (V2X).
- **تخزين البيانات**: عملية التخزين المادي أو التخزين السحابي للبيانات في نسق رقمي أياً كان شكله. وعادة ما تتم هذه المرحلة في آن واحد تقريباً مع مرحلة جمع البيانات.
- **استخدام البيانات**: سلسلة من الأنشطة التي تضطلع بها المنظمات بشأن البيانات الدينامية في الاتصالات من مركبة إلى كل شيء (V2X)، من قبيل البحث عن البيانات وتحليلها ومعالجتها. وتشمل هذه المرحلة تحديث البيانات وإنتاج بيانات جديدة.

- **انتقال البيانات:** عملية نقل البيانات إلى أطراف ثالثة خارجية. وهذا يشمل عرضَ البيانات وتوفيرَها للمستعملين في الاتصالات من مركبة إلى كل شيء (V2X). ويشمل ذلك أيضاً عملية توفير البيانات فيما بينهم في إطار التعاون بين الشركات والمؤسسات في الاتصالات من مركبة إلى كل شيء (V2X).
- **إتلاف البيانات:** عملية جعل البيانات غير متاحة بشكل دائم أو مؤقت باستخدام وسائل مادية أو تقنية. ويمكن أن يُعزى إتلاف البيانات إلى اعتبارات متعلقة بالتكلفة الواقعة على عاتق المؤسسة وإلى مسألة الامتثال الخارجي أو متطلبات العمل. وينبغي، لا سيما إذا كانت هناك لوائح مناسبة للاحتفاظ بالبيانات، أن يقوم مقدمو الخدمات بمحو أو إخفاء هوية صاحب البيانات المجمَّعة بشكل مناسب بحيث يتعذَّر استعادة البيانات التي بلغت الحد الأقصى الجائز للاحتفاظ بها أو التي لم يعد للمستعملين إذن باستخدامها.
- **النسخ الاحتياطي للبيانات واستعادتها:** عملية نسخ كل البيانات أو جزء منها في وسائط تخزين أخرى لمنع فقدان البيانات واستعادة البيانات الأصلية بفضل النَّسخ الاحتياطية في حالة فقدان البيانات.

2.6 تحليل التهديدات

تواجه أيضاً البيانات في الاتصالات من مركبة إلى كل شيء (V2X) تهديدات وتحديات أمنية مماثلة لتلك المعرّفة في التوصيتين [ITU-T X.1603] و[ITU-T X.1641]. وتشمل بعض هذه التهديدات والتحديات الأمنية المتعلقة بالبيانات في الاتصالات من مركبة إلى كل شيء (V2X)، على سبيل المثال لا الحصر، التهديدات والتحديات المعروضة في الجدول 6-1.

الجدول 6-1 – التهديدات والتحديات وفقاً لدورة حياة البيانات في الاتصالات من مركبة إلى كل شيء (V2X)

دورة حياة البيانات	التهديدات والتحديات الأمنية
جمع البيانات	أ) جمع البيانات دون تخويل ب) الثغرات الأمنية في السطح البيني للتحصيل ج) الانتحال د) العبث والاعتراض هـ) النفاذ إلى الخدمة غير الآمن و) النفاذ الإداري غير المخوَّل به
إرسال البيانات	أ) الاعتراض ب) التنكر ج) التنصت د) النفاذ غير المخوَّل به هـ) هجوم رفض الخدمة (DoS)
تخزين البيانات	أ) فقدان البيانات وتسربها ب) عدم توفر الخدمة
استعمال البيانات	أ) إساءة استخدام البيانات ب) التهديدات من الداخل ج) الثغرات الأمنية في النظام د) التنصت
انتقال البيانات	أ) إساءة استخدام البيانات ب) الثغرات الأمنية في النظام ج) البيانات الكاذبة د) هجوم رفض الخدمة
إتلاف البيانات	أ) الانتحال ب) الثغرات الأمنية في النظام
النسخ الاحتياطي للبيانات واستعادتها	أ) الثغرات الأمنية في النظام

7 البيانات المصنَّفة في الاتصالات من مركبة إلى كل شيء (V2X)

تعرض هذه الفقرة سياسة تصنيف البيانات التي تتناولها الاتصالات من مركبة إلى كل شيء (V2X). وتُصنف البيانات في ستة أنماط كالآتي: بيانات نعوت الأغراض، وبيانات حالة المركبة، وبيانات التصور البيئي، وبيانات التحكم في المركبة، وبيانات خدمة التطبيقات، والبيانات الشخصية للمستخدم، ويرد وصفها في الفقرة 2.7.

1.7 تحديد هوية البيانات استناداً إلى سيناريوهات الاتصالات من مركبة إلى كل شيء (V2X)

يجوز تحديد هوية البيانات التي تتناولها الاتصالات من مركبة إلى كل شيء (V2X) بالاستناد إلى سيناريو الاتصالات الفعلي. وتصنّف التوصية ITU-T X.1372 سيناريوهات الاتصالات من مركبة إلى كل شيء (V2X) على النحو التالي: الاتصالات من مركبة إلى مركبة (V2V) ومن مركبة إلى بنية تحتية (V2I) ومن مركبة إلى جهاز جوال (V2D) ومن مركبة إلى مشاة (V2P). وتصف هذه الفقرة عمليات الاتصالات ذات الصلة وبيانات كل سيناريو من سيناريوهات الاتصالات.

1.1.7 البيانات في الاتصالات من مركبة إلى مركبة (V2V)

تحدد التوصية [ITU-T X.1372] ثلاثة سيناريوهات للاتصالات من مركبة إلى مركبة (V2V)؛ وهي إذاعة تحذير من مركبة إلى مركبة، والاتصالات من مركبة إلى مركبة بين مجموعات المركبات، والاتصالات من مركبة إلى مركبة بواسطة المنارات الإلكترونية. وفي سيناريو نشر التحذير من مركبة إلى مركبة، تنشر رسالة التحذير من مركبة إلى أخرى. وفي سيناريو الاتصالات V2V بين مجموعات المركبات، تتبادل مجموعات من المركبات حالة المركبة فيما بينها. وفي سيناريو الاتصالات V2V بواسطة المنارات الإلكترونية، ترسل كل مركبة معلومات عن حالتها. يوضح الجدول 7-1 البيانات في اتصال V2V.

الجدول 7-1 – البيانات في الاتصالات من مركبة إلى مركبة (V2V)

الفئة	السيناريو	البيانات
من مركبة إلى مركبة	نشر التحذير من مركبة إلى مركبة (V2V)	• رسالة تحذير • رسالة سلامة أساسية (BSM) • رسالة توعية تعاونية (CAM)
	الاتصالات V2V بين مجموعات المركبات	• رسالة سلامة أساسية • رسالة توعية تعاونية
	الاتصالات V2V بواسطة المنارات الإلكترونية	• رسالة سلامة أساسية • رسالة توعية تعاونية

وترد المواصفات التقنية لرسالة السلامة الأساسية ورسالة التوعية التعاونية في الوثيقتين [b-SAE J2735] و[b-ETSI TS 102 637-2] على التوالي.

2.1.7 البيانات في الاتصالات من مركبة إلى بنية تحتية (V2I)

حددت التوصية [ITU-T X.1372] سيناريوهين للاتصالات من مركبة إلى بنية تحتية (V2I)؛ وهما التحذير من مركبة إلى بنية تحتية (V2I) وتبادل المعلومات من مركبة إلى بنية تحتية (V2I). ويتيح سيناريو التحذير من مركبة إلى بنية تحتية (V2I) تبادل رسائل التحذير بين المركبة والبنية التحتية. وأثناء تبادل المعلومات في الاتصالات بين المركبة والبنية التحتية (V2I)، تتواصل المركبة والبنية التحتية مع بعضها لتحديث معلومات المرور و/أو المعلومات المتعلقة بخدمات الإعلام الترفيهي. ويبيّن الجدول 7-2 البيانات في الاتصالات من مركبة إلى بنية تحتية (V2I).

الجدول 7-2 – البيانات في الاتصالات من مركبة إلى بنية تحتية (V2I)

الفئة	السيناريو	البيانات
من مركبة إلى بنية تحتية	التحذير بين المركبة والبنية التحتية	• رسالة تحذير
	تبادل المعلومات بين المركبة والبنية التحتية	• اللافتات المعروضة داخل المركبة • المعلومات المعروضة داخل المركبة • طور الإشارة • زمن إشارة المرور • أحوال سطح الطريق • أحوال الطقس • أحوال مسافة الرؤية • معلومات عن أشغال الطرق

3.1.7 البيانات في الاتصالات من مركبة إلى جهاز جوال (V2D)

في سيناريو الاتصالات من مركبة إلى جهاز جوال (V2D)، تتواصل المركبة مع الأجهزة الجوالة من قبيل الهاتف الذكي والحاسوب المحمول ونظام الملاحة في المركبة. وتحدّد التوصية [ITU-T X.1372] سيناريوهين من سيناريوهات الاتصالات من مركبة إلى جهاز جوال (V2D)؛ وهما الاتصالات من مركبة إلى جهاز جوال عبر روابط غير مباشرة، والاتصالات من مركبة إلى جهاز جوال عبر روابط مباشرة. والفرق بين هذين السيناريوهين هو أسلوب الاتصالات، وكلاهما يتعامل مع نفس أنماط البيانات. وتَعتبر التوصية [ITU-T X.1372] أن الاتصالات من مركبة إلى مشاة (V2P) حالة محددة من الاتصالات من مركبة إلى جهاز جوال (V2D). ويبيّن الجدول 7-3 البيانات في الاتصالات من مركبة إلى جهاز جوال (V2D).

الجدول 7-3 – البيانات في الاتصالات من مركبة إلى جهاز جوال (V2D)

الفئة	السيناريو	البيانات
من مركبة إلى جهاز جوال	الاتصالات من مركبة إلى جهاز جوال (V2D) عبر روابط غير مباشرة/مباشرة	• بيانات عتاد المركبة • بيانات برمجيات المركبة • بيانات عتاد الجهاز • بيانات برمجيات الجهاز • بيانات منصة الخدمات • بيانات خدمة التطبيقات

2.7 تصنيف البيانات

تصف هذه الفقرة تصنيف البيانات التي تتناولها الاتصالات من مركبة إلى كل شيء (V2X).

وتؤخذ في الاعتبار البيانات في الاتصالات من مركبة إلى كل شيء (V2X) للالتزام بالقوانين واللوائح المتعلقة بحماية البيانات الشخصية مثل اللائحة العامة لحماية البيانات (GDPR) ولا يمكن للبيانات التي ورد وصفها في هذه التوصية أن تشير إلى معلومات متعلقة بشخص محدد أو يمكن تحديده.

1.2.7 بيانات نعوت الأغراض

تشير بيانات نعوت الأغراض إلى نعوت الكيانات في الاتصالات من مركبة إلى كل شيء (V2X)، التي يمكن تقسيمها إلى ثلاثة أنواع، وهي نعوت المركبات والأجهزة المتنقلة ومنصات الخدمات السحابية:

- تتعلق بيانات نعوت المركبات بخواص المركبات مثل العلامة التجارية والنوع والشعار واللون.
- تشير بيانات نعوت الجهاز المتنقل إلى الخواص المتعلقة بالجهاز المتنقل مثل العلامة التجارية والنوع واللون.
- تشير بيانات نعوت منصة الخدمات إلى الخواص المتعلقة بمنصة الخدمات، مثل المراجعة والتصنيع وما إلى ذلك.

2.2.7 بيانات حالة المركبة

تشير بيانات حالة المركبة إلى حالة المركبة ذات الصلة الوثيقة بخدمة المعلومات في الاتصالات من مركبة إلى كل شيء (V2X). وهي تشمل حالات تشغيل هذه الأنظمة ومعْلماتها، مثل نظام الدفع في المركبة ونظام هيكل المركبة ونظام سلامة المركبة ونظام جسم المركبة ونظام الراحة في المركبة والنظام الكهربائي للمركبة.

وبعبارة أدق، تتضمن البيانات المتعلقة بحالة المركبة معلومات بشأن البيانات المستمدة من وحدة التحكم في المركبة (مثل إشارة التحكم في المضخة والإنذار الخاص بجهاز استشعار ضغط الهواء وإشارة كابح الحركة السلكية، وما إلى ذلك)، ونظام الإرسال (مثل عزم المحرك ومعدل استهلاك الوقود، وما إلى ذلك)، ونظام التبريد (مثل درجة حرارة سائل التبريد)، ونظام صندوق التروس (مثل بيانات انطلاق المركبة وتسارعها، وما إلى ذلك)، ونظام السلامة (مثل حالة الوسادة الهوائية وحالة استعمال حزام الأمان، وما إلى ذلك)، ونظام هيكل المركبة (مثل معلومات بشأن وضع شبكة المركبة ونظام القيادة ونظام الكبح المانع للانزلاق ونظام رصد ضغط الإطارات، وما إلى ذلك)، ونظام وسائل الراحة (مثل البيانات المتعلقة بفتحات تكييف الهواء وتعديل وضعية المقاعد ونظام النوافذ ونظام الإنارة، وما إلى ذلك) والأنظمة المساعدة الأخرى.

واستناداً إلى وصف حالات تشغيل المركبة، يمكن تقسيم بيانات حالة المركبة إلى نوعين هما البيانات عندما تكون المركبة في حالة دينامية والبيانات عندما تكون المركبة في حالة سكونية.

- ترتبط بيانات الحالة الدينامية للمركبة بالحالات التشغيلية لأنظمة المركبة. ويمكن أخذ حالة نظام تكييف الهواء كمثال، حيث يعتمد على درجة الحرارة والرطوبة في السيارة.
- ترتبط بيانات الحالة السكونية للمركبة بحالات الحالة السكونية لأنظمة تكييف الهواء، مثل حالة استعمال حزام الأمان وحالة تكييف الهواء، وما إلى ذلك.

3.2.7 بيانات التصور البيئي

تتصل بيانات التصور البيئي بشكل رئيسي بالبيئة الخارجية للمركبات، بما في ذلك معلومات عن المعدات الخارجية والمطاريف والمشاة فيما يخص الاتصالات على متن المركبات أو تفاعلات خدمات المعلومات في الاتصالات من مركبة إلى كل شيء (V2X)، بما في ذلك على سبيل المثال لا الحصر معلومات عن السرعة وإشارات المرور والبنية التحتية للطرق في الاتصالات بين المركبات. والمعلومات التي تجمعها رادارات قياس السرعة والكاميرات والتي تتعلق بالبنية التحتية للطرق واتجاه القيادة والتحرك وحالة القيادة والتحرك والسرعة والمسافة وبيانات الحالة المحتملة ذات الصلة بوقوع حادث تصادم أو عدم وقوعه والبيانات المتعلقة بمحطات الشحن الكهربائي (شحن البطاريات) وغيرها من المعدات التي جرى اقتناؤها للمركبات الكهربائية، والتي تُعتبر أيضاً من عناصر البيانات البيئية.

4.2.7 بيانات التحكم في المركبة

تتعلق بيانات التحكم في المركبة بالتحكم في المركبة في الاتصالات من المركبة إلى كل شيء (V2X)، وتتضمن بشكل رئيسي ثلاثة أنواع فرعية من البيانات هي بيانات التحكم في المركبة من أجل القيادة الذاتية/القيادة بواسطة مساعد ذكي، والتشغيل عن بُعد، والقيادة عن بُعد:

- بيانات التحكم في المركبة من أجل القيادة الذاتية/القيادة بواسطة مساعد ذكي هي البيانات المرتبطة بتعليمات التحكم المتعلقة بالقيادة الذاتية أو القيادة بواسطة مساعد ذكي. وتَستند البيانات إلى معالجة التصور البيئي وأنظمة اتخاذ القرار الذكية، وتُستخدم للحصول على بيانات من أجل سلوك التحكم الذكي في المركبات، مثل الكبح أو القيادة الإلكترونية والتغيير الآلي للسرعة والتحكم المتكامل في هيكل المركبة.
- تشير بيانات التحكم في المركبة للتشغيل عن بُعد إلى التعليمات الموجهة للمركبات من خلال التطبيقات ومنصات الخدمات وما إلى ذلك، وهي تشمل البيانات المتعلقة بقفل/فتح الأبواب عن بُعد والتحكم عن بُعد في مكيّف الهواء والتحكم في تشغيل النوافذ والإضاءة عن بُعد وما إلى ذلك.

- بيانات التحكم في المركبة للقيادة عن بُعد حيث يتم تقسيم حالة استخدام القيادة عن بُعد إلى عدة حالات فرعية من خلال التمييز بين الإنسان كسائق عن بُعد أو "السحابة" كسائق محتمل عن بُعد. وتشير بيانات التحكم في المركبة للقيادة عن بُعد إلى تدفقات الفيديو الخارجية للمركبة التي تُظهر أوضاع الممرات حول المركبة أو تدفقات الصوت الخارجية للمركبة التي يتم تسليمها إلى السائق عن بُعد كدعم لقراراته. بالإضافة إلى ذلك، يمكن أن تشير بيانات القيادة عن بُعد إلى تدفقات الفيديو أو الصوت الداخلية للمركبة، التي تُسلم إلى السائق عن بُعد في حالات المراقبة. علاوةً على ذلك، تشير بيانات التحكم في السيارة للقيادة عن بُعد إلى البيانات الموجودة في تعليمات التحكم عن بُعد من السائق عن بُعد إلى المركبة، مثل تعليمات التسارع أو المناورة، والتي قد تُعد وتُرسل عند تشغيلها بواسطة حدث تحكم، مثل تعليمات المكابح [b-ETSI TR 126 985]، [b-3GPP TR 22.886].

5.2.7 بيانات خدمة التطبيقات

تتعلق بيانات خدمة التطبيقات بتطبيق تفاعل المعلومات في الاتصالات من المركبة إلى كل شيء (V2X). وهي تشير إلى البيانات المتعلقة بخدمات المعلومات في الاتصالات من المركبة إلى كل شيء (V2X)، إلى جانب بيانات نعوت الأغراض، وبيانات حالة المركبة، وبيانات التصور البيئي، وبيانات التحكم في المركبة، والبيانات الشخصية للمستعمل، بما في ذلك، على سبيل المثال لا الحصر، بيانات الإعلام والترفيه، وإدارة السلامة على الطرق وبيانات التحكم، وبيانات الخدمات المتصلة بالمركبات وما إلى ذلك:

- تتعلق بيانات الإعلام والترفيه بخدمات الترفيه المقدمة في الاتصالات من المركبة إلى كل شيء (V2X)، مثل تنزيل الوسائط المتعددة وتصفح المواقع الإلكترونية والاشتراك في البث الإذاعي لفئة سكانية معينة فضلاً عن التنبؤات الجوية وما إلى ذلك.
- ترتبط بيانات إدارة السلامة على الطرق والتحكم فيها بالسلامة على الطرق وإدارة حركة المرور، مثل الإنذار المبكر المتعلق بالسلامة على الطرق، والإنقاذ في حالات الطوارئ، ومراقبة المركبة وإدارتها عن بُعد، وما إلى ذلك.
- ترتبط بيانات الخدمات المتصلة بالمركبة بخدمات ما بعد البيع في الاتصالات من المركبة إلى كل شيء (V2X)، مثل صيانة المركبة وإدارة المركبات المستعملة والتأمين المالي والتجارة الإلكترونية ذات الصلة. فعلى سبيل المثال، تندرج وتيرة صيانة أنواع معينة من قطع غيار المركبات المنتمية إلى علامات تجارية معينة ضمن بيانات الخدمات المتعلقة بالمركبة.

6.2.7 بيانات المستعمل الشخصية

تشير البيانات الشخصية للمستعمل إلى المعلومات الشخصية المتعلقة بالمستعمل، التي تُستخدم و/أو تتولد في الاتصالات من المركبة إلى كل شيء (V2X). ولا تتناول هذه الفقرة تصنيف بيانات المستعمل الشخصية وحمايتها.

ولذلك، إذا كانت البيانات المدرجة كأمثلة في الجدول 7-4 مقابلة للبيانات الشخصية للمستعمل المحدّدة في القوانين واللوائح المتعلقة بالخصوصية مثل اللائحة العامة لحماية البيانات، تجب هذه اللائحة سياسة التصنيف.

3.7 مستويات أمن البيانات

استناداً إلى الاعتبارات المرتبطة بأهداف أمن البيانات، وأهمية البيانات، وأثر الأحداث الأمنية المحتملة، يمكن تصنيف كل فئة من فئات البيانات إلى ثلاثة مستويات هي:

- **المستوى 1** (البيانات التي تحظى بأدنى مستوى من الحماية)، ويتضمن البيانات المتاحة للجمهور في الاتصالات من المركبة إلى كل شيء (V2X) مثل إصدار برمجية منصة الاتصالات من المركبة إلى كل شيء (V2X).
- **المستوى 2** (البيانات التي تحظى بحماية متوسطة)، ويتضمن بيانات يلزم حمايتها بتدابير أمنية، مثل بيانات المركبة التي تم الحصول عليها في الاتصالات من مركبة إلى مركبة (V2V) وحساب الدخول وكلمة السر للاتصالات من المركبة إلى كل شيء (V2X).
- **المستوى 3** (البيانات التي تحظى بحماية عالية)، ويتضمن بيانات تتطلب حماية أقوى من المستوى 2 (البيانات التي تحظى بحماية متوسطة) في الاتصالات من مركبة إلى كل شيء (V2X)، مثل المعلومات المتعلقة بالمعاملات المالية في الاتصالات من مركبة إلى جهاز جوال (V2D)، وبيانات الأداء الرئيسية للمركبة ومعلومات استيقان الهوية للاتصالات من مركبة إلى كل شيء (V2X).

وتشير البيانات السرية إلى البيانات السرية الواردة من المؤسسات ذات الصلة بالاتصالات من مركبة إلى كل شيء (V2X) فقط، ولا تتضمن المعلومات الشخصية للمستعملين.

ويقدم الجدول 7-4 معلومات مفصلة عن مستويات أمن البيانات وأمثلة عليها في الاتصالات من مركبة إلى كل شيء (V2X).

الجدول 7-4 – أمثلة على مستويات أمن البيانات في الاتصالات من مركبة إلى كل شيء (V2X)

فئة البيانات في الاتصالات من مركبة إلى كل شيء (V2X)		مستوى أمن البيانات في الاتصالات من مركبة إلى كل شيء (V2X)	أمثلة
بيانات نعوت الأغراض	بيانات نعوت المركبة	المستوى 1	العلامة التجارية للمركبة أو نوعها أو شعارها أو لونها.
		المستوى 2	معلمات أداء نوع معيّن من المركبات.
		المستوى 3	بيانات تشكيل أنساق العتاد والبرمجيات الخاصة بنوع معين من المركبات.
	بيانات نعوت الأجهزة المتنقلة	المستوى 1	العلامة التجارية لمطراف متنقّل ونوعه وشعاره ولونه.
		المستوى 2	بيانات حالة المعدات المتعلقة ببعض الوظائف الهامة في الاتصالات من مركبة إلى كل شيء (V2X).
		المستوى 3	المعلمات الهامة لأداء نوع من أنواع الأجهزة المتنقلة والمعلومات المتعلقة بتشكيله.
	بيانات نعوت منصة الخدمة السحابية	المستوى 1	نوع منصة الخدمة السحابية واسمها.
		المستوى 2	معلومات عن العتاد أو نظام التشغيل أو برمجية التطبيق.
		المستوى 3	المعلمات الهامة لمنصة الخدمات والمعلومات المتعلقة بتشكيلها.
بيانات حالة المركبة	بيانات الحالة الدينامية للمركبة	المستوى 1	حالة نظام تكييف الهواء. درجة الحرارة داخل المركبات.
		المستوى 2	حالة تشغيل الوسادة الهوائية والأحزمة الهوائية، وما إلى ذلك. البيانات التي تلتقطها أجهزة الاستشعار داخل المركبة والتي ترتبط ارتباطاً وثيقاً بالقيادة الهامة للمركبة، مثل ضغط الهواء في العجلات.
		المستوى 3	المؤشرات التقنية الأساسية لتشغيل المركبة. البيانات التي تستقبلها أجهزة الاستشعار داخل المركبة والتي ترتبط ارتباطاً وثيقاً بالقيادة الهامة للمركبة، من قبيل البيانات الواردة من أجهزة الاستشعار الخاصة بالتصادم.
	بيانات الحالة السكونية للمركبة	المستوى 1	وتيرة استعمال نظام تكييف الهواء في وقت معين.
		المستوى 2	متوسط استهلاك المركبة للوقود.
		المستوى 3	البيانات السرية لنظام المركبة.
بيانات التصور البيئي	بيانات تصوّر البيئة الخارجية للمركبة	المستوى 1	نوع الطريق (طريق سريع، أو طريق ريفي، أو طريق مشاة)، وحالة الطريق (طريق جيدة أو مبتلة أو زلقة)، والسرعة القصوى المسموح بها، وتوزيع إشارات المرور وحالتها، والازدحام على الطرق، وحوادث السير، وما إلى ذلك.
		المستوى 2	في سيناريو الاتصالات من مركبة إلى مركبة، المعلومات بعد إزالة حساسيتها للمركبات القريبة، مثل المعلومات المتعلقة بالموقع الفعلي وخط الطول وخط العرض والتوقيت المحدث وسرعة القيادة واتجاه الذهاب وتغيّر الممرات. في سيناريو الاتصالات من مركبة إلى مشاة، البيانات بعد إزالة حساسيتها مثل موقع المشاة والمسافة الفاصلة والسرعة وحالة حركة المشاة المقتربين، وإمكانية وقوع تصادم.
		المستوى 3	في سيناريوهات الاتصالات من مركبة إلى مركبة، المعلومات المتعلقة بالمركبات المجاورة في فترة زمنية معينة بعد إزالة حساسيتها، مثل المعلومات المتعلقة بطريق السفر والموقع والوقت ومواقف السيارات، وما إلى ذلك.

الجدول 7-4 – أمثلة على مستويات أمن البيانات في الاتصالات من مركبة إلى كل شيء (V2X)

فئة البيانات في الاتصالات من مركبة إلى كل شيء (V2X)		مستوى أمن البيانات في الاتصالات من مركبة إلى كل شيء (V2X)	أمثلة
بيانات التحكم في المركبة	بيانات التحكم في المركبة من أجل القيادة الذاتية/القيادة بواسطة مساعد ذكي	المستوى 1	البيانات الصوتية لإعطاء إرشادات داعمة في إطار المساعدة الداعمة.
		المستوى 2	في التطبيق المتعلق بالبقاء في الممر، ضمن نظام القيادة الذكية المساعدة، عندما تأخذ المركبة بالانحراف عن ممر القيادة، ترسَل بيانات أوامر للتحذير مثل اهتزاز عجلة القيادة أو ظهور إشارة الضوء الأحمر أو الضوء الأخضر على لوحة القيادة.
		المستوى 3	تعليمات التأكيد الصادرة عن النظام الذكي لركن المركبات في إطار نظام الركن الآلي.
	بيانات التحكم في المركبة من أجل التشغيل عن بُعد	المستوى 1	بيانات عامة مقروءة متعلقة برصد الاتصالات من مركبة إلى كل شيء (V2X) عن بُعد.
		المستوى 2	تعليمات لبدء تشغيل المركبة عن بُعد أو بدء قيادة المركبة.
		المستوى 3	تعليمات تنفيذية متعلقة بالتحكم عن بُعد في عدة مركبات، مثل أسطول من المركبات، من خلال منصة خدمات الاتصالات من مركبة إلى كل شيء (V2X).
	بيانات التحكم في المركبة من أجل القيادة عن بُعد	المستوى 1	يمكن استخدام تدفقات الفيديو وتدفقات الصوت الداخلية للمركبة التي يمكن أن تكون متطلبات التأخير فيها أقل صرامة من متطلبات الفيديو والصوت الخارجية للمركبة، من قبل السائق عن بُعد لمراقبة الحالة داخل المركبة.
		المستوى 2	يمكن تسليم تدفقات الصوت الخارجية للمركبة إلى السائق عن بُعد لنقل الضوضاء وأصوات الأبواق الصادرة عن المركبات الأخرى.
		المستوى 3	تُستخدم أجهزة الاستشعار أو أجهزة العرض مثل الشاشة أو نظام الصوت لتعليمات المناورة الصادرة عن السائق عن بُعد. ويجب توفير التعليمات بمستوى عالٍ من الموثوقية وبكمون منخفض ويجب الإخطار باستلامها، خاصة فيما يتعلق بحدث الإنذار (على سبيل المثال، تعليمات المكابح). بيانات جهاز الاستشعار الفيديوي (الكاميرا) والصوتي (الميكروفون) (ربما أيضا بيانات الرادار أو جهاز استشعار كشف الضوء وتحديد المدى (lidar)) تسجل الأصوات أو مقاطع الفيديو الخارجية للتعرف المبكر وغير المرئي على العوائق في الطريق مثل مركبات الطوارئ والمشاة وما إلى ذلك. يمكن إرسال بيانات جهاز استشعار حالة المركبة (التسارع، والسرعة، والاتجاه، والموقع، وما إلى ذلك) بفاصل زمني ثابت من المركبة إلى السائق عن بُعد بموثوقية عالية لأن بعض تدفقات أجهزة الاستشعار قد تكون ضرورية لعمليات القيادة الصحيحة.
بيانات خدمات التطبيقات	بيانات الإعلام والترفيه	المستوى 1	بيانات البث الراديوي.
		المستوى 2	تصفّح سجلات التسوق عبر الإنترنت بعد إزالة الحساسية.
		المستوى 3	تسجيلات صوتية وفيديوية بعد إزالة الحساسية في تطبيقات خدمات المعلومات.
	بيانات إدارة السلامة على الطرق والتحكم فيها	المستوى 1	بيانات للإنذار بوجود ازدحام على الطرق، والإنذار بحوادث السير في الوقت الفعلي، وما إلى ذلك.
		المستوى 2	بيانات للإنذار باحتمال حدوث تصادم بسبب ركن المركبة أمام مركبة في صف انتظار.
		المستوى 3	بيانات رصد المركبات على الطرق عن بُعد.
	بيانات الخدمات المتصلة بالمركبة	المستوى 1	بعد إزالة الحساسية، تُسجَّل بيانات سلوك استعمال النظام الترفيهي المتعلقة بالاستعمال والتشغيل والمعلومات الأخرى للنظام الترفيهي للمركبة.
		المستوى 2	بعد إزالة الحساسية، بيانات سلوك المركبة المتعلق بسلوك قيادة المركبة.

الجدول 7-4 – أمثلة على مستويات أمن البيانات في الاتصالات من مركبة إلى كل شيء (V2X)

فئة البيانات في الاتصالات من مركبة إلى كل شيء (V2X)		مستوى أمن البيانات في الاتصالات من مركبة إلى كل شيء (V2X)	أمثلة
		المستوى 3	البيانات بعد إزالة الحساسية، مثل التفضيلات الشخصية لمالك السيارة وعاداته السلوكية استناداً إلى الوقت الذي تستغرقه الرحلة، والمسار، والموقع، وبيانات السلوك المتعلق باستخدام نظام الإعلام والترفيه، أو المعلمات الأساسية للمركبة استناداً إلى بيانات حالة المركبة وبيانات التصور البيئي، وما إلى ذلك.
بيانات المستعمل الشخصية	لا ينطبق	لا ينطبق	لا ينطبق

ويوصف محتوى الجدول 7-4 على النحو التالي:

1) لا ينطبق: N/A

2) البيانات بعد إزالة الحساسية، الوارد وصفها في الجدول 7-4، لا يمكن أن تكشف بشكل مباشر أو غير مباشر عن المعلومات الشخصية للأفراد أو أن تشير إليها، بعد معالجتها بوسائل مبهمة مجهولة الهوية أو بوسائل تقنية أخرى. وتشمل أساليب إزالة حساسية البيانات على سبيل المثال لا الحصر إغفال الهوية ومنع التعرف عليها والتنوع وإلغاء البيانات واضطراب البيانات والخصوصية التفاضلية وما إلى ذلك. وينبغي للمنظمة المرتبطة بالاتصالات من مركبة إلى كل شيء (V2X) أن تتخذ تدابير ملائمة لإزالة حساسية البيانات استناداً إلى دراسة شاملة لخصائص موضوع البيانات، ومستوى حساسية البيانات، ومتطلبات تشغيل البيانات.

8 متطلبات الأمن

تعرض هذه الفقرة متطلبات الأمن الأساسية، ومتطلبات الأمن الوسيطة، ومتطلبات الأمن المتقدمة، التي تتوافق تماماً مع بيانات المستويات 1-3.

1.8 مستوى متطلبات الأمن

استناداً إلى فئات البيانات المصنَّفة، تُحدَّد الطرائق أو التدابير الأمنية لكل مستوى. وهناك ثلاثة مستويات أمنية لمتطلبات الأمن يمكن تبنيها: متطلبات الأمن الأساسية ومتطلبات الأمن الوسيطة ومتطلبات الأمن المتقدمة. وبصفة عامة، تراعى متطلبات الأمن الأساسية لحماية المستوى 1 (البيانات التي تحظى بأدنى قدر من الحماية)، وتراعى متطلبات الأمن الوسيطة لحماية المستوى 2 (البيانات التي تحظى بحماية متوسطة)، وتراعى متطلبات الأمن المتقدمة لحماية المستوى 3 (البيانات التي تحظى بحماية عالية). ويصف الجدول 8-1 متطلبات الأمن حسب مستوى أمن بيانات الاتصالات من مركبة إلى كل شيء (V2X)

ويمكن أن تختار المؤسسات أيضاً التدابير الأمنية حسب وضعها أو حسب سرية البيانات.

الجدول 8-1 – متطلبات الأمن حسب مستوى أمن بيانات الاتصالات من مركبة إلى كل شيء (V2X)

مستوى أمن بيانات الاتصالات من مركبة إلى كل شيء (V2X)	مستوى متطلبات الأمن		
	أساسية	وسيطة	متقدّمة
المستوى 1 (البيانات التي تحظى بأدنى قدر من الحماية)	*	لا ينطبق	لا ينطبق
المستوى 2 (البيانات التي تحظى بحماية متوسطة)	*	*	لا ينطبق
المستوى 3 (البيانات التي تحظى بحماية عالية)	*	*	*
*: مشمول لا ينطبق: N/A			

2.8 متطلبات الأمن الأساسية

(1) جمع البيانات

- ينبغي تصنيف البيانات في الاتصالات من مركبة إلى كل شيء (V2X) بناء على مجموعة من الأهداف المتعلقة بأمن البيانات وعلى أهمية البيانات وأثر الأحداث الأمنية المحتملة.
- ينبغي تطبيق مبدأ "الحدّ الأدنى" في عملية جمع البيانات. ولا تُجمع سوى البيانات المتصلة بوظائف الأعمال.
- ينبغي تصنيف البيانات المجمعة وإدارتها وفقاً لطرائق تصنيف البيانات حسبما ورد وصفه في الفقرتين 6 و7. وينبغي وضع وتنفيذ تدابير أمنية تختلف باختلاف مستويات البيانات.

(2) إرسال البيانات

- ينبغي ألا يكون متطلب الأمن الشامل لإرسال البيانات في الاتصالات من مركبة إلى كل شيء (V2X) أقل من متطلب الأمن لشبكة اتصالات عامة.
- ينبغي، وفقاً لمختلف فئات البيانات، اعتماد إجراءات للأعمال، وسيناريوهات للمخاطر الأمنية المتعلقة بالاتصالات من مركبة إلى كل شيء (V2X)، واستراتيجيات وتدابير أمنية مختلفة لإرسال البيانات.
- ينبغي استخدام بروتوكولات الأمن مثل بروتوكول أمن طبقة النقل (TLS) لضمان أمن إرسال البيانات في سيناريوهات الاتصالات بين المركبة والكيانات الأخرى.
- ينبغي أن يكون من الممكن الكشف عن تعرّض البيانات للتلف أثناء الإرسال.

(3) تخزين البيانات

- بالنسبة إلى البيانات المخزَّنة في مطاريف المركبات وفي منصات الخدمات، ينبغي اعتماد آليات تشفير للبيانات في المعدات والأنظمة المتعلقة بالاتصالات من مركبة إلى كل شيء (V2X). وينبغي دعم المعلمات، مثل الخوارزمية والقوة وأسلوب التجفير، بتشكيلة اختيارية.
- ينبغي أن يتسنى ضمان أمن البيانات المخزنة في الذاكرة المؤقتة في منصة الخدمات أو نظام المركبة. وينبغي تجفير البيانات المخزنة في نظام التخزين المؤقت.
- بالنسبة للبيانات المخزنة في مطاريف المركبات وفي منصات الخدمات، ينبغي اعتماد آليات التحكم في النفاذ إلى البيانات لمنع النفاذ غير المخول إليها وتعديلها وحذفها والنفاذ إلى المعلومات بين الميادين.
- ينبغي أن يتسنى التحقق من سلامة البيانات في عملية التخزين لمنع إتلاف البيانات وحذفها واختراقها. وينبغي توفير معلومات لإنذار المستعمل عند المسّ بسلامة البيانات.

(4) استخدام البيانات

- ينبغي معالجة البيانات في نطاق التخويل الممنوح وفي نطاق الحد الأدنى من احتياجات الأعمال.
- ينبغي أن يكون استخدام البيانات مخولاً وأن يتم التحقق من هذا التخويل.
- ينبغي أن يُتقيد في الغرض من استخدام البيانات ونطاق هذا الاستخدام بأحكام القوانين واللوائح الوطنية ذات الصلة.
- أثناء تحليل البيانات واستخلاصها، ينبغي توقيع بيانات المصدر ونتائج الاستخلاص بغية منع الحذف الخبيث للبيانات أو العبث بها أو إساءة استخدامها دون قيود.
- من أجل نقل البيانات أو تصديرها بين أجهزة وأنظمة ومنصات إنترنت المركبات، ينبغي اتخاذ تدابير إدارية وتقنية لضمان الأمن.

(5) انتقال البيانات

- يجب إجراء تقييم للقدرات الأمنية قبل انتقال البيانات لضمان سلامة انتقال البيانات.
- ينبغي ضمان استمرارية الأعمال والتطبيقات عند انتقال البيانات بين مختلف أجهزة البيانات.

- ينبغي إعداد مخطط انتقال، وتقييم جدواه والمخاطر ذات الصلة، ثم وضع تدابير للتحكم في المخاطر طبقا لذلك عند التحضير لانتقال البيانات.

(6) إتلاف البيانات

- ينبغي وضع استراتيجية لإتلاف البيانات ونظام لإدارة الإتلاف من أجل توضيح موضوع الإتلاف وعملية الإتلاف. وينبغي استحداث آلية فحص وموافقة لإتلاف البيانات، وينبغي إيجاد دور إشرافي متعلق بالتدمير للإشراف على عملية التدمير.
- ينبغي اتخاذ تدابير لإزالة البيانات التي بلغت الحد الأقصى الجائز للاحتفاظ بها، أو ينبغي إتلافها على الفور عندما يتوقف المستعملون عن إعطاء الإذن لها.
- ينبغي اتخاذ تدابير للمساعدة على إزالة البيانات المتبقية من انتقال البيانات أو من الأعمال.
- ينبغي اتخاذ تدابير لإزالة جميع نسخ البيانات الاحتياطية.

(7) النَّسخ الاحتياطي للبيانات واستعادة البيانات

- ينبغي لآليات النسخ الاحتياطي للبيانات واستعادتها أن تُنشأ قبل انتقال البيانات.
- ينبغي إتاحة النسخ الاحتياطي للبيانات واستعادتها محليا.
- ينبغي وضع آلية منتظمة لتخزين كامل البيانات، وينبغي ألا تقل الدورة الزمنية الموصى بها عن مرة في الأسبوع.
- ينبغي أن تخضع البيانات الاحتياطية لنفس الحقوق التي تخضع لها البيانات الأصلية فيما يتعلق بالتحكم في النفاذ ومتطلبات التخزين الآمن.

3.8 متطلبات الأمن الوسيطة

متطلبات الأمن الوسيطة هي مجموعة إجمالية من متطلبات الأمن الأساسية. واستناداً إلى متطلبات الأمن الأساسية في كل مرحلة من مراحل دورة حياة البيانات، تضاف المتطلبات التالية:

(1) جمع البيانات

بالإضافة إلى الوفاء بمتطلبات الأمن الأساسية، ينبغي أيضاً الوفاء بالمتطلبات التالية:

- أثناء جمع البيانات من المستوى 2، ينبغي الاحتفاظ بنسخ احتياطية للبيانات الأصلية لتجنب إسقاط البيانات وفقدانها.
- ينبغي اعتماد آليات تعرّف لضمان الاستيقان لعملية جمع البيانات.
- ينبغي اعتماد آليات للتحقق من البيانات لضمان سلامة جمع البيانات.

(2) إرسال البيانات

بالإضافة إلى الوفاء بمتطلبات الأمن الأساسية، ينبغي أيضاً الوفاء بالمتطلبات التالية:

- ينبغي أن يَعتمد إرسالُ البيانات من خلال منصة الخدمات الأساسية للمركبات وإنترنت المركبات اتصالات عبر شبكة خاصة أو شبكة خاصة افتراضية لتحقيق العزل عن الإنترنت.
- في الاتصالات من مركبة إلى مركبة (V2V) ومن مركبة إلى بنية تحتية (V2I)، ينبغي أن تكون هناك شهادة هوية موثوقة يمكنها التحقق من هوية عقدة إرسال البيانات، وينبغي ألا تكشف معلومات الاستيقان عن معلومات متعلقة بالخصوصية.
- ينبغي أن تكون المركبة قادرة على تحديد طلبات التوصيل غير القانوني الواردة من شبكات خلوية كي تتمكن من ترشيح الرزم الخبيثة.
- فيما يتعلق ببيانات المستوى 2، مثل بيانات تعليمات التحكم عن بُعد، ينبغي التحقق من موثوقية مصدر البيانات لضمان عدم تزوير البيانات.

(3) تخزين البيانات

بالإضافة إلى الوفاء بمتطلبات الأمن الأساسية، ينبغي أيضاً الوفاء بالمتطلبات التالية:

- ينبغي أن يتسنى التحقق من سلامة البيانات في عملية التخزين لمنع التلاعب بالبيانات وحذفها واختراقها، وينبغي أن تتاح تدابير الاستعادة اللازمة في حال المس بسلامة البيانات.
- ينبغي أن تحدَّد معلومات تحديد الهوية فيما يخص ملفات البيانات المخزَّنة في المركبة الذكية الموصولة (ICV)، ومنصات الخدمات والتطبيقات، لتجنب استخدام هذه الملفات في الأجهزة والأنظمة غير المخوَّلة.
- بالنسبة لنظام التخزين المؤقت لمنصة الخدمات في الاتصالات من مركبة إلى كل شيء (V2X)، ينبغي الاحتفاظ بسجلات تشغيلية محددة لحماية بيانات المستوى 2 المخزنة في الذاكرة المؤقتة.
- ينبغي تحديد العملية الكاملة لإدارة سجل البيانات لتجنب التهديدات الناجمة عن رفض البيانات.

(4) استخدام البيانات

بالإضافة إلى الوفاء بمتطلبات الأمن الأساسية، ينبغي أيضاً الوفاء بالمتطلبات التالية:

- فيما يتعلق بالبحث عن البيانات في المستوى 2، ينبغي أن تكون معالجة العمليات، مثل البحث والعرض الخارجي والإحصاءات، معالجة مبهمة.
- ينبغي التدقيق في استخدام البيانات من المستوى 2 وإنتاج سجل تدقيق.

(5) انتقال البيانات

بالإضافة إلى الوفاء بمتطلبات الأمن الأساسية، ينبغي أيضاً الوفاء بالمتطلبات التالية:

- ينبغي إعداد مخطط انتقال، وتقييم جدواه والمخاطر ذات الصلة، ثم وضع التدابير المقابلة للتحكم في هذه المخاطر، عند التحضير لانتقال البيانات.

(6) إتلاف البيانات

بالإضافة إلى الوفاء بمتطلبات الأمن الأساسية، ينبغي أيضاً الوفاء بالمتطلبات التالية:

- ينبغي التأكد من أن مساحة التخزين الخاصة بموارد الاتصالات من مركبة إلى كل شيء (V2X)، مثل الملفات والأدلة وسجلات قواعد البيانات لا يتم تحريرها أو إعادة تخصيصها لمستعملين آخرين قبل إزالة هذه الموارد بشكل كامل.
- بالنسبة للمطراف الموجود على متن المركبة، ومن أجل منع تسرب البيانات جرّاء استبدال قطع من المركبة، ينبغي أن يتسنى إتاحة وظيفة لمحو بيانات مطراف المركبة، وذلك لضمان عدم إمكانية استعادة بيانات مطراف المركبة التي جرى محوها.

(7) النَّسخ الاحتياطي للبيانات واستعادتها

بالإضافة إلى الوفاء بمتطلبات الأمن الأساسية، ينبغي أيضاً الوفاء بالمتطلبات التالية:

- بالنسبة للنَّسخ الاحتياطي المحلي أو عن بُعد للبيانات، ينبغي نسخ البيانات بأكملها مرة واحدة على الأقل كل أسبوع، كما ينبغي نسخ البيانات الاحتياطية الإضافية مرة واحدة يومياً على الأقل. وبالإضافة إلى ذلك، ينبغي إنشاء آلية لإجراء نُسخ احتياطية متعددة.
- ينبغي تجفير النُّسخ الاحتياطية للبيانات المخزنة.

4.8 متطلبات الأمن المتقدمة

متطلبات الأمن المتقدمة هي مجموعة فوقية من متطلبات الأمن الوسيطة. واستناداً إلى متطلبات الأمن الوسيطة في كل مرحلة من مراحل دورة حياة البيانات، ينبغي الوفاء بجميع المتطلبات التالية.

(1) جمع البيانات

- متطلبات الحماية هي نفسها الواردة في متطلبات الأمن الوسيطة.

(2) إرسال البيانات

بالإضافة إلى الوفاء بمتطلبات الأمن الخاصة بمتطلبات الأمن الوسيطة، ينبغي أيضاً الوفاء بالمتطلبات التالية:

- ينبغي أن يتسنى كشف الأضرار التي تلحق بسلامة البيانات أثناء الإرسال، واتخاذ التدابير اللازمة لاستعادة البيانات عند الكشف عن أي مس بسلامتها.
- بالنسبة للبيانات السرية المتعلقة بالمستوى L3، ينبغي اعتماد الاستيقان المتبادل للتعامل مع التهديدين المتمثلين في التلاعب بالبيانات وتسربها بسبب انتحال كيانات خارجية للهوية.

(3) تخزين البيانات

بالإضافة إلى الوفاء بمتطلبات الأمن الخاصة بمتطلبات الأمن الوسيطة، ينبغي أيضاً الوفاء بالمتطلبات التالية:

- ينبغي اعتماد مخطط تخزين تجفير أمن العتاد لضمان سرية بيانات المركبات ومنصات الخدمات وتطبيقات المطاريف المتنقلة الذكية والبنية التحتية المقامة على جانبي الطريق.
- ينبغي أن يتسنى التحقق من سلامة البيانات في عملية التخزين لمنع التلاعب بالبيانات وحذفها واختراقها، وينبغي توفير تدابير الاستعادة اللازمة عند المس بسلامة البيانات.

(4) استخدام البيانات

بالإضافة إلى الوفاء بمتطلبات الأمن الخاصة بمتطلبات الأمن الوسيطة، ينبغي أيضاً الوفاء بالمتطلبات التالية:

- ينبغي أن يتم إقرار سلطة التشغيل الثانوية باعتماد أسلوب تخويل عدة أشخاص.
- ينبغي إجراء عزل لترابط البيانات بغية منع تسرب البيانات بسبب تحليل رابطة البيانات في شتى الأنظمة أو المنصات أو التطبيقات.
- ينبغي دعم إزالة الحساسية الدينامية عند استعمال البيانات السرية.

(5) انتقال البيانات

متطلبات الحماية هي نفسها الواردة في متطلبات الأمن الوسيطة.

(6) إتلاف البيانات

بالإضافة إلى الوفاء بمتطلبات الأمن الخاصة بمتطلبات الأمن الوسيطة، ينبغي أيضاً الوفاء بالمتطلبات التالية:

- ينبغي توفير وسائل لمنع استعادة البيانات التي تم إتلافها.

(7) النسَّخ الاحتياطي للبيانات واستعادتها

بالإضافة إلى الوفاء بمتطلبات الأمن الخاصة بمتطلبات الأمن الوسيطة، ينبغي أيضاً الوفاء بالمتطلبات التالية:

- ينبغي توفير تدابير الاستيقان الأمني، من قبيل استيقان الهوية، لضمان عدم عمل نُسخ احتياطية للبيانات محلياً أو عن بُعد وعدم إجراء عمليات استعادة البيانات إلا بعلْم من المستعملين المخولين أو تحت رقابتهم.

بيبليوغرافيا

[b-ITU-T X.1217] Recommendation ITU-T X.1217 (2021), *Guidelines for applying threat intelligence in telecommunication network operation*.

[b-ITU-T X.1751] Recommendation ITU-T X.1751 (2020), *Security guidelines for big data lifecycle management by telecommunication operators*.

[b-3GPP TR 22.886] 3GPP TR 22.886 V16.2.0 (2018), *Study on enhancement of 3GPP Support for 5G V2X Services (Release 16).*

[b-ETSI TR 126 985] ETSI TR 126 985 V16.0.0 (2020), *5G Vehicle-to-everything (V2X) Media handling and interaction (3GPP TR 26.985 version 16.0.0 Release 16).*

[b-ETSI TS 102 637-2] ETSI TS 102 637-2 (2011), *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*.

[b-SAE J2735] *V2X Communications Message Set Dictionary*, (July 2020).

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، 2023